CoreSec: Uma Ontologia como Ferramenta Educacional para Apoio no Ensino de Disciplinas de Segurança da Informação

Ryan Ribeiro de Azevedo[1,2,3], Robson Ytallo Silva Oliveira[1], Fred Freitas[1], Silas Cardoso de Almeida[3], Edson Costa de Barros Carvalho Filho[1], Marcelo José Siqueira Coutinho Almeida[1,2]

[1]Centro de Informática – Universidade Federal de Pernambuco (CIN-UFPE)
Caixa Postal 15.064 – 91.501-970 – Recife – PE – Brasil

[2]Coordenação de Informática
Centro Federal de Educação Tecnológica da Paraíba (CEFET-PB) – João Pessoa, PB – Brasil

[3]Coordenação de Sistemas de Informação
Faculdade Sete de Setembro (FASETE) – Paulo Afonso – BA - Brasil

{rra2,ryso,fred,ecdbcf,mjsca}@cin.ufpe.br, silasprogrammer@gmail.com

Abstract. *In academic area of Informatics, there are several difficulties to learn disciplines related to security of the information. That can be comprised with the low index of student's comprehension. This work aims at contributing to surpass the difficulties, offering mechanisms, through ontology development, in the education and collaboration among students in the security of the information learning. The proposal presents the CoreSec ontology and is based in the first experience of that ontology in class.*

Resumo. *No meio acadêmico de Computação, existem inúmeras dificuldades no aprendizado das disciplinas relacionadas à Segurança da Informação. Isso pode ser constatado através do baixo índice de assimilação dos estudantes. Este trabalho visa contribuir para superar as dificuldades, fornecendo mecanismos, através do desenvolvimento de ontologias, no ensino e na colaboração entre os alunos no aprendizado de Segurança da Informação. A proposta apresenta a ontologia CoreSec e baseia-se na primeira experiência dessa ontologia em sala de aula.*

1. Introdução

Lecionar disciplinas da área de Segurança da Informação é um desafio em virtude das características e peculiaridades das informações a serem repassadas [D. Frinke 2003]. Aos estudantes devem ser apresentados, de forma sistematizada, conceitos, técnicas e ferramentas utilizadas tanto para comprometer, assim como para proteger sistemas computacionais.

Com base na constatação acima, estabelece-se a necessidade de considerar a dinamicidade do processo de aprendizado e de aquisição do conhecimento dos alunos ao longo da realização de cursos ou disciplinas de Segurança da Informação utilizando-se

de ferramentas que possuam modelos gráficos ou teorias lógicas, tal como uma ontologia, construindo e reconstruindo conhecimentos e habilidades.

Dentro desse contexto, o objetivo do trabalho é apresentar e utilizar uma *Core Ontology* (ontologia de domínio), com conceitos mais genéricos e abstratos de determinado domínio de conhecimento, como ferramenta computacional para fins didáticos, denominada *CoreSec*, que visa à aplicação dos conceitos relacionados a Segurança da Informação.

São apresentadas neste trabalho práticas de ensino e aprendizagem sobre Segurança da Informação com a utilização da *CoreSec* aos alunos do curso superior de bacharelado em Sistemas de Informação da Faculdade Sete de Setembro localizada na cidade de Paulo Afonso no estado da Bahia com uma média anual de 60 alunos.

Proporcionando assim, que os mesmos consolidem o conhecimento aprendido com atividades práticas e que possam desenvolver ontologias de aplicação a partir da *CoreSec*, para aplicações como: Segurança Computacional, Gestão de Riscos, Segurança em Computação Autonômica, elicitação de requisitos de segurança no desenvolvimento de projetos de *software* seguros entre outras.

As demais seções deste artigo estão organizadas conforme descrição a seguir. Na Seção 2, é apresentada uma breve descrição dos conceitos relacionados a Ontologias. Em seguida, na Seção 3, é descrito o processo de Ensino-Aprendizagem com Ontologias. Na próxima seção, é explicado como foi construída a *CoreSec*. Na Seção 5, os dados utilizados nos experimentos e seus resultados são apresentados. Por fim, a Seção 6 aponta as conclusões sobre o trabalho e apresenta trabalhos futuros.

