Um Estudo de Caso para Avaliação do *Knowledge Unified Process* para o Desenvolvimento de Ontologias

Daniela F. Brauner
e-mail: dani@inf.puc-rio.br

Anarosa A. F. Brandão
e-mail: anarosa@inf.puc-rio.br

Leonardo M. Cunha
e-mail: leocunha@inf.puc-rio.br

Carlos J. P. de Lucena
e-mail: lucena@inf.puc-rio.br

PUC-RioInf.MCC50/03 November, 2003

Abstract: Knowledge Unified Process (KUP) is an ontology development process that brings together activities from other ontology development methodologies and some software development best practices. This process has been applied to a case study, the ontology development process of an information security alert ontology, to evaluate its usage. The evaluation was based in an instance of an evaluation framework for methodologies and methods. As a result, we believe that KUP's iterative and controlled approach contributes to the ontology development process although there are still some deficiencies that should be tackled so that the process can become more comprehensive.

Keywords: ontology engineering, ontology, semantic web.

Resumo: Este trabalho mostra um estudo de caso no desenvolvimento de uma ontologia para auxiliar nas tarefas de um sistema de alertas de segurança da informação. Para tal, foi utilizado o *Knowledge Unified Process* (KUP), um processo para desenvolvimento de ontologias, que unifica atividades oriundas de metodologias distintas e as melhores práticas de desenvolvimento de software adaptadas para o desenvolvimento de ontologias. Com o objetivo de avaliar seu desempenho, instanciou-se um *framework* de avaliação de metodologias e métodos. Como resultado, a abordagem iterativa e controlada do KUP caracterizou sobremaneira sua utilização no desenvolvimento de ontologias, porém algumas carências da área de engenharia de ontologias ainda merecem atenção especial para que o processo torne-se ainda mais abrangente.

Palavras-chave: engenharia de ontologias, ontologia, web semântica

Sponsored by CAPES.

1. Introdução

A World Wide Web (WWW) tem se mostrado um excelente repositório de informações, haja visto o aumento exponencial do número de páginas ativas disponíveis para consulta. Esta quantidade de informação disponível na WWW fez com que a eficácia dos serviços de busca (Altavista, Google, Yahoo, etc) fosse reduzida devido, principalmente, à grande variedade de significados distintos que um termo pode abranger.

O conteúdo das páginas web não passava de informações sem significado para os computadores até o surgimento da Web Semântica. Ao adicionar semântica às informações que trafegam na rede, torna-se viável a comunicação entre máquinas e a recuperação de informação na *web* com menos ambigüidades. Para tanto, é necessária a definição dos conceitos e relacionamentos de um determinado domínio de conhecimento através da utilização de ontologias.

Neste trabalho, é apresentada a avaliação do processo *Knowledge Unified Process* (KUP) (Orlean, D. & Lucena, C., 2003) utilizando o *framework* de avaliação proposto em (Fernández-López, M. & Gómez-Pérez, A., 2002). Como estudo de caso foi desenvolvido o projeto de uma ontologia para auxiliar nas tarefas do sistema e-BTS - Boletim Técnico de Segurança Eletrônico, desenvolvido com o objetivo de monitorar ameaças de segurança à sistemas de software (Orlean, D.; Magalhães, J. & Pinto, L., 2003). Neste contexto, foi utilizada uma instanciação do KUP para guiar o desenvolvimento da ontologia, com o objetivo de avaliar seu desempenho em uma aplicação real, além de contribuir para o seu aprimoramento.

Este trabalho é composto por cinco seções. Na seção 2 são apresentados conceitos relacionados à ontologia e Web Semântica e a descrição de algumas metodologias para o desenvolvimento de ontologias. A seção 3 descreve o estudo de caso realizado. A seção 4 mostra alguns critérios para avaliação de metodologias e métodos para o desenvolvimento de ontologias e a seção 5 apresenta as considerações finais sobre a avaliação do KUP. Em anexo estão os artefatos produzidos durante o projeto e desenvolvimento do estudo de caso.

2. Ontologias

Utilizamos ontologias para descrever explicitamente conceitos e relações de uma área de conhecimento em particular. Uma ontologia é uma especificação formal do domínio incluindo um vocabulário (termos da área) e um conjunto de sentenças lógicas (axiomas) expressando as restrições para interpretação deste vocabulário.

De acordo com (Guarino, N., 1998), existem diferentes tipos de ontologias classificadas de acordo com seus níveis de generalidade, como segue:

- *Ontologias de alto nível:* descrevem conceitos gerais como espaço, tempo, evento, que são independentes de um domínio específico.

- *Ontologias de domínio:* descrevem o vocabulário particular relacionado a um domínio específico através da especialização dos conceitos introduzidos na ontologia de alto nível.

- *Ontologias de tarefas:* descrevem o vocabulário para descrição de tarefas ou atividades através da especialização das ontologias de alto nível.

- *Ontologias de aplicação:* são as ontologias mais específicas, onde os conceitos das ontologias de domínio correspondem aos papéis exercidos pelas entidades do domínio na realização de uma atividade descrita na ontologia de tarefas.

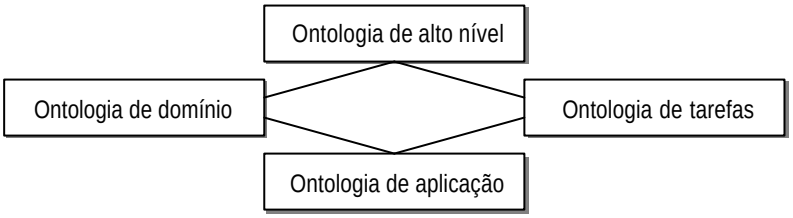

Figura 1: Diferentes tipos de ontologias e seus relacionamentos

FONTE: (Guarino, N., 1998)

Na Figura 1, é explicitado o relacionamento entre os diferentes níveis de classificação de ontologias. Uma ontologia de aplicação baseia-se na reutilização dos conceitos definidos numa ontologia de domínio e nas atividades descritas numa ontologia de tarefas. Estas, por sua vez, baseiam-se nos conceitos mais gerais definidos na ontologia de alto-nível.

No contexto da Web, ontologias são utilizadas para anotar semanticamente o conteúdo disponibilizado, o que permite que agentes de software compreendam a semântica embutida nas páginas Web, sem ambigüidade, viabilizando o intercâmbio de informações. Assim, a Web torna-se um ambiente onde agentes de software e usuários podem trabalhar de forma cooperativa. Esta é a idéia introduzida pela Web Semântica, uma evolução da Web atual idealizada por Berners-Lee em (Berners-Lee, T., 1990).

Segundo Gómez-Pérez (1999), uma ontologia possui cinco componentes principais para formalização do conhecimento: classes, relações, funções, axiomas e instâncias. Uma classe representa conceitos do domínio, que por sua vez podem ser abstratos ou concretos, elementares ou compostos, reais ou fictícios. Um conceito é uma descrição de algo: uma tarefa, ação, processo, etc. As relações representam interações entre conceitos do domínio (por exemplo: "subclasse de"). As relações possuem um caso especial, as funções. As funções geram elementos a partir de outros elementos do domínio. (por exemplo: o preço de um carro usado é calculado em função do modelo do carro, data de fabricação e quilometragem). Os axiomas são utilizados para modelar sentenças que são sempre verdadeiras. Por fim, as instâncias são utilizadas para representar os elementos do domínio.

Uma vez identificados os componentes de uma ontologia e sua utilidade, serão mostradas algumas metodologias propostas para seu projeto e desenvolvimento.

2.1. Engenharia de Ontologias

Foi visto anteriormente que uma ontologia deve explicitar o conhecimento sobre um determinado domínio. A tarefa de construção de uma ontologia não é fácil, dado o nível de detalhamento que se deseja alcançar nas descrições do domínio. A engenharia de ontologias é uma área de pesquisa que permite o projeto lógico de uma base de conhecimento, conceitualização do domínio, definição do significado dos conceitos básicos, teorias sofisticadas e tecnologias de um domínio, permitindo o acúmulo de conhecimento (Mizoguchi, R. & Ikeda, M.,1996). Portanto, o objetivo da engenharia de ontologias é capturar o conhecimento de um domínio de uma forma genérica e criar meios de melhor desenvolver uma ontologia para promover um entendimento compartilhado.

A engenharia de ontologias requer a definição e padronização de um ciclo de vida da ontologia bem como metodologias e técnicas que guiem seu desenvolvimento (Blázquez, M. *et alli*, 1998).

Assim como no desenvolvimento de software, para o desenvolvimento de uma ontologia existem metodologias, métodos e processos que definem as atividades a serem executadas durante o ciclo de vida da ontologia.

Muitos paralelos já foram feitos entre engenharia de ontologias e engenharia de software (arquiteturas e padrões), mas poucos foram discutidos e desenvolvidos na prática. Porém foram detectadas semelhanças com o paradigma de projeto orientado à objetos, e similaridades entre as fases do desenvolvimento de ontologias com processos de desenvolvimento de software. (Devedezic, V., 2002).

2.2. Metodologias e Métodos para Projeto e Desenvolvimento de Ontologias

Devido ao fato da engenharia de ontologias ser ainda uma área de pesquisa relativamente imatura, cada grupo de pesquisa utiliza sua própria metodologia (Gómez-Pérez, A. *et alli*, 1996). A seguir serão apresentadas algumas destas metodologias, métodos e/ou processos para projeto e desenvolvimento de ontologias.

2.2.1. Método CYC

Este método surgiu da experiência de desenvolvimento da base de conhecimento CYC ((Lenat *et alli*, 1990) *in* (OntoWeb Group, 2002)). Esta base foi construída para servir como uma enciclopédia do conhecimento humano, contendo uma grande quantidade de conhecimento de senso comum descrevendo objetos e ações do cotidiano.

A Cyc pode ser usada na identificação de inconsistências, contradições e violações do senso comum. Esta base de conhecimento pode servir como uma ontologia de alto nível, dando

suporte à recuperação de informações na Web. Pode também ser usada na identificação de inconsistência em bancos de dados, como por exemplo na verificação de informações sobre um empregado que foi demitido antes de nascer (Lenat, D.B., 1995).

A cada fase do método é desenvolvida uma ontologia contendo os conceitos mais abstratos e esta é refinada para representação do conhecimento. A primeira fase propõe a identificação e codificação do conhecimento explícito e implícito que aparecem nas fontes de conhecimento. A seguir, de posse deste conhecimento, é sugerido que novos conceitos sejam inferidos com o auxílio de ferramentas de processamento de linguagem natural e/ou aprendizado de máquina.

2.2.2. Metodologia de Uschold & King

Esta metodologia foi construída para o desenvolvimento do projeto da *Enterprise Ontology* (Uschold, M. & King, M., 1995), uma ontologia para dar suporte à modelagem de processos empresariais. Esta metodologia descreve as seguintes etapas para o desenvolvimento de ontologias:

1. **Identificação do propósito e escopo:** nesta etapa são definidos o propósito da criação da ontologia e seu uso pretendido.

2. **Construção da ontologia:** esta etapa é realizada em três passos:
   - *Captura da ontologia:* onde ocorre a identificação dos conceitos chave e relacionamentos do domínio, produção de definições textuais precisas e sem ambigüidade para estes conceitos e relacionamentos e a identificação dos termos para referenciar os conceitos e relacionamentos. Para a identificação dos conceitos chave são propostas três possíveis estratégias: partindo dos conceitos mais concretos para os mais abstratos (*bottom-up*), dos mais abstratos para os mais concretos (*top-down*), ou partindo dos conceitos mais relevantes para os mais abstratos e para os mais concretos (*middle-out*).

   - *Codificação:* nesta etapa o conhecimento capturado na etapa anterior é representado explicitamente em uma linguagem formal para especificação de ontologias.

   - *Integração de ontologias existentes:* durante as etapas anteriores podem ser aproveitadas definições de ontologias existentes, porém a metodologia não orienta o projetista como proceder.

3. **Avaliação:** nesta etapa são utilizadas atividades de avaliação da ontologia.

4. **Documentação:** a metodologia recomenda que roteiros sejam estabelecidos para documentação da ontologia, possivelmente diferindo de acordo com o tipo e propósito da ontologia. Todas as suposições devem ser documentadas, tanto as que dizem respeito aos conceitos principais quanto as relativas às primitivas usadas para expressar as definições da ontologia.

2.2.3. Metodologia de Grüninger & Fox

Esta metodologia é baseada na experiência de desenvolvimento da ontologia do projeto TOVE (Grüninger, M. & Fox, M.S., 1995) no domínio de processos de negócios e modelagem de atividades. Basicamente, esta metodologia constrói um modelo lógico do conhecimento que será especificado por meio de uma ontologia. Isto é, esta metodologia é um método formal baseado em lógica que transforma os cenários informais expressos em linguagem natural num modelo computável expresso em lógica. Para isso, é feita uma descrição informal da especificação do que deve constar na ontologia para então ser formalizada. As seguintes etapas são propostas nesta metodologia:

1. **Captura dos cenários motivacionais:** identificação de problemas que não são cobertos pelas ontologias existentes no domínio em questão. As soluções fornecidas para estes cenários fornecem uma semântica informal aos conceitos e relações que serão posteriormente incluídos na ontologia.

2. **Formulação de questões de competência informais:** as questões de competência são geradas a partir dos cenários motivacionais e a ontologia deve ser capaz de respondê-las através dos axiomas e definições.

3. **Especificação da terminologia da ontologia numa linguagem formal:** a partir das questões de competência informais são extraídos termos que serão utilizados para a especificação da terminologia numa linguagem formal. A terminologia da ontologia deve ser especificada em lógica de primeira ordem ou na linguagem equivalente KIF (*Knowledge Interchange Format*). Os termos identificados nesta etapa permitirão que definições e restrições sejam expressas por meio de axiomas.

4. **Formulação das questões de competência formais:** a partir das questões de competências informais e da terminologia especificada em linguagem formal, serão definidas as questões de competência formais.

5. **Especificação dos axiomas:** os axiomas especificam as definições dos termos da ontologia e das restrições de sua interpretação. Eles são definidos em sentenças de primeira ordem e fornecerão a semântica, ou significado, desses termos.

6. **Verificação da completude da ontologia:** a completude é verificada através do questionamento da ontologia utilizando as questões de competência formais. São definidas condições que verifiquem a completude das soluções dos questionamentos.

2.2.4. Método KACTUS

O objetivo do projeto *Espirit KACTUS* foi utilizar uma ontologia para dar suporte à investigação da viabilidade do reuso de conhecimento em sistemas complexos. ((Bernaras, A. *et alli*, 1996) *in* (OntoWeb Group, 2002)).

A idéia principal deste método é construir a ontologia que representa o conhecimento necessário a uma aplicação durante o desenvolvimento da aplicação. Esta ontologia de aplicação pode ser construída a partir da reutilização de outras ontologias de domínio e de tarefas e pode ser integrada às próximas ontologias construídas. Portanto, a cada aplicação desenvolvida, são desempenhadas as seguintes tarefas:

1. **Especificação da aplicação:** a especificação possibilita a identificação do contexto da aplicação e uma visão dos componentes que ela modela.

2. **Projeto preliminar:** nesta etapa são definidos os conceitos de alto nível da ontologia que são relevantes a partir das listas de termos e de tarefas geradas na etapa anterior.

3. **Refinamento e estruturação da ontologia:** nesta etapa a ontologia de alto nível é refinada e estruturada com o objetivo de chegar a uma versão definitiva.

2.2.5. METHONTOLOGY

METHONTOLOGY (Fernández-López, M. *et alli*, 1997) é um *framework* que dá suporte à construção de ontologias. O METHONTOLOGY inclui: a identificação do processo de desenvolvimento da ontologia, ciclo de vida envolvendo protótipos, um método para especificação de ontologias em nível de conhecimento e tradutores multi-línguas que transformam automaticamente as especificações em código. Para o processo de desenvolvimento da ontologia são descritas as seguintes atividades:

- **Atividades de Gerência de Projeto:** são atividades relacionadas ao gerenciamento do projeto da ontologia, incluindo planejamento, controle e garantia de qualidade.

- **Atividades Orientadas ao Desenvolvimento:** são atividades ligadas diretamente ao desenvolvimento da ontologia, tais como: especificação, conceitualização, formalização, implementação e manutenção.

- **Atividades de Suporte:** estas atividades são executadas paralelamente ao desenvolvimento da ontologia e referem-se a aquisição de conhecimento, avaliação da ontologia, integração e documentação.

METHONTOLOGY propõe um ciclo de vida para a ontologia envolvendo protótipos, permitindo a adição, alteração e remoção de termos a cada nova versão (protótipo) da ontologia. Para isso, o conhecimento é expresso utilizando-se um conjunto de representações intermediárias para então gerar a ontologia final utilizando tradutores. Estas representações intermediárias são utilizadas na fase de conceitualização para organizar e estruturar o conhecimento adquirido. Esta fase dá suporte à construção de ontologias no nível de conhecimento. É construído um glossário de termos, árvores de classificação e diagramas de relações binárias. Dicionário de conceitos e tabelas de relações binárias, classes, instâncias, atributos de classes, axiomas lógicos, fórmulas, entre outras, são exemplos das representações intermediárias propostas por essa metodologia.

O ambiente para construção de ontologias que utiliza este *framework* é chamado ODE (*Ontology Design Environment*) (Blázquez, M. *et alli*, 1998). Seu objetivo é dar suporte aos engenheiros de ontologia durante o ciclo de vida do processo de desenvolvimento da ontologia. Este ambiente procura automatizar cada atividade de desenvolvimento da ontologia e automaticamente integrar os resultados de cada fase com as entradas da fase seguinte.

2.2.6. Método SENSUS

SENSUS (Swartout, B. *et alli*, 1996) é uma ontologia criada para prover uma estrutura conceitual ampla a fim de trabalhar com tradução de máquina. A SENSUS contém tanto conceitos de alto nível quanto específicos, é de ampla cobertura, possuindo aproximadamente 50.000 conceitos organizados hierarquicamente de acordo com os níveis de abstração. Em contraste com a CYC, a SENSUS foi desenvolvida pela extração e união de informações de diferentes recursos eletrônicos ao invés de ser construída do zero.

O método SENSUS é baseado na seguinte hipótese: se duas bases de conhecimento são construídas a partir de uma mesma ontologia, o conhecimento será melhor compartilhado entre elas pois compartilharão uma estrutura comum. Portanto, a idéia principal é utilizar a SENSUS como ponto de partida para construção de ontologias de domínio adicionando a ela os termos específicos do domínio em questão.

