UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Roberto Marinho

UM MODELO PARA AVALIAÇÃO DINÂMICA DE RISCO UTILIZANDO ONTOLOGIA

Florianópolis

2014

Roberto Marinho

UM MODELO PARA AVALIAÇÃO DINÂMICA DE RISCO UTILIZANDO ONTOLOGIA

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do Grau de Mestre em Ciência da Computação
Orientadora: Profa. Dra. Carla Merkle Westphall.

Florianópolis
2014

Ficha de identificação da obra elaborada pelo autor
através do Programa de Geração Automática da Biblioteca Universitária
da UFSC.

Marinho, Roberto
Um modelo para avaliação dinâmica de risco utilizando ontologia / Roberto Marinho ; orientadora, Carla Merkle Westphall - Florianópolis, SC, 2014.
117 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da Computação. 2. Controle de Acesso. 3. Ontologia. 4. RAdAC. 5. Computação em Nuvem. I. Merkle Westphall, Carla . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Roberto Marinho

UM MODELO PARA AVALIAÇÃO DINÂMICA DE RISCO UTILIZANDO ONTOLOGIA

Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Ciência da Computação, e aprovada em sua forma final pelo Programa de Pós Graduação em Ciência da Computação da Universidade Federal de Santa Catarina

Florianópolis, 27 de Junho de 2014.

_____
Prof. Dr. Ronaldo dos Santos Mello
Coordenador do Curso

Banca Examinadora:

_____
Prof.ª Dr.ª Carla Merkle Westphall
Orientadora
Universidade Federal de Santa Catarina

_____
Prof. Dr. Alexandre Moraes Ramos
Universidade Federal de Santa Catarina

_____
Prof.ª Dr.ª Patricia Della Méa Plentz
Universidade Federal de Santa Catarina

_____
Prof. Dr. Ricardo Alexandre R. de Moraes
Universidade Federal de Santa Catarina

Dedico este trabalho aos meus pais, minha namorada e meus amigos.

AGRADECIMENTOS

Agradeço aos meus pais, por todos os ensinamentos que me fizeram chegar até aqui. Agradeço a minha namorada Natália, por todo amor e incentivo dados durante essa caminhada. Aos meus amigos da BRy Tecnologia, um especial obrigado por terem dado o apoio para que essa conquista pudesse ser possível. E por fim, a minha orientadora Dra. Carla Merkle Westphall, que sempre acreditou no meu trabalho e nos frutos que ele daria.

I am the master of my fate:
I am the captain of my soul.
(William Ernest Henley, 1875)

RESUMO

Em computação, o controle de acesso é motivado pela necessidade de divulgar o acesso à informação, recursos e serviços somente para entidades autorizadas. Dentre os modelos de controle de acesso atuais, o RAdAC destaca-se por possibilitar um controle dinâmico e situacional na avaliação do acesso, baseando-se no risco de acesso para aceitar ou negar requisições. Neste contexto, o presente trabalho tem como objetivo oferecer um modelo para avaliação dinâmica de risco a partir do modelo RAdAC, amparando-se no uso de ontologia para realização do cálculo de risco. Na proposta apresentada, a composição do risco total relacionado a uma requisição de acesso é composta pelos riscos de contexto, riscos considerando confidencialidade, integridade e disponibilidade das ações, e do risco considerando o histórico do sujeito. A partir do mapeamento das diversas variáveis envolvidas no cálculo de risco de contexto em sentenças de uma ontologia, o modelo busca inferir dinamicamente o risco de contexto no acesso a um determinado dado, baseando-se nos fatores de risco disponíveis e seus determinados pesos.

Palavras-chave: Controle de Acesso, Ontologia, RAdAC, Cloud Computing.

ABSTRACT

In computing, access control is motivated by the need to promote access to information, resources and services only to authorized entities. Among the existing access control models, RAdAC stands out by allowing a dynamic and situational control in the evaluation of access, relying on the risk assessment to accept or deny requests.

This work aims to provide a model for dynamic risk assessment from the RAdAC model, supported by the use of ontologies to perform the calculation of risk. In the proposal presented here, the composition of the total risk associated to an access request comprises the context risk, the risk considering confidentiality, integrity and availability of the actions, and the risk considering the history of the subject.

From the mapping of the different variables involved in the calculation of context risk in sentences of an ontology, the model seeks to dynamically infer the context risk during the access to a specific data, based on the available risk factors and their weights.

Keywords: Access Control, Ontology, RAdAC, Cloud Computing.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

XML – eXtensible Markup Language
DAC – Discretionary Access Control
MAC – Mandatory Access Control
RBAC – Role-based Access Control
ACL – Access Control List
ABAC – Attribute Based Access
OWL – Ontology Web Language
RDF – Resource Description Framework
RDFS – Resource Description Framework Schema
URIs – Uniform Resource Identifier
W3C – World Wide Web Consortium
C.I.A. – Confidentiality, Integrity and Availability
SSL – Secure Socket Layer
JSON – JavaScript Object Notation
PHP – PHP: Hypertext Preprocessor

SUMÁRIO

1 INTRODUÇÃO

Nesse capítulo apresenta-se uma introdução ao trabalho desenvolvido, inicialmente através de uma contextualização. A seguir, são apresentados a descrição do problema a ser tratado, a hipótese testada, os objetivos gerais e específicos, as limitações, e o método de pesquisa. A organização do restante do trabalho é exposta ao final do capıtulo.

1.1 CONTEXTO

Os atuais mecanismos disponíveis para controlar o acesso às informações não possuem a flexibilidade e a base para a tomada de decisões necessárias para apoiar os objetivos do compartilhamento de informações. No mundo real, as decisões são regularmente tomadas por autoridades, podendo essas, dar acesso e compartilhar informações sigilosas em situações que fogem das condições ideais de segurança (MCGRAW, 2009).

Essas decisões são movidas por fatores situacionais e necessidades operacionais, sendo realizadas com a convicção de que os benefícios operacionais do compartilhamento das informações superam o potencial risco de segurança em compartilhá-las. O foco de tais decisões é alcançar o sucesso operacional em detrimento ao risco de segurança adicional, dado qualquer número de fatores situacionais.

A base para a tomada dessas decisões é a compreensão da necessidade operacional, o risco de segurança resultante, as políticas e procedimentos operacionais que regem a situação, e o conhecimento dos efeitos da tomada de decisões semelhantes no passado. Entretanto, embora seja essencial para as autoridades ter a liberdade para tomar essas decisões, é improvável que eles tenham uma compreensão total do risco de segurança associado a suas decisões.

A parte crítica da implementação do compartilhamento eficaz de informações consiste no estabelecimento de um processo de controle de acesso em nível de objeto, que possa lidar com as realidades do ambiente do compartilhamento de informações. O conceito de controle de acesso proposto para atingir esse ambiente é chamado Risk-Adaptable Access Control (RAdAC) (MCGRAW, 2009). O RAdAC se distingue dos modelos tradicionais por apresentar flexibilidade e adaptabilidade, visando adaptar as decisões de controle de acesso para as situações correntes, além de determinar o acesso baseando-se em um

cálculo de risco de segurança e necessidade operacional, e não apenas na comparação de atributos.

A utilização de ontologias no desenvolvimento e adaptação de modelos de controle de acesso, visando proporcionar flexibilidade e dinamicidade na tomada de decisões já é explorada em diversos trabalhos (FININ et al., 2008; DERSINGH et al., 2009). Entretanto, o uso de ontologias no contexto de avaliação dinâmica de risco, ancoradas no modelo de controle de acesso RAdAC, consiste em um tema ainda pouco explorado pela literatura.

1.2 PROBLEMA E HIPÓTESE

Muitos modelos para controle de acesso dinâmico foram desenvolvidos objetivando proporcionar uma maior flexibilidade no controle de decisão. Dentre eles, os modelos de controle baseados em risco e contexto surgiram buscando resolver o problema de ambientes dinâmicos em que a aplicação dos modelos tradicionais apresenta problemas (JASON Program Office, 2004). Em situações excepcionais, a partir de operações emergenciais, também conhecidas como "*break the glass*", os modelos baseados em risco conseguem liberar o acesso para um usuário previamente não autorizado.

O modelo RAdAC destaca-se por levar em consideração diversos fatores na composição do risco, bem como a necessidade operacional da requisição. Entretanto, a avaliação do risco é relacionada diretamente com fatores de risco estáticos e seus respectivos pesos, que podem não estar disponíveis durante a realização da requisição de acesso.

Este trabalho testa a hipótese de que, com o auxílio de ontologias, é possível adaptar o cálculo de risco aos fatores de risco disponíveis no momento da requisição, além de inferir dinamicamente fatores de risco previamente não explicitados.

1.3 JUSTIFICATIVA

Embora existam diversos estudos no que tange a avaliação de risco dentro da área de controle de acesso, a maior parte deles acaba por focar-se em métodos estáticos e/ou direcionados a ambientes específicos de aplicação.

Este trabalho, no entanto, busca permitir que a avaliação de risco seja realizada de acordo com o ambiente em que encontra-se a requisição de acesso e os dados do sistema. Para alcançar este objetivo,

utiliza-se do conhecimento que os administradores possuem sobre o próprio sistema, permitindo a criação de regras baseadas nas particularidades e especificidades do mesmo.

O trabalho de Briton & Brown (2007) explora em parte essa característica adaptativa ao subdividir os fatores de risco em diversas partes e atribuir pesos para cada um deles de acordo com a visão dos administradores do sistema. Entretanto, a avaliação do histórico do sujeito é realizada de forma simplória, não oferecendo também um método para avaliar os riscos de confiabilidade, integridade e disponibilidade.

Outros trabalhos, como: Saripalli & Walters (2010), Fall et al. (2011), Sharma et al.(2012), entre outros, fornecem métricas muito interessantes, mas que são voltadas a ambientes estáticos. Este trabalho no entanto, busca ser adaptativo ao ponto que, o cálculo dos fatores de risco envolvidos no cálculo de risco podem ser inferidos ou adaptados para qualquer tipo de ambiente, utilizando para tal, apenas o conhecimento dos próprios administradores do sistema.

1.4 OBJETIVOS

1.4.1 Objetivo Geral

O presente trabalho tem por objetivo desenvolver um modelo dinâmico de cálculo de risco baseado no RAdAC e amparado pelo uso de ontologia, objetivando utilizá-la para calcular o risco de acesso a um determinado objeto em variados cenários e situações.

Um protótipo do modelo RAdAC deve ser implementado, proporcionando a decisão de acesso a recursos em situações excepcionais, fornecendo informações sobre o processo de construção dos fatores de risco e avaliação dos mesmos na composição final do risco de acesso.

1.4.2 Objetivos Específicos

Os objetivos específicos que podem ser citados são:

- Estudar os atuais modelos de controle de acesso;
- Identificar problemas e limitações nos modelos de controle de acesso dinâmico existentes;

- Propor um modelo para avaliação dinâmica de fatores de risco a partir dos atuais modelos de controle de acesso;
- Implementar e validar o modelo proposto;

1.5 ESCOPO

Devido ao fato do trabalho ser voltado à área de controle de acesso, algumas questões são desconsideradas para estabelecer um menor espectro na extensão da pesquisa desenvolvida. O escopo deste trabalho pode ser definido pelos seguintes fatores:

- O modelo considera que as requisições são realizadas em um ambiente sem demais restrições, além da própria avaliação de risco e necessidade operacional;
- O modelo considera que todos os recursos e usuários possuem as informações necessárias ao próprio modelo para a realização do cálculo dos fatores de risco;
- O modelo considera que as políticas de acesso não serão alteradas dinamicamente pelos administradores do sistema;

1.6 METODOLOGIA

Esta seção apresenta os procedimentos metodológicos utilizados durante o desenvolvimento do modelo para avaliação dinâmica de risco baseado em ontologia, bem como os processos realizados para validação do mesmo.

1.6.1 Classificação da Pesquisa

O estudo em questão tem por objetivo gerar conhecimento na área de segurança da computação, mais especificamente na área de modelos de controle de acesso dinâmico. Um protótipo para avaliar a validade do modelo proposto é desenvolvido, apoiando-se em testes de acesso e de desempenho.

Do ponto de vista da natureza da pesquisa, este trabalho se classifica como uma pesquisa aplicada, tendo por objetivo gerar um produto, com finalidades imediatas, baseando-se em conhecimentos prévios (JUNG, 2004). Silva e Menezes (2001) descrevem que a pesquisa aplicada busca gerar conhecimentos para aplicação prática

dirigida à solução de problemas específicos, envolvendo verdades e interesses locais.

Do que diz respeito à abordagem, a pesquisa é caracterizada como quantitativa, pois os resultados obtidos são explicitados quantitativamente através das avaliações de desempenho realizadas sobre o protótipo, transformando em números os resultados e informações com o intuito de classificá-los e analisá-los.

Quanto aos objetivos da pesquisa, este trabalho se caracteriza como uma pesquisa exploratória, pois visa proporcionar maior familiaridade com o problema investigado a fim de torná-lo explícito.

Por fim, o procedimento técnico utilizado será o de uma pesquisa bibliográfica, pois coleta e análise dos dados serão realizadas com base em materiais já publicados, constituído principalmente de livros, artigos de periódicos e materiais disponibilizados na Internet (GIL, 1991).

1.6.2 Etapas da Pesquisa

As etapas de pesquisa inerentes ao trabalho são:

- Pesquisa Bibliográfica: A pesquisa bibliográfica compreende o estudo e análise das atuais propostas no âmbito de modelos de controle de acesso dinâmicos, especialmente o RAdAC;

- Análise do estado da arte: A pesquisa é realizada focando em artigos disponibilizados em bases de dados de pesquisa acadêmica como: IEEExplore, Portal ACM, Science Direct, Springer, etc.