2. Ontologias

Diversas definições têm surgido a fim de descrever o que é uma ontologia. Atualmente, a mais conhecida é “uma especificação formal e explícita de uma conceituação compartilhada” [Gruber 1995], onde ser *formal* implica em declarativamente definida, portanto, compreensível para agentes e sistemas; e*xplícita* significa que os elementos e suas restrições estão claramente definidos; *conceitualização* trata de um modelo abstrato de uma área de conhecimento ou de um universo limitado de discurso; *compartilhada*, indica um conhecimento consensual, seja uma terminologia comum da área modelada, ou acordada entre os desenvolvedores dos agentes que se comunicam. Sendo assim, ontologias, em um nível de abstração mais alto, estabelecem uma terminologia comum e não-ambígua para o domínio em questão.

Recentemente o uso de ontologias tem se popularizado através de diversas outras subáreas da Ciência da Computação, tais como: Engenharia de Software, Banco de Dados e Sistemas de Informação. Um dos principais responsáveis por esse fenômeno é *Tim Berners Lee*, através do que ele convencionou chamar de *Web* Semântica [T. Berners-Lee et al. 2001].

Para [Guizzard 2000] “o termo ontologia é usado em concordância com a definição de [Guarino 1998], ou seja, ontologias são tratadas como um artefato computacional composto de um vocabulário de conceitos, suas definições e suas possíveis propriedades, um modelo gráfico mostrando todas as possíveis relações entre os conceitos e um conjunto de axiomas formais que restringem a interpretação dos

conceitos e relações, representando de maneira clara e não ambígua o conhecimento do domínio".

Diversas razões motivam o desenvolvimento de uma ontologia, de acordo com [Noy e McGuinness 2001] algumas dessas motivações são:

- Compartilhar entendimento comum da estrutura de informação entre pessoas ou entre agentes de software;
- Permitir o reuso de conhecimento de um domínio. Caso exista uma ontologia que modele adequadamente certo conhecimento de um domínio, ela pode ser compartilhada e usada por pessoas que desenvolvam aplicações nesse e em outros domínios;
- Tornar explícitas pressuposições de um domínio. As ontologias fornecem um vocabulário para representação do conhecimento. Esse vocabulário tem por trás uma conceitualização que o sustenta, evitando assim interpretações ambíguas;
- Separar conhecimento de domínio de conhecimento operacional;
- Analisar um conhecimento de um domínio.

3. Processo de Ensino-Aprendizagem com Ontologias

A aprendizagem é um processo individual e intransferível sendo completo quando envolve a assimilação, construção e reconstrução de conhecimento e habilidades [Lopes e Wilhelm. 2006]. Já afirmava [Freire 1996] que "ensinar não é transferir conhecimento, mas criar possibilidades para a sua própria produção ou sua construção". Sendo assim, é fundamental a ação constante e consciente por parte do aluno que deve sair de sua posição passiva de assistir a aula, para uma ação conjunta com o professor de fazer a aula [Anastasiou e Alves 2004] [Lopes e Wilhelm 2006].

De acordo com [Lopes e Wilhelm 2006], é exigida uma nova postura do professor utilizando-se de ferramentas que permitam ao aluno construir, junto com seus colegas, o seu próprio processo de aprendizagem. Segundo [Lévy 1993], as tecnologias podem ser pensadas como tecnologias da inteligência, pois elas se articulam com nosso sistema cognitivo de forma que não conseguiríamos pensar sem seu auxílio. Ainda de acordo com [Lévy 1993], as tecnologias se transformam em tecnologias da inteligência ao se constituírem em ferramentas que auxiliam e configuram o pensamento, tendo nele, portanto, um papel constitutivo.

Neste contexto pedagógico, o desenvolvimento de ontologias de aplicação a partir de uma Ontologia de Domínio com conceitos mais genéricos e abstratos de determinado domínio do conhecimento, oferece uma potencialidade metodológica interessante, permitindo que os alunos tenham um entendimento comum de determinado domínio e que possam desenvolver novos modelos consensuais em colaboração com outros alunos e professores tornando o processo de Ensino-Aprendizagem multidisciplinar. Construindo e reconstruindo conhecimento e habilidades, aliando os benefícios e vantagens do uso de ontologias e de suas tecnologias de desenvolvimento com as vivências necessárias nos processos de ensinar e aprender.