A representação da ontologia da SENSUS pode ser descrita na forma de uma árvore, onde a raiz representa o termo mais abstrato e as folhas os mais específicos. A partir desta representação a construção da ontologia de domínio se dá da seguinte maneira:

1. São extraídos os termos específicos do domínio e colocados como folhas.
2. São incluídos todos os conceitos no caminho das folhas à raiz da SENSUS na nova ontologia.
3. São adicionados os termos que são relevantes para o domínio.
4. São incluídos como sub-árvore à SENSUS aqueles nós que possuem diversos caminhos a partir deles.

O software utilizado para construir ontologias seguindo esta metodologia é o Ontosaurus (Swartout, B., 1997). Ontosaurus possui interface web acessível de qualquer navegador e representa o conhecimento na linguagem de programação LOOM[1] (Ding, Y., 2001), permitindo tradução para Ontolingua, KIF e C++.

2.2.7. Metodologia On-To-Knowledge

A metodologia OTK (*On-To-Knowledge*) (Sure, Y. & Studer, R., 2002), tem o objetivo de introduzir e manter aplicações de gestão do conhecimento baseadas em ontologias. Para isso, propõe as seguintes atividades:

[1] LOOM é uma linguagem de programação de alto-nível baseada em lógica de primeira ordem que especifica um modelo declarativo expressivo e explícito, possui suporte dedutivo poderoso e disponibiliza serviços para bases de conhecimento.

1. **Meta-processo de Conhecimento:** são realizadas atividades para introdução de uma nova solução de gestão e manutenção do conhecimento numa organização, isto é, a fase inicial de introdução de uma aplicação baseada em ontologia. Este processo consiste nas seguintes atividades: estudo de viabilidade, inicialização, refinamento, avaliação, aplicação e evolução da ontologia.

    - *Estudo de viabilidade:* Nesta etapa ocorre a identificação de problemas, oportunidades e potenciais soluções, servindo como suporte à decisão para viabilidades econômicas, técnicas e de projeto.

    - *Inicialização:* Nesta etapa são realizadas atividades de especificação de requisitos, onde são definidos: o objetivo, domínio e escopo da ontologia. Além disso, são definidas regras do projeto, definindo convenções e regras de modelagem. São identificadas as fontes de conhecimento, os usuários, questões de competência e aplicações suportadas pela ontologia.

    - *Refinamento:* Nesta etapa é feita a extração de conhecimento das fontes de conhecimento. Esta metodologia propõe a utilização do método de extração (*top-down*, *middle-out* e *bottom-up*) mais aplicável às fontes de conhecimento disponíveis. É realizada também a formalização da ontologia, o engenheiro da ontologia deve considerar as vantagens e limitações de cada linguagem formal para escolher a mais apropriada.

    - *Avaliação:* Nesta etapa é definido um *framework* de avaliação de ontologias e tecnologias relacionadas. Esta etapa é iterativamente ligada à etapa anterior, pois os resultados gerados por esta etapa podem detectar falhas na representação da ontologia e servirão de entrada para a etapa de refinamento.

    - *Aplicação e evolução:* Esta etapa faz a aplicação da ontologia em sistemas baseados em ontologias. Ainda nesta etapa são recomendadas práticas para o engenheiro de ontologias lidar com evolução/atualização da ontologia.

2. **Processo de Conhecimento:** O foco deste processo é a utilização contínua da aplicação de gestão de conhecimento implementada na organização. Neste processo são realizadas as seguintes atividades:

    - *Criação do conhecimento e/ou importação de documentos e metadados:* o conhecimento deve ser criado ou convertido para que se ajuste às convenções da organização.

    - *Captura do conhecimento:* Identificação do contexto dos ítens de conhecimento para elucidar sua importância e relacionamentos.

    - *Recuperação e acesso ao conhecimento:* A ontologia pode ser utilizada para recuperação e acesso, derivando visões adicionais do conhecimento. Uma ontologia

permite derivar relacionamentos e descrições inferindo através de um mecanismo de inferência apropriado.

- *Utilização do conhecimento:* A ontologia facilita a utilização e reutilização do conhecimento. Na maioria das vezes não é o conhecimento por si só o mais interessante numa organização, e sim as derivações que podem ser feitas a partir desse conhecimento e que adicionam valor a este conhecimento.

2.2.8. Knowledge Unified Process (*KUP*)

O KUP *(Knowledge Unified Process)*, é um processo unificado proposto em (Orlean, D. & Lucena, C., 2003), para desenvolvimento de ontologias e bases de conhecimento que deverão ser utilizadas no contexto do desenvolvimento de aplicações para a Web Semântica.

Este processo surgiu da unificação de características oriundas de diferentes metodologias da engenharia de ontologias. Para garantir a qualidade do processo de desenvolvimento de ontologias, o KUP foi baseado nos critérios de avaliação de metodologias para desenvolvimento de ontologias propostos por (Fernández-López, M. & Gómez-Pérez, A., 2002). Além disso, o KUP adapta e integra as melhores práticas em desenvolvimento de software apresentadas pelo RUP (*Rational Unified Process*) (Rational Team,1998). O processo baseia-se também nas atividades apresentadas no padrão definido pela IEEE para a construção de processos de ciclo de vida e de desenvolvimento de software (IEEE Computer Society, 1995) visando atender o conjunto de critérios para avaliação de metodologias e processos de desenvolvimento de ontologias e bases de conhecimento.

O principal problema apontado no desenvolvimento de software é com relação ao risco que se mantém alto durante todo o processo, até que seja tarde demais para mudar alguma decisão que tenha sido tomada anteriormente. Para resolver esse tipo de problema foram identificadas seis práticas principais: desenvolvimento iterativo, gerência de requisitos, uso de componentes arquiteturais, modelagem visual, verificação contínua de qualidade e gerência de mudanças. Apesar destas melhores práticas terem sido propostas para resolver problemas presentes em desenvolvimento de software, elas foram aproveitadas no KUP durante a unificação das atividades.

O KUP é composto de três fases principais que são executadas de maneira iterativa para minimizar os riscos durante o processo e não apenas em fases avançadas do projeto, como é comum em processos de desenvolvimento em cascata. As fases propostas são as seguintes:

- **Fase de Concepção:** esta fase focaliza a análise de viabilidade do projeto, a estratégia de desenvolvimento da ontologia, o escopo e levantamento de requisitos.

- **Fase de Construção:** o foco desta fase é o projeto, a implementação e a implantação da ontologia, sem deixar de lado os novos requisitos que podem surgir e mudanças na estratégia.

- **Fase de Evolução:** esta fase focaliza a integração de novos requisitos ao projeto, através da inclusão de novos conceitos, relações e axiomas na ontologia.

Durante as fases do processo, algumas atividades executadas nas disciplinas geram artefatos. Uma disciplina agrupa atividades que integram um processo específico de acordo com determinado tema. Um artefato é tudo aquilo que é produzido, consumido ou modificado por uma atividade. Existem diversos tipos de artefatos possíveis, como documentos, modelos, código fonte e até mesmo programas inteiros.

O diagrama da Figura 2 descreve as iterações entre as atividades de cada disciplina nas fases propostas pelo KUP. Pode-se observar que na fase de Concepção a iteração inicial foca suas atenções na disciplina de Análise de Requisitos, iniciando também atividades de Projeto e Implementação. Na fase de Construção, um esforço maior é despendido para o Projeto, a Implementação e a Implantação, havendo, no entanto, uma continuidade das atividades de Análise de Requisitos, com a inclusão de novos itens necessários. A fase de Evolução envolve em suas iterações um esforço mais distribuído entre as disciplinas, porém, normalmente menor que na fase de Construção. Em todas as fases vemos a realização de atividades de Instanciação do KUP, uma Análise de Viabilidade prévia e sucessivas atividades relacionadas aos Processos de Suporte e Gerência do Projeto.

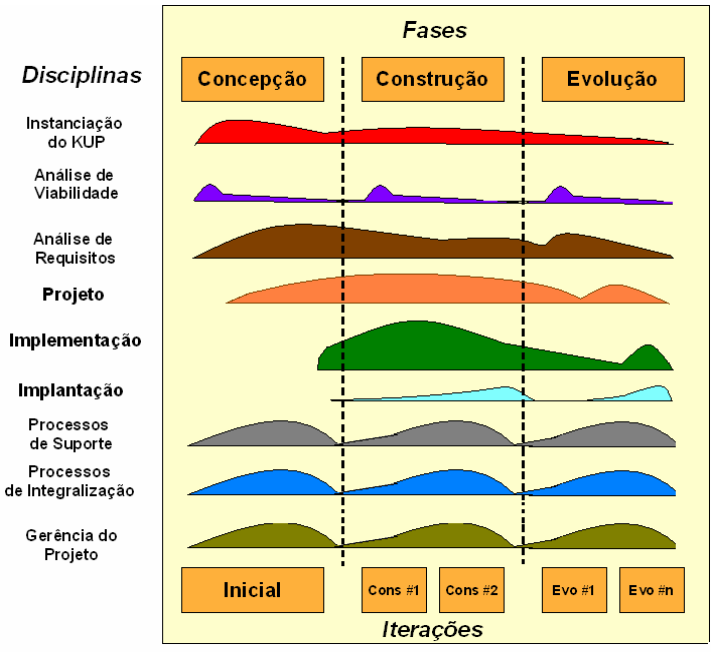

Figura 2: Diagrama de iterações entre disciplinas e fases do *KUP*

Neste contexto, será apresentada uma breve descrição das disciplinas que organizam as atividades e artefatos do KUP, mais detalhes podem ser obtidos em (Orlean, D. & Lucena, C., 2003):

- **Instanciação do KUP:** nesta disciplina é proposta a atividade de Instanciação do *Framework* de Processos que inclui a definição das fases, disciplinas, papéis, atividades e artefatos que farão parte do processo concreto que será utilizado no projeto. Devem ser escolhidos os elementos que garantam a expressividade necessária para a execução do processo bem como a facilidade de execução. Ainda nesse contexto devem ser definidos critérios de monitoramento e controle e de gerência de qualidade do processo. A segunda atividade é a Elaboração do Fluxo para a Execução do Processo Concreto, identificando as disciplinas, atividades e artefatos envolvidos com as respectivas dependências entre tais elementos.

- **Análise de viabilidade:** nesta disciplina é feito um estudo preliminar para a identificação prévia de possíveis oportunidades que possam acelerar o processo de desenvolvimento ou de possíveis problemas que possam aumentar o seu risco. Esta análise é focada em aspectos técnicos, econômicos e de projeto, de forma a minimizar os riscos nas fases seguintes. Após a Análise de Viabilidade o projetista deve ser capaz de decidir se o projeto é viável ou não, bem como direcionar as próximas etapas no sentido de minimizar os riscos avaliados. Esta disciplina gera um artefato contendo a Análise de Viabilidade que será a base para a identificação dos requisitos realizada na próxima disciplina.

- **Análise de requisitos:** compreende atividades iterativas que permitem desenvolver a especificação de requisitos da ontologia ou das aplicações que farão uso dela. Ao final desta etapa será gerado um artefato contendo o resultados dessas atividades. Esta análise subdivide-se em três atividades:

  - *Identificação de Propósito e Escopo:* Durante esta etapa é definido o propósito da construção da ontologia e qual será seu uso pretendido. Uma ontologia pode ser usada apenas para estruturar uma base de conhecimento, para a anotação de páginas na web, como um meio para integrar aplicações, entre diversas outras utilidades. Para organizar a descrição do uso de uma ontologia, Uschold e Grüninger (1996) propuseram o conceito de Espaços de Uso seguindo três categorias:

    Comunicação: diferentes aspectos relacionados ao uso de ontologias são utilizados para facilitar a comunicação entre pessoas de uma organização, como por exemplo :

    - Geração de modelos normativos;
    - Criação de uma rede de relacionamentos;
    - Garantia de consistência e inexistência de ambigüidades;
    - Integração de diferentes perspectivas.

    Interoperabilidade: para permitir que usuários, sistemas e agentes possam trocar dados entre si. Existem diversas dimensões de interoperabilidade, tais como:

    - Uso de ontologia como inter-língua;
    - Possibilitar a troca de informações.

Engenharia de Sistemas: envolve a aplicação de ontologias no suporte ao projeto e desenvolvimento de sistemas de software, tais como:

- Especificação;
- Confiabilidade;
- Reusabilidade.

- *Captura dos Cenários Motivacionais:* identificação de possíveis situações e problemas que não são cobertos pelas ontologias existentes no domínio em questão. A partir deles serão inferidas possíveis soluções a serem desenvolvidas. Estas soluções fornecem uma semântica informal aos conceitos e relações que serão posteriormente incluídos na ontologia.

- *Elicitação de Requisitos e Atores:* nesta atividade são levantados os requisitos para o desenvolvimento do projeto e os atores dos cenários de uso da ontologia. Aqui são identificadas as fontes de informação, identificados os atores e os cenários de uso da ontologia. Os atores são usuários típicos, outras aplicações e agentes de software que farão uso da ontologia ou das aplicações que forem desenvolvidas a partir dela. Estes papéis permitirão elaborar os cenários de uso da ontologia. Para a elaboração dos Cenários e Casos de Uso, o KUP propõe a utilização de três abordagens sobre as quais o projetista pode optar por aquela que melhor adapte-se às necessidades do projeto em desenvolvimento. São elas: Casos de Uso do Rational Unified Process extendido para o KUP, Léxico Ampliado da Linguagem e Cenários, proposto por (Breitman, K. & Leite, J.C., 2003), Diagramas de Interação com o Usuário (UIDs), propostos no Método OOHDM (Schwabe, D. & Rossi, G., 1998). Estas atividades têm como objetivo facilitar o processo de identificação das tarefas que terão que ser resolvidas com o suporte da ontologia. Para isso é feita a identificação das tarefas nos cenários de uso e são formuladas e estratificadas as questões de competência a devem ser respondidas pela ontologia.

- **Projeto:** esta disciplina compreende atividades que serão executadas com o objetivo de apresentar uma representação coerente e consistente da ontologia que atenda aos requisitos especificados. As atividades descritas são as seguintes:

  - *Conceitualização:* nesta atividade é proposta a extração dos termos a partir do artefato que descreve as questões de competência informais (gerado na disciplina anterior). Com base na terminologia extraída devem ser formuladas as questões de competência formais. Parte-se então para a construção de um Modelo Conceitual para a ontologia. Para isso, primeiramente constrói-se a taxonomia da ontologia, identificando-se as relações de especialização ou generalização entre os conceitos identificados nesta atividade. O segundo passo, para construção do modelo conceitual, é a adição das relações não taxonômicas entre os conceitos (Sure, Y. & Studer, R., 2002).

  - *Formalização:* A partir do modelo conceitual gerado na atividade anterior, parte-se para a sua formalização. Nesta atividade são propostas sub-atividades: integração das ontologias identificadas na etapa anterior, escolha da linguagem de

representação, especificação formal da terminologia, axiomas e questões de competência.

- *Avaliação da Ontologia Projetada e Refinamento:* atividade executada após a Formalização da Ontologia, para que seja possível identificar omissões e erros no artefato gerado. O foco da avaliação da ontologia proposta no KUP está na verificação da completude da ontologia. Isto é, dependendo do tipo de ontologia desenvolvida**,** essa verificação pode ser feita tanto a partir dos requisitos levantados na disciplina de Análise de Requisitos (verificando-se, por exemplo, como os Cenários Motivacionais foram satisfeitos pela nova ontologia), quanto a partir das Questões de Competência da ontologia.

  Uma avaliação bem sucedida teria, por exemplo, as Questões de Competência, propostas até a iteração corrente, respondidas com base nos termos e axiomas da ontologia. Caso isto não seja verdade, a ontologia deve ser refinada até que todas as omissões ou erros sejam solucionados e as Questões de Competência respondidas.

  Realizadas as atividades da disciplina de projeto, são gerados dois artefatos:
  - Modelo Conceitual da Ontologia;
  - Ontologia descrita em Linguagem Formal.

- **Implementação:** disciplina com atividades que transformam a representação conceitual da ontologia em sua implementação. Para isso, é preciso identificar a linguagem e o ambiente de engenharia de ontologias mais adequados ao projeto. Esta disciplina divide-se nas seguintes atividades:

  - *Escolha da linguagem de representação de conhecimento:* para a representação da ontologia, o KUP apresenta algumas linguagens de representação de conhecimento e orienta o projetista a escolher àquela que melhor atenda às demandas do projeto. A partir da análise de requisitos, o projetista deve identificar as necessidades do projeto e identificar a linguagem de representação de ontologia mais adequada. Para isso, o KUP disponibiliza ao projetista uma tabela (Tabela 2.2.8-1) baseada em um estudo comparativo entre diversas linguagens, apontando os elementos fundamentais de representação de conhecimento e o suporte dado pela linguagem (Ribière, M. & Charlton, P., 2001). O projetista preenche a coluna "Requisitos" identificando as demandas em "Críticas", "Necessárias", "Úteis" e "Dispensáveis", podendo assim, rejeitar linguagens que não tenham elementos fundamentais necessários ao seu projeto. O resultado desta tabela, associado com a classificação das categorias e formalismo das linguagens apresentadas, permite ao projetista classificar as linguagens de acordo com sua adequação ao projeto.

Tabela 2.2.8-1: Tabela para guiar o usuário na escolha da linguagem de representação.

	KIF	OKBC	XOL	RDF(S)	OIL	DAML + OIL	Requisitos
Elementos principais							
Conceitos	+	+	+	+	+	+	
Relações	+	+	+	+	+	+	
Funções	+	-	-	-	+	+	
Instâncias	+	+	+	+	-	+	
Axiomas	+	-	-	-	+	+	
Axiomas aceitáveis							
Negação	+	-	-	-	+	+	
Conjunção	+	-	-	-	+	+	
Disjunção	+	-	-	-	+	+	
Taxonomia dos conceitos							
Sub-classes	+	+	+	+	+	+	
Herança múltipla	+	+	+	+	-	+	
Meta-classes	+	+	-	+	-	+	
Propriedades							
Propriedades multi-valoradas	+	+	+	+	-	+	
Hierarquia das propriedades (subPropertyOf)	+	+	-	+	-	+	
Propriedade-inversa	+	+	+	-	+	+	
Facetas							
Valor de propriedade padrão	-	+	+	-	-	-	
Restrições de tipo	+	+	+	+	+	+	
Restrições de cardinalidade	+	+	+	-	+/-	+	
Outras restrições de propriedade	+	+	+	-	+	+	
Outras características							
Inclusão de meta informação	+	-	+	-	+	+	
Inclusão de outras ontologias	-	-	-	-	+	+	
Tipos de dados primitivos	+	+	+	-	-	-	

- *Escolha do ambiente de engenharia de ontologia:* até a versão disponibilizada da documentação do KUP esta atividade encontrava-se apenas proposta, não contendo a descrição das tarefas a serem desempenhadas. Escolhida essa linguagem, o KUP orienta o projetista a escolher o ambiente de engenharia de ontologia onde é apresentado um estudo comparativo sobre as alternativas de ambientes (Gómez-Pérez *et alli*, 2001).