- Desenvolvimento: Com base na pesquisa realizada é proposto um modelo para avaliação dinâmica de risco baseado em ontologia.

- Avaliação: Consiste na implementação de um protótipo de um modelo de controle de acesso dinâmico, visando avaliar a utilização de ontologia na obtenção de fatores de riscos e avaliação de acesso.

- Publicação: Desenvolvimento de um artigo sobre o tema abordado e os resultados obtidos. Artigo aceito na *International Conference on Security and Management* -

SAM 2014: "*A Dynamic Approach to Risk Calculation for the RAdAC Model"* – Qualis B3.

1.7 ORGANIZAÇÃO DO TEXTO

O restante do trabalho está organizado da seguinte forma: o capítulo 2 elenca diversos modelos de controle de acesso, com uma abordagem especial sobre o RAdAC; o capítulo 3 apresenta conceitos sobre ontologia e suas formas de representação; o capítulo 4 enumera os trabalhos relacionados abordados; o capítulo 5 descreve o modelo proposto; o capítulo 6 demonstra como o modelo foi implementado; o capitulo 7 apresenta os resultados obtidos; e por fim, o capítulo 8 traz a conclusão do trabalho.

2 MODELOS DE CONTROLE DE ACESSO

O capítulo a seguir tem por objetivo elucidar os modelos de controle de acesso mais importantes e utilizados atualmente. As definições aqui estabelecidas serão utilizadas durante o decorrer desse trabalho.

2.1 CONTROLE DE ACESSO

Controle de acesso é definido como o processo pelo qual garante-se que todo e qualquer acesso às informações ou recursos de um determinado sistema computacional é controlado, de modo que, somente requisições autorizadas possam ser realizadas (SAMARATI; VIMERCATI, 2001). O processo de autorização é determinado por um modelo que especifica regras a serem utilizadas na avaliação das requisições de acesso ao sistema, que por sua vez, é dividido em três conjuntos de entidades principais:

Sujeitos: Representam as entidades que buscam acessar os recursos e informações do sistema através de requisições de acesso.

Recursos: São os objetos acessados pelo Sujeitos. Representam as informações, recursos e dados requisitados pelos Sujeitos.

Ações: São identificadas pelas operações que os Sujeitos realizam sobre os Recursos, representando a forma de acesso requisitada. As ações realizadas sobre o sistema podem alterar o seu estado e o estado dos recursos disponibilizados pelo mesmo, alterando também as características de disponibilidade, confidencialidade e integridade dos recursos afetados.

Além das entidades supramencionadas, os sistemas de controle de acesso são também compostos por políticas e mecanismos de controle de acesso. Enquanto as políticas correspondem às descrições que buscam especificar quais conjuntos de comportamentos podem ou não ser realizados no sistema, os mecanismos de controle de acesso correspondem a procedimentos que visam aplicar tais políticas sobre o sistema.

Desta forma, as políticas de um sistema podem ser representadas de diversas maneiras, de acordo com a necessidade de torná-las legíveis a humanos ou máquinas. Implementações dos mecanismos de controle de acesso envolvem funções de hardware e software aplicadas sobre as políticas, criando modelos de controle de acesso. Dentre os modelos de controle de acesso mais tradicionais, destacam-se o Discretionary

Access Control (DAC), o Mandatory Access Control (MAC) e o Role-based Access Control (RBAC) (SAMARATI; VIMERCATI, 2001).

2.2 DAC

O DAC (*Discretionary Access Model*) compreende um modelo em que o controle de acesso à informação é realizado com base na identidade e nas autorizações dos usuários. Estas autorizações especificam para cada usuário, ou grupo de usuários, e para cada objeto no sistema, o modo de acesso (ex: leitura, escrita ou execução) que é permitido ao usuário sobre o objeto. Neste modelo, cada requisição realizada por um usuário para acessar um objeto é checada com base em autorizações específicas. Deste modo, caso exista uma autorização declarando que o usuário tem acesso ao objeto em um determinado modo específico, o acesso é garantido, caso contrário, o acesso é negado.

A flexibilidade oferecida pelo modelo DAC faz com que ele seja adequado para vários sistemas e aplicações, entretanto, ele não é capaz de fornecer uma garantia real sobre o fluxo da informação em um sistema, uma vez que a disseminação da informação não é controlada (SANDHU, 1994).

2.3 MAC

O modelo MAC (*Mandatory Access Control*) realiza o controle de acesso com base em uma classificação de sujeitos e objetos pertencentes a um sistema. Neste modelo, um nível de segurança é atribuído a cada usuário e objeto no sistema. O nível de segurança associado a um objeto reflete a sensibilidade da informação contida no objeto. Por sua vez, o nível de segurança associado a um usuário reflete a confiabilidade depositada neste usuário para que ele não divulgue informações a usuários que não tem permissão de vê-las. O nível de segurança consiste em um elemento pertencente a um conjunto hierárquico, e dessa forma, o acesso a um objeto por um sujeito é possível apenas se algum relacionamento é satisfeito entre os níveis de segurança associados com ambos, sujeito e objeto (SANDHU, 1994).

2.4 RBAC

O modelo RBAC (*Role-Based Access Control*) controla o acesso dos usuários à informação com base nas atividades executadas pelos

usuários no sistema. Este tipo de modelo, baseado em papéis, requer a identificação destes papéis no sistema, de modo que, um papel pode ser definido como um conjunto de ações e responsabilidades associadas a uma atividade de trabalho em particular. Desta forma, ao invés de especificar todos os acessos que cada usuário pode ou não executar, o controle de acesso sobre os objetos é especificado por papéis, que por sua vez, são vinculados aos usuários por meio de autorizações.

Um usuário desempenhando um papel é autorizado a executar todos os acessos para os quais esse papel está autorizado. De um modo geral, um usuário pode desempenhar diferentes papéis em diferente ocasiões, assim como o mesmo papel pode ser desempenhado por diversos usuários, até mesmo, simultaneamente (SANDHU, 1994).

2.5 ABAC

No modelo ABAC (*Attribute-Based Access Control*) a decisão sobre a autorização é realizada com base em valores de atributos. Atributos são um conjunto de propriedades que podem ser associados a uma identidade. Essa identidade, por sua vez, pode ser um sujeito, um recurso, ou até mesmo um ambiente relacionado com a interação entre um usuário e uma aplicação.

Os atributos podem ser relacionados aos sujeitos (ex: Papel, identidade, idade, nacionalidade, etc.), aos recursos (Ex: local, peso, tamanho, valor, etc.), ou ao ambiente (hora do dia, data do sistema, idioma do sistema, etc.).

No modelo ABAC, as decisões de autorização são baseadas em atributos das entidades relacionadas, que por sua vez, são estabelecidos por credenciais digitalmente assinadas, nas quais, os emissores das credenciais confirmam e aferem os atributos das entidades. (SHENG & HONG, 2006).

2.6 UCON

O UCON (abreviatura de *Usage Control*) é um framework conceitual, que busca ampliar as possibilidades do controle de acesso, cobrindo as necessidades do controle de acesso de uma maneira sistemática, e fornecendo um framework genérico e unificado para proteger recursos digitais. O modelo UCON não é um substituto para os tradicionais modelos de controle de acesso, gerenciamento de segurança e DRM, mas sim, um modelo que engloba estas três áreas e vai além em sua definição e escopo (SANDHU & JAEHONG, 2004).

O UCON consiste em oito componentes principais: sujeito, atributos do sujeito, objetos, atributos dos objetos, direitos, autorizações, obrigações e condições. Enquanto o modelo tradicional de controle de acesso utiliza apenas autorização para lidar com o processo de decisão, o UCON utiliza autorizações, obrigações e condições funcionais de predicados para avaliar a decisão de uso (ZHU & WEN, 2012).

Conceitualmente, o UCON foi originalmente baseado no paradigma de superdistribuição, desta forma, a informação eletrônica está disponível livremente, porém seu acesso é controlado (SANDHU & PARK, 2002).

2.7 RADAC

O *Risk-Adaptable Access Control* (RAdAC) é um novo modelo de controle de acesso proposto pela NSA (*National Security Agency*), concebido no contexto de ambientes modernos de computação em larga escala e que possibilita um controle dinâmico e situacional na tomada de decisões. O escopo desses ambientes consiste em um conjunto de recursos de informação conectados ponta a ponta e globalmente, permitindo a coleta, processamento, armazenamento, disseminação e gerenciamento de informações sob demanda (KANDALA; SANDHU & BHAMIDIPATI, 2011). Essa abordagem exige um equilíbrio dinâmico entre a necessidade de acessar informações em vista das prioridades, riscos e custos de comprometimento de informações, bem como, da avaliação da situação geral operacional e de risco do sistema.

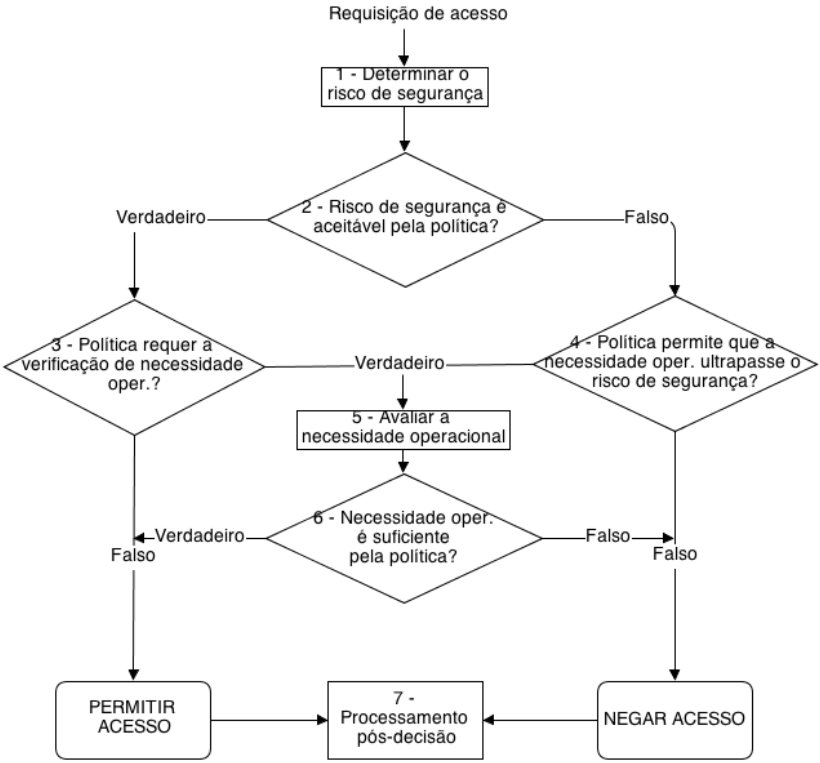
De acordo com McGraw (2009), RAdAC é um modelo de controle de acesso que determina o acesso com base em um cálculo de risco de segurança e de necessidade operacional, e não apenas em uma comparação de atributos. O RAdAC considera diversos fatores no intuito de determinar os riscos de segurança e a necessidade operacional de cada decisão de acesso, tais como:

- Grau de confiança no individuo que solicita o acesso
- Sensibilidade da informação a ser acessada
- Qualidade de proteção que pode ser conferida a informação
- Função do individuo
- A criticidade da informação para a operação
- Incerteza
- Histórico de decisões de acesso

Além desses fatores, o modelo RAdAC destaca-se por permitir a adaptação dos seus limites de decisão e utilizar políticas especificas para tomada de decisão, de forma que, uma necessidade operacional pode vir a superar os riscos de segurança envolvidos em uma operação.

A Figura 1 ilustra o fluxo para tomada de decisão em um ambiente onde o modelo de controle de acesso RAdAC é utilizado.

Figura 1 – Fluxograma RAdAC



2.7.1 Necessidade Operacional

Em modelos de controle de acesso tradicionais, a necessidade operacional é definida sob o pretexto da “necessidade de saber”, sendo usada na maioria das vezes para restringir o acesso à determinada informação, do que permitir o acesso a ela (MCGRAW, 2009).

Entretanto, a necessidade operacional pode ser vista de várias formas, manifestando-se de maneiras diferentes de acordo com o escopo ao qual está inserida, e a política da organização.

Um funcionário solicitando acesso a uma área restrita em uma determinada situação pode ter a necessidade operacional da sua requisição diminuída ou aumentada de acordo com seu perfil de acesso, nível de acesso, histórico, etc. No modelo RAdAC, a necessidade operacional é utilizada para avaliar se a requisição de acesso poderá ser efetuada ou não, em contraponto ao risco mensurado.

3 RISCO

O risco é o dano potencial que pode surgir em um processo atual ou futuro e é geralmente representado pela probabilidade de ocorrência de um evento indesejado e o seu impacto resultante (DIEP et al., 2007).

Os modelos de controle de acesso baseados em risco realizam uma análise de risco na requisição para fazer uma decisão de acesso. Esta análise de risco pode ser qualitativa ou quantitativa. Nos métodos qualitativos diferentes escalas de risco, como por exemplo, escalas alta, média e baixa, são utilizadas e geralmente a valoração é feita através da opinião de um especialista. Já nos métodos quantitativos existe uma maneira de atribuir um valor numérico que representa o risco de uma requisição de acesso.

Em métodos quantitativos, o risco de um evento normalmente é representado pelo cálculo expresso na Fórmula 1.

Fórmula 1 - Risco

$$R = P \times I$$

Em (1), P é a probabilidade de ocorrência do evento e I é o impacto da ocorrência do evento. Em situações onde há um histórico de acessos e onde o impacto pode ser quantificado, especialmente em valores numéricos, o cálculo torna-se mais fácil, mas há situações onde esses itens não são facilmente obtidos ou onde deseja-se considerar também outras características e, para isso, existem diversas propostas de cálculo de risco.