4. Proposta

Neste trabalho apresentamos a *CoreSec* uma ontologia de domínio para o domínio de Segurança servindo portanto de linhas-guia para o desenvolvimento de ontologias de aplicação para a segurança da informação, a *CoreSec* pode ser classificada sobre diversos aspectos. Utilizaremos a classificação proposta por [Guarino 1998], que esta dividida em: *i*) ontologia genérica, *ii*) ontologia de domínio, *iii*) ontologia de tarefa e *iv*) ontologia de aplicação. A ontologia aqui apresentada pretende ser a mais genérica possível, facilitando o ensino e aprendizagem em disciplinas de Segurança da Informação, bem como, do desenvolvimento de ontologias de aplicação para o domínio de segurança a partir da *CoreSec*, em cursos de graduação e pós-graduação nas áreas de Computação e Informática, preparando os alunos para atuar em um mercado promissor e carente de especialistas.

A *CoreSec* foi desenvolvida utilizando as seguintes metodologias, métodos e técnicas da Engenharia de Ontologias: *Methontology* [Fernández et al. 1997] baseada no padrão IEEE [IEEE 1996] para desenvolvimento de software e desenvolvimento de Sistemas Baseados em Conhecimento, a metodologia baseada em questões de competência que a ontologia deve ser capaz de responder proposta por [Uschold e Grüninger 1996], método 101 proposto por [Noy e McGuinness 2001] como complemento a *Methontology* e princípios de desenvolvimento de *Core Ontologies* propostos por [Valente e Breuker 1996].

Utilizou-se a linguagem OWL – *Web Ontology Language*, que incorpora facilidades para publicar e compartilhar a ontologia proposta via *Web* [OWL 2006] além de ser proposta como padrão pelo W3C[1] e está sendo utilizada pela *Web* Semântica [T. Berners-Lee et al. 2001]. A ferramenta utilizada para a construção da mesma foi o *Framework Protégé* [Protégé 2006].

A seguir são descritas algumas das principais classes modeladas na *CoreSec*:

- ***Vuulnerabilidade*.** Devem possuir instâncias sobre vulnerabilidades de acordo com o domínio da qual foi especializada. A partir dessa classe partem as relações que informam qual o tipo de vulnerabilidade em questão, suas conseqüências e correções.
- ***Componente*.** Possui informações a respeito dos possíveis componentes de acordo com o domínio especializado. A exemplo do relacionamento com a classe ***ComponenteTecnico*** que possui instâncias a respeito de componentes como ***Hardware*** e ***Software*** e também a respeito de produtos que possuem vulnerabilidades.
- ***RequisitosSegurança*.** Poderá ser especializada para conter instâncias sobre domínios específicos para levantamento de requisitos, a exemplo, do desenvolvimento seguro de software, onde classes adicionais como ***SecurityAudit***, ***TOEAcess*** e ***TrustedPath*** de acordo com a [ISO/IEC 15.408 1999] podem ser adicionadas.

[1] *World Wide We b Consortium* - www.w3c.org

- ***AnaliseRisco.*** Faz parte do relacionamento com a classe ***GerenciamentoRisco*** e são sub-classes de ***ManipulacaoRisco*** e tem por objetivo especificar os níveis de risco, tolerância e probabilidade de sua ocorrência, bem como, o impacto nos negócios caso uma ameaça venha a ser explorada por um atacante, define também os controles utilizados para mitigar a probabilidade de ocorrência de um determinado ataque. Essa classe e seus relacionamentos podem ser reusados como componentes para se realizar apenas o gerenciamento de riscos independente do domínio de aplicação.
- ***ValorSegurança.*** Possui instâncias a respeito dos níveis de risco e segurança que um determinado ambiente, dependendo do seu domínio específico deva possuir, esta classe tem forte relação com a classe ***AnaliseRisco***.
- ***Politica.*** Possui instâncias que descrevem as políticas de segurança sendo adotadas pela organização. Essas políticas são descritas por meio de instâncias específicas de acordo com normas adotadas.
- ***Contramedidas.*** Possui instâncias relacionadas a contramedidas de segurança que devem ser realizadas nas organizações em seus planos de continuidade de serviços caso um ataque a um dos ativos seja bem sucedido.