- *Codificação da ontologia na linguagem escolhida:* até a versão disponibilizada da documentação do KUP esta atividade encontrava-se apenas proposta, não contendo a descrição das tarefas a serem desempenhadas.

- **Implantação:** esta disciplina compreende os esforços necessários para integrar a ontologia desenvolvida nas potenciais aplicações identificadas nas disciplinas anteriores do projeto. As atividades propostas incluem: identificação das aplicações a serem desenvolvidas, desenvolvimento do Diagrama de *Deployment* das aplicações, seleção das ferramentas para implantação dos serviços de manipulação e consulta das ontologias e bases de conhecimento, desenvolvimento das aplicações e implantação.

- **Processos de Suporte:** nesta disciplina são propostas atividades de operação, suporte, manutenção e arquivamento da ontologia e suas aplicações. Na versão disponibilizada do KUP estas atividades não estão descritas.

- **Processos de Integralização:** nesta disciplina são propostas atividades de aquisição de conhecimento, verificação e validação, gestão de configuração da ontologia, documentação e treinamento. Na versão disponibilizada da documentação do KUP estas atividades não estão descritas.

- **Gerência do Projeto:** paralelamente às demais disciplinas do KUP, é realizada a disciplina de gerência de projeto, para assegurar o gerenciamento no decorrer do ciclo de vida da ontologia. Para isto, são propostas atividades de gerenciamento, tais como: definição da equipe, definição de prazos e cronograma.

  Para facilitar a definição dos papéis dos participantes do projeto, o KUP apresenta a Tabela 2.2.8-1, que mostra alguns papéis de referência e disciplinas e atividades de possíveis atuações.

Tabela 2.2.8-2: Indicação dos papéis e atuação dos participantes do projeto de ontologia.

Papel de Referência	Disciplinas e Atividades
Gerente de Projeto	Todas as disciplinas e atividades.
Analista de Requisitos	Disciplina de Análise de Requisitos e atividades de Validação e Refinamento.
Engenheiro de Conhecimento	Disciplinas de Análise de Requisitos, Projeto e Implementação da ontologia.
Especialista de Domínio	Disciplinas de Análise de Requisitos e Projeto.
Arquiteto de Aplicação	Disciplina de Implantação.

FONTE: Orlean, D. & Lucena, C., 2003.

Introduzidos os conceitos de ontologia e engenharia de ontologias, e identificadas as propostas para engenharia de ontologias, o KUP foi instanciado para desenvolvimento do estudo de caso proposto.

3. Estudo de Caso: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação

A ontologia a ser desenvolvida usando o KUP tem como finalidade dar suporte à uma aplicação existente, o e-BTS – Boletim Técnico de Segurança Eletrônico, um sistema para alerta à ameaças de segurança, cujo contexto é descrito a seguir.

Atualmente, com o crescente número de ataques maliciosos aos ambientes corporativos, está cada vez mais difícil manter-se atualizado com os riscos emergentes que podem comprometer os diversos sistemas e aplicações destas organizações. Por isso, manter-se atualizado na área de segurança da informação é o segredo para implementar ações preventivas e/ou corretivas para manter os serviços das empresas e proteger os ambientes corporativos. Através da disponibilização de boletins técnicos de segurança abrangentes e personalizados, o e-BTS – Boletim Técnico de Segurança Eletrônico, sistema desenvolvido com o objetivo de monitorar ameaças de segurança à sistemas de software, fornecerá aos

seus clientes informações atualizadas para proteção, indicando medidas de prevenção e/ou correção às ameaças aos seus ativos tecnológicos.

Ao configurar o serviço, o usuário informa ao sistema e-BTS quais os componentes que formam os ativos existentes em sua organização. O e-BTS passa, então, a monitorar as ameaças (vulnerabilidades ou códigos maliciosos) que possam afetar os componentes cadastrados, e, por sua vez, os ativos do cliente.

Para o monitoramento das ameaças a estes ativos, o usuário cria seus boletins e define os graus de severidade, confiabilidade e impacto das ameaças que deseja monitorar. Para que o usuário receba os alertas de segurança, ele precisa definir os destinatários e respectivos endereços eletrônicos, podendo especificar uma ou mais pessoas responsáveis pelo recebimento dos alertas do e-BTS.

Para disponibilizar os boletins técnicos, o e-BTS tem um serviço de coleta de informações, que busca e recupera documentos distribuídos na rede, contendo informações sobre ameaças a sistemas. Diariamente, diversas fontes de informação publicam novos alertas sobre ameaças, que podem ser desde vulnerabilidades até ameaças de um novo vírus sendo disseminado através de correio eletrônico. No manual do e-BTS são citadas algumas fontes, tais como: Symantec™ DeepSight™ Alert Services, CERT® Coordination Center (CERT/CC) e o Portal TechNet.

Devido ao fato desse domínio ser de grande abrangência, a diversidade de padrões e termos utilizados nas informações disponibilizadas na rede dificulta a integração destas informações distribuídas. Portanto, ao coletar tais informações, o e-BTS deve ser capaz de classificá-las e armazená-las na base de conhecimento de acordo com seu conteúdo para posterior tradução e edição. Além disso, as diversas fontes devem apresentar credibilidade para que as informações sejam enviadas aos clientes. O grau de credibilidade, bem como o grau de severidade, também são classificados pelo e-BTS a cada alerta recebido.

Após as informações terem sido coletadas, traduzidas e editadas, são gerados os boletins técnicos para serem enviados pelo e-BTS. Estes boletins deverão ser personalizados de acordo com as configurações pré-estabelecidas para cada usuário. Neste contexto, identificou-se que as tarefas desempenhadas pelo e-BTS poderiam ser auxiliadas através da utilização de uma descrição formal dos conceitos envolvidos nas tarefas deste sistema.

As tarefas do e-BTS poderiam ser auxiliadas pelos conceitos e relacionamentos descritos por documentos XML (*eXtensible MarKUP Language*[2]) da aplicação atual, pois, a linguagem XML desempenha um importante papel no intercâmbio de dados na internet, mas é preciso esclarecer suas limitações. Embora XML não represente a solução definitiva para a interoperabilidade entre sistemas, ela provê uma camada fundamental para sua construção. Em XML, uma espécie de alfabeto comum é estabelecida, o que nos permite dar significado às palavras, porém este alfabeto não fornece suporte à formação de sentenças com significado semântico (Smith, H. & Poulter, K., 1999). De fato, a sintaxe XML expressa classes de objetos, atributos e relações de hierarquia e adjacência, desta

[2] http://www.w3.org/XML/Core/

forma sua expressividade é limitada para modelar semanticamente os objetos (Cover, R., 1998). Um exemplo disso explicita-se quando a partir de um documento XML e sua especificação, não é possível a geração de conhecimento a partir de inferências simples sobre a estrutura do documento. As aplicações baseadas em descrições XML requerem o conhecimento embutido nas suas implementações e dependendo das regras utilizadas e da lógica da programação, mesmo em aplicações baseadas num mesmo documento XML podem ser geradas conclusões diferentes.

Por este motivo, foi dada a preferência ao uso de ontologias para auxiliar nas tarefas do e-BTS. As limitações de XML são contornadas ao utilizarmos ontologias descritas numa linguagem de representação que permita inferências cujos resultados serão os mesmos independente da lógica de programação utilizada. A utilização desta forma de representação, além de viabilizar a interoperabilidade interna dos diferentes módulos do e-BTS facilitaria sua extensão.

Portanto, neste trabalho foi iniciado o projeto da ontologia que fará uma descrição explícita dos conceitos envolvidos na funcionalidade do sistema e-BTS. Para a posterior implantação desta ontologia no sistema, torna-se essencial sua integração com uma ontologia que descreva os conceitos do domínio de segurança da informação envolvidos nas atividades do sistema, definindo um vocabulário comum e possibilitando um entendimento compartilhado dentre os diversos módulos do sistema. Estas ontologias integradas formarão uma ontologia de aplicação para gestão do conhecimento em segurança da informação dando suporte às atividades do e-BTS. Segundo Guarino (1998), um sistema de informação pode ser guiado por uma ontologia mas, para que isto aconteça, ela precisa definir conceitos e relacionamentos envolvidos na aplicação (sistema de informação). Dando continuidade a este estudo, novas iterações do KUP serão essenciais para o refinamento do protótipo da ontologia desenvolvido neste trabalho.

Para o desenvolvimento do protótipo inicial da ontologia de tarefas foi utilizada uma instância do *Knowledge Unified Process* (KUP), com o objetivo de servir como caso-teste e avaliar seu desempenho no desenvolvimento do projeto de uma ontologia.

3.1. Instanciação do *KUP*

Esta seção mostra as disciplinas do KUP aplicadas ao estudo de caso para construção da ontologia para auxiliar nas tarefas de gestão do conhecimento em segurança da informação. Esta ontologia será futuramente integrada a outras ontologias e ao e-BTS, e seus conceitos e relacionamentos devem fornecer suporte às tarefas desempenhadas pelo sistema.

O *Framework* de Processos proposto pelo KUP é formado por disciplinas iterativas onde são gerados artefatos. Estas atividades devem ser instanciadas para cobrir apenas as necessidades do projeto a ser desenvolvido. Neste contexto, para este estudo de caso serão utilizadas as disciplinas de análise de viabilidade, análise de requisitos, projeto da ontologia e implementação. As etapas de implantação e manutenção e evolução serão indicações para trabalhos futuros, onde um protótipo da aplicação utilizando a ontologia para guiar suas tarefas poderá ser desenvolvido.

As atividades apresentadas a seguir foram instanciadas para este estudo de caso:

- **Análise de viabilidade**: nesta disciplina foram identificados aspectos relacionados à disponibilidade de recursos para o desenvolvimento do projeto. Os recursos necessários, tais como: equipe, fontes de informação do domínio, recursos tecnológicos, entre outros. Os resultados da análise estão no Artefato de Análise de Viabilidade no Anexo I deste documento. Por ser um processo iterativo a análise de viabilidade foi executada ao longo do projeto, viabilizando a continuidade do desenvolvimento a cada iteração, dados os requisitos levantados, desempenho da equipe, entre outros. Por outro lado identificou-se a necessidade desta ser executada também antes da instanciação do KUP. Assim, a instanciação só é realizada se o projeto for viável.

- **Análise de requisitos:** nesta disciplina foram identificados os objetivos da construção da ontologia, os cenários que motivaram sua construção, as fontes de informação disponíveis e usuários (Anexo II). Para identificação das tarefas do sistema, foi instanciada a descrição dos Casos de Uso proposta pelo KUP baseado nos casos de uso do RUP. Nesta atividade foi identificada a necessidade de alteração do *template* de Descrição dos Casos de Uso proposto pelo KUP. Na coluna onde são descritas as "Consultas à Base de Conhecimento", foi sugerida a alteração da sua identificação para "Manipulação da Base de Conhecimento", tendo em vista que o sistema fará consultas e inserções nesta base. Alguns exemplos dos casos de uso identificados neste estudo de caso estão no Anexo III deste documento. A partir dos casos de uso, foram identificadas as tarefas e as questões de competência (Anexo IV) que a ontologia deve ser capaz de responder durante a execução de cada tarefa. Para este estudo de caso, este artefato foi adaptado do template disponibilizado pelo KUP, a coluna interna da tabela, originalmente disponibilizada para estratificação das questões de competência, foi eliminada em virtude do alto grau de dificuldade desta atividade.

- **Projeto:** nesta disciplina a primeira atividade instanciada foi a conceitualização. Esta atividade propõe a extração dos conceitos, propriedades e relações a partir do artefato que descreve as questões de competência (Anexo IV) gerado na disciplina de Análise de Requisitos. A partir deste artefato, é indicada a representação da ontologia utilizando um modelo conceitual, com o objetivo de facilitar o entendimento da ontologia sem que seja necessário entender a linguagem de representação escolhida e facilitar a troca de informações entre os membros da equipe. Para isso, é indicada a construção da taxonomia da ontologia, identificando-se as relações de especialização ou generalização entre os conceitos identificados nos artefatos anteriores. Porém, para a construção da taxonomia, torna-se essencial a identificação da hierarquia dos conceitos. Neste trabalho, sugere-se a descrição dos conceitos (Anexo V) para identificação das relações hierárquicas, para então, gerar a representação da ontologia. Neste trabalho a representação taxonômica encontra-se no Anexo VI deste documento e foi gerada na ferramenta Dumpont DAML[3] (programa com interface web para visualização da taxonomia de uma ontologia codificada em DAML).

[3] http://www.daml.org/2001/03/dumpont/

- **Implementação:** a partir da taxonomia da ontologia a implementação foi feita no ambiente de desenvolvimento de ontologias OilEd 3.5[4] (Figura 3.1-1). Este editor formaliza a ontologia em diversas linguagens de representação de ontologias, porém a linguagem escolhida foi DAML+OIL[5]. O código-fonte em DAML+OIL do protótipo da ontologia resultante encontra-se no Anexo VII deste documento. A escolha do ambiente foi impulsionada pela sua gratuidade.

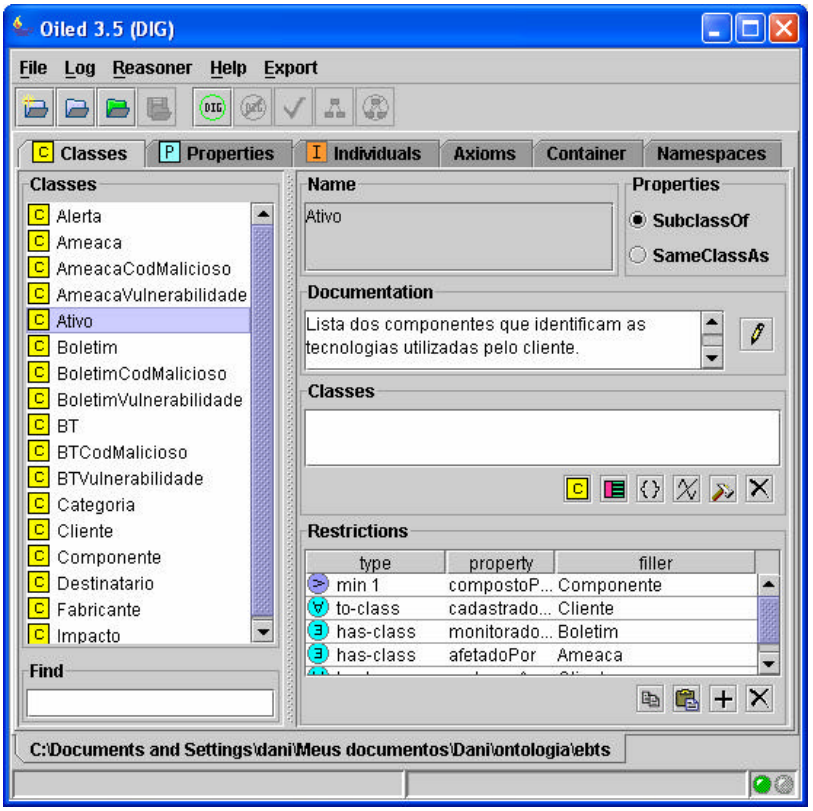

Figura 3.1-1: Editor de ontologias OilEd 3.5.

4. O *Framework* para Avaliação de Metodologias e Métodos

Neste trabalho utilizou-se uma instanciação do *framework* proposto em (Fernández-López, M. & Gómez-Pérez, A., 2002) para avaliação do KUP. Este *framework* adapta as atividades apresentadas no padrão definido pela IEEE para o desenvolvimento de software (IEEE Computer Society, 1990) para o desenvolvimento de ontologias. Segundo Férnandez-López e Gómez-Pérez (2002), uma ontologia é parte de produtos de software, portanto deve ser desenvolvida por metodologias que atendam aos padrões propostos para desenvolvimento de software com algumas adaptações às características especiais de ontologias. Os critérios de avaliação propostos pelo *framework* são os seguintes:

[4] http://oiled.man.ac.uk/
[5] http://www.daml.org/

1. **Segundo a estratégia de construção proposta na metodologia:**

   - *Ciclo de vida proposto:* identificar se a metodologia propõe um conjunto de etapas que deve ser seguido para a construção de ontologia, descrevendo as atividades de cada etapa e a relação entre estas etapas.

   - *Dependência com relação à aplicação da ontologia:* verificar o nível de dependência entre a ontologia e sua aplicação. A classificação é feita em: dependente, semi-dependente ou independente.

     Dependente de aplicação: a ontologia é dependente de aplicação quando sua construção se baseia na sua aplicação, como uma base de conhecimento ou software;

     Semi-dependente da aplicação: identifica-se, durante a especificação, possíveis cenários de uso da ontologia.

     Independente de aplicação: Quando a ontologia tem como objetivo apenas representar a conceitualização de um domínio, isto é, quando o processo é independente dos usos pretendidos da ontologia (seja em uma base de conhecimento, agentes, etc).

   - *Utilização de ontologias base:* verificar se a metodologia possibilita o reuso de uma ontologia como um ponto de partida para o domínio, ou até mesmo a reutilização de conceitos e relações existentes em ontologias distintas.

   - *Estratégia pra identificação de conceitos:* identificar o tipo de estratégia utilizada pela metodologia. Existem três estratégias para identificação dos conceitos: do mais concreto para o mais abstrato (*bottom-up*), do mais abstrato para o mais concreto (*top-down*), ou do mais relevante para o mais abstrato e mais concreto (*middle-out*).

2. **Segundo o processo de desenvolvimento de ontologia proposto na metodologia:** este critério adapta o padrão de processo de desenvolvimento de software, IEEE 1075-1995 (IEEE Computer Society, 1995). Para cada atividade do *framework* levantamos sua existência na metodologia avaliada e o nível de detalhamento.

   - *Processos de Gerenciamento do Projeto:* detecta a existência do processo de gerência de projeto. São desempenhadas tarefas relacionadas a inicialização, monitoramento e controle do projeto, tais como: definição da equipe, definição de cronograma, criação de um *framework* de processos no projeto da ontologia, entre outras.

   - *Processos orientados ao desenvolvimento de ontologias:* verifica se a metodologia propõe os processos relacionados ao desenvolvimento, instalação, operação e manutenção da ontologia, que estão subdivididos em:

     Processo de Pré-desenvolvimento: realizados antes do desenvolvimento real da ontologia. Envolvem atividades de estudo de viabilidade do projeto,

estudo do ambiente de instalação da ontologia e da possibilidade de integração da ontologia em outros sistemas.
Processo de Desenvolvimento: devem ser realizadas tarefas de *especificação de requisitos.* Similarmente aos projetos de bases de conhecimento, é imprudente codificar a partir da aquisição do conhecimento, sendo necessária a atividade de projeto para posterior implementação.
Processos de Pós-desenvolvimento: realizados após o desenvolvimento e estão relacionados com a instalação (integração em um sistema), operação, suporte, manutenção e arquivamento da ontologia.