No modelo RAdAC (Risk-Adaptive Access Control) o controle de acesso é adaptativo e é baseado no cálculo do risco de acesso do usuário (JASON, 2004; MCGRAW, 2009). Este cálculo é feito em tempo real e deve garantir a segurança do sistema.

3.1 PROBABILIDADE DE OCORRÊNCIA

Com o intuito de calcular a probabilidade de ocorrência que uma potencial vulnerabilidade pode exercer dentro de um ambiente de risco, os seguintes fatores devem ser levados em consideração:

- Motivação e capacidade da fonte de ameaça;
- Natureza da vulnerabilidade;
- Existência e eficácia dos controles atuais;

A probabilidade de ocorrência de uma potencial vulnerabilidade pode ser expressa de em níveis de probabilidade, a partir da classificação das probabilidades ou da definição de limites nos casos quantitativos. A tabela X apresenta um exemplo de divisão de níveis de probabilidade em três diferentes graus.

Tabela 1 – Probabilidade de Ocorrência

Nível	**Definição da Probabilidade de Ocorrência**
Alto	A fonte de ameaça é altamente motivada e suficientemente capaz. Os controles para prevenir que a vulnerabilidade seja explorada são ineficazes.
Médio	A fonte de ameaça é motivada e capaz, mas os controles estão em um lugar onde é possível impedir que a vulnerabilidade seja explorada.
Baixo	A fonte de ameaça não possui motivação e capacidade, ou os controles conseguem prevenir que a vulnerabilidade seja explorada.

3.2 IMPACTO

O impacto negativo de um evento de segurança pode ser descrito em termos da perda ou degradação da integridade, disponibilidade e/ou confidencialidade das informações de um sistema. Cada uma destas três metas de segurança possuem consequências (ou impactos) gerados a partir do não cumprimento das mesmas:

Perda de Integridade: A integridade dos dados e do sistema remete ao requisito que estabelece que toda informação deve ser protegida de modificações indevidas. Dessa forma, a integridade é perdida caso alterações não autorizadas sejam realizadas nos dados ou no sistema de TI, tanto de maneira intencional, quanto acidental. Se a perda de integridade dos dados ou do sistema não for corrigida, o uso continuado do sistema contaminado, ou de dados contaminados, pode resultar em imprecisão, fraude ou decisões errôneas. Além disso, a violação de integridade pode ser o primeiro passo em um ataque contra a disponibilidade e confidencialidade do sistema. Por todas essas razões, a perda de integridade acaba por reduzir confiança em um sistema de TI.

Perda de Disponibilidade: Se um sistema de TI de missão crítica não está disponível para seus usuários finais, a missão da organização pode

ser afetada. A perda de funcionalidade do sistema e de sua efetividade operacional pode resultar em perda de produtividade, e consequentemente, impedir o desempenho das funções dos usuários finais no que tange o suporte a missão organizacional.

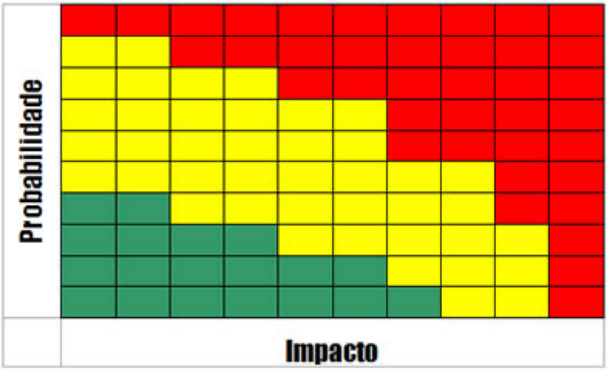
Perda de Confidencialidade: A confidencialidade do sistema e dos dados diz respeito à proteção da informação ante sua exposição não autorizada. O impacto dessa exposição em informações confidenciais varia desde o comprometimento da segurança nacional, à exposição de dados pessoais. A divulgação de informações não autorizadas, não previstas ou não intencionais, pode resultar na perda da confiança pública, e até mesmo, na instauração de ações legais contra a organização.

3.3 MATRIZ DE RISCO

A matriz de probabilidade/consequência é uma representação que permite combinar classificações qualitativas ou semiquantitativas de consequências e probabilidades, buscando produzir um nível de risco ou uma classificação de risco (ISO/IEC 31010).

Matrizes de Risco são utilizadas para classificar riscos, fontes de riscos ou tratamento de riscos com base no nível de risco mensurado. As entradas para a matriz de risco são escalas personalizadas de risco e consequência, além de uma matriz apresentando a combinação entre as duas. As escalas de classificação do risco podem ser feitas de maneira quantitativa ou qualitativa, a partir da avaliação dos resultados da relação probabilidade X consequência de cada elemento da matriz.

Tabela 2 - Matriz de Risco



4 ONTOLOGIA

Várias são as definições encontradas sobre o termo “ontologia” na literatura. Gruber (2007) afirma que ontologia corresponde a uma especificação de uma conceituação, descrevendo conceitos e seus inter-relacionamentos. Borst (1997), por sua vez, define ontologia como: “uma especificação formal, explícita de uma conceitualização compartilhada”. Pela definição de Borst (1997), “especificação formal” representa algo legível aos computadores, “explícita” são os conceitos, relações, funções, propriedades, restrições e axiomas explicitamente definidos, “conceitualização” compreende um modelo abstrato de um fenômeno do mundo real, e “compartilhada” representa conhecimento consensual.

No que tange a área tecnológica, a W3C afirma que “*uma ontologia define os termos utilizados para descrever e representar uma área de conhecimento*”. Nesta definição, as ontologias são usadas por pessoas, bancos de dados e aplicativos que precisam compartilhar informações de um determinado domínio. As ontologias incluem definições de conceitos básicos utilizáveis por computadores em um domínio e os relacionamentos entre estas definições. Desta forma, as ontologias codificam o conhecimento em um domínio específico, e também o conhecimento que abrange vários domínios, tonando tal conhecimento reutilizável.

Neste âmbito, apesar da variedade de definições encontradas na literatura, grande parte dessas definições acaba por concluir que o principal objetivo da construção de ontologias é possibilitar que o conhecimento seja compartilhado e reutilizado.

No restante deste capítulo são apresentados os atuais métodos para representação de ontologias e seus inter-relacionamentos, bem como, as vantagens e desvantagens da utilização de cada um dos métodos.

4.1 FORMAS DE REPRESENTAÇÕES DE ONTOLOGIA

4.1.1 RDF

O Resource Description Framework (RDF) pertence à família de especificações da W3C e fornece um modelo de dados para anotações na Web Semântica. O RDF foi construído sob modelos de dados anteriores, como o Dublin Core e o PICS (platform for Internet content

selectivity), de modo que, uma declaração RDF (RDF triple) é sempre escrita da forma:

Sujeito Propriedade Objeto

O RDF permite anotar recursos da Web em termos de propriedades nomeadas. Os valores de propriedades nomeadas (objetos) podem ser URIrefs de recursos da Web ou literais, como por exemplo, representações de valores de dados (tais como inteiros e strings). Um conjunto de declarações RDF é chamado RDF graph. Para representar declarações RDF de uma forma processável por máquina, o RDF define uma sintaxe específica da Linguagem Padronizada de Marcação Genérica (XML), conhecida como DF / XML.

Os recursos RDF-anotados (ou seja, indivíduos) são geralmente nomeados por referências URI's (Uniform Resource Identifier). Estas URIs são strings que identificam recursos da Web.

Uma referência URI (ou URIref) consiste em uma URI em conjunto com um identificador de fragmento opcional no final. Por exemplo, a referência URI http://www.example.org/Elephant#Ganesh consiste no URI http://www.example.org/Elephant e (separado pelo caractere #) o identificador de fragmento Ganesh. Por convenção, os namespaces que são fonte de muitos recursos, são URIs com o caractere #. Por exemplo, http://www.example.org/Elephant# é um namespace. Recursos sem URIrefs são chamados de nós em branco; um nó em branco indica a existência de um recurso, sem mencionar explicitamente o URIref desse recurso (STAAB, S. & STUDER, 2009).

Quadro 1 - Ontologia em RDF

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
@prefix ex: <http://example.org/#>
@prefix elp: <http://example.org/Animal#>
elp:Ganesh ex:mytitle "A resource called Ganesh" ;
ex:mycreator "Pat Gregory" ;
ex:mypublisher : b1 .
: b1 elp:name "Elephant United".
```

4.1.2 RDFS

O RDFS (Resource Description Framework Schema) pode ser visto como uma primeira tentativa para expressar ontologias simples com sintaxe RDF. Em RDFS, os recursos predefinidos rdfs: class, rdfs: Resource e rdf: Property podem ser usados para definir classes

(conceitos), recursos e propriedades (papéis), respectivamente. Ao contrário do Dublin Core, o RDFS não predefine propriedades de informação, mas um conjunto de meta-propriedades que podem ser usados para representar um quadro de premissas em ontologias:

- rdf:type: a instância de um relacionamento
- rdfs:subClassOf: a propriedade que modela a hierarquia subordinação entre as classes.
- rdfs:subPropertyOf: a propriedade que modela a hierarquia subordinação entre propriedades.
- rdfs:domain: a propriedade que restringe todas as instâncias de uma propriedade particular para descrever instâncias de um determinada classe
- rdfs:range: a propriedade que restringe todas as instâncias de uma propriedade particular a ter valores que são instâncias de uma determinada classe.

Quadro 2 - Ontologia em RDFS

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>
@prefix elp: <http://example.org/Animal#>
elp:Animal rdf:type rdfs:Class .
elp:Habitat rdf:type rdfs:Class .
elp:Elephant rdf:type rdfs:Class ; rdfs:subClassOf elp:Animal .
elp: liveIn rdf:type rdf:Property ;
rdfs:domain elp:Animal ; rdfs:range elp:Habitat .
elp:south-sahara rdf:type elp:Habitat .
elp:Ganesh rdf:type elp:Elephant ; elp: liveIn elp:south-sahara .
```

As declarações RDFS são simplesmente RDF triples, não fornecendo restrições sintáticas sobre as mesmas. O Quadro 2 mostra uma ontologia animal em RDFS; ela possui três classes: elp:Animal, elp:Habitat e elp:Elephant (que é uma subclasse de animal - rdfs:subClassOf elp: Animal), uma propriedade elp:liveIn, e os rdfs: domínio e rdfs:range os quais são elp:Animal e elp:Habitat, respectivamente. Além disso, ela afirma que o recurso elp:Ganesh é uma instância de elp:Elefante, e que tal instância elp:liveIn um elp:Habitat chamado elp:south-sahara.

De uma maneira geral, o RDFS é um esquema de linguagem ontológica simples que suporta apenas classes e propriedades

hierarquias, bem como restrições de domínio e alcance para propriedades (STAAB, S. & STUDER, 2009).

4.2 OWL

A expressividade do RDF e do RDF Schema é deliberadamente muito limitada. Essa limitação deve-se ao fato do RDF ser restrito a predicados binários, enquanto o RDF Schema se limita a uma hierarquia de subclasses e propriedades, com as definições de domínio e alcance dessas propriedades. A partir desta constatação, o Grupo de Trabalho sobre Ontologia da W3C (Web Ontology Working Group of W3C) identificou uma série de casos de uso característico de ontologias na Web que exigem muito mais expressividade do que o RDF e o RDF Schema podem proporcionar. Assim surgiu o começo da definição da OWL, a linguagem que se destina a ser a língua padrão – e amplamente aceita na Web Semântica – no desenvolvimento de ontologias.

A W3C Web Ontology Language (OWL) consiste em uma linguagem da web semântica desenvolvida para representar o conhecimento sobre objetos, grupos de objetos e as relações entre os objetos de maneira rica e complexa. (W3C, 2012).

Linguagens ontológicas permitem que usuários escrevam de forma explicita conceptualizações formais de modelos de domínios. Essas conceptualizações devem: ser sintática e semanticamente bem definidas; possuir um eficiente suporte para inferência; possuir um poder de expressividade alto; e proporcionar conveniência em sua expressão. A importância de uma sintaxe bem definida se dá a partir da necessidade do processamento da informação por máquinas. A linguagem OWL é construída sobre o RDF e o RDFS, possuindo o mesmo tipo de sintaxe que seus precursores.

Uma semântica bem definida descreve com precisão o significado do conhecimento, não dando margem a interpretações subjetivas e ambíguas. Desta forma, formalização semântica permite que humanos raciocinem sobre determinado conhecimento.

A semântica é um pré-requisito para o suporte a inferência, permitindo verificar a consistência da ontologia e do conhecimento, buscando verificar as relações entre as classes não intencionais, e automaticamente classificar instâncias em classes. Tais verificações são valiosas na concepção de grandes ontologias, onde vários autores estão envolvidos, e na integração e compartilhamento de ontologias a partir de várias fontes. A semântica formal e o suporte a inferência são normalmente fornecidas através do mapeamento de uma ontologia a um

formalismo lógico conhecido, fazendo uso de motores de inferência (reasoners) automatizados dedicados a estes formalismos. A linguagem OWL é mapeada parcialmente em uma descrição lógica, e faz uso de reasoners como FACT, HERMIT e o RACER (STAAB, S. & STUDER, 2009).

4.2.1 OWL Full

A linguagem OWL completa é chamada de OWL Full e utiliza todas as primitivas existentes em OWL. Ela permite combinar essas primitivas de forma arbitrária com o RDF e o RDF Schema e não requer a disjunção de classes, propriedades, indivíduos e valores de dados. A vantagem da OWL Full está no fato dela ser totalmente compatível com o RDF, tanto sintática quanto semanticamente, ou seja, qualquer documento RDF é também um documento OWL Full. Como desvantagem, a linguagem tornou-se tão poderosa quanto indecidível, não fornecendo garantias para a realização de inferências de maneira eficiente.