Como já mencionado, a ontologia foi implementada utilizando a linguagem OWL e o *Framework Protégé*. É apresentado na Figura 1 a hierarquia de algumas das principais classes definidas na *CoreSec*. Algumas classes foram omitidas por questões de espaço.

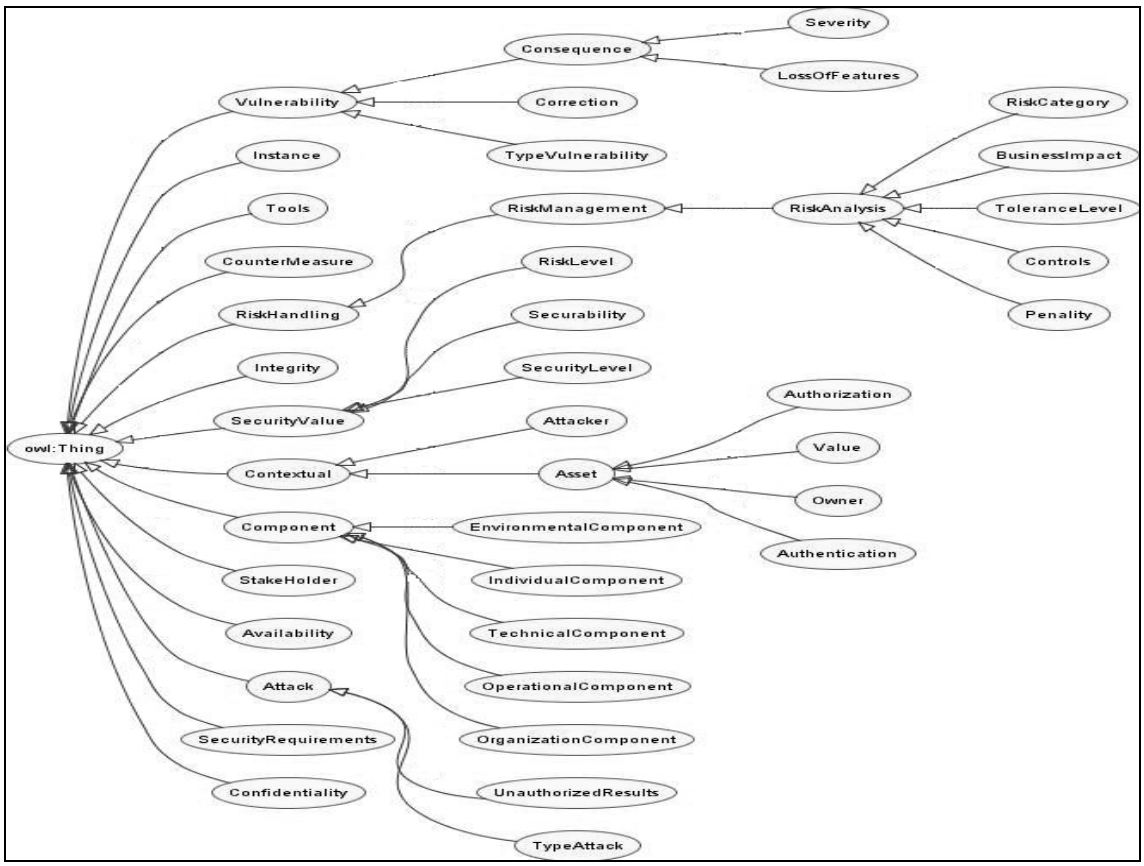

Figura 1. Parte da hierarquia de classes da *CoreSec.*

5. Análise da *CoreSec* e Apresentação dos Resultados

As experiências de aulas sobre Segurança da Informação utilizando a *CoreSec* foram realizadas com os alunos do IV período do curso superior de Bacharelado em Sistemas de Informação do semestre 2007.2 do horário noturno na disciplina Sistemas de Informação da Faculdade Sete de Setembro localizada na cidade de Paulo Afonso – BA, que totaliza um grupo de 28 alunos. As mesmas aulas sobre Segurança da Informação, porém, sem a utilização da *CoreSec* foram ministradas aos alunos do semestre anterior 2007.1 da mesma disciplina, período e turno, formado por um grupo de 18 alunos.