- *Processos complementares:* detecta a existência das tarefas necessárias para completar as atividades de projeto da ontologia. Composto de atividades que asseguram a finalização e qualidade do projeto. São realizadas ao mesmo tempo que os processos orientados ao desenvolvimento e cobrem as atividades de aquisição de conhecimento, verificação e validação, gerenciamento da configuração da ontologia, documentação e treinamento, dando instruções às pessoas que são responsáveis pela manutenção e aprimoramento do conhecimento dos integrantes da equipe de desenvolvimento.

- **Segundo o uso da metodologia:** este critério verifica o nível de maturidade da metodologia, isto é, o seu uso em projetos, aceitação em outros grupos de pesquisa e as ontologias desenvolvidas.

- **Segundo o suporte tecnológico proposto:** identificar as ferramentas que provêem suporte total ou parcial para a metodologia ou método avaliado.

Para este estudo de caso, este *framework* de avaliação foi instanciado com a eliminação dos últimos critérios: a análise do uso da metodologia e das ferramentas que a suportam, visto que o KUP é um processo novo.

5. Estudo comparativo entre as metodologias apresentadas

O objetivo desta seção é apresentar a avaliação do *Knowledge Unified Process (KUP).* Para isso, foi utilizada uma instância do *framework* de avaliação para metodologias e métodos, apresentado na seção 4, e os resultados comparados com outras avaliações de metodologias e métodos para construção de ontologias realizadas em estudos anteriores (OntoWeb Group, 2002 e Fernández-López, M. & Gómez-Pérez, A., 2002).

A Tabela 5-1 mostra o estudo comparativo para avaliação das metodologias quanto à identificação de atividades relacionadas à estratégia de construção da ontologia. A Tabela 5-2 mostra o resultado do estudo comparativo avaliando a existência de atividades do processo de desenvolvimento da ontologia. Ambas as tabelas são extensões às tabelas apresentadas em estudos anteriores (OntoWeb Group, 2002 e Fernández-López, M. & Gómez-Pérez, A., 2002), apresentando a inclusão da avaliação do *KUP* seguindo o mesmo critério de preenchimento dos campos de avaliação.

Tabela 5-1: Comparativo para avaliação do *KUP* quanto às atividades relacionadas à estratégia de construção da ontologia.

Característica	Cyc	Uschold & King	Grüninger & Fox	KACTUS	METHONTOLOGY	SENSUS	OTK	*KUP*
Ciclo de vida proposto	Evoluindo em protótipos	Não proposto	Evoluindo em protótipos / incremental	Evoluindo em protótipos	Evoluindo em protótipos	Não proposto	Incremental e cíclico com evolução em protótipos	Iterativo e incremental
Dependência com relação à aplicação da ontologia	Independente da aplicação	Independente da aplicação	Semi-dependente da aplicação	Dependente da aplicação	Independente da aplicação	Semi-dependente da aplicação	Dependente da aplicação	Independente, semi-dependente ou dependente da aplicação.
Utilização de ontologias base	Sim	Não	Não	Não	Não	Sim	Dependente dos recursos disponíveis para o projeto	Dependente dos recursos disponíveis para o projeto
Estratégia para identificação de conceitos	Não especificado	*Middle-out*	*Middle-out*	*Top-down*	*Middle-out*	Não especificado	*Top-down*, *bottom-up* ou *middle-out* dependente da aplicação	*Top-down*, *bottom-up* ou *middle-out*

Tabela 5-2: Comparativo para avaliação do *KUP* quanto às atividades relacionadas ao processo de desenvolvimento da ontologia

Característica			Cyc	Uschold & King	Grüninger & Fox	KACTUS	METHONTOLOGY	SENSUS	OTK	*KUP*
Processo de Gerenciamento do Projeto	Inicialização do projeto		Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Descrita	Descrita em detalhes
	Controle e monitoramento do projeto		Não proposta	Não proposta	Não proposta	Não proposta	Proposta	Não proposta	Descrita	Proposta
	Gestão de qualidade da ontologia		Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Descrita	Proposta
Processos orientados ao desenvolvimento da ontologia	Processo de pré-desenvolvimento	Estudo do ambiente	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Proposta	Descrita em detalhes
		Estudo de viabilidade	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Descrita	Descrita em detalhes
	Processo de Desenvolvimento	Requisitos	Não proposta	Proposta	Descrita em detalhes	Proposta	Descrita em detalhes	Proposta	Descrita em detalhes	Descrita em detalhes
		Projeto	Não proposta	Não proposta	Descrita	Descrita	Descrita em detalhes	Não proposta	Descrita	Descrita em detalhes
		Implementação	Proposta	Proposta	Descrita	Proposta	Descrita em detalhes	Descrita	Descrita	Descrita em detalhes
	Processo de Pós-desenvolvimento	Instalação	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Proposta	Proposta
		Operação	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Descrita	Proposta
		Suporte	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Descrita	Proposta
		Manutenção	Não proposta	Não proposta	Não proposta	Não proposta	Proposta	Não proposta	Proposta	Proposta
		Arquivamento	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Proposta
Processos complementares	Aquisição de conhecimento		Proposta	Proposta	Proposta	Não Proposta	Descrita em detalhes	Não proposta	Descrita	Proposta
	Verificação e validação		Não proposta	Proposta	Proposta	Não Proposta	Descrita em detalhes	Não proposta	Proposta	Proposta
	Gestão de configuração da ontologia		Não proposta	Não proposta	Não proposta	Não proposta	Descrita em detalhes	Não proposta	Proposta	Proposta
	Documentação		Proposta	Proposta	Proposta	Não Proposta	Descrita em detalhes	Não proposta	Descrita	Proposta
	Treinamento		Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Não proposta	Descrita	Proposta

Para facilitar o entendimento das tabelas apresentadas vale destacar que os valores preenchidos nos campos das tabela se referem à identificação da atividade na metodologia avaliada. Quando o campo é preenchido com "Proposta" significa que a atividade foi apenas citada na metodologia como uma atividade essencial, mas nenhuma descrição das tarefas foi indicada pela metodologia. Quando o campo contiver o valor "Descrita", quer dizer que a atividade foi identificada e suas tarefas indicadas na metodologia avaliada, porém ela não guia o projetista em sua execução. Quando "Descrita em detalhes" significa que foram especificados os detalhes sobre a execução das tarefas da atividade identificada na metodologia guiando o projetista na execução da atividade. Para atividades que não foram sequer citadas na metodologia avaliada, o campo correspondente contém o valor "Não proposta".

A partir dos resultados apresentados nas Tabelas 5-1 e 5-2, serão descritas as características avaliadas no *KUP* seguindo os critérios de avaliação:

Segundo a Estratégia de Construção da Ontologia

- *Ciclo de vida proposto:*

Pela sua abordagem iterativa, o KUP suporta mudanças de requisitos durante a execução do projeto, permitindo que as falhas de projeto possam ser descobertas durante o desenvolvimento e as decisões possam ser tomadas sem grandes impactos. Caracteriza-se uma iteração em um ciclo completo de desenvolvimento finalizando com uma versão da ontologia. Esta versão é incrementada a cada nova iteração, caracterizando o ciclo de vida do KUP como iterativo e incremental.

A cada versão da ontologia é possível uma verificação de completude (avaliação). De forma similar a algumas metodologias para o desenvolvimento de ontologias, que utilizam o ciclo de vida evoluindo em protótipos, tais como: METHONTOLOGY e On-To-Knowledge, o KUP permite a geração de artefatos intermediários que resolvam sub-conjuntos de problemas no domínio. Por organizar os resultados de cada atividade em artefatos, o KUP facilita a reutilização dos resultados de cada atividade para a identificação e organização das atividades subseqüentes.

Nesse contexto, o processo permite a integração contínua de novos conceitos e relações à ontologia, atenuando os riscos do projeto relacionados ao acréscimo ou eliminação de requisitos e mudanças táticas durante o andamento do projeto. Por este motivo, esta abordagem iterativa exige um controle superior à abordagem tradicional. Portanto, para manter o desenvolvimento controlado é necessário um bom gerenciamento do projeto.

- *Dependência com relação às aplicações geradas:*

O KUP, similar ao Processo Unificado para Desenvolvimento de Software RUP (*Rational Unified Process*) (Booch, G. *et alli*, 1999), é proposto como uma orientação ao projetista, isto é, deve ser adaptado a cada necessidade, escolhendo-se quais fases são aplicáveis a cada projeto específico. Dependendo das disciplinas, atividades e artefatos instanciados no

projeto, a dependência com relação à aplicação da ontologia pode ou não existir. Um exemplo disso está ao instanciar a disciplina de Análise de Requisitos, onde é realizada a atividade de identificação dos espaços de uso da ontologia. Neste caso, o restante do processo torna-se dependente com relação à aplicação da ontologia. O KUP indica a instanciação desta atividade por facilitar o processo de identificação das tarefas que terão que ser resolvidas com o suporte da ontologia e orienta na identificação do escopo e delimitação do domínio de conhecimento a ser mapeado.

- *Utilização de ontologias base:*

A arquitetura baseada em componentes utilizada pelo RUP e adaptada ao KUP propondo a divisão do domínio de conhecimento em sub-domínios, facilita o reuso de ontologias para a descrição de partes do domínio.

Durante a disciplina de Análise de Requisitos, o artefato gerado contém a captura dos cenários motivacionais (Anexo II). Nesta atividade, são identificadas ontologias existentes para reutilização, descritos os problemas não resolvidos por elas e apresentadas as possíveis soluções. Em seguida, na atividade de Elicitação de Requisitos, é proposta a identificação das fontes de informação, onde uma ontologia existente pode ser identificada, porém não foram descritas estratégias de reutilização e integração desses conceitos.

- *Estratégia para identificação de conceitos:*

Para extração dos conceitos realizada na atividade de Conceitualização da Ontologia, durante a Disciplina de Projeto, o KUP propõe a definição de uma estratégia de identificação de conceitos (*top-down, middle-out* ou *bottom-up*) tendo em vista a disponibilidade das fontes de informação e a clareza dos objetivos da ontologia.

O KUP guia a identificação dos conceitos com base no artefato que descreve as Questões de Competência Informais (Anexos IV e V). Porém, este artefato, gerado na atividade de Elicitação de Requisitos da disciplina de Análise de Requisitos, guia o usuário à estratégia de identificação de conceitos *middle-out*, pois este artefato contém os conceitos mais relevantes e a partir deles obtemos os conceitos mais abstratos e concretos. Conseqüentemente, percebeu-se pouca flexibilização da estratégia para identificação de conceitos quando é instanciada a atividade que gera este artefato.

Segundo o processo de desenvolvimento de ontologia

- *Processos de Gerenciamento do Projeto:*

O *KUP* propõe a disciplina de Gerência de Projeto. Nesta disciplina é descrita a execução de algumas atividades de gerenciamento de maneira iterativa, desempenhadas durante o processo de desenvolvimento da ontologia, tais como: acompanhamento da execução de cada disciplina e atividade pelo seu responsável (verificação e aprovação dos artefatos), gerência do cronograma, entre outras.

Porém, similarmente ao desenvolvimento de software utilizando a abordagem iterativa do *RUP*, os projetos do *KUP* não são fáceis de implementar, planejar e controlar. O gerente terá desafios maiores principalmente nos seus primeiros projetos e nas fases iniciais de desenvolvimento, onde os riscos são mais altos. A partir do momento que adquire experiência, o profissional encontrará mais facilidade no controle de projetos maiores e mais complexos (Kruchten, P., 2000).

- *Processos orientados ao desenvolvimento de ontologias:*

  Processo de Pré-desenvolvimento

  A disciplina de análise de viabilidade do *KUP* descreve atividades para solucionar não só os problemas que afetam o projeto e desenvolvimento da ontologia, mas também do ambiente em que esta será introduzida, isto é, as aplicações que farão uso dela. Portanto são cobertas as atividades de Estudo do Ambiente e Estudo de Viabilidade indicadas no *framework* de avaliação.

  Processo de Desenvolvimento

  A disciplina de Análise de Requisitos do *KUP* mapeia a atividade de Requisitos do *framework* de avaliação. Ao final desta disciplina foi gerado o artefato de Análise de Requisitos (Anexo II) que descreve os requisitos que deverão ser satisfeitos pela ontologia. A tabela da atividade de identificação das questões de competência (Anexo IV) contém as questões de competência identificadas e os conceitos e relacionamentos extraídos a partir destas questões. Este artefato foi alterado do original disponibilizado pelo KUP. No artefato original é proposta a atividade de extratificação das questões de competência, ou seja, a identificação das dependências entre as questões de competência identificadas. Neste estudo de caso, por ser uma tarefa complexa, dada a inexperiência da equipe envolvida no projeto esta atividade foi eliminanda da instanciação e do artefato.

  A disciplina de Projeto do KUP mapeia a atividade de Projeto sugerida pelo *framework* de avaliação. Nesta disciplina é proposta a modelagem conceitual da ontologia. A partir dela os especialistas no domínio, projetistas e os usuários possuem uma forma de entendimento fácil da ontologia facilitando a comunicação entre os membros do projeto e apresentando uma visão concisa do projeto sem que seja necessário analisar sua especificação formal. O modelo conceitual para ontologias proposto em On-To-Knowledge (Sure, Y. & Studer, R., 2002), descreve os relacionamentos taxonômicos e não-taxonômicos entre os conceitos através de uma representação em grafos. Similarmente, na versão da documentação disponível do KUP, é apresentado um exemplo da representação gráfica de uma ontologia baseada em (Daconta, M. *et alli*, 2003), porém a construção deste modelo não é guiada, sendo, por isso, não utilizada neste estudo de caso.

  A Disciplina de Implementação do KUP mapeia a atividade de Implementação proposta no *framework* de avaliação. Nesta disciplina, o KUP guia o projetista apresentando diversas linguagens de implementação e deixa a cargo do projetista escolher a que melhor se adapte ao seu estudo de caso. Isso também acontece com a

escolha do ambiente de engenharia de ontologias. Por ser uma metodologia nova, até o momento não existe um ambiente para desenvolvimento de ontologias que dê suporte às atividades propostas pelo KUP. Porém, por ser um processo unificado, algumas atividades, oriundas de outras metodologias, possuem ferramentas que fornecem este suporte e podem ser também utilizadas quando o KUP é adotado no projeto da ontologia.

Processos de Pós-desenvolvimento

Na disciplina de Processos de Suporte, o *KUP* apenas propõe a execução das atividades avaliadas, tais como: operação, suporte, manutenção e arquivamento da ontologia.

- *Processos complementares:*

O *KUP* propõe as atividades dos processos complementares na disciplina de Processos de Integralização. Nesta disciplina são propostas as atividades de aquisição de conhecimento, verificação e validação, gestão de configuração da ontologia, documentação e treinamento, porém não são descritas as tarefas a serem realizadas. As demais metodologias, exceto KACTUS e SENSUS, descrevem ou apenas propõem a necessidade de algumas atividades dos processos complementares.

6. Conclusões

Como resultado deste estudo, identificou-se que poucas metodologias propostas até o momento relevaram importantes aspectos relacionados ao desenvolvimento de ontologias. O *KUP*, por sua vez, já foi desenvolvido baseado nos resultados obtidos de avaliações realizadas a partir do mesmo *framework* (Fernández-López, M. & Gómez-Pérez, A., 2002) utilizado neste trabalho para sua avaliação. Portanto, neste trabalho, sua avaliação serviu como prova da satisfatibilidade da unificação em relação aos critérios de avaliação. Num contexto geral, o *KUP* atende aos critérios considerados importantes no desenvolvimento de ontologias sugeridos no *framework* de avaliação.

Além disso, por reunir as melhores práticas de desenvolvimento de software adaptadas para o desenvolvimento de ontologias e por ser um processo iterativo, o *KUP* apresentou resultados satisfatórios, caracterizando sobremaneira algumas vantagens dessa abordagem no desenvolvimento de ontologias.

Por outro lado, por ser um processo novo, ainda precisa ser aplicado a outros estudos de caso para que seu desempenho possa ser avaliado por completo. Assim, será possível identificar fragilidades no desenvolvimento de ontologias em outros domínios de aplicação, para então ser refinado e adquirir maturidade e aceitação na comunidade de engenharia de ontologias.

Neste contexto, algumas sugestões são indicadas ao *KUP* para que ele seja refinado e não só satisfaça as características essenciais avaliadas pelo *framework* proposto por Fernández-López e Gómez-Pérez (2002), como também ofereça suporte a algumas necessidades da área de engenharia de ontologias:

- **Guiar a instanciação do *KUP*:** para uma instanciação do *framework* de processos adequada, poderiam ser indicadas as atividades essenciais e opcionais de acordo com a demanda do projeto. Como por exemplo, a atividade de identificação dos cenários de uso, que é uma atividade essencial para o desenvolvimento de uma ontologia de aplicação, auxiliando na identificação das tarefas da ontologia. A ausência desta atividade no projeto pode acarretar a geração de ontologias que podem não descrever satisfatoriamente o domínio de tarefas. Além disso, sugere-se que a disciplina de Instanciação do KUP seja inicializada após um primeiro contato com a disciplina de Análise de Viabilidade. Desta forma, torna-se uma tarefa mais intuitiva ao gerente do projeto, pois poderá instanciar o processo de maneira coerente com os recursos disponíveis.

- **Descrição de técnicas de gerenciamento de projeto:** pela sua abordagem iterativa, os projetos do *KUP* não são fáceis de implementar, planejar e controlar (Kruchten, P., 2000). Em virtude da engenharia de ontologias ser uma área em expansão, os desafios do desenvolvimento iterativo devem ser melhor controlados e gerenciados. Neste contexto, sugere-se que os detalhes das atividades de gerenciamento do KUP sejam refinados, evitando assim, que os riscos da abordagem iterativa de desenvolvimento de software reflitam no desenvolvimento de ontologias.

- **Estratégia de identificação de conceitos:** as atividades de identificação de conceitos propostas pelo *KUP* parecem suficientes para instâncias pequenas, tal qual como realizado neste estudo de caso. Porém, no desenvolvimento de projetos de grande porte, esta abordagem poderá tornar-se ineficiente. Um exemplo de desenvolvimento de ontologia de grande porte é mostrado em Gandon (2002), onde através de um estudo de caso, sugere a utilização de ferramentas de processamento de linguagem natural nas fontes de informação disponíveis. Assim, a atividade de identificação dos conceitos é facilitada para a utilização da engenharia de ontologias em grande escala, onde existem muitos conceitos a serem identificados.