4.2.2 OWL DL

A fim de recuperar a eficiência computacional, a OWL DL (Description Logic) é uma sublinguagem da OWL Full que restringe a maneira que os construtores de OWL e RDF podem ser utilizados.

Ela visa alcançar o máximo de expressividade, completude (todas as conclusões são garantidas serem computáveis) e decidibilidade (todas as computações terminarão em um tempo finito) computacional, incluindo todas as construções da linguagem OWL, mas adicionando restrições as mesmas.

A desvantagem do uso da OWL DL está no fato da perda da total compatibilidade com o RDF, ou seja, um documento RDF, em geral, tem que ser estendido em alguns aspectos e restringido em outros antes que seja um documento OWL DL válido.

4.2.3 OWL Lite

A OWL Lite consiste em uma limitação ainda maior da OWL DL, reduzindo-se a um subconjunto dos construtores de linguagem da OWL DL. Como resultado, ela torna-se uma linguagem de fácil entendimento e implementação, mas com expressividade restrita (STAAB, S. & STUDER, 2009).

4.3 SPARQL

A linguagem de consulta SPARQL (SPARQL Protocol and RDF Query Language) é uma recomendação da W3C para consultas em RDF desde 2008, tornando-se a linguagem padrão para este fim. O propósito do SPARQL é permitir que arquivos em formato RDF sejam consultados através de uma linguagem semelhante à SQL, aceitando que o usuário combine dados de diversos arquivos RDF a partir de várias fontes distintas.

4.3.1 Consultas em SPARQL

A linguagem de consulta SPARQL é baseada no casamento de padrões gráficos. O padrão gráfico mais simples é o padrão triplo, que é como um RDF Triple, mas com a possibilidade da existência de uma variável, ao invés de um termo RDF, no lugar do sujeito, do predicado ou do objeto (STAAB & STUDER, 2009).