Inicialmente foram explicados os conceitos básicos a respeito da *Web* Semântica, ontologias e Segurança da Informação e apresentados aos alunos: axiomas referentes à *CoreSec*, suas classes, propriedades, o que cada classe poderia possuir como instâncias e como poderiam ser os relacionamentos entre suas classes, desenvolvendo assim, habilidades nos alunos como criatividade e raciocínio.

A *CoreSec* completa com seus relacionamentos foi apresentada aos alunos e os mesmos constataram que poderiam criar novas ontologias para domínios específicos de segurança e que estavam discutindo corretamente e entendendo de forma clara sobre a área e tema de pesquisa, ao contrário da turma anterior (2007.1), onde os alunos se queixavam que não estavam entendendo do domínio de estudo e que havia muita informação para decorar. Percebeu-se que os alunos já conseguiam entender da área e tema de pesquisa: Segurança da Informação, por terem discutido anteriormente de forma colaborativa a respeito dos artefatos apresentados.

Para avaliar e consolidar os conceitos ensinados e aprendidos a turma 2007.2 foi dividida em três grupos em atividades práticas assim como os da instância 2007.1 e os alunos da turma 2007.2 produziram as seguintes ontologias a partir da *CoreSec*: Uma Ontologia para Elicitação de Requisitos de Segurança em Projetos de Software apresentada na Figura 2 desenvolvida pelo Grupo 1.

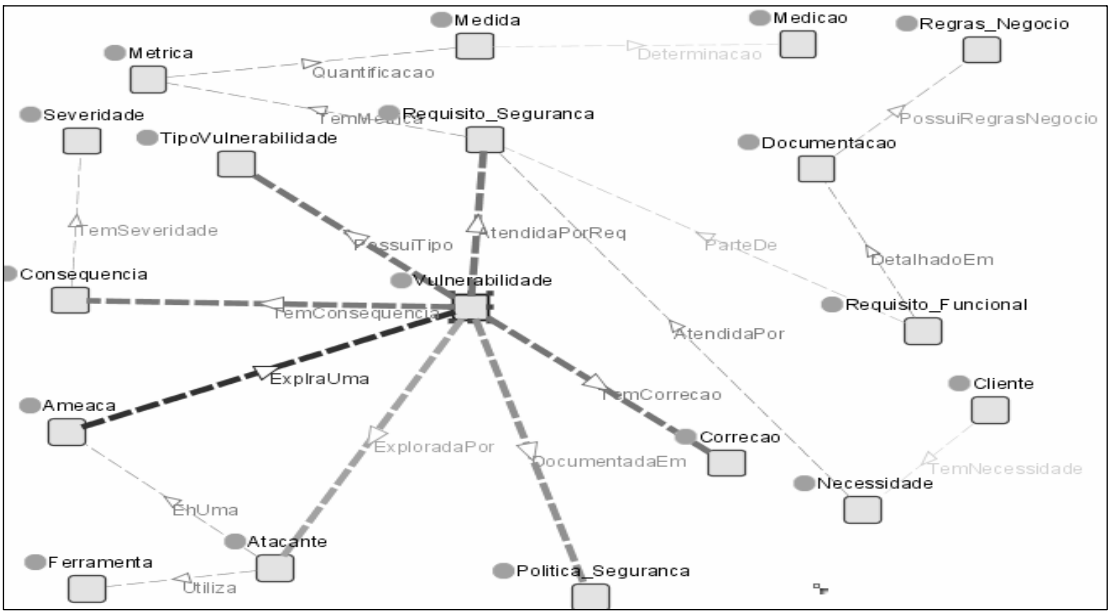

Figura 2. Parte das classes e relacionamentos da ontologia para elicitação de requisitos de segurança em projetos de desenvolvimento de software.

Uma Ontologia para Gestão de Segurança em Ambientes de Computação Autonômica apresentada na Figura 3 desenvolvida pelo Grupo 2 baseada em [Almeida et al. 2007] e utilizando-se da *CoreSec*.