- **Estratégia de identificação da hierarquia:** neste estudo de caso, a hierarquia foi obtida através do entendimento do domínio. Para isso, foi construído um glossário da ontologia, contendo os conceitos extraídos através das demais atividades do *KUP*. A partir deste glossário foi identificada a hierarquia dos conceitos através de suas definições. Porém, esta estratégia precisa ser detalhada para garantir que projetistas inexperientes possam gerar a taxonomia dos conceitos da ontologia que expresse adequadamente a realidade a ser mapeada.

- **Fornecer suporte à evolução e extensão da ontologia:** em conseqüência ao dinamismo das informações disponíveis na Web e seu crescimento acelerado, as ontologias também devem ser adaptáveis às evoluções. Diversos fatores impulsionam a manutenção e evolução de ontologias, tais como: erros em versões anteriores, nova modelagem do domínio, novas terminologias criadas, entre outros (Heflin, J. *et alli*, 2003). Além disso, a expectativa de construção de uma biblioteca de ontologias formando uma base para o desenvolvimento de ontologias complementa a idéia da

reutilização de ontologias possibilitando o compartilhamento do conhecimento entre sistemas e agentes de software. Até o momento, existem muitas dúvidas sobre como selecionar uma ontologia satisfatória para reuso e como extender uma ontologia existente (Jones, D. *et alli*, 1998). Um projetista pode encontrar uma ontologia para reutilização que disponibilize até 90% da expressividade necessária para o seu projeto, porém os 10% não descritos podem ser críticos. Neste caso, o projeto da ontologia deve reutilizar a ontologia encontrada e estendê-la, acrescentando somente os conceitos não mapeados do domínio. Os fundamentos que impulsionaram a extensão de ontologias foram introduzidos pelo Método SENSUS (Swartout, B., 1997), porém já existem propostas para extensão automática de ontologias de domínio (Alfonseca, E. & Manandhar, S., 2002). A re-engenharia de ontologias é outra abordagem indicada quando existe a necessidade de reutilização de ontologias, seu objetivo é recuperar e transformar um modelo conceitual de uma ontologia implementada em um novo modelo conceitual (Gómez-Pérez, A. & Benjamins, V.R., 1999). É importante ficar nítida a diferença entre evolução de ontologias e extensão de ontologias, nesta última não ocorrem mudanças na ontologia original, apenas um acréscimo de conceitualização. Por sua vez, o KUP, para ser considerado um processo abrangente, deve considerar o suporte a estas características, necessitando uma atenção especial pois tratam-se de características essenciais ao projeto de ontologias.

- **Documentação do KUP:** além de uma metodologia propor práticas e atividades para o desenvolvimento de um projeto, ela deve ser clara e oferecer instruções que viabilizem a sua utilização. Como o KUP é um processo novo, ainda apresenta alguma carência nas instruções para sua utilização (manuais, guias, etc) tanto para a condução do projeto, quanto na execução das atividades e preenchimento dos formulários dos artefatos. Sugere-se a criação de manuais a partir da experiência obtida na aplicação do KUP em projetos reais, como por exemplo, deste estudo de caso.

- **Integração do KUP com o processo de desenvolvimento de aplicações para Web Semântica:** O KUP, dá suporte ao desenvolvimento de ontologias para aplicações na Web Semântica. Estas aplicações devem ser desenvolvidas seguindo um processo de desenvolvimento de software de preferência da equipe. Neste contexto é interessante estudar a viabilidade da integração desses processos. Esta integração sugere a reutilização de artefatos, especificações e outros resultados, evitando a replicação de trabalho e documentação.

7. Trabalhos Futuros

- Dando continuidade a este estudo de caso, sugere-se o refinamento da ontologia desenvolvida através da implementação das demais iterações das etapas do *KUP*. Sugere-se ainda sua integração a uma ontologia de domínio para gestão de conhecimento em segurança da informação e a implantação da ontologia de aplicação resultante desta união no sistema e-BTS. Assim, viabilizará a avaliação do *KUP* no desenvolvimento de outros tipos de ontologias e nas demais iterações do processo. Além disso, para implantação da ontologia gerada, será necessária a adaptação do e-

BTS para dar suporte à semântica disponibilizada por ela, transformando-o em uma aplicação para Web Semântica baseado em uma ontologia. Para o desenvolvimento da ontologia de domínio proposta, algumas fontes de informação devem ser analisadas para extração de conceitos, tais como: taxonomias, thesaurus, metadados e outras ontologias existentes. Alguns exemplos destas fontes de informação podem ser encontrados no Anexo VIII deste documento.

- Devido a experiência adquirida a partir deste estudo de caso, comprovou-se, na prática, que a engenharia de ontologias não é uma tarefa trivial. Considerando que a maioria dos projetistas não possui experiência suficiente nesta área, sugere-se o desenvolvimento de um ambiente de engenharia de ontologias que ofereça suporte as disciplinas e atividades propostas pelo *KUP*, considerando também outras atividades relevantes identificadas como resultado deste trabalho, tais como: versionamento, migração, integração e reutilização de ontologias. Além disso, sugere-se o estudo da integração do *KUP* com metodologias de desenvolvimento de Sistemas Multi-Agentes para desenvolvimento de aplicações para Web Semântica utilizando agentes. Neste contexto, dada a interação de agentes com as ontologias, tanto as ontologias quanto os agentes poderão ser desenvolvidos de forma integrada.

Referências Bibliográficas

ALFONSECA, E. & MANANDHAR, S.: **An Unsupervised Method for General Named Entity Recognition And Automated Concept Discovery.** Proceedings of the First International Conference on General WordNet, 2002.

ALFONSECA, E. & MANANDHAR, S.: **Proposal for Evaluating Ontology Refinement Methods.** Language Resources and Evaluation (LREC), 2002.

BERNARAS, A.; LARESGOITI, I. & CORERA, J.: **Building and Reusing Ontologies for Electrical Network Applications.** Proceedings of the 12th European Conference on Artificial Intelligence (ECAI'96), 1996. 298-302.

BERNERS-LEE, T.; HENDLER, J. & LASSILA, O.: **The Semantic Web**, Scientific American, May 2001.

BERNERS-LEE, T.: **Information Management: A Proposal**, CERN, March 1989, May 1990.

BERNERS-LEE, T.: **The World Wide Web – Past, Present and Future**, http://www.w3.org/2002/04/Japan/Lecture.html, ultimo acesso em 19/05/2003.

BERNERS-LEE, T.: **Semantic Web Road Map**, http://www.w3.org/DesignIssues/Semantic.html, ultimo acesso em 19/05/2003.

BLÁZQUEZ, M.; FERNÁNDEZ-LÓPEZ, M.; GARCIA-PINAR, J.M.; GÓMEZ-PÉREZ, A.: **Building Ontologies at the Knowledge Level using the Ontology Design Environment**. Knowledge Acquisition of Knowledge-Based Systems Workshop (KAW), 1998.

BOOCH, G.; JACOBSON, I. & RUMBAUGH, J.: **The Unified Software Development Process**. Addison-Wesley, 1999.

BREITMAN, K. & LEITE, J.C.: **Lexicon Based Ontology Construction** 2nd. International Workshop on Software Engineering for Large Scale Multi Agent Systems - SELMAS - ACM computer Press, Portland Oregon, 2003.

COVER, R.: **XML and Semantic Transparency**. Technology Reports, 1998. Cover Pages, http://www.oasis-open.org/cover/xmlAndSemantics.html, último acesso em 11/09/2003.

DACONTA, M.; OBRST, L. & SMITH, K.: **The Semantic Web – A Guide to the Future of XML, Web Services and Knowledge Management**.. Wiley Publishing Inc, Indiana. 2003.

DEVEDEZIC, V.: **Understanding Ontological Engineering.** Comm. of ACM, April-2002, vol. 45, n. 4, 136-144.

DING, Y.: **Ontology: The enabler for the Semantic Web.** A review of ontologies with the Semantic Web in view. Journal of Information Science, 2001. 27(6) 377-384(8).

FERNÁNDEZ LÓPEZ, M.: **Overview of Methodologies for Building Ontologies**, Proceedings of IJCAI-99, Workshop on Ontologies and Problem-Solving Methods (KRR5), Stockholm, Sweden, 1999.

FERNÁNDEZ-LÓPEZ, M. & GÓMEZ-PÉREZ, A.: **Overview and Analysis of methodologies for building ontologies** Knowledge Engineering Review (KER). Vol. 17[2]. 2002. Pags: 129-156.

FERNÁNDEZ-LÓPEZ, M.; GOMEZ-PÉREZ, A.; JURISTO, N.: **METHONTOLOGY: From Ontological Art Towards Ontological Engineering** Workshop on Ontological Engineering. Spring Symposium Series. AAAI97 Stanford, USA, 1997.

GANDON, F.: **Ontology Engineering: A Survey and a Return on Experience.** Institut de Recherche en Informatique et Automatique – INRIA. Nº 4396, 2002.

GÓMEZ-PÉREZ, A.: **Ontological Engineering: A State of the Art**.. Expert Update, British Computer Society, Autumn, vol. 2, n. 3, 33-43, 1999.

GÓMEZ-PÉREZ, A.; JURISTO, N. & PAZOS, J.: **Evaluation and assessment of knowledge sharing technology.** In N. J. Mars (editor), Towards Very Large Knowledge Bases. KBKS 95. IOS Press, Amsterdam, 1995. pp., 289-296.

GÓMEZ-PÉREZ, A. & BENJAMINS, V.R.: **Overview of Knowledge Sharing and Reuse Components: Ontologies and Problem-Solving Methods.** Proceedings of the IJCAI-99 workshop on Ontologies and Problem-Solving Methods (KRR5). Stockholm, Sweden, August 2, 1999.

GRÜNINGER, M. & FOX, M.S.: **Methodology for the design and evaluation of ontologies.** Workshop on Basic Ontological Issues in Knowledge Sharing. Montreal, Canada, 1995.

GUARINO, N.: **Formal Ontology and Information System.** Proceedings of FOIS'98, Trento, Italy, 6-8 June 1998. Amsterdam, IOS Press, pp. 3-15.

HEFLIN, J.; VOLZ, R. & DALE, J.: **Requirements for a Web Ontology Language**, 2003. Editor's Working Draft of the Ontology Web Language (OWL) 1.0 Specification. http://lists.w3.org/Archives/Public/www-webont-wg/2003Jan/att-0055/01-webont-req.html, ultimo acesso em 28/06/2003.

IEEE COMPUTER SOCIETY: **Standard Glossary of Software Engineering Terminology**. Std. 610.12-1990. New York., 1990.

IEEE COMPUTER SOCIETY: **Guide for Software Quality Assurance Planning**. Std. 730.1-1995. New York, 1995.

JONES, D.; BENCH-CAPON, T. & VISSER, P.: **Methodologies for Ontology Development**. Proceedings IT&KNOWS Conference of the 15th IFIP World Computer Congress, Budapest, Chapman-Hall, 1998.

KRUCHTEN, P.: **From Waterfall to Iterative Lifecycle – A tough transition for project managers.** Rational Software White Paper - TP1735/00, 2000.

LENAT, D.B.: **CYC: A Large-Scale Investment in Knowledge Infrastructure.** Comm. of ACM, November-1995, vol. 38, n. 11, 33-38.

LENAT, D.B. & GUHA, R.V.: **Building Large Knowledge-based Systems**. Addison-Wesley Publishing Company, Inc., 1990.

MIZOGUCHI, R. & IKEDA, M.: **Towards Ontology Engineering**. Technical Report AI-TR-96-1, I.S.I.R., Osaka University, 1996.

NOY, N. & MCGUINESS, D.L.: **Ontology Development 101: A Guide to Create Your First Ontology**, 2000.
http://protege.stanford.edu/publications/ontology_development/ontology101...html, ultimo acesso em 19/05/2003.

ONTOWEB GROUP, 2002. **Deliverable 1.4: A survey on methodologies for developing, maintaining, evaluating and reengineering ontologies**,
http://www.ontoweb.org/download/deliverables/D1.4-v1.0.pdf, último acesso em 19/05/2003.

ONTOWEB GROUP, 2003. **Deliverable 1.5: A Survey of Ontology Learning Methods and Techniques.** http://ontoweb.aifb.uni-karlsruhe.de/Members/ruben/Deliverable%201.5, último acesso em 29/06/2003.

ORLEAN, D. & LUCENA, C.: **Um Processo Unificado para Engenharia de Ontologias**. Rio de Janeiro, 2003. Dissertação de Mestrado – Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

ORLEAN, D.; MAGALHÃES, J. & PINTO, L.: **Módulo Security Solutions: Manual de Utilização do Sistema E-BTS**, 2003

PEASE, A.: **Why Use DAML?** Teknowledge, 2002,
http://www.daml.org/2002/04/why.html, ultimo acesso em 11/09/2003.

RATIONAL TEAM: **Rational Unified Process: Best Practices for Software development Teams.** Rational Software White Paper. TP026B, Rev 11/01, 1998.

RIBIÈRE, M. & CHARLTON, P.: **Ontology Overview**. Networking and Applications Lab. Centre de Recherche de Motorola. Espace Technologique. Commune de Saint Aubin, Paris, 2001.

SCHWABE, D. & ROSSI, G.: **An Object Oriented Approach to Web-Based Application Design.** Theory and Practice of Object Systems 4(4), 1998. Wiley and Sons, New York, ISSN 1074-3224).

SMITH, H. & POULTER, K.: **The Role of Shared Ontology in XML-Based Trading Architectures.** Ontology.org. Included within Communications of the ACM, special issue on Agent Software, 1999, http://www.ontology.org/main/papers/cacm-agents99.html, ultimo acesso em 11/09/2003.

SURE, Y. & STUDER, R: **On-To-Knowledge Methodology – Final Version.** On-To-Knowledge EU IST-1999-10132 Project Deliverable D18 (WP5). Institute AIFB, University of Karlsruhe, 2002.

SWARTOUT, B.; RAMESH, P.; KNIGHT, K.; RUSS, T.: **Toward Distributed Use of Large-Scale Ontologies**. In Proceedings of the Tenth Knowledge Acquisition for Knowledge-based Systems Workshop, November 9-14, 1996. Banff, Alberta, Canada.

USCHOLD, M. & GRÜNINGER, M.: **Ontologies: Principles Methods and Applications**. Knowledge Sharing and Review. Vol. 11 Number 2. 1996.

USCHOLD, M. & KING, M.: **Towards a Methodology for Building Ontologies**. Workshop on Basic ontological Issues in Knowledge Sharing, 1995.

Anexo I

Análise de Viabilidade

Projeto: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação	
Data: 23/06/2003	**Resp. pelo documento:** Daniela Brauner
Versão: 0.2	**Status:**

Oportunidades:

Quais são as oportunidades que demandam o projeto e desenvolvimento desta ontologia ou das aplicações que farão uso dela?

Com o crescente número de ataques maliciosos aos ambientes corporativos, está cada vez mais difícil manter-se atualizado com os riscos emergentes que podem comprometer os diversos sistemas e aplicações destas organizações.

Manter-se atualizado com as informações de segurança da informação é o segredo para implementar ações preventivas e/ou corretivas para manter os serviços das empresas e proteger os ativos corporativos disponíveis.

Através da disponibilização de boletins técnicos de segurança abrangentes e personalizados, o e-BTS – Boletim Técnico de Segurança Eletrônico, fornecerá aos seus clientes informações atualizadas indicando medidas de prevenção e/ou correção às ameaças que colocam em risco os softwares (componentes) que possuem.

Problemas:

Quais são os problemas que afetam o projeto e desenvolvimento da ontologia ou das aplicações que farão uso dela? Como esses problemas podem ser minimizados?

Atualmente, são diversas as fontes de informação das quais podem ser coletadas informações atualizadas sobre ataques a sistemas. Estas fontes distribuídas, disponibilizam informações sem padronização. Portanto, ao coletar tais informações, o e-BTS deve ser capaz de classificá-las de acordo com seu conteúdo.

Soluções potenciais:

Quais são as potenciais soluções para os problemas enfrentados?

O e-BTS disponibilizará os boletins técnicos contendo alertas sobre ameaças que afetam os sistemas dos usuários que adquirirem o seu serviço. Este sistema implementará um serviço de informações, que busca e recupera documentos distribuídos na rede, contendo informações sobre ameaças a sistemas. Devido ao fato do domínio ser de grande abrangência, a diversidade de padrões e termos utilizados nas informações disponibilizadas na rede dificultam a integração destas informações distribuídas. Além disso, para a geração dos boletins técnicos, dada a falta de padronização dessas informações, a utilização de uma ontologia resolveria este problema, definindo um vocabulário comum para o domínio em questão e permitindo o relacionamento entre elementos de informação.

A solução encontrada para os problemas e oportunidades levantados é a construção de uma ontologia para Gestão de Conhecimento em Segurança da Informação. Esta ontologia definirá um vocabulário comum para disponibilização de informações padronizadas para extração de informações de fontes distribuídas e para facilitar o relacionamento entre diferentes conceitos, possibilitando a interoperabilidade entre os módulos do sistema, bem como a personalização dos boletins técnicos do e-BTS.

Patrocinadores e Interessados:

Pessoas:

Equipe de desenvolvimento do e-BTS.

Empresas e Organizações:

Laboratório de Engenharia de Software – LES/PUC-RIO.
Módulo Security Solutions – empresa patrocinadora do Projeto e-BTS.

Contexto:

Qual a disponibilidade de recursos econômicos, técnicos e de projeto para sua execução?

Recursos Econômicos:

Os recursos econômicos envolvidos são disponibilizados pelas empresas e organizações que desenvolvem o Projeto do e-BTS.

Recursos Técnicos:

- *Está disponível um protótipo do e-BTS sem a utilização de ontologias.*
- *São disponibilizadas diversas fontes de informação para consulta do domínio, tais como: diagramas de use case, diagramas E-R, documentos, web sites e relatórios identificados em detalhes no artefato de Análise de Requisitos.*
- *Existem especialistas no domínio à disposição para entrevistas, tais como: consultores da Módulo Security e os integrantes da equipe do Projeto e-BTS.*
- *Existem ferramentas disponíveis para edição de ontologias.*
- *Não foram encontradas ontologias para reutilização de conceitos no domínio de Segurança da Informação.*

Recursos de Projeto:

- *Uma sub-equipe da equipe do Projeto e-BTS, composta por duas pessoas, foi alocada para o desenvolvimento do projeto e implementação da ontologia.*
- *Existe a disponibilidade de tempo para viabilizar o desenvolvimento da ontologia.*

Decisões:

Quais as decisões tomadas após a Análise de Viabilidade?

Realizada a Análise de Viabilidade foi constatado que é viável a implementação deste projeto para desenvolvimento da ontologia para o e-BTS, dados os diversos fatores levantados neste artefato.

Anexo II

Análise de Requisitos

Identificação de Propósito e Escopo da Ontologia

Projeto: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação	
Data: 25/06/2003	**Resp. peb documento:** Daniela Brauner
Versão: 0.2	**Status:**

Propósito e Escopo da Ontologia

Por que a ontologia será construída e quais seus usos pretendidos?