Quadro 3 - Consulta utilizando SPARQL

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
SELECT ?c WHERE
{ ?c rdf:type rdfs:Class }
```

O Quadro 3 busca todos os padrões de triplas onde a propriedade é do tipo rdf:type e o objeto é igual a rdfs:Class, ou seja, a consulta irá buscar todas as classes existentes no arquivo RDF consultado.

4.4 PROTÉGÉ

O software Protégé Desktop consiste em um ambiente para edição de ontologias que dispõe de diversas funcionalidades. Possui suporte a OWL 2 Web Ontology Language, além de conexões diretamente na memória para *reasoners* (motores de inferência) como o HermiT e o Pellet.

O Protégé Desktop possibilita a criação e edição de uma ou mais ontologias em um único workspace através de uma interface configurável e dispões de inúmeros plug-ins para sua integração com outras aplicações. Através de sua interface, é possível criar uma

ontologia, realizar inferências sobre ela e exportar o resultado em diversos formatos, dentre eles RDF/XML, OWL, OWL-DL, Turtle, etc.

5 TRABALHOS RELACIONADOS

Embora exista um importante número de contribuições no campo de controle de acesso para sistemas distribuídos, alguns temas ainda são relativamente novos, e por esse motivo, não foram completamente explorados em todos seu potencial. O conceito de avaliação dinâmica de risco (RAdAC) é um destes temas.

Neste capítulo são elencados trabalhos que possuem relacionamento com a dissertação apresentada. Os trabalhos são divididos em duas seções, na seção 4.1 estão presentes as contribuições relacionadas ao modelo de controle de acesso RAdAC. Na sessão 4.2 encontram-se os trabalhos que se relacionam com o desenvolvimento de modelos de controle de acesso com auxílio de ontologia.

5.1 MODELOS DE AVALIAÇÃO DINÂMICA DE RISCO

Dentre as principais contribuições no que tange modelos de avaliação dinâmica de risco, foram selecionados os trabalhos que mais estabeleceram correlação com o tema desenvolvido. Desta forma, os trabalhos de Britton & Brown (2007), Saripalli & Walters (2010), Fall et al. (2011), Sharma et al.(2012) e Arias-Barcos et al.(2012) representam o grupo de trabalhos mais importantes e utilizados - direta ou indiretamente - no desenvolvimento desta dissertação.

O trabalho de Britton & Brown (2007) mostra-se a mais importante contribuição para o modelo desenvolvido nesta dissertação. A partir das quantificações e definições de fatores de riscos, o trabalho oferece a base para a criação do modelo aqui apresentado. Britton e Brown (2007) desenvolveram um modelo no qual os fatores que compõe o risco no modelo RAdAC são explicitados e divididos em grupos, atribuindo pesos e estabelecendo definições para cada fator de risco.

A definição de risco utilizada compreende a relação entre probabilidade de ocorrência e consequência de ocorrência de um evento, divididas nos níveis baixa, média e alta. A quantificação dos pesos para cada fator de risco foi realizada por especialistas na área de segurança, e o resultado obtido foram vinte e sete fatores de risco divididos em seis grupos.

Saripalli & Walters (2010) define o risco como uma combinação da probabilidade de ocorrência de um evento que ameace à segurança e o seu grau de severidade, medido como o seu impacto. A partir desta definição, são utilizadas propriedades de confidencialidade, integridade e disponibilidade das ações para realizar o cálculo do risco.

O trabalho de Fall et al. (2011) propõe a utilização do modelo RAdAC com a quantificação de alguns fatores de risco por meio de técnicas de aprendizado de máquina. Algumas situações específicas de risco são apresentadas, mas nenhuma implementação ou simulação é realizada.

Sharma et al.(2012) desenvolveram um modelo de controle de acesso baseado em risco e voltado à aplicações médicas na nuvem *(e-health)*. No trabalho citado, o modelo usado no cálculo do risco baseia-se nos resultados anteriormente obtidos, na probabilidade de ocorrência de um evento e no custo relacionado à disponibilidade, integridade e confidencialidade dos dados. As métricas para o cálculo do risco foram criadas a partir das ações: criar, visualizar, modificar e deletar. Cada uma dessas ações é classificada de acordo com os dados sobre os quais elas estão operando, e o resultado que cada operação pode gerar.

Arias-Barcos et al.(2012) descreve os desafios relacionados com a gerência de identidades federadas em nuvem computacional. A avaliação de risco é utilizada como um método que busca possibilitar a construção de federações de identidades dinâmicas na nuvem. São estabelecidas métricas de segurança para autenticação, confidencialidade, integridade, não-repúdio, responsabilidade, disponibilidade e privacidade. Arias-Barcos et al.(2012) estabelece também, que cada uma das métricas de segurança deve ser aplicada a uma forma de quantificação do risco baseada na probabilidade de ocorrência do evento gerador do risco e o impacto de ocorrência desse evento. Entretanto, o trabalho não apresenta valores numéricos para as métricas citadas, estabelecendo apenas uma descrição semântica dos mesmos.

5.2 MODELOS DE CONTROLE DE ACESSO QUE FAZEM USO DE ONTOLOGIA

O trabalho de Sandhu (2004), aborda a avaliação dinâmica de risco a partir da extensão de componentes do modelo UCON, agrupando características similares entre UCON e RAdAC, e adicionando componentes específicos do modelo RadAC, como o Risk Evaluation e o Access History.

Dersing et al. (2009), por sua vez, desenvolveu um modelo em que usa contextos semânticos – representados com o uso de ontologia - a fim de determinar dinamicamente a atribuição apropriada de papéis para um sistema de gerenciamento de incidentes.

Finin, et al. (2008) estuda a relação entre a Web Ontology Language (OWL) e do Controle de Acesso Baseado em Papéis (RBAC), abordando duas maneiras diferentes para apoiar o modelo RBAC padrão NIST em OWL e, em seguida, discutir como as construções OWL podem ser estendidas para o modelo RBAC ou outros modelos baseados em atributos.

Tsai & Shao (2011) faz uso de ontologia em seu trabalho ao utilizá-la para construir uma hierarquia de papéis para um domínio específico em um modelo RBAC.

Por fim, mas não menos importante, Bernabe et at. (2011) descreve em seu estudo, um modelo de autorização que permite o gerenciamento de diversas funcionalidades como RBAC, hRBAC, cRBAC e HO. Neste ambiente, o modelo de controle de acesso utilizou-se de Web Semântica para descrever o modelo de autorização e as regras de acesso ao conteúdo armazenado na nuvem.

6 MODELO DINÂMICO PARA O CÁLCULO DE RISCO

Este capítulo destina-se a apresentar o modelo para cálculo dinâmico de risco proposto, explicando detalhes de sua arquitetura e funcionamento. As premissas expressas aqui são utilizadas no desenvolvimento do protótipo exposto no capítulo 6.

6.1 O MODELO

O modelo de controle de acesso dinâmico utilizado como base para este trabalho é o RAdAC. No capítulo 2, o modelo RAdAC foi descrito como um modelo capaz de avaliar dinamicamente o risco de acesso a um determinado dado. Entretanto, uma das principais dificuldades para o uso do RAdAC consiste em encontrar uma forma efetiva de cálculo de risco.

Britton & Brown (2007) foram pioneiros ao tentar classificar os componentes do risco em diversos fatores e fornecer métricas para eles. Contudo, em situações reais de requisição de acesso, a disponibilidade de informações sobre os fatores de risco representa um grande problema para o cálculo do risco, à medida que, com a ausência de determinados fatores, o risco pode não ser mensurado corretamente, ou nem ao menos ser calculado.

A Tabela 4 traz os pesos de cada fator de risco definidos por Britton & Brown (2007), enquanto a estrutura geral do modelo desta dissertação é mostrada na Figura 3. O conteúdo mostrado no balão *context* corresponde aos fatores de risco de contexto disponíveis para avaliação do risco de contexto. Os atributos passados nas informações de contexto (*Wired, Admin, Desktop, Browser)* possuem valores definidos pelo provedor de serviço, e devem ser multiplicados pelos pesos dos respectivos fatores de risco (*Connection Type, Role, Machine Type* e *Application*) para o cálculo do risco de contexto.

Entretanto, se esta operação sempre for realizada da mesma forma, diferentes fatores contidos nas informações de contexto irão gerar diferentes valores de risco de contexto para a mesma requisição de acesso. Por exemplo: imagine que durante uma tentativa de acesso a um dado, as informações de contexto disponíveis são apenas: "*Role*: *Admin*; *Machine Type*: *Destkop*; e *Connection Type*: *Wired*". De acordo com a Tabela 4, estes fatores seriam mapeados com os pesos: 2.777778 (*Role*), 2.380952(*Machine Type*) e 2.380952(*Connection Type*). Assumindo-se arbitrariamente que os valores de risco de "*Admin*", "*Desktop*" e "*Wired*", em uma escala de 0 à 10, são respectivamente: 3, 5 e 2, o

cálculo do risco de contexto, de acordo com Britton e Brown(2007) seria definido por: (2. 777778 * 3) + (2.380952 * 5) + (2.380952 * 2) = 24.9999.

A partir do momento em que mais fatores de risco forem conhecidos, o risco de contexto (24.9999) será também alterado, não importando se o contexto manteve-se inalterado e apenas mais informações sobre ele foram obtidas.

O modelo aqui apresentado busca solucionar este problema a partir de um ajuste nos pesos de cada fator a medida em que os mesmos estão disponíveis. Além disso, procura através do uso de ontologia, inferir dinamicamente fatores de risco de contexto que podem ser derivados a partir dos fatores de contexto existentes.

Outro ponto abordado é a composição do risco total não apenas por fatores de risco relacionados ao contexto, mas também às características de segurança da ações e ao histórico do sujeito. Com esta abordagem, a composição do risco torna-se mais completa e coerente, visto que as informações de contexto sozinhas podem não representar todas as características de uma requisição de acesso.

Os seguintes fatores compõem o modelo dinâmico para calcular o risco:

- Contexto: características dos sujeitos que solicitam o acesso, características dos componentes de TI, características dos objetos ou da informação requerida, fatores ambientais, fatores da situação e heurísticas;
- Características de segurança das ações: as características de confidencialidade, integridade e disponibilidade das ações sobre o recurso;
- Histórico do sujeito: o sujeito possui ações prévias no sistema que são guardadas na forma de um histórico para recompensar o bom uso ou penalizar o mau uso do sistema, de acordo com o comportamento prévio do sujeito;

6.1.1 RISCOS DE CONTEXTO

Os riscos de contexto são provenientes dos fatores de risco e seus respectivos pesos determinados no trabalho de Britton & Brown (2007)(Tabela 4), no qual uma quantificação dos pesos dos fatores foi realizada e validada por especialistas.

Britton & Brown(2007) desenvolveram este modelo com intuitos militares, o que é indicado pela presença de alguns dos fatores de riscos levantados, como *Operational Environment Threat Level* e *Specific Mission Role*. Devido ao foco desta dissertação não ser exclusivamente militar, o modelo aqui apresentado utiliza as métricas desenvolvidas por Britton |& Brown (2007) apenas como base, direcionando-se mais à busca e construção de relacionamento entre os fatores de riscos apresentados.

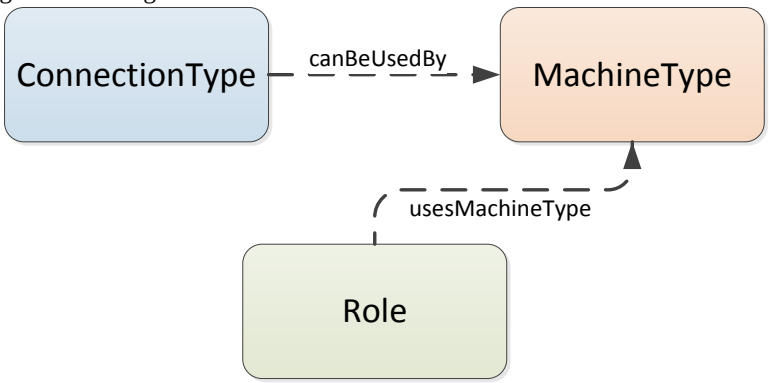
No modelo apresentado nesta dissertação, os inter-relacionamentos propostos entre os fatores de risco podem ser definidos usando-se o conhecimento detalhado sobre a arquitetura e o comportamento do sistema que o provedor de serviço possui (LANDWEHR et al.,2012).

A Fórmula 2 abaixo mostra como é obtido o fator de risco *Role* (Papel) a partir do conhecimento do fator de risco *ConnectionType* (Tipo de Conexão). Nela, sabendo-se que o tipo de conexão usado na requisição é *wireless*, por exemplo, é possível buscar por tipos de máquinas que, no sistema em questão, estão autorizadas a utilizar o tipo de conexão *wireless*. Então, a partir do tipo de máquina encontrado, é possível buscar quais Papéis (*Roles*) usam esse específico tipo de máquina.

Fórmula 2

$$ConnectionType(?d) \wedge MachineType(?m) \wedge canBeUsedBy(?d, ?m) \wedge usesMachineType(?r, ?m) \Rightarrow Role(?r)$$

Figura 2 - Fluxograma da Fórmula 2



Seguindo este modelo de obtenção de fatores de risco, dez regras foram criadas a título de demonstração do funcionamento do modelo proposto nesta dissertação, e são apresentadas na Tabela 3. É importante frisar, que as regras desenvolvidas não são imutáveis, de modo que, cada provedor de acesso pode implementá-las, ampliá-las e modificá-las da maneira como melhor lhe servir.

Tabela 3 - Propriedades de Relacionamento Criadas

Fator de Risco: Atributo	**Propriedade de Relacionamento:**	**Fator de Risco: Atributo**
ConnectionType: Wired	*canBeUsedBy*	MachineType: Desktop
Role: Admin	*usesMachineType*	MachineType: Desktop
MachineType: PDA	*usesConnectionType*	ConnectionType: Wireless
Role: TeamLeader	*hasMinimumEducationLevel*	EducationLevel: Especialist
Role: TeamLeader	*hasMinimumRank*	Rank: E1
Application: Browser	*usesEncryptionLevel*	EncryptionLevel: SSL
TransactionType: Query	*usesApplication*	Application: Database
clearenceLevel: TopSecret	*hasMinimumRole*	Role: TeamLeader
RiskKnowledge: NoneRiskKnowledge	*hasTrustLevel*	TrustLevel: LowTrustLevel
Currentlocation: UnknownLocation	*hasOperationalThreatLevel*	Operational Threat Level: Severe
ClassificationLevel: TopSecret	*hasEncriptionLevel*	EncryptionLevel: PKI

Tabela 4 - Fatores de Risco

Fator de Risco	**Peso**
Characteristics of Requester	16.66667
Role	2.777778
Rank	2.777778
Clearance Level	2.777778
Access Level	2.777778
Previous Violations	2.777778
Education Level	2.777778
Characteristics of IT Components	16.66667
Machine Type	2.380952
Application	2.380952
Connection Type	2.380952
Authentication Type	2.380952
Network	2.380952
QoP/Encryption Level	2.380952
Distance from requester to source	2.380952
Heuristics	16.66667
Risk Knowledge	8.333333
Trust Level	8.333333
Situational Factors	16.66667
Specific Mission Role	3.333333
Time Sensitivity of Information	3.333333
Transaction Type	3.333333
Auditable or Non-auditable	3.333333
Audience Size	3.333333
Environmental Factors	16.66667
Current Location	8.333333
Operational Environment Threat Level	8.333333
Characteristics of Information Requested	16.66667
Classification Level	3.333333
Encryption Level	3.333333
Network Classification Level	3.333333
Permission Level	3.333333
Perishable/ Non-Perishable	3.333333

Fonte - Britton & Brown (2007)

6.1.2 Riscos Considerando as Características de Segurança das Ações

Para o cálculo dos riscos que envolvem confidencialidade, integridade e disponibilidade das ações sobre os recursos, são utilizadas as métricas desenvolvidas no trabalho de Saripalli & Walters (2010). Neste cálculo, o risco é calculado com base no impacto que determinado acesso pode ocasionar, sendo dividido em: impacto baixo (1-5), impacto moderado (6-10) e impacto alto (11-15).

O trabalho de Saripalli & Walters (2010) quantifica a perda de confidencialidade, integridade e disponibilidade em três níveis de impacto baseando-se no efeito e potencial do dano que a perda pode acarretar. No modelo apresentado nesta dissertação, a escala de 1 à 15 corresponde ao risco de confidencialidade, integridade e disponibilidade, podendo ser adaptada com a criação de mais níveis de impacto.

6.1.3 Riscos Considerando o Histórico do Sujeito

Completando os três pilares que compõe o Risco Total de segurança, existe o risco prévio baseado no histórico do sujeito, que compreende uma pontuação correspondente às ações anteriores realizadas pelo sujeito. Ações consideradas negativas incrementam o risco histórico do sujeito, enquanto ações positivas o decrementam.

Neste contexto, o risco baseado no histórico do sujeito é representado em uma escala de 0 à 10, de modo que, após cada tentativa de acesso, o histórico de cada sujeito é atualizado de acordo com o resultado da ação realizada.

6.1.4 Risco Total

A função que calcula o risco total é definida pela Fórmula 3. Os pesos de cada um dos fatores são representados por p1, p2 e p3, respectivamente. Valores possíveis para os pesos poderiam ser 0.5, 0.3 e 0.2, por exemplo, ou qualquer outro valor considerado adequado para o sistema considerado.

Fórmula 3 - Cálculo do Risco Total

Risco Total = *p1 * risco de contexto + p2 * risco considerando confidencialidade, integridade e disponibilidade + p3 * risco prévio considerando histórico do sujeito*

A Fórmula 3 surgiu depois do estudo detalhado dos trabalhos relacionados (SHARMA et al., 2012; SARIPALLI e WALTERS, 2010), e descreve o cálculo do risco de forma concisa considerando um amplo espectro dos fatores envolvidos.

6.2 ESTRUTURA DO MODELO

A infraestrutura do modelo desenvolvido é apresentada na Figura 3. Nele, o usuário solicita à aplicação o acesso a um determinado dado, a aplicação por sua vez, constrói um arquivo XML definindo o contexto, que é composto por um conjunto de atributos utilizado para calcular o risco do acesso do usuário (risco total). A *tag* chamada "Context" representa o conteúdo dessa requisição. No cenário da Figura 3 são considerados os atributos de tipo de conexão (*ConnectionType*), papel do usuário (*Role*), tipo de máquina (*MachineType*) e o tipo de aplicação que está sendo usada no acesso (*Application*) para definir o contexto do acesso a ser considerado no cálculo do risco.

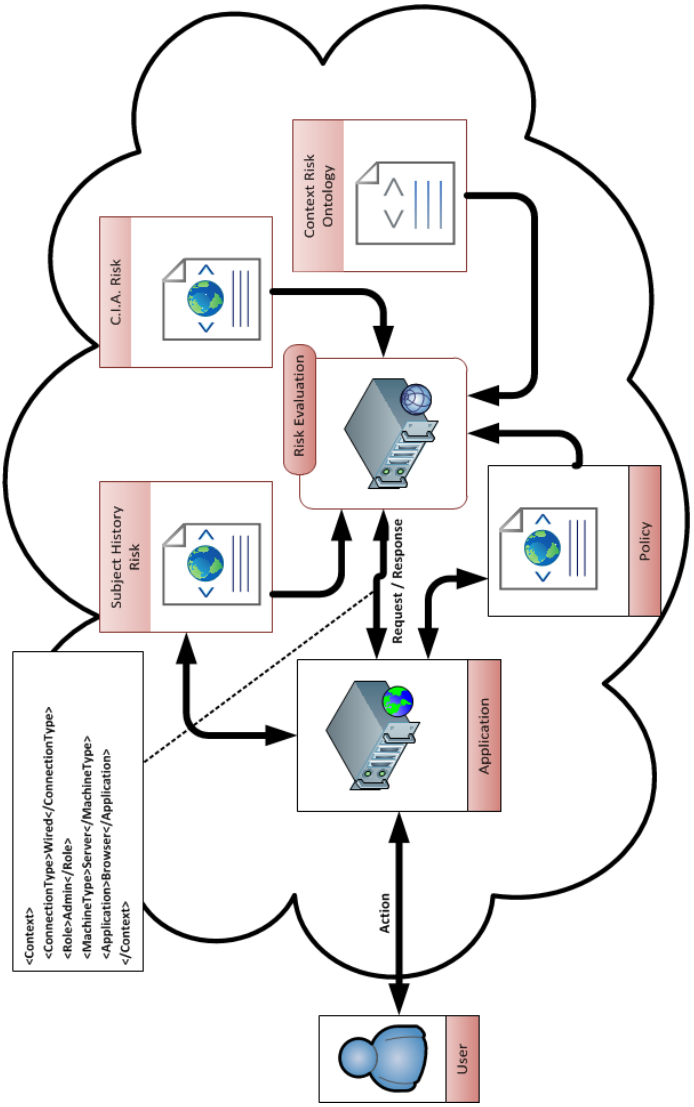
Os fatores de risco envolvidos no cálculo de riscos de confidencialidade, integridade e disponibilidade são mapeados em um arquivo XML separado, chamado de *C.I.A. Risk*, e que é responsável por fornecer o risco considerando a confidencialidade, integridade e disponibilidade das ações. As identidades dos sujeitos e seus respectivos históricos de acesso são armazenadas em outro arquivo chamado *Subject History Risk*. Este arquivo é modificado ao fim de cada requisição de acesso e provê o risco prévio considerando histórico do sujeito.

A ontologia utilizada para inferir fatores de risco de contexto a partir de atributos enviados pela *tag context* é representada por um arquivo OWL chamado de *Context Risk Ontology*.

Por fim, o servidor responsável pela avaliação do Risco, chamado de *Risk Evaluator*, retém as informações contidas nos arquivos XML e realiza as consultas necessárias para extrair as informações contidas na ontologia, realizando os cálculos sobre os fatores de risco disponíveis baseando-se na Fórmula 3.

Entretanto, como a disponibilidade e validação de todos os fatores de risco de contexto em determinados ambientes é complexa, e algumas vezes inaplicável, o modelo apresentado não necessita que todos os fatores sejam fornecidos para realização do cálculo de risco. Levando-se em conta apenas os fatores disponíveis, os pesos de cada fator de contexto são redistribuídos de acordo com a existência dos demais fatores, criando assim, um contexto dinâmico.

Figura 3- Infraestrutura do modelo



7 IMPLEMENTAÇÃO DO MODELO

Neste capítulo é apresentado um protótipo de um sistema de cálculo dinâmico de risco que busca avaliar políticas de controle de acesso de forma dinâmica, utilizando o modelo de controle de acesso RAdAC.

7.1 DESCRIÇÃO DA IMPLEMENTAÇÃO

O modelo proposto foi implementado em três diferentes partes. A primeira parte corresponde a criação da ontologia representando o riscos de contexto, seus fatores de risco e inter-relacionamentos. A segunda parte destina-se a oferecer o suporte para a utilização dos riscos considerando as características de segurança das ações e do histórico do sujeito. A terceira – e mais importante – parte, fornece os métodos para a realização de consultas dinâmicas à ontologia gerada.

A seção 6.2 descreve o processo de criação da ontologia que representa os fatores de risco de contexto. A seção 6.3 apresenta os métodos utilizados na manipulação dos arquivos responsáveis por armazenar as informações referentes aos riscos considerando as características de segurança das ações e o risco baseado no histórico do sujeito. Por fim, a sessão 6.4 demonstra como são realizadas as consultas dinâmicas baseadas nos fatores de risco de contexto conhecidos, e também como os pesos dos fatores são ajustados e o risco final obtido.

A estrutura geral da implementação do modelo é mostrada ao final do capítulo através da Figura 4 e os trechos de código-fonte mostrados nos Apêndices B e C foram escritos na linguagem PHP.

7.2 ONTOLOGIA E FATORES DE RISCO DE CONTEXTO

Uma ontologia escrita em OWL (*Ontology Web Language*) foi criada com o auxílio do software Protégé (PROTÉGÉ, 2013), mapeando todos os fatores de risco em classes e subclasses, atribuindo os pesos definidos por Britton & Brown (2007) a cada classe que representa fatores de risco de contexto.

O resultado deste mapeamento foi a criação de uma ontologia contendo 27 classes, divididas em 6 diferentes grupos. Diversos indivíduos (instâncias) destas classes foram também criadas, com o objetivo de possibilitar a realização de inferências de fatores de risco a partir dos fatores disponíveis e contidos nas informações de contexto.

De acordo com as especificações contidas no trabalho de Britton & Brown (2007), cada classe possui um peso específico que deve ser considerado durante o cálculo do risco. Entretanto, representar estes pesos - que são valores literais - como propriedades das classes em OWL exige um esquema de modelagem chamado *"punning"*. O *punning* permite que objetos sejam mapeados tanto como classes, quanto instâncias, possibilitando que os mesmo sejam validados com base no contexto no qual estão inseridos. No modelo aqui apresentado, todos os fatores de risco são representados também em instâncias, e deste modo, as classes e instâncias que as representam são denotadas com o mesmo URI. Por exemplo, o URI *http://semanticweb.org/marinho/ontologies/2014/risk-ontology#machineType*, representa tanto a classe *machineType*, quanto a instância *machineType*, que possui a *dataProperty Weight* (Peso) com o valor 2.3809 (vide Tabela 4).

Outra importante abordagem realizada, consiste na identificação de sinônimos na composição das instâncias que fazem parte dos fatores de risco de contexto. No modelo de Britton & Brown (2007) os atributos passados como parâmetros para o calculo do risco baseado em fatores são mapeados de forma unitária, ou seja, será necessário estabelecer um valor de risco tanto para o atributo "SSL" quanto para "Secure Socket Layer".

Para solucionar este problema, o modelo proposto neste trabalho oferece a possibilidade de criação de contextos semânticos entre instâncias com nomes distintos, facilitando o processo de criação de políticas de controle de acesso por parte dos provedores de acesso.

Desta forma, as instâncias podem ser atreladas umas as outras com base na propriedade *owl*:*sameAs* (Quadro 4).

Quadro 4 - SameAs Exemplo