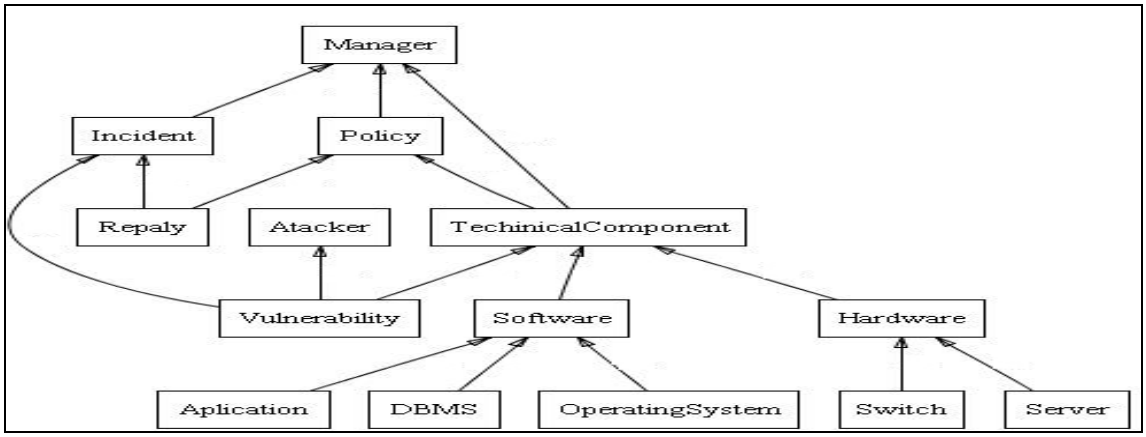

Figura 3. Parte das classes e relacionamentos da ontologia para gestão de segurança em ambientes de computação autonômica.

Uma Ontologia para Gestão de Riscos em Segurança da Informação apresentada na Figura 4 desenvolvida pelo Grupo 3.

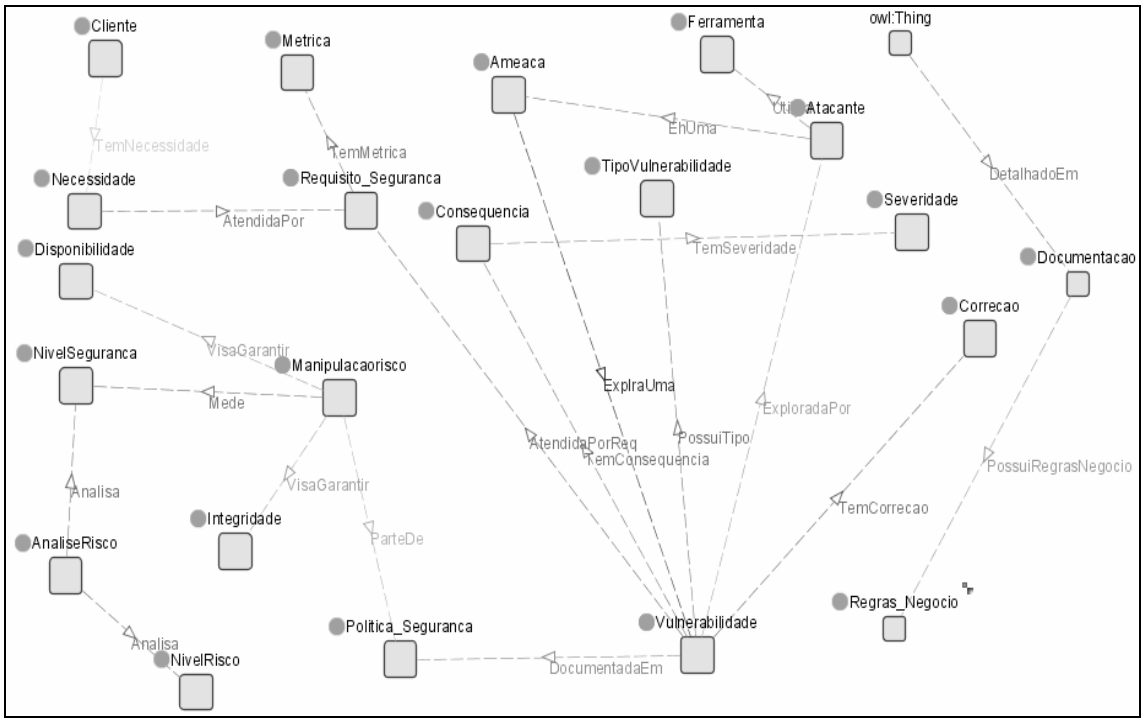

Figura 4. Parte das classes e relacionamentos da ontologia para gestão de riscos em segurança da informação.