Por que a ontologia será construída?

(descrever os propósitos para a construção da ontologia)

A ontologia será construída para dar suporte às tarefas do sistema e-BTS (Boletim Técnico de Segurança Eletrônico), conceitualizando as informações necessárias para a execução das tarefas do e-BTS.

Quais seus usos pretendidos?

A ontologia será utilizada para definir e padronizar os conceitos envolvidos nas tarefas desempenhadas pelo e-BTS, descrevendo as tarefas do sistema e permitindo a interoperabilidade entre seus módulos. Algumas tarefas do sistema são: a padronização dos conceitos extraídos das fontes externas de informação, a tradução automática ou semi-automática dos termos das ameaças recebidas e a personalização dos relatórios.

Descrição dos usos pretendidos da ontologia

Identificação dos Espaços de uso:

(marcar, na lista abaixo, quais os espaços de uso que identificam os propósitos da ontologia)

Comunicação	
Modelos Normativos	☐
Relacionamento entre Itens de Informação	☒
Consistência e criação de definições não-ambíguas	☒
Integração de diferentes perspectivas organizacionais	☒
Interoperabilidade	
Uso de ontologias como uma "inter-língua" para facilitar traduções entre diferentes padrões e modelos	☒

Dimensões da Interoperabilidade	
Interna	☒
Externa	☐
Integração de ontologias de diferentes domínios	☐
Integração de Ontologias entre diferentes ferramentas	☒
Engenharia de Sistemas	
Especificação de sistemas de software	☒
Confiabilidade (checagem automática ou semi-automática de consistência)	☒
Reusabilidade	☒

Potenciais usuários:

Quais são os potenciais usuários – agentes, aplicações, pessoas, etc..?

A princípio, os usuários desta ontologia serão: os agentes de software do e-BTS responsáveis pela importação dos termos extraídos de fontes externas distribuídas na rede; e os agentes de software do e-BTS responsáveis pela personalização dos boletins técnicos, os clientes do sistema responsáveis pela configuração do sistema, seleção de sistemas de software (ativos), sistema de tradução com o tradutor e sistema de edição com o editor.

Benefícios

Quais os benefícios que a ontologia trará para a execução das tarefas dos potenciais usuários e para as aplicações desenvolvidas?

Facilitará o reconhecimento dos termos do domínio para padronizar semanticamente os conceitos utilizados nos alertas disponibilizados pelas fontes externas. Além disso, relacionará as informações dos clientes com as ameaças disponíveis possibilitando a inferência para personalização dos relatórios de segurança enviados pelo sistema e-BTS aos seus clientes.

Aplicações:

Que aplicações (ou tipos de aplicações) deverão (ou poderão) fazer uso dessa ontologia?

Módulos do e-BTS que farão uso da ontologia:
– Wrapper (importador de informação sobre alertas de segurança)
– Sistema de suporte (tradução e edição)
– Sistema de geração de relatórios personalizados
– Base de conhecimento de ameaças

Captura dos Cenários Motivacionais

Projeto: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação	
Data: 25/06/2003	**Resp. pelo documento:** Daniela Brauner
Versão: 0.2	**Status:**

Cenários Motivacionais

Ontologias Disponíveis:

(ontologias que mapeiam, total ou parcialmente, o domínio em questão)

Por ser uma ontologia de tarefas do e-BTS, isto é, descreve as tarefas específicas da aplicação, não foram encontradas ontologias que descrevam o domínio em questão ou parte dele.

Motivação:

Por que as ontologias atuais não resolvem os problemas descritos na fase de Estudos Preliminares?

Como não foram encontradas ontologias neste domínio de aplicação, para sua descrição contamos apenas com vocabulários, taxonomias e definições em XML.

Cenários Motivacionais:

Cenários motivacionais são narrativas de problemas não resolvidos por ontologias existentes, apresentando possíveis soluções. Descrição dos cenários de uso que permitam resolver estes problemas.

O e-BTS recebe os alertas de ameaças de fontes externas e distribuídas na rede. Para armazenar essas informações, que serão posteriormente processadas pelo sistema, é realizada a importação e classificação desses dados para a base de conhecimento do sistema. Para esta tarefa deve ser identificado o tipo de ameaça, bem como os componentes vulneráveis a ela, o impacto causado, a estratégia de suavização indicada, a severidade e credibilidade do alerta, entre outras informações. Além disso, no módulo de tradução e edição do sistema torna-se necessária a identificação dos conceitos para permitir a tradução automática dos termos padrões, facilitando o trabalho do tradutor e armazenando na base de conhecimento as alterações feitas pelo editor. Para isso torna-se necessária a definição de um vocabulário comum no domínio de segurança da informação, definindo conceitos e relacionamentos entre esses conceitos. No módulo de geração dos relatórios personalizados é necessária a identificação dos clientes relacionados às ameaças, através da verificação dos componentes relacionados à ameaça e os componentes definidos nos ativos dos clientes.

Decisões:

Que decisões foram tomadas após a execução desta atividade?

Em virtude de não existirem ontologias que possam ser reutilizadas foi identificada a necessidade de construção de uma ontologia para Gestão de Conhecimento em Segurança da Informação.

Elicitação de Requisitos

Projeto: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação	
Data: 25/06/2003	**Resp. pelo documento:** Daniela Brauner
Versão: 0.2	**Status:**

Elicitação de Requisitos

Fontes de Informação

Identificação das possíveis fontes de informação e as estratégias de análise

Fonte	
Especialistas no Domínio	Estratégia de Análise
- Equipe de desenvolvimento do e-BTS *- Consultores da Módulo Security*	(como as informações serão extraídas dos especialistas?) *- Entrevistas*
Ontologias Existentes	
Não encontradas	
Dicionários	
Dicionário de dados do e-BTS *Glossário da Módulo Security*	
Thesauri	
National Criminal Justice Reference Service *http://abstractsdb.ncjrs.org/content/Thesaurus/Thesaurus_Search.asp*	
Fontes Internas	
Bancos de dados	
Listas de índices	
Legislações	
Templates	
Template dos boletins enviados pelo e-BTS.	
Descrições de produtos, projetos, pessoas.	
Descrição do Symantec Deep Sight Alert Services	

White-papers
Páginas Web
Página da Módulo Security *http://www.modulo.com.br*
Relatórios
Relatórios sobre vulnerabilidade do Symantec Deep Sight Alert *Relatórios sobre código malicioso do Symantec Deep Sight Alert*
Gráficos e diagramas
Use cases da aplicação e-BTS atual *Modelo E-R da aplicação e-BTS atual*
Documentos em geral
Outros
Aplicação do e-BTS atual (sem fundamentos de Web Semântica)
Especificações
Padrões

Elicitação de Atores
(pessoas, agentes de software, software e serviços que farão uso da ontologia)

- *Usuários do e-BTS (editor, tradutor, cliente)*
- *Wrapper do e-BTS*
- *Sistema de Suporte*
- *Sistema de Relatório*

Cenários e Casos de Uso
Descrição das formas de utilização da ontologia pelos atores

Técnica
Qual a técnica escolhida para descrição dos casos de uso da ontologia?

Casos de Uso (RUP)	☒
Cenários (Leite)	☐
Cenários, Casos de Uso e UIDs (OOHDM)	☐

Anexos:
Documentos anexos (artefatos e resultados)

Casos de Uso	Anexo III
Questões de Competência	Anexo IV
Composição das Questões de Competência (Tarefas)	Anexo IV
Outros	
Glossário da terminologia	Anexo V
Modelo conceitual	Anexo VI
Formalização da ontologia	Anexo VII

Anexo III

Exemplos de Casos de Uso para Ontologias

Importação de informações das fontes externas

Atores: *Serviço de alerta, Wrapper, Tradutor.*
Finalidade: Receber a ameaça para ser processado.
Pré-condições: Deve existir um *Tradutor* cadastrado no sistema.
Visão geral: O *Wrapper* recebe um alerta enviado por um *Serviço de alerta*. O *Wrapper* identifica o tipo de ameaça contido neste alerta e solicita à ontologia os elementos que a compõem. O *Wrapper* extrai os elementos que compõem a ameaça de seu conteúdo e armazena essas informações na base de conhecimento. O *Sistema de Suporte* cadastra uma pendência para o *Tradutor.*

Seqüência típica de eventos:

Ação do ator	Resposta do sistema	Consulta a Ontologia	Manipulação da Base de Conhecimento
1.Este caso de uso se inicia, quando um alerta é enviada pelo *Serviço de alerta* (fonte de informação externa).			
	2. O *Wrapper* recebe a ameaça, identifica seu tipo e obtém os elementos que a compõem na ontologia, para então extraí-los do conteúdo da ameaça.		
		3. A ontologia informa ao *Wrapper* os elementos que compõem o tipo de ameaça.	
.	4. O *Wrapper* extrai os elementos que compõem a ameaça de seu conteúdo e armazena essas informações na base de conhecimento		
			5.Uma nova instância do tipo de ameaça recebida é criada na base de conhecimento. Os elementos de informação extraídos são relacionados a essa instância.
	6. O *Sistema de Suporte* cadastra uma pendência para o *Tradutor* da ameaça recebida.		

Tradução das ameaças

Atores: *Sistema de Suporte, Tradutor, Editor.*

Finalidade: Traduzir as ameaças pendentes na lista de pendências do *Tradutor*.

Pré-condições: O *Tradutor* deve estar autenticado pelo sistema e possuir ameaças pendentes na sua lista de pendências. Deve existir um *Editor* cadastrado no sistema.

Visão geral: O *Tradutor* seleciona uma ameaça de sua lista de pendências. A base de conhecimento fornece os elementos de informação a serem traduzidos pelo *Sistema de Suporte* e o *Tradutor*. Os termos padrões do alerta são identificados na ontologia e traduzidos automaticamente. Os termos sem tradução são consultados na base de conhecimento e passados ao *Tradutor.* O *Tradutor* faz a tradução do conteúdo destes elementos de informação e atualiza-os na base de conhecimento. O *Sistema de Suporte* elimina a ameaça da lista de pendências do *Tradutor*. O *Sistema de Suporte* cadastra a ameaça na lista de pendências do *Editor.*

Seqüência típica de eventos:

Ação do ator	Resposta do sistema	Consulta a Ontologia	Manipulação da Base de Conhecimento
1.Este caso de uso se inicia, quando um *Tradutor* verifica sua lista de pendências. O *Tradutor* solicita a ameaça pendente à base de conhecimento.			
			2. A base de conhecimento fornece a ameaça solicitada ao *Tradutor*.
	3. O *Sistema de Suporte* identifica os termos padrões da ameaça para solicitar a tradução automática à ontologia.		
		4. A ontologia informa ao *Sistema de Suporte* os termos padrões da ameaça.	
	5. O *Sistema de Suporte* pesquisa na base de conhecimento os termos padrões da ameaça.		
			6. A base de conhecimento informa ao *Sistema de Suporte* as respectivas traduções dos termos padrões da ameaça.
	7. O *Sistema de Suporte* identifica os termos que ficaram sem tradução. O *Sistema de Suporte* envia os termos para o *Tradutor* realizar a tradução destes.		

Ação do ator	Resposta do sistema	Consulta a Ontologia	Manipulação da Base de Conhecimento
8.O *Tradutor* traduz os termos sem tradução automática. O *Tradutor* atualiza os elementos de informação traduzidos da ameaça na base de conhecimento.			
			9. A instância da ameaça é atualizada na base de conhecimento com os elementos de informação traduzidos.
	10. O *Sistema de Suporte* retira a pendência do *Tradutor*. O *Sistema de Suporte* cadastra uma pendência para o *Editor*.		

Fluxos alternativos:

8.1 O *Tradutor* cancela a operação. Encerra-se o use-case.

Anexo IV

Identificação de Tarefas

Projeto: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação	
Data: 23/06/2003	**Resp. pelo documento:** Daniela Brauner
Versão: 0.2	**Status:**

Lista de Tarefas		
Id.	**Tarefa**	**Questões de Competência Relacionadas**
01	Importação de informações das fontes externas	Qual o tipo da ameaça de um alerta? Quais os componentes ameaçados por uma ameaça? Quais os ativos afetados por uma ameaça? Quais os impactos causados por uma ameaça? Quais os fabricantes dos componentes ameaçados por uma ameaça? Quais as categorias dos componentes ameaçados por uma ameaça? Quais as versões dos componentes ameaçados por uma ameaça? ...entre outras.
02	Tradução e edição das ameaças	Quais os componentes ameaçados por uma ameaça? Quais os impactos causados por uma ameaça? Quais os fabricantes dos componentes ameaçados por uma ameaça? Quais as categorias dos componentes ameaçados por uma ameaça? Quais as versões dos componentes ameaçados por uma ameaça? Quais as estratégias de suavização indicadas para uma ameaça? ...entre outras.
03	Geração de relatórios personalizados (boletins técnicos)	Dada uma (nova) ameaça: Qual seu tipo? Quais os componentes ameaçados por ela? Qual o impacto causado por ela? Qual sua severidade? Dado um boletim (que monitora os ativos ameaçados): Qual cliente o configurou? Para quais destinatários ele é enviado? Qual a taxa de impacto mínima selecionada pelo cliente? Qual a taxa de credibilidade mínima selecionada pelo cliente? Qual a taxa de urgência mínima selecionada pelo cliente? Quais componentes ele monitora? Quais ativos ele monitora? Dado um ativo (ameaçado por uma nova ameaça): Quais os componentes a compõem? Quais boletins que o monitoram? Qual cliente o configurou? Para quais clientes deve ser enviado o boletim técnico contendo a ameaça? Quais os tipos de boletins técnicos gerados? ...entre outras.

Formulação da Questões de Competência

Projeto: Uma Ontologia para Suporte às Tarefas de Gestão de Conhecimento em Segurança da Informação	
Data: 23/06/2003	**Resp. pelo documento:** Daniela Brauner
Versão: 0.2	**Status:**

Questões de Competência			
Id	**Questão de Competência**	**Conceitos**	**Relação**
01	- Quais os destinatários cadastrados de um cliente?	Cliente Destinatário	possui pertenceA
02	- Quais os boletins configurados pelo cliente?	Cliente Boletim	cadastra cadastradoPor
03	- Quais os ativos cadastrados pelo cliente?	Cliente Ativo	possui pertenceA cadastra cadastradoPor
04	- Quais os destinatários configurados em um boletim?	Boletim Destinatário	enviadoPara recebe
05	- Quais os ativos monitorados por um boletim?	Boletim Ativo	monitora monitoradoPor
06	- Quais os componentes compõem um ativo?	Ativo Componente	compostoPor compoe
07	- Qual o fabricante de um componente?	Componente Fabricante	fabricadoPor fabrica
08	- Qual a categoria de um componente?	Componente Categoria	temCategoria
09	- Qual a versão de um componente?	Componente Versão	temVersao
10	- Quais são as categorias de componentes fabricadas por um fabricante?	Fabricante Componente Categoria	fabrica fabricadoPor

Id	Questão de Competência	Conceitos	Relação
11	- Quais são os fabricantes de componentes de uma categoria?	Categoria Componente Fabricante	fabricadoPor fabrica
12	- Quais os (as versões de) componentes monitorados por um boletim?	Boletim Componente	monitora monitoradoPor
13	- Quais as categorias possuem componentes monitorados por um boletim?	Boletim Componente Categoria	monitora monitoradoPor
14	- Quais os fabricantes possuem componentes monitorados por um boletim?	Boletim Componente Fabricante	monitora monitoradoPor
15	- Quais componentes possui um cliente?	Cliente Componente	possui pertenceA
16	- Quais as categorias de componentes de um cliente?	Cliente Componente Categoria	possui pertenceA
17	- Quais os fabricantes dos componentes de um cliente?	Cliente Componente Fabricante	possui pertenceA
18	- Quais as versões de componentes de um cliente?	Cliente Componente Versão	possui pertenceA
19	- Quais os componentes afetados por uma ameaça?	Ameaça Componente	Afeta afetadoPor
20	- Quais as versões de componentes afetadas por uma ameaça?	Ameaça Componente Versão	afeta afetadoPor
21	- Quais os fabricantes de componentes afetados por uma ameaça?	Ameaça Componente Fabricante	afeta afetadoPor
22	- Quais as categorias de componentes afetadas por uma ameaça?	Ameaça Componente Categoria	afeta afetadoPor

Id	Questão de Competência	Conceitos	Relação
23	- Quais os ativos afetados por uma ameaça?	Ameaça Ativo	afeta afetadoPor
24	- Quais boletins são afetados por uma ameaça?	Ameaça Boletim	afeta afetadoPor
25	- Quais os clientes afetados por uma ameaça?	Ameaça Cliente	afeta afetadoPor
26	- Quais os destinatários afetados por uma ameaça?	Ameaça Destinatário	afeta afetadoPor
27	- Qual o assunto trata uma ameaça?	Ameaça Assunto	temAssunto
28	- Qual a última alteração existente de uma ameaça?	Ameaça ÚltimaAlteração	temUltimaAlteracao
30	- Qual o sumário de uma ameaça?	Ameaça Sumário	temSumario
31	- Qual a descrição técnica de uma ameaça?	Ameaça DescriçãoTécnica	temDescricaoTecnica
32	- Qual a mudança no log de uma ameaça?	Ameaça MudançaNoLog	temMudancaLog
33	- Quais os impactos podem ser causados por uma ameaça?	Ameaça Impacto	causa caudadoPor
34	- Quais as estratégias de suavização indicadas para uma ameaça?	Ameaça EstratégiasDeSuavização	temSuavizacao
35	- Quais os tipos de ameaças existentes?	Ameaça AmeaçaCódigoMalicioso AmeaçaVulnerabilidade	subClassOf
36	- Qual a origem de uma ameaça de código malicioso?	AmeaçaCódigoMalicioso Origem	temOrigem