```
<rdf:Description rdf:about="#secureSocketLayer">
  <owl:sameAs rdf:resource="#SSL"/>
</rdf:Description>
```

A ontologia gerada pode ser visualizada no Apêndice A em formato OWL, e na Figura 4 ela é representada com o nome de *Context Risk Ontology*.

7.3 RISCO CONSIDERANDO AS CARACTERÍSTICAS DE SEGURANÇA DAS AÇÕES

Para implementar o risco relacionado as características de segurança das ações, um arquivo XML (na Figura 4, chamado de *Subject History Risk XML File*) é utilizado como descritor dos recursos disponíveis para acesso.

Seguindo o modelo de Saripalli & Walters (2011), este arquivo XML possui informações que possibilitam o cálculo do risco a partir da Fórmula 4, na qual o risco é gerado a partir da multiplicação entre a probabilidade de um comprometimento de segurança (P) e o impacto/consequência de um acesso indevido (I).

Fórmula 4 - Cálculo do Risco - Saripalli & Walters (2011)

$$R = P * I$$

A estrutura do arquivo é mostrada de forma simplificada no Quadro 5. A cada requisição de acesso realizada, o arquivo é lido e as informações para o cálculo do risco são obtidas. A *tag* "impact" fornece o impacto do acesso em uma escala de 1 à 15, na qual (1-5) representa um baixo impacto, (6-10) um impacto moderado e (11-15) um alto impacto. As *tags* "*access*" e "*access_violation*" provêm a probabilidade de um comprometimento de segurança. A probabilidade deste comprometimento está diretamente relacionada com o número de tentativas de acesso indevido que um recurso recebe. No modelo aqui apresentado, o impacto é calculado dividindo-se o número de acessos (*access)* pelo número de tentativas de violação de acesso *(acess_violation)*. A partir das informações contidas no Quadro 5, o valor do risco considerando as características de segurança das ações é calculado na Fórmula 5.

Fórmula 5 - Exemplo de Cálculo do Risco

$$R= (5/20)*10 => R= 2.5$$

Quadro 5 - Estrutura do Arquivo XML destinado ao Risco - Recursos

```
<?xml version="1.0"?>
 <files>
  <file>
   <file_path>/home/files/secret.txt</file_path>
   <impact>10</impact>
   <access>20</access>
   <access_violation>5</access_violation>
  </file>
 </files>
```

No Apêndice C é exibida a função que realiza a incrementação no número de acessos ao final do processo de requisição de acesso. A classe fileClass é responsável pelas alterações no arquivo XML no que tange os recursos disponíveis para acesso. Além da função mencionada, existem ainda funções para incrementar violações de acesso, alterar o nível de impacto, cadastrar novos arquivos, excluir arquivos e ler o conteúdo das informações sobre os arquivos que deseja-se calcular o risco de acesso.

7.4 RISCO PRÉVIO BASEADO NO HISTÓRICO DO SUJEITO

A implementação do risco baseado no histórico do sujeito segue basicamente a mesma metodologia utilizada na seção anterior.

Um arquivo XML (na Figura 4, chamado de *C.I.A XML File*) é utilizado para mapear os sujeitos que realizam requisições de acesso ao sistema e seus históricos de acesso. O Quadro 6 apresenta a estrutura desse arquivo, contendo, o nome do usuário, que deverá ser único, e sua classificação de segurança *(rate)*.

Quadro 6 – Estrutura do arquivo XML destinado ao Risco - Sujeitos

```
<?xml version="1.0"?>
 <users>
  <user>
   <name>Username</name>
   <rate>5</rate>
  </user>
 </users>
```

Ao final de cada acesso este arquivo deve ser atualizado pelo provedor de serviço, alterando a classificação de segurança do sujeito após o término da utilização do recurso. O Apêndice B apresenta um trecho da classe *userClass*, responsável por manipular os dados referentes ao risco do histórico do sujeito.

7.5 CONSULTAS DINÂMICAS E O RISCO TOTAL

A partir dos fatores de risco de contexto fornecidos durante uma requisição de acesso, uma ou mais consultas são montadas dinamicamente de acordo com o número de fatores de risco disponíveis e quais demais fatores deseja-se descobrir.

Para que essa abordagem funcione corretamente, o provedor de acesso deve possuir um mapeamento prévio que informe sobre quais fatores possuem inter-relacionamentos e quais as propriedades que fornecem esses inter-relacionamentos.

O Quadro 7 apresenta um exemplo de consulta criada dinamicamente para descobrir mais fatores de risco e buscar os pesos de todos os fatores e valores dos atributos passados no contexto.

A consulta é montada em partes de acordo com os atributos passados para a avaliação do risco de contexto. No Quadro 7 a busca é realizada a partir dos atributos disponíveis *Desktop*, *Http* e *Phd*. A partir destes atributos são procurados os pesos dos fatores de risco dos quais eles pertencem, juntamente com os valores de risco dos atributos.

No terceiro trecho do Quadro 7 o atributo *Wired* é usado para buscar novos atributos e fatores de risco. A partir da propriedade *canBeUsedBy* que indica qual tipo de máquina pode utilizar determinado tipo de conexão, e a propriedade *usesMachineType* que aponta os tipos de usuário *(Roles)* que usam certo tipo de máquina, é possível buscar atributo(s) do tipo *Role*, seus valores de risco, e o peso do fator de risco *Role*.

Quadro 7 - Construção das Consultas

```
PREFIX risk:
<http://www.semanticweb.org/marinho/ontologies/2014/risk-
ontology#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX rdfs:< http://www.w3.org/2000/01/rdf-schema#>
SELECT ?riskFactor ?weight ?value
```

```
WHERE {
    {risk:Desktop a ?riskFactor.
    ?riskFactor risk:weight ?weight.
    risk:Desktop risk:value ?value}
```

```
UNION
    { risk: Wired risk:canBeUsedBy ?MachineTypeRiskAtribute.
    ?riskAtribute risk:usesMachineType ?MachineTypeRiskAtribute.
    ?riskAtribute a ?riskFactor .
    ?riskFactor risk:weight ?weight.
    ?riskAtribute risk:value ?value}
```

```
UNION
```

```
        {risk:Wired a ?riskFactor .
        ?riskFactor risk:weight ?weight.
        risk:Wired risk:value ?value}
UNION
        {risk:Phd a ?riskFactor .
        ?riskFactor risk:weight ?weight.
        risk:Phd risk:value ?value}
```

É importante salientar, que de acordo com a estrutura do modelo proposto (Figura 3), as informações de contexto são disponibilizadas em um arquivo no formato XML no qual os fatores de risco e atributos de risco estão contidos. Entretanto, devido a classificação dos atributos de risco em instâncias das classes que representam fatores de risco, não é necessário que seja explicitado à qual fator de risco um atributo de risco pertence, uma vez que, caso esse atributo seja único e não pertença a mais de um fator de risco, o mesmo será automaticamente inferido como instância da classe de seu respectivo fator de risco.

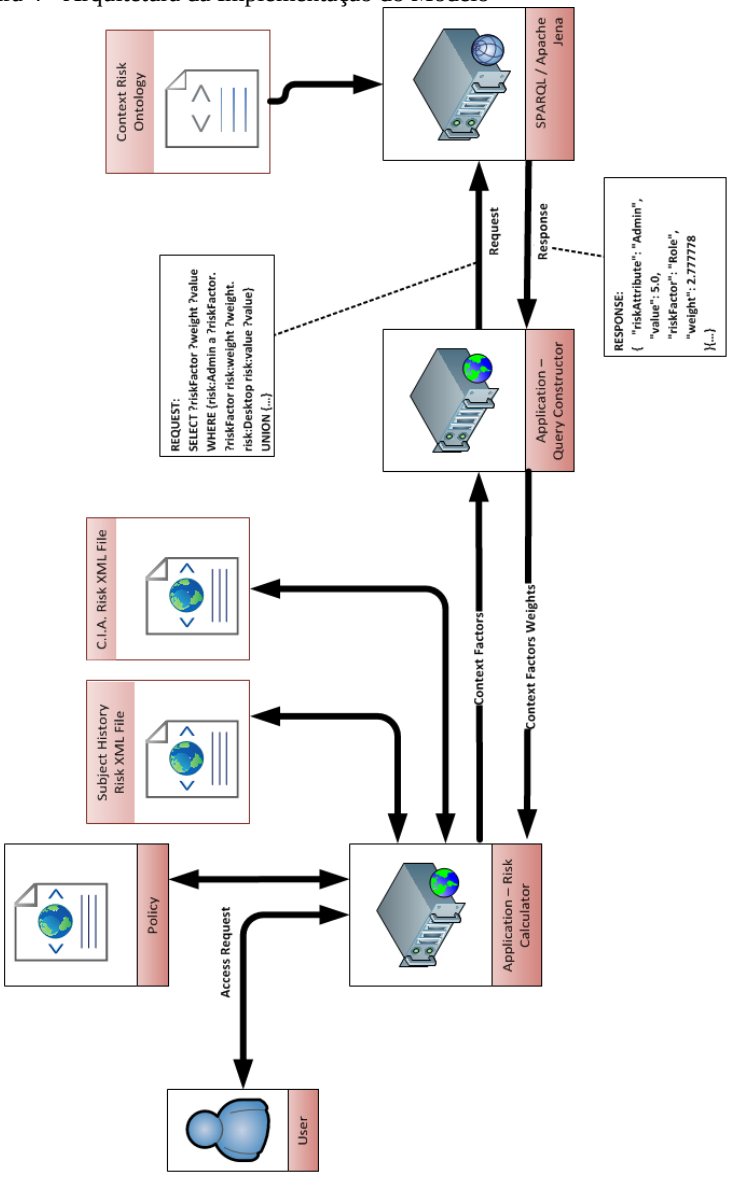
Outra abordagem proposta pelo presente modelo consiste na especificação dos fatores de risco descritos por Britton & Brown (2007) em subfatores. Desta forma, o fator de risco *authenticationType*, por exemplo, pode ser subdividido em *secureAuthenticationType* e *normalAuthenticationType*. O Quadro 8 mostra um modelo de consulta no qual, a partir do atributo *UsernameAndPassword*, é possível inferir o tipo de aplicação (*Application)* que utiliza este atributo.

Quadro 8 - Consulta utilizando Subfatores

```
PREFIX risk:
 <http://www.semanticweb.org/marinho/ontologies/2014/risk-
ontology#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>

