# CoreSec: Uma Ontologia de Domínio para Auxiliar a Gestão de Segurança da Informação

**Ryan Ribeiro de Azevedo[1], Fred Freitas[1], Marcelo José Siqueira Coutinho Almeida[1], Wendell Campos Veras[1], Edson Costa de Barros Carvalho Filho[1]**

[1]Centro de Informática – Universidade Federal de Pernambuco (CIN-UFPE)
Caixa Postal 7851 – 50.732-970 – Recife – PE – Brasil
{rra2, fred, mjsca, wcv, ecdbcf}@cin.ufpe.br

## 1. Introdução

A garantia da Segurança da Informação em ambientes corporativos exige uma eficaz e eficiente aquisição e distribuição de conhecimento a respeito de riscos, vulnerabilidades e ameaças que podem ser exploradas. Os problemas com a Segurança da Informação passaram a ser uma questão estratégica para os negócios. Com uma base de conhecimento a respeito destes aspectos as organizações poderão desenvolver e implantar mecanismos de proteção, correção e prevenção de acordo com os SLAs (Acordos de Níveis de Serviços) exigidos para que seus serviços estejam sempre disponíveis, íntegros e confiáveis.

As organizações já não investem em TI (Tecnologia da Informação) sem maiores justificativas, gerentes devem justificar seus orçamentos anualmente e convencer a diretoria da razoabilidade de riscos, segurança, viabilidade financeira, retorno econômico e garantias de nível de qualidade de serviço dos projetos que propõem. Projetos são escolhidos através de metodologias que consideram riscos, segurança, custo e ganhos financeiros. O foco da análise se distancia das questões de TI puras para se concentrar na efetiva contribuição de TI para o negócio da empresa.

Sendo assim, apresentamos a *CoreSec* (ontologia de domínio) para o domínio de riscos e segurança, com intuito de auxiliar a Governança de TI, definindo assim, uma base de informações comum, um aumento na capacidade de tratamento e utilização da informação e uma visão de alto nível entre os envolvidos. As demais seções deste artigo estão estruturadas da seguinte forma: a Seção 2 foca na proposta em desenvolvimento e resultados parciais. Por fim, na Seção 3 apresenta-se às considerações finais e trabalhos futuros.

## 2. Proposta e Resultados Parciais

A *CoreSec* esta sendo desenvolvida com a utilização da metodologia *Methontology* [Fernández et al 1997]. Utilizamos a linguagem OWL, que incorpora facilidades para publicar e compartilhar a ontologia proposta via *Web* além de ser proposta como padrão pelo W3C, e sendo utilizada pela *Web* Semântica, permitindo expressividade de alto nível e inferência implícita. A ferramenta utilizada para a desenvolvimento da mesma é o *Framework Protégé*. É apresentado na Figura 1 parte do modelo implementado gerado pelo *plugin owl viz* do *Framework Protégé*.

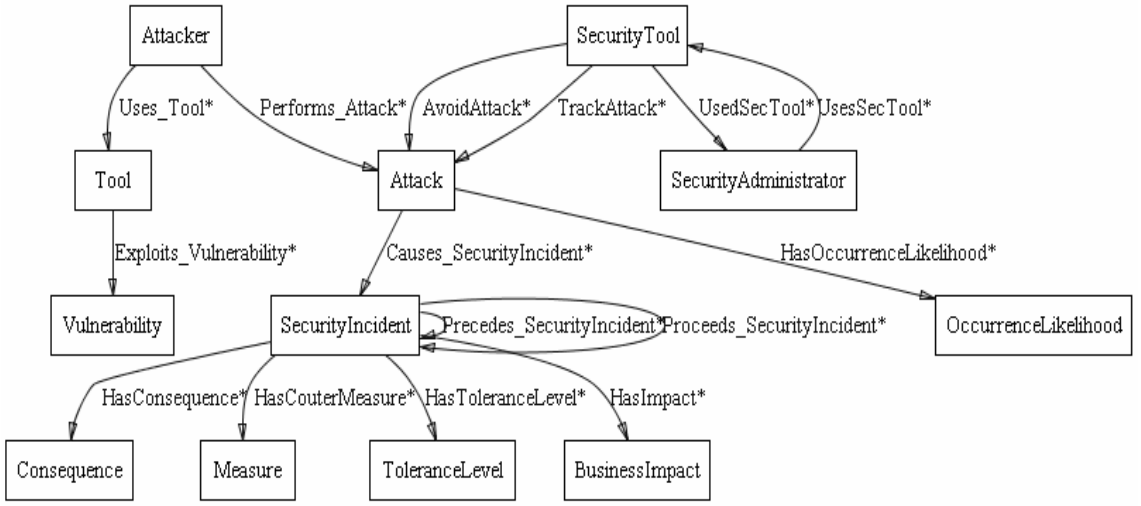


**Figura 1. Parte dos conceitos definidos para a CoreSec.**

Também esta sendo desenvolvida uma aplicação denominada *CoreEditor* para manipulação, avaliação e utilização da *CoreSec* pelos responsáveis pela Segurança da Informação das corporações. O uso do *CoreEditor* contribui com a melhoria na tomada de decisões minimizando o impacto que problemas de segurança podem causar em uma corporação, bem como, apoiar os administradores de segurança nas tomadas de decisões a respeito de problemas relacionados a segurança em nível gerencial.

Com intuito de validar o trabalho, algumas consultas foram definidas baseadas nas seguintes questões de competência que a *CoreSec* deve ser capaz de responder: se um agente mal intencionado explorar uma vulnerabilidade e realizar um ataque do tipo *DDoS – Distributed Denial of Service* ou *DoS – Denial of Service* por exemplo, qual a conseqüência destes ataques para organização? Qual a probabilidade de ocorrência desse ataque? Qual é o impacto nos negócios? Quais ativos são atingidos? Qual nível de tolerância é permitido? Quais controles utilizar para mitigar a exploração de tal vulnerabilidade? Qual o nível de risco aceitável?. Utilizando o módulo de consultas do *CoreEditor* consultas com a linguagem SPARQL foram realizadas e seus resultados são satisfatórios e respondem as questões de competência definidas.

## 3. Considerações Finais e Trabalhos Futuros

A *CoreSec* cumpre o papel ao qual se propõe, se constituindo em uma ferramenta computacional que poderá ser utilizada para o tratamento e utilização da informação a respeito de riscos e segurança da informação, possibilitando a tomada de decisões estratégicas de alinhamento de TI e Segurança aos negócios das organizações. Como trabalho futuro, pretende-se estender as funcionalidades do *CoreEditor* e conceitos da *CoreSec* ampliando-a para domínios mais específicos da segurança computacional, apoiando cada vez mais o nível gerencial corporativo para que possam tomar decisões de forma eficaz e eficiente.

## Referências

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