Id	Questão de Competência	Conceitos	Relação
37	- Quais os sintomas que podem ser identificados de uma ameaça de código malicioso?	AmeaçaCódigoMalicioso Sintomas	temSintomas
38	- Quais as medidas de desinfecção indicadas a uma ameaça de código malicioso?	AmeaçaCódigoMalicioso MedidasDeDesinfecção	temDesinfeccao
39	- Quais os cenários de ataque de uma ameaça de vulnerabilidade?	AmeaçaVulnerabilidade CenáriosAtaque	temCenariosAtaque
40	- Quais as explorações de uma ameaça de vulnerabilidade?	AmeaçaVulnerabilidade Explorações	temExploracoes
41	- Quais as soluções sugeridas para uma ameaça de vulnerabilidade?	AmeaçaVulnerabilidade Soluções	temSolucoes
42	- Quais os créditos de uma ameaça de vulnerabilidade?	AmeaçaVulnerabilidade Créditos	temCreditos
43	- Quais os tipos de boletins existentes?	Boletim BoletimVulnerabilidade BoletimCódigoMalicioso	subClassOf
44	- Qual a taxa de impacto das ameaças de código malicioso monitoradas por um boletim de código malicioso?	BoletimCódigoMalicioso TaxaImpactoMinima AmeaçaCódigoMalicioso TaxaImpacto	monitora monitoradoPor temTaxaImpacto
45	- Qual a taxa de urgência das ameaças de vulnerabilidade monitoradas por um boletim de vulnerabilidade?	BoletimVulnerabilidade TaxaUrgênciaMinima AmeaçaVulnerabilidade TaxaUrgência	monitora monitoradoPor temTaxaUrgencia
46	- Qual a credibilidade da ameaça de vulnerabilidade monitorada por um boletim de vulnerabilidade?	BoletimVulnerabilidade CredibilidadeMinima AmeaçaVulnerabilidade Credibilidade	monitora monitoradoPor temCredibilidade

Id	Questão de Competência	Conceitos	Relação
47	- Qual a taxa de risco das ameaças de código malicioso monitoradas por um boletim de código malicioso?	BoletimCódigoMalicioso TaxaRiscoMinima AmeaçaCódigoMalicioso TaxaRisco	monitora monitoradoPor temTaxaRisco
48	- Qual a taxa de severidade das ameaças de código malicioso monitoradas por um boletim de código malicioso?	BoletimCódigoMalicioso TaxaSeveridadeMinima AmeaçaCódigoMalicioso TaxaSeveridade	monitora monitoradoPor temTaxaSeveridade
49	- Qual o índice de devastação das ameaças de código malicioso monitoradas por um boletim de código malicioso?	BoletimCódigoMalicioso ÍndiceDevastaçãoMinimo AmeaçaCódigoMalicioso ÍndiceDevastação	monitora monitoradoPor temIndiceDevastacao

Anexo V

Terminologia extraída das questões de competência

Conceito	Significado
Alerta	É o aviso que o sistema recebe das fontes externas de informação contendo uma ameaça a componentes.
Ameaça	Uma circunstância, ação, evento, ou pessoa com o potencial de causar danos a um sistema em forma de destruição ou modificação dos dados através da violação de segurança. Vulnerabilidade ou código malicioso são os tipos de ameaças existentes.
CódigoMalicioso	Tipo de ameaça onde um código programado por um usuário mal intencionado é introduzido em um sistema com propósito malicioso.
Vulnerabilidade	Tipo de ameaça onde o estado de um componente se encontra vulnerável a ataques, permitindo execução de comandos, acesso a dados restritos e outras ações.
Assunto	Nome único e descritivo que identifica o pacote do software afetado pela ameaça e detalhes adicionais. É atributo de uma Ameaça de Código Malicioso e de uma Ameaça de Vulnerabilidade.
Ativo	Lista dos componentes que definem as tecnologias utilizadas pelo cliente.
Boletim	Monitor configurado pelo cliente para monitorar ameaças que afetam seus ativos.
BoletimCódigoMalicioso	Monitor configurado pelo cliente para monitorar ameaças de código malicioso que afetam seus ativos.
BoletimVulnerabilidade	Monitor configurado pelo cliente para monitorar ameaças de vulnerabilidade que afetam seus ativos.
BT	Boletim técnico de segurança. Relatório enviado ao Cliente contendo informações sobre as Ameaças. Pode ser de dois tipos: BTCodMalicioso e BTVulnerabilidade.
BTCodMalicioso	Boletim técnico de segurança. Relatório enviado ao Cliente contendo informações sobre as Ameaças de Código Malicioso configuradas para serem monitoradas.
BTVulnerabilidade	Boletim técnico de segurança. Relatório enviado ao Cliente contendo informações sobre as Ameaças configuradas para serem monitoradas.
Categoria	É um atributo de um componente, contendo a categoria a qual este componente pertence.
CenáriosAtaque	É um atributo de uma Ameaça de Vulnerabilidade contendo a descrição das maneiras que um usuário malicioso tem para fazer uso da vulnerabilidade dos componentes.

Conceito	Significado
Cliente	É um usuário cadastrado no sistema que recebe e-mails contendo ameaças monitoradas pelos seus boletins configurados no sistema para monitorarem seus conjuntos de componentes cadastrados (ativos do cliente).
Componente	Sistema computacional ou uma parte importante para operação de um sistema (ex.: hardware, software e dados). Possui uma categoria, um fabricante e versões.
Credibilidade	É um atributo de uma Ameaça de Vulnerabilidade contendo a medida de quanto é confiável a informação sobre a vulnerabilidade. Os possíveis valores são: Relatórios conflitantes, Fonte única, Fonte confiável, Detalhes conflitantes, Múltiplas fontes, Confirmado pelo fornecedor e Desconhecido.
CredibilidadeMinima	É um atributo de um Boletim de Vulnerabilidade configurado pelo cliente contendo a credibilidade mínima das instâncias de ameaças de vulnerabilidade que serão monitoradas pelo boletim do cliente.
Créditos	É um atributo de uma Ameaça de Vulnerabilidade contendo informações a respeito do descobridor da vulnerabilidade, mailing lists ou fóruns que tratam sobre uma vulnerabilidade.
DataAtualização	É um atributo de uma Ameaça contendo a data da sua última atualização.
DescriçãoTécnica	É um atributo de uma Ameaça contendo uma descrição técnica detalhada da natureza da ameaça.
Destinatário	É um atributo configurado por um cliente, contendo o e-mail para o qual será enviado o boletim técnico.
Suavização	É um atributo de uma Ameaça contendo uma indicação das estratégias de suavização disponíveis para reduzir o impacto da ameaça aos componentes afetados por ela.
Explorações	É um atributo de uma Ameaça de Vulnerabilidade contendo informações de estratégias de exploração, links para códigos de exploração, código de exploração ou exemplos de ações de exploração para possibilitar a identificação de uma vulnerabilidade.
Fabricante	É um atributo de um componente, contendo o nome do seu fabricante.
Impacto	É um atributo de uma Ameaça de Vulnerabilidade contendo uma descrição do impacto causado quando um componente vulnerável é invadido.
Impactos	É um atributo de uma Ameaça de CódigoMalicioso contendo uma os tipos de impactos e respectivas taxas que são utilizadas para calcular a TaxaImpacto de uma Ameaça de Código Malicioso.

Conceito	Significado
ÍndiceDevastação	É um atributo de uma Ameaça de CódigoMalicioso contendo um valor que reflete a extensão que um código malicioso se espalha pelo sistema.
ÍndiceDevastaçãoMínimo	É um atributo de um Boletim de CódigoMalicioso configurado pelo usuário contendo o índice de devastação mínimo das instâncias de ameaças de código malicioso que serão monitoradas pelo boletim do cliente.
MedidasDeDesinfecção	É um atributo de uma Ameaça de Código Malicioso contendo uma descrição dos passos necessários para limpar o sistema sem a necessidade de instalação de um software anti-vírus.
MudançaNoLog	É um atributo de uma Ameaça contendo a enumeração de todas as mudanças das entradas da ameaça.
Origem	É um atributo de uma Ameaça de Código Malicioso contendo a Região geográfica onde o autor do código provavelmente estava quando criou o código.
Sintomas	É um atributo de uma Ameaça de Código Malicioso contendo uma descrição dos sinais que um componente infectado apresenta.
Soluções	É um atributo de uma Ameaça de Vulnerabilidade contendo descrições de soluções para a vulnerabilidade, tais como: métodos para suavizar o impacto, patches e/ou atualizações dos fornecedores.
Sumário	É um atributo de uma Ameaça de Vulnerabilidade contendo uma breve descrição da vulnerabilidade e uma rápida descrição do seu efeito.
TaxaImpacto	É um atributo de uma Ameaça de CódigoMalicioso contendo o cálculo do impacto de cada ação do código malicioso.
TaxaImpactoMinima	É um atributo de um Boletim de CódigoMalicioso configurado pelo usuário contendo a taxa de impacto mínima das instâncias de ameaças de código malicioso que serão monitoradas pelo boletim do cliente.
TaxaRisco	É um atributo de uma Ameaça de CódigoMalicioso contendo a medida de estimativa do perigo de uma instância de uma ameaça.
TaxaRiscoMinima	É um atributo de um Boletim de CódigoMalicioso configurado pelo usuário contendo a taxa de risco mínima das instâncias de ameaças de código malicioso que serão monitoradas pelo boletim do cliente.

Conceito	Significado
TaxaSeveridade	É um atributo de uma Ameaça de Vulnerabilidade contendo a medida de quanto uma ameaça é severa. É um valor de 1 a 100. É baseada no impacto, disponibilidade, autenticação e se é remoto e/ou local.
TaxaSeveridadeMínima	É um atributo de um Boletim de Vulnerabilidade configurado pelo usuário contendo a taxa de severidade mínima das instâncias de ameaças de vulnerabilidade que serão monitoradas pelo boletim do cliente.
TaxaUrgência	É um atributo de uma Ameaça de Vulnerabilidade contendo a medida de quão rápido precisa-se agir para consertar ou suavizar os efeitos da ameaça. É um valor quantitativo de 1 a 10.
TaxaUrgênciaMínima	É um atributo de um Boletim de Vulnerabilidade configurado pelo cliente contendo a taxa de urgência mínima das instâncias de ameaças de vulnerabilidade que serão monitoradas pelo boletim do cliente.
ÚltimaAlteração	É um atributo de uma Ameaça contendo a descrição da razão da atualização da ameaça.
Versão	É um atributo de um componente, contendo a versão deste componente.

Anexo VI

Taxonomia da Ontologia

Class Hierarchy

- Alerta (compostoPor)
- Ameaca (afeta, compoe, monitoradoPor, temAssunto, temDataAtualizacao, temDescricao, temMudancaLog, temSuavizacao, temUltimaAlteracao)
    - AmeacaCodMalicioso (causa, monitoradoPor)
        - instance BackDoor
        - instance Hoaxes
        - instance Nisances
        - instance Trojans
        - instance Virus
        - instance Worms
    - AmeacaVulnerabilidade (monitoradoPor, temCenario, temCenarioAtaque, temImpacto, temSumario)
- Ativo (afetadoPor, cadastradoPor, compostoPor, monitoradoPor, pertenceA)
- BT (enviadoPara, geradoPor)
    - BTCodMalicioso (geradoPor)
    - BTVulnerabilidade (geradoPor)
- Boletim (cadastradoPor, gera, monitora)
    - BoletimCodMalicioso (gera, monitora)
    - BoletimVulnerabilidade (gera, monitora)
- Categoria (possui)
    - instance ServidorWeb
    - instance SistemasOperacionais
- Cliente (cadastra, possui)
- Componente (afetadoPor, cadastradoPor, compoe, fabricadoPor, monitoradoPor, pertenceA, temCategoria, temFabricante, temVersao)
- Destinatario (cadastradoPor, pertenceA, recebeDe, temEmail)
- Fabricante (fabrica)
    - instance IBM
    - instance Microsoft
    - instance Oracle
- Impacto (causadoPor, temValor)
    - instance DegradacaoPerformance
    - instance NaoMalicioso

Anexo VII

Implementação da ontologia (DAML+OIL)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<rdf:RDF xmlns:daml="http://www.daml.org/2001/03/daml+oil#"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:oiled="http://img.cs.man.ac.uk/oil/oiled#"
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#" xmlns:xsd="http://www.w3.org/2000/10/XMLSchema#">
    <daml:Ontology rdf:about="">
        <dc:title>&amp;quot;Protótipo da ontologia de tarefas para auxiliar
            nas tarefas do sistema e-BTS&amp;quot;</dc:title>
        <dc:date>17/09/2003</dc:date>
        <dc:creator>Daniela Brauner</dc:creator>
        <dc:description>Esta ontologia apresenta conceitos para auxiliar
            nas tarefas do sistema e-BTS, caracterizando-se um protótipo
            de uma ontologia de tarefas.</dc:description>
        <dc:subject>segurança da informação, ameaças, alerta, código
            malicioso, vulnerabilidade</dc:subject>
        <daml:versionInfo>0.1</daml:versionInfo>
    </daml:Ontology>
    <daml:Class rdf:about="#BoletimCodMalicioso">
        <rdfs:label>BoletimCodMalicioso</rdfs:label>
        <rdfs:comment><![CDATA[Um tipo de Boletim. É configurado pelo cliente para monitorar apenas as
ameaças de código malicioso que afetam os componentes dos seus ativos.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T14:37:52Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Class rdf:about="#Boletim"/>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitora"/>
                <daml:toClass>
                    <daml:Class rdf:about="#AmeacaCodMalicioso"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#gera"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BTCodMalicioso"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#BTCodMalicioso">
        <rdfs:label>BTCodMalicioso</rdfs:label>
        <rdfs:comment><![CDATA[Boletim técnico de segurança. Relatório enviado ao Cliente contendo
informações sobre as Ameaças de Código Malicioso configuradas para serem monitoradas.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:38:38Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Class rdf:about="#BT"/>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#geradoPor"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BTCodMalicioso"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Impacto">
        <rdfs:label>Impacto</rdfs:label>
        <rdfs:comment><![CDATA[Tipos de impactos causados por uma Ameaça de CódigoMalicioso. Cada tipo
possui suas respectivas taxas que são utilizadas para calcular a TaxaImpacto de uma Ameaça de Código
Malicioso. ]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T18:14:32Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temValor"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#real"/>
            </daml:Restriction>
```

```
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#causadoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#AmeacaCodMalicioso"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temValor"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#real"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#causadoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#AmeacaCodMalicioso"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Componente">
        <rdfs:label>Componente</rdfs:label>
        <rdfs:comment><![CDATA[Sistema computacional ou uma parte importante para operação de um sistema
(ex.: hardware, software e dados) para o qual o cliente estará monitorando ameaças. ]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T22:21:56Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#compoe"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#Ativo"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temFabricante"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Fabricante"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temCategoria"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Categoria"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temVersao"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#integer"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="1">
                <daml:onProperty rdf:resource="#pertenceA"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Categoria"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="0">
                <daml:onProperty rdf:resource="#pertenceA"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitoradoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#Boletim"/>
                </daml:hasClass>
```

```
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#afetadoPor"/>
        <daml:hasClass>
            <daml:Class rdf:about="#Ameaca"/>
        </daml:hasClass>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#compoe"/>
        <daml:hasClass>
            <daml:Class rdf:about="#Ativo"/>
        </daml:hasClass>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#temFabricante"/>
        <daml:toClass>
            <daml:Class rdf:about="#Fabricante"/>
        </daml:toClass>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#temCategoria"/>
        <daml:toClass>
            <daml:Class rdf:about="#Categoria"/>
        </daml:toClass>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#temVersao"/>
        <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#integer"/>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction daml:minCardinalityQ="1">
        <daml:onProperty rdf:resource="#pertenceA"/>
        <daml:hasClassQ>
            <daml:Class rdf:about="#Categoria"/>
        </daml:hasClassQ>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction daml:minCardinalityQ="0">
        <daml:onProperty rdf:resource="#pertenceA"/>
        <daml:hasClassQ>
            <daml:Class rdf:about="#Cliente"/>
        </daml:hasClassQ>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#monitoradoPor"/>
        <daml:hasClass>
            <daml:Class rdf:about="#Boletim"/>
        </daml:hasClass>
    </dam l:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#afetadoPor"/>
        <daml:hasClass>
            <daml:Class rdf:about="#Ameaca"/>
        </daml:hasClass>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
        <daml:onProperty rdf:resource="#cadastradoPor"/>
        <daml:hasClass>
            <daml:Class rdf:about="#Cliente"/>
        </daml:hasClass>
    </daml:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <daml:Restriction>
```

```
                <daml:onProperty rdf:resource="#fabricadoPor"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Fabricante"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#BoletimVulnerabilidade">
        <rdfs:label>BoletimVulnerabilidade</rdfs:label>
        <rdfs:comment><![CDATA[Um tipo de Boletim. É configurado pelo cliente para monitorar apenas as
ameaças de vulnerabilidade que afetam os componentes dos seus ativos.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T14:44:22Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Class rdf:about="#Boletim"/>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitora"/>
                <daml:toClass>
                    <daml:Class rdf:about="#AmeacaVulnerabilidade"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#gera"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BTVulnerabilidade"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#AmeacaCodMalicioso">
        <rdfs:label>AmeacaCodMalicioso</rdfs:label>
        <rdfs:comment><![CDATA[Tipo de ameaça onde um código programado por um usuário mal intencionado
é introduzido em um sistema com propósito malicioso.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:26:33Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Class rdf:about="#Ameaca"/>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#causa"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Impacto"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitoradoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#BoletimCodMalicioso"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#BT">
        <rdfs:label>BT</rdfs:label>
        <rdfs:comment><![CDATA[Boletim técnico de segurança. Relatório enviado ao Cliente contendo
informações sobre as Ameaças configuradas para serem monitoradas.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:38:52Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#geradoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#Boletim"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#enviadoPara"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Destinatario"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
```

```
    <daml:Class rdf:about="#Ativo">
        <rdfs:label>Ativo</rdfs:label>
        <rdfs:comment><![CDATA[Lista dos componentes que identificam as tecnologias utilizadas pelo
cliente.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T22:21:03Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="1">
                <daml:onProperty rdf:resource="#compostoPor"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Componente"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#cadastradoPor"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitoradoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#Boletim"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#afetadoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#Ameaca"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#pertenceA"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Destinatario">
        <rdfs:label>Destinatario</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo configurado por um cliente, contendo o e-mail para o qual
será enviado o boletim técnico.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T21:34:12Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temEmail"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="1">
                <daml:onProperty rdf:res ource="#cadastradoPor"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="1">
                <daml:onProperty rdf:resource="#pertenceA"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#recebeDe"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BT"/>
                </daml:toClass>
            </daml:Restriction>
```

```
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temEmail"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="1">
                <daml:onProperty rdf:resource="#cadastradoPor"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:minCardinalityQ="1">
                <daml:onProperty rdf:resource="#pertenceA"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#recebeDe"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BT"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#BTVulnerabilidade">
        <rdfs:label>BTVulnerabilidade</rdfs:label>
        <rdfs:comment><![CDATA[Boletim técnico de segurança. Relatório enviado ao Cliente contendo
informações sobre as Ameaças de Vulnerabilidade configuradas para serem monitoradas.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:39:47Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Class rdf:about="#BT"/>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#geradoPor"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BTVulnerabilidade"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Boletim">
        <rdfs:label>Boletim</rdfs:label>
        <rdfs:comment><![CDATA[Módulo do sistema configurado pelo cliente para monitorar ameaças que
afetam os compoenentes dos seus ativos.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T21:55:12Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitora"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Ameaca"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitora"/>
                <daml:toClass>
                    <daml:Class>
                        <daml:unionOf>
                            <daml:List>
                                <daml:first>
                                    <daml:Class rdf:about="#AmeacaCodMalicioso"/>
                                </daml:first>
                                <daml:rest>
                                    <daml:List>
                                    <daml:first>
                                    <daml:Class rdf:about="#AmeacaVulnerabilidade"/>
                                    </daml:first>
                                    <daml:rest>
                                    <daml:nil/>
                                    </daml:rest>
```