SELECT ?riskFactor ?weight ?value ?atribute
WHERE
        { risk:UsernameAndPassword a ?risksubFactor.
        ?risksubFactor rdfs:subClassOf ?riskFactor.
        ?atribute risk:usesAuthenticationType ?risksubFactor .
        ?riskFactor risk:weight ?weight.
        ?atribute risk:value ?value}
```

Figura 4 - Arquitetura da Implementação do Modelo



De acordo com a Figura 4, as consultas à ontologia são realizadas através da biblioteca SPARQL contida no framework Apache Jena. O resultado desta consulta é retornado à aplicação em formato JSON e transformado em objetos. Os resultados são parseados e os pesos dos fatores de risco localizados são reajustados de acordo com o número de fatores de risco encontrados.

Definindo formalmente, o peso ajustado (P_A) de cada fator de risco (x) corresponde ao somatório de todos os pesos de fatores de riscos (P_T), divido pelo somatório de fatores de risco disponíveis (P_F), multiplicado por seu próprio peso.

Fórmula 6 - Redistribuição de Pesos dos Fatores de Risco

$$P_A(x)=\left(\frac{\sum P_T}{\sum P_F}\right) P_F(x)$$

Por exemplo, caso estejam disponíveis apenas as informações sobre os fatores de risco do grupo *Characteristics of Requester*, o peso de cada fator desta classe (2.7777) é multiplicado em razão do percentual que esses fatores representam no cálculo total do risco:

Fórmula 7 - Exemplo de Redistribuição de Pesos dos Fatores de Risco

100 (Somatório total dos fatores de risco) / 16.6666 (somatório dos fatores de risco disponíveis) * 2. 7777 = 16.6666

Desta forma o novo peso ajustado para cada fator da grupo *Characteristics of Requester* é 16.6666.

Ao fim do ajuste, os valores dos atributos de contexto, que são fornecidos pela política implementada para o sistema (chamada de *Policy* na Figura 4) são multiplicados pelos pesos dos seus respectivos fatores de risco. Todos os valores de risco são então somados, formando o Risco de Contexto.

De acordo com a Fórmula 3, o Risco de Contexto deverá ser adicionado ao Risco considerando as características de segurança das ações (Seção 6.2) e ao Risco baseado no histórico do sujeito (Seção 6.3) para o cálculo do Risco Total.

8 RESULTADOS EXPERIMENTAIS

Este capítulo destina-se a apresentar os testes realizados com base no modelo de cálculo de risco descrito nesta dissertação. A formação do risco de contexto de maneira dinâmica é o principal tema do capítulo, no qual, diferentes cenários são mostrados com o objetivo de comparar a medição do risco em diferentes situações.

A Tabela 5 fornece um cenário no qual todos os fatores de risco de contexto são conhecidos, e dessa forma, a ontologia é utilizada apenas para buscar os pesos de cada fator de risco e os valores de cada atributo passado através do contexto.

Tabela 5 - Cenário 1 – Todos os Fatores Disponíveis

Fator de Risco	**Peso**	**Atributo**	**Valor**
Characteristics of Requester	16.66667		
Role	2.777778	TeamLeader	7
Rank	2.777778	E3	8
Clearance Level	2.777778	Secret	4
Access Level	2.777778	No	10
Previous Violations	2.777778	No	0
Education Level	2.777778	Phd	2
Characteristics of IT Components	16.66667		
Machine Type	2.380952	PDA	10
Application	2.380952	Database	4
Connection Type	2.380952	Wireless	8
Authentication Type	2.380952	User/Password	7
Network	2.380952	Internet	9
QoP/Encryption Level	2.380952	WEP	5
Distance from requester to source	2.380952	10000km	8
Heuristics	16.66667		
Risk Knowledge	8.333333	None	10
Trust Level	8.333333	Low	9
Situational Factors	16.66667		
Specific Mission Role	3.333333	SuportTeam	2
Time Sensitivity of Information	3.333333	Needed Now	2
Transaction Type	3.333333	Query	2

Auditable or Non-auditable	3.333333	Auditable	2
Audience Size	3.333333	SinglePerson	2
Environmental Factors	16.66667		
Current Location	8.333333	Unknown	10
Operational Environment Threat Level	8.333333	Severe	10
Characteristics of Information Requested	16.66667		
Classification Level	3.333333	TopSecret	10
Encryption Level	3.333333	PKI	1
Network Classification Level	3.333333	JWICS	9
Permission Level	3.333333	ReadOnly	9
Perishable/ Non-Perishable	3.333333	NonPerishable	9

Com todos os fatores disponíveis, o risco de contexto calculado para o cenário 1 foi de 692.5, em uma escala que vai de 0 à 1000.

Para calcular a efetividade do modelo proposto nesta dissertação, foram excluídos alguns fatores de contexto, conforme mostrado na Tabela 6. Deste modo, a partir das informações disponíveis, três diferentes abordagens foram realizadas buscando mensurar o risco de contexto. Primeiramente, o risco de contexto foi calculado apenas com base dos fatores de risco disponíveis. Depois, o risco de contexto foi calculado com base na redistribuição dos pesos de cada fator de risco de acordo com a Fórmula 6. Por fim, o risco foi calculado utilizando a redistribuição de pesos e também os métodos de inferência de fatores de risco mostrados na Tabela 3.

Tabela 6 - Cenário 2 - Alguns Fatores de Risco Disponíveis

Fator de Risco	Peso	Atributo	Valor
Characteristics of Requester	16.66667		
Role	2.777778	TeamLeader	7
Rank	2.777778	E3	8
Clearance Level	2.777778	Secret	4
Access Level	2.777778	???	?
Previous Violations	2.777778	???	?
Education Level	2.777778	???	?
Characteristics of IT Components	16.66667		
Machine Type	2.380952	PDA	10
Application	2.380952	???	?

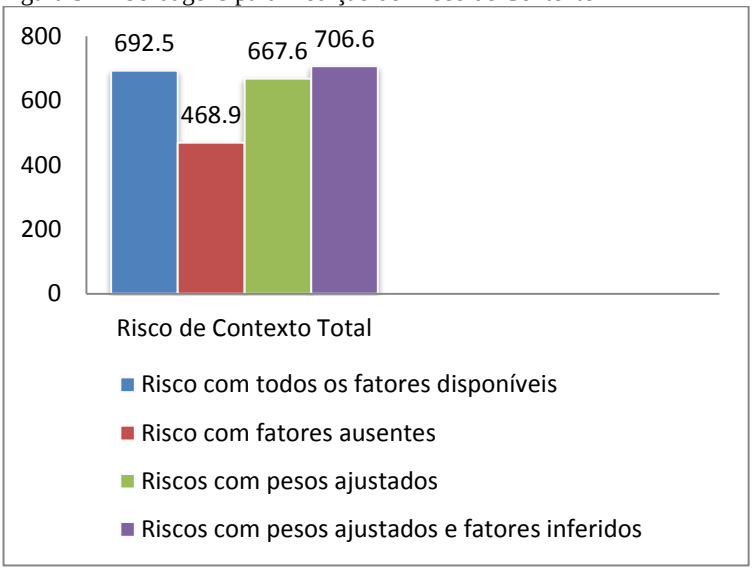
Connection Type	2.380952	???	?
Authentication Type	2.380952	User/Password	7
Network	2.380952	Internet	9
QoP/Encryption Level	2.380952	WEP	5
Distance from requester to source	2.380952	10000km	8
Heuristics	16.66667		
Risk Knowledge	8.333333	None	10
Trust Level	8.333333	???	?
Situational Factors	16.66667		
Specific Mission Role	3.333333	SuportTeam	2
Time Sensitivity of Information	3.333333	Needed Now	2
Transaction Type	3.333333	Query	2
Auditable or Non-auditable	3.333333	Auditable	2
Audience Size	3.333333	SinglePerson	2
Environmental Factors	16.66667		
Current Location	8.333333	Unknown	10
Operational Environment Threat Level	8.333333	???	?
Characteristics of Information Requested	16.66667		
Classification Level	3.333333	TopSecret	10
Encryption Level	3.333333	PKI	1
Network Classification Level	3.333333	JWICS	9
Permission Level	3.333333	ReadOnly	9
Perishable/ Non-Perishable	3.333333	NonPerishable	9

O resultado de cada uma das abordagens pode ser visualizado na Figura 5. Como esperado, o risco de contexto foi menor quando menos fatores estavam disponíveis: 468.9. A partir do reajuste dos pesos dos fatores de risco de contexto, o risco de contexto assemelhou-se ao risco mensurado quando todos os fatores de risco de contexto estavam disponíveis (667.6).

Ao realizar a abordagem completa, que representa o modelo de cálculo de risco de contexto proposto nessa dissertação, o risco de contexto final ficou bem próximo ao risco-base (que é o risco mensurado quando todos os fatores de risco estão disponíveis). O motivo do risco de contexto com pesos ajustados e fatores inferidos ser maior do que o risco-base reside no fato da inferência TeamSpecialist

hasMinimumEducationLevel Especialist ter aumentado o risco do fator *Characteristics of Requester*, uma vez que, no cenário 1, o atributo do fator de Risco *Role* era *Admin*, que possui um valor de risco menor do que *Especialist*.

Figura 5 - Abordagens para medição do Risco de Contexto



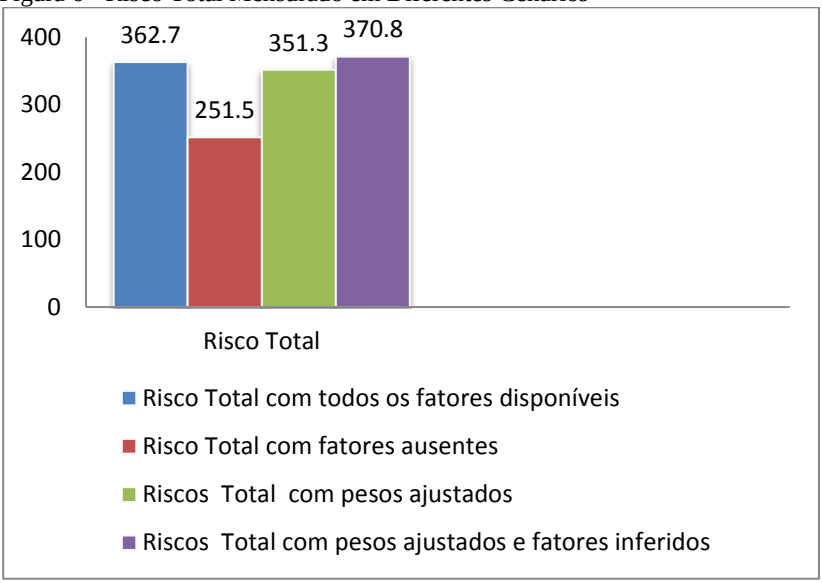
Ao fim do processo para obtenção do risco de contexto em cada cenário, o risco de contexto mensurado é utilizado na composição do risco total, conforme indicado na Fórmula 3.

Para todos os cenários foram usados os mesmos riscos considerando confidencialidade, integridade e disponibilidade, e riscos considerando o histórico do sujeito expostos nos Quadro 5 e Quadro 6. Entretanto, os valores de riscos obtidos nos dois tipos de risco supracitados foram multiplicados por 10 para que ficassem na mesma escala do risco de contexto aferido nos cenários apresentados.

Risco Total = *0.5 * risco de contexto + 0.3 * (2.5*10) + 0.2 * (5*10)*

Os valores do Risco Total para cada cenário são exibidos na Figura 6.

Figura 6 - Risco Total Mensurado em Diferentes Cenários



8.1 CENÁRIO REDUZIDO

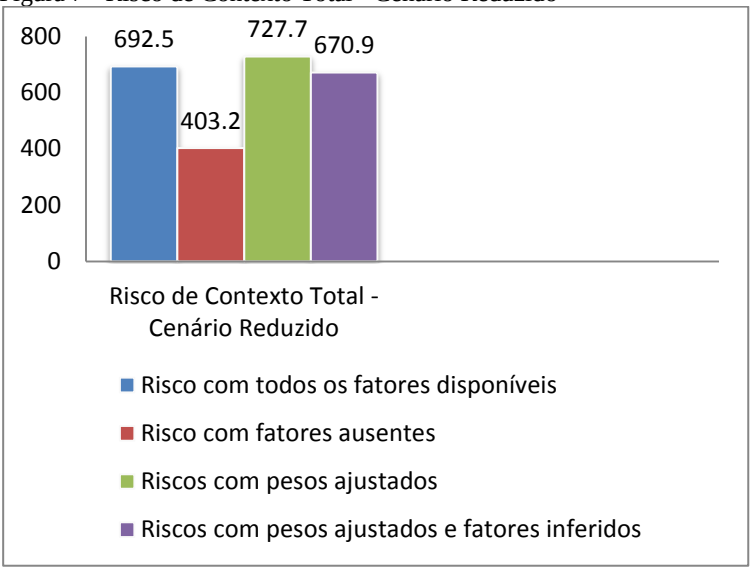
Com o intuito de validar o conjunto mínimo de fatores de risco que devem estar disponíveis na geração do cálculo de risco, um cenário foi criado a partir de um número reduzido de fatores de risco. Nessa abordagem, optou-se por estabelecer que, no mínimo cinquenta porcento dos fatores de risco de cada grupo de risco devem estar disponíveis para a correta aplicação das inferências e métricas. Dessa forma, a probabilidade de eventuais desvios sobre o peso original dos fatores de risco pode ser minimizada, corroborando assim, para que o cálculo do risco total mantenha uma escala uniforme. A Tabela 6 apresenta os fatores disponíveis no cálculo de risco do Cenário 4 (Cenário Reduzido), enquanto a Figura 7 compara o cenário reduzido com os demais cenários mensurados anteriormente.

Tabela 6 - Cenário 4 – Mínimo de Fatores de Risco Disponíveis

Fator de Risco	Peso	Atributo	Valor
Characteristics of Requester	16.66667		
Role	2.777778	TeamLeader	7
Rank	2.777778	E3	8
Clearance Level	2.777778	Secret	4

Access Level	2.777778	???	?
Previous Violations	2.777778	???	?
Education Level	2.777778	???	?
Characteristics of IT Components	16.66667		
Machine Type	2.380952	PDA	10
Application	2.380952	???	?
Connection Type	2.380952	???	?
Authentication Type	2.380952	User/Password	7
Network	2.380952	Internet	9
QoP/Encryption Level	2.380952	WEP	5
Distance from requester to source	2.380952	???	8
Heuristics	16.66667		
Risk Knowledge	8.333333	None	10
Trust Level	8.333333	???	?
Situational Factors	16.66667		
Specific Mission Role	3.333333	SuportTeam	2
Time Sensitivity of Information	3.333333	Needed Now	2
Transaction Type	3.333333	Query	2
Auditable or Non-auditable	3.333333	???	2
Audience Size	3.333333	???	2
Environmental Factors	16.66667		
Current Location	8.333333	Unknown	10
Operational Environment Threat Level	8.333333	???	?
Characteristics of Information Requested	16.66667		
Classification Level	3.333333	???	10
Encryption Level	3.333333	???	1
Network Classification Level	3.333333	JWICS	9
Permission Level	3.333333	ReadOnly	9
Perishable/ Non-Perishable	3.333333	NonPerishable	9

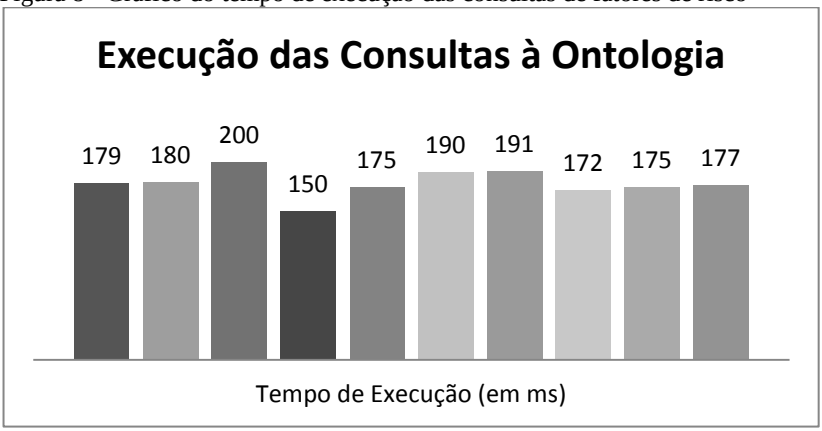
Figura 7 - Risco de Contexto Total - Cenário Reduzido



8.2 AVALIAÇÃO DE DESEMPENHO

Um benchmark (Figura 8) sobre o tempo de execução das consultas que buscam por fatores de risco de contexto dentro da ontologia foi realizado. Esse benchmark visou mensurar o tempo de avaliação do cálculo de risco e sua computabilidade. O computador utilizado foi um Intel Core 2 Quad 3.2 Ghz, com 4Gb de memória RAM 1333mhz.

Figura 8 - Gráfico do tempo de execução das consultas de fatores de risco



9 CONCLUSÃO

Com a criação de novos modelos de controle de acesso como o RAdAC, surgiu a necessidade de novas abordagens para tratar o acesso a ambientes dinâmicos e diferentes.

A possibilidade de estabelecer métricas para o cálculo de risco de acesso através de ontologias no modelo RAdAC, permite uma ampliação do espectro de utilização deste modelo de controle de acesso, uma vez que, em diferentes ambientes, os fatores de risco não estão presentes da mesma forma.

A implementação desenvolvida em um ambiente de computação em nuvem provê um modelo para avaliação dinâmica do risco na forma de um protótipo. Vários outros testes são necessários para realizar inferências em tempo real com um número maior de dados.

As contribuições científicas deste trabalho que podem ser citadas são: (a) uma forma quantitativa de cálculo de risco considerando os aspectos de contexto, características de segurança (confidencialidade, integridade e disponibilidade) e histórico do sujeito; (b) desenvolvimento de uma ontologia para prover o controle de acesso flexível e dinâmico baseado no RAdAC.

O aspecto dinâmico e flexível do modelo proposto existe porque mesmo em ambientes onde os fatores de risco e seus pesos sejam conhecidos, o cálculo do Risco Total não depende estritamente que todos os fatores sejam conhecidos no momento do acesso. Como benefício, um valor informando o risco mensurado sempre será obtido, restando aos desenvolvedores do modelo, desenvolver políticas de controle de acesso determinando quais fatores de risco são obrigatórios para a validação do cálculo realizado.

Nos trabalhos relacionados descritos no capítulo 4, o artigo de Arias-Cabarcos et al. (2012) não apresenta valores numéricos para as métricas ou como esses valores devem ser obtidos, apenas uma descrição semântica de cada métrica. Em SANTOS et al., (2013) políticas de risco na forma de arquivos XML usam diferentes métricas de risco mas o administrador ou usuário devem explicitar os métodos de quantificação. O trabalho de Britton & Brown (2007) apresenta a ideia de cálculo usada como base na fórmula proposta neste artigo. No trabalho de Farroha e Farroha (2012) o cálculo em tempo real do risco de segurança para cada decisão de acesso é citado como desafio para a implementação do modelo RAdAC. Características de confidencialidade, integridade e disponibilidade também foram consideradas nos trabalhos de (SHARMA et al., 2012; SARIPALLI e

WALTERS, 2010). No trabalho de Dersingh (2009), ontologias são usadas para atribuir papéis de forma dinâmica. Entretanto, nenhum dos trabalhos relacionados usa ontologias para tornar flexível o cálculo de risco em contextos dinâmicos, compostos por métricas ou variáveis diferentes.

Dentre os trabalhos futuros que podem ser citados está a implementação de um software de controle de acesso voltado para o ambiente Web voltado à realização de testes e medições de desempenho adaptando e refinando o modelo proposto neste trabalho.

REFERÊNCIAS

ARIAS-CABARCOS, P. et al. A metric-based approach to assess risk for “on cloud” federated identity management. Journal of Network and Systems Management, v. 20, n. 4, p. 513–533, 2012.

BERNABE, JORGE BERNAL; PEREZ, JUAN M.MARIN; CALERO, JOSE M.ALCARAZ; CLEMENTE, FELIX J.GARCIA; PEREZ, GREGORIO MARTINEZ; SKARMETA, ANTONIO F.GOMEZ, "Towards an authorization system for cloud infrastructure providers,"Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on , vol., no., pp.333,338, 18-21 Jul 2011

BORST, W. Construction of Engineering Ontologies for Knowledge Sharing and Reuse. PhD thesis, University of Twente, P.O. Box 217 - 7500 AE Enschede - The Netherlands, 1997.

BREITMAN, K. K.; LEITE, J. C. S. P.. Ontologias–Como e porque criá-las. Anais do Simpósio Brasileiro de Computação, XXIII JAI - Jornada de Atualização em Informática, 2004.

BRITTON, D. W., BROWN, I. A. A Security Risk Measurement for The RAdAC Model. 2007. Master Thesis, Naval Postgraduate School, USA, 2007. [Online]. Disponível em: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467180.

CHOUDHARY, R. A policy based architecture for NSA radac model. In: IEEE Information Assurance Workshop - IAW ’05, 6th edition, Estados Unidos, Proceedings… IEEE: IEEE Press, 2005. p. 294–301.

DERSINGH, A.; LISCANO, R.; JOST, A.; FINNSON, J., "Dynamic Role Assignment Using Semantic Contexts," Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conference on , vol., no., pp.1049,1054, 26-29 May 2009.

DIEP, N. N. et al. Contextual risk-based access control. In: Security and Management. [S.l.: s.n.], 2007. p. 406–412.

FARROHA, B.; FARROHA, D. Challenges of operationalizing dynamic system access control: Transitioning from abac to radac. In: 2012 IEEE International Systems Conference (SysCon), [S.e], Vancouver, Canada, Proceedings…IEEE: IEEE Press, 2012. p. 1–7.

FALL, D. et al. Toward Quantified Risk-Adaptive Access Control for Multi-tenant Cloud Computing. In: Proceedings of the 6th Joint Workshop on Information Security (JWIS2011), 2011.

FININ, T.; JOSHI, A.; KAGAL, L.; NIU, J.; SANDHU, R.; WINSBOROUGH, W.; THURAISINGHAM, B. ROWLBAC: representing role based access control in OWL. In: 13th ACM symposium on Access control models and technologies, 13th edition, Estados Unidos. Proceedings ACM: ACM Press, 2008. p 73-82.

GIL, A. Métodos e técnicas de pesquisa social. 3. ed. São Paulo: Atlas, 1991. 207 p.

GRUBER, T. A translation approach to portable ontologies. Knowledge Acquisition, 5(2):199-220, 1993.

GRUBER, T. What is an ontology. 2007. [Online] Disponível em: http://tomgruber.org/writing/ontology-definition-2007.htm

HAI-BO SHEN; FAN HONG, "An Attribute-Based Access Control Model for Web Services," Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on, vol., no., pp.74,79, Dez. 2006

JAEHONG, P; SANDHU, R;. 2004. “The UCON ABC usage control model.” ACM Trans. Inf. Syst. Secur. 7, 1 Fev 2004.

JAEHONG PARK; SANDHU, R., "Originator control in usage control," Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on , vol., no., pp.60,66, 2002

JASON Program Office. Horizontal Integration: Broader Access Models for Realizing Information Dominance. [S.l.], 2004. [Online]. Disponível em: http://www.fas.org/irp/agency/dod/jason/classpol.pdf.

JUNG, C. Metodologia Científica: Ênfase em pesquisa tecnológica. 2004 [Online]. Disponível em: http://www.jung.pro.br.

JUNLI ZHU; QIAOYAN WEN, "SaaS Access Control Research Based on UCON," Digital Home (ICDH), 2012 Fourth International Conference on , vol., no., pp.331,334, 23-25 Nov. 2012

KANDALA, S.; SANDHU, R.; BHAMIDIPATI, V., "An Attribute Based Framework for Risk-Adaptive Access Control Models," Availability, Reliability and Security (ARES), 2011 Sixth International Conference on , vol., no., pp.236,241, 22-26 Ago 2011

KARP, Alan H.; HAURY, Harry; DAVIS, Michael H. From ABAC to ZBAC: the evolution of access control models. Hewlett-Packard Development Company, LP, v. 21, 2009.

McGRAW, Robert W. Risk-Adaptable Access Control (RAdAC). In: NIST Privilege (Access) management Workshop, [s.e.], USA. NIST: Set. 2009. [Online]. Disponível em: http://csrc.nist.gov/news_events/privilege-management-workshop/radac-Paper0001.pdf.

PROTÉGÉ. Protégé-owl api. 2013. [Online]. Disponível em: http://protege.stanford.edu/plugins/owl/api

SAMARATI, P.; VIMERCATI, S. de. Access control: Policies, models, and mechanisms. In: FOCARDI, R.; GORRIERI, R. (Ed.). Foundations of Security Analysis and Design. [S.l.: s.n.], 2001, (Lecture Notes in Computer Science, v. 2171). p. 137–196.

SANTOS, D. R.; WESTPHALL, C.M.; WESTPHALL, C.B. Risk-based Dynamic Access Control for a Highly Scalable Cloud Federation". In: SECURWARE 2013 - The Seventh International Conference on Emerging Security Information, Systems and Technologies, 7th edition, Barcelona. Proceedings IARIA: XPS Press, 2013. pp. 8 – 13.

SARIPALLI, P.; WALTERS, B. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In: 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), 3 rd edition,

USA. Proceedings... IEEE: IEEE Press, 2010. pp. 280-288. doi: 10.1109/CLOUD.2010.22.

SHARMA, M. et al. Using risk in access control for cloud-assisted ehealth. In: High Performance Computing and Communication 2012 - IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 9th edition, USA. Proceedings. IEEE: IEEE Press, 2012. p. 1047–1052

SILVA, E.; E. MENEZES. Metodologia da Pesquisa e Elaboração de Dissertação. Laboratório de Ensino a Distância da UFSC, 2001.

STAAB, S. & STUDER, R. Handbook on Ontologies (2nd ed.). Springer Publishing Company, Incorporated, 2009.

WEI-TEK TSAI; QIHONG SHAO, "Role-Based Access-Control Using Reference Ontology in Clouds," Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on , vol., no., pp.121,128, 23-27 Mar 2011

APÊNDICE A – Ontologia Desenvolvida