As ontologias produzidas pelos alunos também foram desenvolvidas utilizando o *Framework Protégé* [Protégé 2006] junto com a linguagem OWL, a utilização da linguagem OWL se deu por ser a linguagem ontológica da Web [OWL 2006], além de permite inferência implícita. Foi utilizado apenas o método 101 proposto por [Noy e McGuinness 2001] para auxiliar nas etapas de desenvolvimento das ontologias de

aplicação desenvolvidas, método escolhido pela simplicidade de suas etapas de desenvolvimento e facilidade em seu entendimento por parte dos alunos. As Figuras apresentadas acima foram geradas pelos *plugins Jambalaia, Ontoviz e OWL Viz.*

No desenvolvimento destas ontologias os alunos tiveram que pesquisar e aprender áreas e temas de pesquisa ainda não estudadas tais como: Inteligência Artificial, Redes de Computadores, Engenharia de Requisitos subárea da Engenharia de Software, Gestão de Riscos, Gestão do Conhecimento e Computação Autonômica tornando o aprendizado interdisciplinar e estimulando o convívio com diferentes professores tornando-os profissionais com as exigências de um mercado competitivo que exige cada vez mais pessoas com diversas habilidades.

Utilizando a *CoreSec* como ferramenta de apoio ao ensino e aprendizagem de Segurança da Informação notou-se que houve resultados satisfatórios de entendimento do domínio de Segurança da Informação. É apresentada na Tabela 1 uma comparação do que foi aprendido entre os alunos do período 2007.2 e dos alunos do período 2007.1 que não utilizaram da *CoreSec* em seu aprendizado.

Tabela 1. Comparação entre assuntos aprendidos e o nível de aprendizagem

Assuntos / Turmas	Web Semântica e Ontologias	Ferramentas de Desenvolvimento se Ontologias	Metodologias, Métodos e Técnicas de desenvolvimento de Ontologias	Linguagem OWL
2007.1	Todos os Grupos	Todos os Grupos	Todos os Grupos	Todos os Grupos
Nível de Aprendizado	Baixo	Baixo	Baixo	Baixo
2007.2	Todos os Grupos	Todos os Grupos	Todos os Grupos	Todos os Grupos
Nível de Aprendizado	Médio	Alto	Alto	Médio
Assuntos / Turmas	Computação Autonômica	Gestão de Riscos	Segurança da Informação	Engenharia de requisitos
2007.1	Grupo 2	Grupo 3	Todos os Grupos	Grupo 1
Nível de Aprendizado	Baixo	Baixo	**Baixo**	Baixo
2007.2	Grupo 2	Grupo 3	Todos os Grupos	Grupo 1
Nível de Aprendizado	Médio	Médio	**Alto**	Médio

Verifica-se pelas ontologias desenvolvidas, pelos seminários e avaliações realizadas durante o semestre pelos alunos da instância 2007.2 que a quantidade e nível de aprendizado de temas distintos e com maior eficiência foi superior se comparada aos alunos da instância 2007.1 que também tiveram acesso aos mesmos tópicos de pesquisa, porém, sem o uso inicial de um artefato como a *CoreSec* e não conseguiram produzir

artefatos de segurança em suas atividades diferente dos alunos da instância posterior. Os resultados apresentados permitem a análise da eficiência do uso da *CoreSec* no processo de ensino e aprendizado do aluno.

6. Conclusão e Trabalhos Futuros

A *CoreSec* cumpre o papel ao qual se propõe, se constituindo em uma ferramenta computacional que poderá ser utilizada para fins didáticos, possibilitando aos professores e estudantes da área de Inteligência Artificial, e mais especificamente da área de Segurança da Informação, implementar e testar diversas formas de implementação com facilidade, a partir do seu uso.