```
                                    </daml:List>
                                </daml:rest>
                            </daml:List>
                        </daml:unionOf>
                    </daml:Class>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#cadastradoPor"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Cliente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:res ource="#gera"/>
                <daml:toClass>
                    <daml:Class rdf:about="#BT"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Categoria">
        <rdfs:label>Categoria</rdfs:label>
        <rdfs:comment><![CDATA[Conjunto de categorias que um componente pode
pertencer.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:32:54Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#possui"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Componente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Alerta">
        <rdfs:label>Alerta</rdfs:label>
        <rdfs:comment><![CDATA[É o aviso que o sistema recebe das fontes externas de informação contendo
uma ameaça a componentes.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:22:39Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction daml:cardinalityQ="1">
                <daml:onProperty rdf:resource="#compostoPor"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Ameaca"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Ameaca">
        <rdfs:label>Ameaca</rdfs:label>
        <rdfs:comment><![CDATA[Uma circunstância, ação ou evento com o potencial de causar danos a um
sistema em forma de destruição ou modificação dos dados através da violação de segurança.
Vulnerabilidade ou código malicioso são os tipos de ameaças existentes. Estas ameaças são recebidas pelo
sistema e-BTS através de fontes de informação externas.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T01:44:31Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temAssunto"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temDescricao"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temDataAtualizacao"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#date"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
```

```
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temMudancaLog"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temSuavizacao"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temUltimaAlteracao"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitoradoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#Boletim"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitoradoPor"/>
                <daml:hasClass>
                    <daml:Class>
                        <daml:unionOf>
                            <daml:List>
                                <daml:first>
                                    <daml:Class rdf:about="#BoletimCodMalicioso"/>
                                </daml:first>
                                <daml:rest>
                                    <daml:List>
                                    <daml:first>
                                    <daml:Class rdf:about="#BoletimVulnerabilidade"/>
                                    </daml:first>
                                    <daml:rest>
                                    <daml:nil/>
                                    </daml:rest>
                                    </daml:List>
                                </daml:rest>
                            </daml:List>
                        </daml:unionOf>
                    </daml:Class>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#afeta"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Componente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction daml:cardinalityQ="1">
                <daml:onProperty rdf:resource="#compoe"/>
                <daml:hasClassQ>
                    <daml:Class rdf:about="#Alerta"/>
                </daml:hasClassQ>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Cliente">
        <rdfs:label>Cliente</rdfs:label>
        <rdfs:comment><![CDATA[É um tipo de usuário cadastrado no sistema (cliente do e-BTS) que recebe
e-mails contendo ameaças monitoradas pelos seus boletins configurados no sistema para monitorarem seus
conjuntos de componentes cadastrados (ativos do cliente).]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T21:33:47Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#cadastra"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Boletim"/>
                </daml:toClass>
            </daml:Restriction>
```

```
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#cadastra"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Ativo"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#cadastra"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Destinatario"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#possui"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Componente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#possui"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Destinatario"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#Fabricante">
        <rdfs:label>Fabricante</rdfs:label>
        <rdfs:comment><![CDATA[Fabricantes de componentes.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:44:52Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#fabrica"/>
                <daml:toClass>
                    <daml:Class rdf:about="#Componente"/>
                </daml:toClass>
            </daml:Restriction>
        </rdfs:subClassOf>
    </daml:Class>
    <daml:Class rdf:about="#AmeacaVulnerabilidade">
        <rdfs:label>AmeacaVulnerabilidade</rdfs:label>
        <rdfs:comment><![CDATA[Tipo de ameaça onde o estado de um componente se encontra vulnerável a
ataques, permitindo execução de comandos, acesso a dados restritos e outras ações.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:27:22Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:subClassOf>
            <daml:Class rdf:about="#Ameaca"/>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temSumario"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temImpacto"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#monitoradoPor"/>
                <daml:hasClass>
                    <daml:Class rdf:about="#BoletimVulnerabilidade"/>
                </daml:hasClass>
            </daml:Restriction>
        </rdfs:subClassOf>
        <rdfs:subClassOf>
            <daml:Restriction>
                <daml:onProperty rdf:resource="#temCenario"/>
                <daml:toClass rdf:resource="http://www.w3.org/2000/10/XMLSchema#string"/>
            </daml:Restriction>
```

```
        </rdfs:subClassOf>
    </daml:Class>
    <daml:ObjectProperty rdf:about="#fabrica">
        <rdfs:label>fabrica</rdfs:label>
        <rdfs:comment><![CDATA[]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:03:25Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#fabricadoPor"/>
        <rdfs:domain>
            <daml:Class rdf:about="#Fabricante"/>
        </rdfs:domain>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#compoe">
        <rdfs:label>compoe</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto compoe um outro objeto
Ex: Componente compoe um Ativo]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T01:51:44Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#compostoPor"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temSuavizacao">
        <rdfs:label>temSuavizacao</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça contendo uma indicação das estratégias de
suavização disponíveis para reduzir o impacto da ameaça aos componentes afetados por
ela.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T19:39:04Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temSuavizacao"/>
    <daml:ObjectProperty rdf:about="#pertenceA">
        <rdfs:label>pertenceA</rdfs:label>
        <rdfs:comment><![CDATA[O inverso ao relacionamento de propriedade.
Um objeto pertence a outro objeto.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T20:35:42Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#possui"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temImpacto">
        <rdfs:label>temImpacto</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça de Vulnerabilidade contendo uma descrição do
impacto causado quando um componente vulnerável é invadido.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T17:56:45Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:domain>
            <daml:Class rdf:about="#AmeacaVulnerabilidade"/>
        </rdfs:domain>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temImpacto"/>
    <daml:ObjectProperty rdf:about="#afetadoPor">
        <rdfs:label>afetadoPor</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto é afetado por outro objeto (sofre algum efeito ou
impacto)]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:55:21Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#afeta"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#possui">
        <rdfs:label>possui</rdfs:label>
        <rdfs:comment><![CDATA[Relacionamento de propriedade. Um objeto possui outro
objeto.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T20:34:04Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#pertenceA"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temCenarioAtaque">
        <rdfs:label>temCenarioAtaque</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça de Vulnerabilidade contendo a descrição das
maneiras que um usuário malicioso tem para fazer uso da vulnerabilidade dos componentes.
]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:38:40Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]>< /oiled:creator>
        <rdfs:domain>
            <daml:Class rdf:about="#AmeacaVulnerabilidade"/>
```

```
        </rdfs:domain>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temCenarioAtaque"/>
    <daml:DatatypeProperty rdf:about="#temVersao">
        <rdfs:label>temVersao</rdfs:label>
        <rdfs:comment><![CDATA[Versão de um componente. A cada nova atualização feita pelo fabricante é
colocado no mercado uma nova versão de um componente contendo novas funcionalidades ou correções de bugs
de versões anteriores. ]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T12:51:56Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdfs:domain>
            <daml:Class rdf:about="#Componente"/>
        </rdfs:domain>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:ObjectProperty rdf:about="#gera">
        <rdfs:label>gera</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto cria outro objeto
Ex: Boletim cria Boletim Técnico]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T22:10:21Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <daml:inverseOf rdf:resource="#geradoPor"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#compostoPor">
        <rdfs:label>compostoPor</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto é composto por outro objeto
Ex: Ativo é composto de Componentes]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T01:58:44Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#compoe"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temSumario">
        <rdfs:label>temSumario</rdfs:label>
        <rdfs:comment><![CDATA[Descrição da ameaça e uma rápida descrição do seu
efeito.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T17:43:33Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temSumario"/>
    <daml:DatatypeProperty rdf:about="#temMudancaLog">
        <rdfs:label>temMudancaLog</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça contendo a enumeração de todas as mudanças
das entradas da ameaça.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T17:54:44Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temMudancaLog"/>
    <daml:DatatypeProperty rdf:about="#temDataAtualizacao">
        <rdfs:label>temDataAtualizacao</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça contendo a data da sua última
atualização.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T17:51:51Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:date/>
        </rdfs:range>
        <rdfs:range>
            <xsd:date/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temDataAtualizacao"/>
    <daml:ObjectProperty rdf:about="#afeta">
```

```
        <rdfs:label>afeta</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto afeta outro objeto (causa algum efeito ou
impacto)]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T18:38:01Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#afetadoPor"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#causa">
        <rdfs:label>causa</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto pode causar uma consequência.
Ex: uma Ameaça de CódigoMalicioso causa Impactos aos componentes que ela afeta.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T18:30:27Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#causadoPor"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#causadoPor">
        <rdfs:label>causadoPor</rdfs:label>
        <rdfs:comment><![CDATA[Uma consequencia é causada por um objeto.
Ex: Determinado impacto pode ser causado por uma Ameaça de CódigoMalicioso.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:09:54Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#causa"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temAssunto">
        <rdfs:label>temAssunto</rdfs:label>
        <rdfs:comment><![CDATA[Nome descritivo que identifica a ameaça e detalhes adicionais. É atributo
tanto de uma Ameaça de Código Malicioso quanto de uma Ameaça de Vulnerabilidade.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:31:19Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temAssunto"/>
    <daml:DatatypeProperty rdf:about="#temEmail">
        <rdfs:label>temEmail</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto possui um atributo Email.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T20:07:53Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:DatatypeProperty rdf:about="#temValor">
        <rdfs:label>temValor</rdfs:label>
        <rdfs:comment><![CDATA[Valor associado a um objeto]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T18:19:16Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:real/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temValor"/>
    <daml:ObjectProperty rdf:about="#fabricadoPor">
        <rdfs:label>fabricadoPor</rdfs:label>
        <rdfs:comment><![CDATA[]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-22T13:09:32Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <daml:inverseOf rdf:resource="#fabrica"/>
        <rdfs:range>
            <daml:Class rdf:about="#Fabricante"/>
        </rdfs:range>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#monitoradoPor">
        <rdfs:label>monitoradoPor</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto é monitorado por outro objeto
Ex: Ameaça é monitorado por Boletim]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T23:03:36Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <daml:inverseOf rdf:resource="#monitora"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temUltimaAlteracao">
        <rdfs:label>temUltimaAlteracao</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça contendo a descrição da razão da atualização
(última alteração) da ameaça.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T19:44:51Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:ObjectProperty rdf:about="#temFabricante">
```

```
        <rdfs:label>temFabricante</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto é fabricado por outro objeto
Ex: Um Componente é fabricado por um Fabricante]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T14:34:33Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:domain>
            <daml:Class rdf:about="#Componente"/>
        </rdfs:domain>
        <rdfs:range>
            <daml:Class rdf:about="#Fabricante"/>
        </rdfs:range>
    </daml:ObjectProperty>
    <daml:UniqueProperty rdf:about="#temFabricante"/>
    <daml:ObjectProperty rdf:about="#recebeDe">
        <rdfs:label>recebeDe</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto recebe (algum objeto) de outro objeto
Ex: Destinatario recebe (Boletim Tecnico) de Boletim]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T22:11:01Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <daml:inverseOf rdf:resource="#enviadoPara"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#geradoPor">
        <rdfs:label>geradoPor</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto é criado por outro objeto
Ex: Boletim Técnico é criado por um Boletim]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:38:19Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#gera"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#enviadoPara">
        <rdfs:label>enviadoPara</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto é enviado para outro objeto
Ex: Boletim Tecnico é enviado para Destinatario]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T22:08:16Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <daml:inverseOf rdf:resource="#recebeDe"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temCenario">
        <rdfs:label>temCenario</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça de Vulnerabilidade contendo a descrição das
maneiras que um usuário malicioso tem para fazer uso da vulnerabilidade dos componentes.
]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T21:33:51Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temCenario"/>
    <daml:ObjectProperty rdf:about="#cadastra">
        <rdfs:label>cadastra</rdfs:label>
        <rdfs:comment><![CDATA[Um usuário do sistema configura determinado recurso disponível para
ele.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T19:58:24Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#cadastradoPor"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#monitora">
        <rdfs:label>monitora</rdfs:label>
        <rdfs:comment><![CDATA[Um objeto monitora outro objeto
Ex: Boletim monitora uma Ameaça]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-16T22:35:22Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <daml:inverseOf rdf:resource="#monitoradoPor"/>
    </daml:ObjectProperty>
    <daml:ObjectProperty rdf:about="#cadastradoPor">
        <rdfs:label>cadastradoPor</rdfs:label>
        <rdfs:comment><![CDATA[Um recurso do sistema é configurado por um usuário do sistema
.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T19:59:09Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <daml:inverseOf rdf:resource="#cadastra"/>
    </daml:ObjectProperty>
    <daml:DatatypeProperty rdf:about="#temDescricao">
        <rdfs:label>temDescricao</rdfs:label>
        <rdfs:comment><![CDATA[É um atributo de uma Ameaça contendo uma descrição técnica detalhada da
natureza da ameaça.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T17:49:16Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
```

```
        <rdfs:range>
            <xsd:string/>
        </rdfs:range>
    </daml:DatatypeProperty>
    <daml:UniqueProperty rdf:about="#temDescricao"/>
    <daml:ObjectProperty rdf:about="#temCategoria">
        <rdfs:label>temCategoria</rdfs:label>
        <rdfs:comment><![CDATA[Faz a relacao do componente com sua respectiva categoria.
Ex: Windows NT pertenceA SistemasOperacionais]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:33:59Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdfs:domain>
            <daml:Class rdf:about="#Componente"/>
        </rdfs:domain>
        <rdfs:range>
            <daml:Class rdf:about="#Categoria"/>
        </rdfs:range>
    </daml:ObjectProperty>
    <daml:Class rdf:about="#AmeacaCodMalicioso">
        <daml:disjointWith>
            <daml:Class rdf:about="#AmeacaVulnerabilidade"/>
        </daml:disjointWith>
    </daml:Class>
    <daml:Class rdf:about="#BoletimCodMalicioso">
        <daml:disjointWith>
            <daml:Class rdf:about="#BoletimVulnerabilidade"/>
        </daml:disjointWith>
    </daml:Class>
    <daml:Class rdf:about="#BoletimCodMalicioso">
        <daml:disjointWith>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </daml:disjointWith>
    </daml:Class>
    <daml:Class rdf:about="#AmeacaVulnerabilidade">
        <daml:disjointWith>
            <daml:Class rdf:about="#BoletimVulnerabilidade"/>
        </daml:disjointWith>
    </daml:Class>
    <rdf:Description rdf:about="#Nisances">
        <rdfs:comment><![CDATA[Um tipo de código malicioso não-replicante que tem efeito inesperado e
benigno com conseqüências de fácil reparo (joke).]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T13:51:07Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#IBM">
        <rdfs:comment><![CDATA[Fabricante de componentes.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T12:26:20Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Fabricante"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#SistemasOperacionais">
        <rdfs:comment><![CDATA[Categoria de um componente]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:35:42Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Categoria"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#Microsoft">
        <rdfs:comment><![CDATA[Fabricante de componentes.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T12:25:22Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Fabricante"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#Virus">
        <rdfs:comment><![CDATA[Um tipo de código malicioso replicante que infecta outros arquivos,
principalmente executáveis, causando danos.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T13:51:12Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#Worms">
        <rdfs:comment><![CDATA[Um tipo de código malicioso não parasita que se replica propositalmente
```

```
em uma cópia evoluída explorando vulnerabilidades da segurança dos sistemas. Explora vulnerabilidades
que não são exclusivamente falhas de software, mas também erros da configuração ou erros do operador.
]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T13:51:15Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#ServidorWeb">
        <rdfs:comment><![CDATA[Categoria de um componente]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T02:37:47Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Categoria"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#Trojans">
        <rdfs:comment><![CDATA[Um tipo de código malicioso com função aparentemente ou realmente útil
que contem as funções (escondidas) adicionais que exploram secretamente as autorizações legítimas do
processo provocandoperda da segurança. Tipo de ataque em que um software aparentemente inofensivo,
inicia de forma escondida, ataques ao sistema.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T13:51:08Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#BackDoor">
        <rdfs:comment><![CDATA[Um tipo de código malicioso que permite que atacantes contornem os
mecanismos de segurança do sistema e acessem o sistema.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T13:51:18Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#DegradacaoPerformance">
        <rdfs:comment><![CDATA[O código malicioso deste tipo afeta a performance do sistema
afetado.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T18:25:32Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Impacto"/>
        </rdf:type>
        <ns0:temValor>
            <xsd:real xsd:value="2"/>
        </ns0:temValor>
    </rdf:Description>
    <rdf:Description rdf:about="#NaoMalicioso">
        <rdfs:comment><![CDATA[Um código malicioso deste tipo nao possui nenhuma ação maliciosa.
]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-18T18:14:05Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[user]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Impacto"/>
        </rdf:type>
        <ns0:temValor>
            <xsd:real xsd:value="1"/>
        </ns0:temValor>
    </rdf:Description>
    <rdf:Description rdf:about="#Hoaxes">
        <rdfs:comment><![CDATA[Um tipo de código malicioso lendário difundido geralmente via e-mail. Um
hoax é recebido no formato de e-mail anunciando alguma ameaça nova e solicita que o usuário envie a
notícia para o maior número de pessoas possíveis.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T13:51:04Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#AmeacaCodMalicioso"/>
        </rdf:type>
    </rdf:Description>
    <rdf:Description rdf:about="#Oracle">
        <rdfs:comment><![CDATA[Fabricante de componentes.]]></rdfs:comment>
        <oiled:creationDate><![CDATA[2003-09-17T12:26:02Z]]></oiled:creationDate>
        <oiled:creator><![CDATA[dani]]></oiled:creator>
        <rdf:type>
            <daml:Class rdf:about="#Fabricante"/>
        </rdf:type>
    </rdf:Description>
</rdf:RDF>
```

Anexo VIII

Fontes de Informação

Identificação	Fonte
A Proposed Taxonomy of Software Weapons - Martin Karresand - Master's thesis in Computer Security, 2002.	http://www.ep.liu.se/exjobb/isy/2002/3345/exjobb.pdf
Common Vulnerabilities and Exposures	http://www.cve.mitre.org/cve/
Glossário da Módulo Security	http://www.modulo.com.br
Internet Security Glossary - Network Working Group - The Internet Society (Maio 2000).	http://www.ietf.org/rfc/rfc2828.txt
National Criminal Justice Reference Service	http://abstractsdb.ncjrs.org/content/Thesaurus/Thesaurus_Search.asp
Security Taxonomy and Glossary – Lynn Wheeler	http://www.garlic.com/%7Elynn/secure.htm
Symantec Security Response Glossary	http://securityresponse.symantec.com/avcenter/glossary/index.html