Como trabalho futuro, pretende-se adicionar as atividades dos alunos dos próximos períodos do ano letivo 2008 o desenvolvimento de uma aplicação *Web* Semântica baseada em agentes utilizando a API *Jena* desenvolvida por *Brian McBride* da *Hewlett-Packard*, usada na criação e manipulação de grafos RDF [JENA 2003], para auxiliar os usuários a manipular a *CoreSec* e as ontologias de aplicação desenvolvidas por eles, permitindo a visualização e navegação em partes da mesma.

O sistema proposto possuirá inicialmente os módulos de inserção, consulta e inferência sendo apresentada ao usuário de maneira fácil e intuitiva para que possam tomar decisões de forma eficaz e eficiente. Pretende-se também estender o uso da *CoreSec* no ensino no curso superior de Bacharelado em Administração da mesma instituição onde os experimentos foram realizados do qual possui como tópico de ensino a Segurança na *Internet*.

Referências

Anastasiou, L.; Alves, L. P. (2004). “Processos de ensinagem na universidade: pressupostos para as estratégias de trabalho em aula.” 3.ed. Joinville : UNIVILLE, 2004. 144 p, il.

Almeida, M. J. S. C., Freitas, F., Azevedo, R, R., Dias, G. A. An Ontology for Information Security Management in Autonomic Computing Environments. *In: Proceedings of the 2nd Latin American Autonomic Computing*, 2007.

D. Frinke. (2003).Who Watches the Security Educators?. IEEE Security & Privacy Magazine, Vol.1, Issue 3, pp. 56-58, May-June, 2003.

Fernández, M. A.; Gómez-Pérez, A.; Juristo, N. (1997). Methontology: From ontological art towards ontological engineering. *In Proceedings of the AAAI Spring Symposium Series*, 1997, p. 33-40.

Freire, P. (1996). “Pedagogia da autonomia: saberes necessários para a prática educativa.” São paulo: Paz e Terra, 1996.

Freitas, F. (2003). Ontologias e a web semântica. In: Renata Vieira; Fernando Osório. (Org.). *Anais do XXIII Congresso da Sociedade Brasileira de Computação*. Campinas: SBC, 2003. v. 8, p. 1-52.

Guizzardi. G. (2000). “Uma abordagem metodológica de desenvolvimento para e com reuso, baseada em ontologias formais de domínio.” Dissertação de Mestrado. Universidade Federal do Espírito Santo. 2000.

Gruber, T. R. (1995). *Towards Principles for the Design of Ontologies Used for Knowledge Sharing*. International Journal of Human and Computer Studies, 43(5/6): 907- 928. 1995.

IEEE (1996). Standard for developing software life cycle processes. IEEE Computing Society, 1996.

JENA 2 Ontology API. (2003). Disponível em: <http://jena.sourceforge.net/ontology/>. Acesso em 01/08/2007.

ISO/IEC 15.408 (1999). "*Information technology – Security techniques - Evaluation criteria for IT security."* 1999, 222p.

Lévy, P. (1993). As tecnologias da inteligência. "O futuro do pensamento na era da informática." Rio de Janeiro: editora 34, 1993

Lopes, M. C., Wilhelm, P. P. H. (2006). Uso de jogos de simulação empresarial como ferramenta educacional: uma análise metodológica. In: Anais do XVII Simpósio Brasileiro de Informática na Educação, Brasília. 2006.

Noy, N. F.; McGuiness, D. L. (2001). "*Ontology development 101: A Guide to Creating Your First Ontology*." Knowledge Systems Laboratory – Stanford University, TR KSL-01-05, 2001.

OWL. (2006). Web ontology language overview - w3c;. *[Online]*. *Disponível: http://www.w3.org/TR/owl-features/ Acessado em: Out. 2006.*

Protégé. (2006) Protégé ontology editor. *[Online]*. *Disponível: http://protege.stanford.edu/doc/users.html Acessado em: Out. 2006.*

T. Berners-Lee, O. Lassila, and J. Hendler. (2001) "The semantic web." *Scientific American*, 5:34–43, 2001.

Uschold, M, Grüninger, M. (1996). *Ontologies: Principles, Methods and Applications*. Knowledge Engineering Review. Vol. 11, Nº 02. June.1996.

Valente, A., Breuker, J. (1996). Towards Principled Core Ontologies. In *B.R. Gaines and M. Mussen, editors, Proceedings of the KAW-96*, Banff, Canada, 1996.