```
<?xml version="1.0"?>


<!DOCTYPE Ontology [
    <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#" >
    <!ENTITY xml "http://www.w3.org/XML/1998/namespace" >
    <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#" >
    <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#" >
]>


<Ontology xmlns="http://www.w3.org/2002/07/owl#"
     xml:base="http://www.semanticweb.org/marinho/ontologies/2014/risk-
ontology"
     xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
     xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
     xmlns:xml="http://www.w3.org/XML/1998/namespace"
     ontologyIRI="http://www.semanticweb.org/marinho/ontologies/2014/risk-
ontology">
    <Prefix name="" IRI="http://www.w3.org/2002/07/owl#"/>
    <Prefix name="owl" IRI="http://www.w3.org/2002/07/owl#"/>
    <Prefix name="rdf" IRI="http://www.w3.org/1999/02/22-rdf-syntax-ns#"/>
    <Prefix name="xsd" IRI="http://www.w3.org/2001/XMLSchema#"/>
    <Prefix name="rdfs" IRI="http://www.w3.org/2000/01/rdf-schema#"/>
    <Prefix name="risk-owl"
IRI="http://www.semanticweb.org/marinho/ontologies/2014/risk-ontology#"/>
    <Declaration>
        <Class IRI="#accessLevel"/>
    </Declaration>
    <Declaration>
        <Class IRI="#application"/>
    </Declaration>
    <Declaration>
        <Class IRI="#audienceSize"/>
    </Declaration>
    <Declaration>
        <Class IRI="#auditableOrNonAuditable"/>
    </Declaration>
    <Declaration>
        <Class IRI="#authenticationType"/>
    </Declaration>
    <Declaration>
```

```
    <Class IRI="#characteristicsOfInformationRequested"/>
  </Declaration>
  <Declaration>
    <Class IRI="#characteristicsOfItComponents"/>
  </Declaration>
  <Declaration>
    <Class IRI="#characteristicsOfRequester"/>
  </Declaration>
  <Declaration>
    <Class IRI="#classificationLevel"/>
  </Declaration>
  <Declaration>
    <Class IRI="#clearanceLevel"/>
  </Declaration>
  <Declaration>
    <Class IRI="#connectionType"/>
  </Declaration>
  <Declaration>
    <Class IRI="#currentLocation"/>
  </Declaration>
  <Declaration>
    <Class IRI="#distanceFromRequesterToSource"/>
  </Declaration>
  <Declaration>
    <Class IRI="#educationLevel"/>
  </Declaration>
  <Declaration>
    <Class IRI="#encryptionLevel"/>
  </Declaration>
  <Declaration>
    <Class IRI="#environmentalFactors"/>
  </Declaration>
  <Declaration>
    <Class IRI="#heuristics"/>
  </Declaration>
  <Declaration>
    <Class IRI="#machineType"/>
  </Declaration>
  <Declaration>
    <Class IRI="#network"/>
  </Declaration>
  <Declaration>
    <Class IRI="#networkClassificationLevel"/>
  </Declaration>
  <Declaration>
```

```
    <Class IRI="#normalAuthenticationType"/>
</Declaration>
<Declaration>
    <Class IRI="#operationalEnvironmentThreatLevel"/>
</Declaration>
<Declaration>
    <Class IRI="#perishableNonPerishable"/>
</Declaration>
<Declaration>
    <Class IRI="#permissionLevel"/>
</Declaration>
<Declaration>
    <Class IRI="#previousViolations"/>
</Declaration>
<Declaration>
    <Class IRI="#qopEncryptionLevel"/>
</Declaration>
<Declaration>
    <Class IRI="#rank"/>
</Declaration>
<Declaration>
    <Class IRI="#riskKnowledge"/>
</Declaration>
<Declaration>
    <Class IRI="#role"/>
</Declaration>
<Declaration>
    <Class IRI="#secureAuthenticationType"/>
</Declaration>
<Declaration>
    <Class IRI="#situationalFactors"/>
</Declaration>
<Declaration>
    <Class IRI="#specificMissionRole"/>
</Declaration>
<Declaration>
    <Class IRI="#timeSensitivityOfInformation"/>
</Declaration>
<Declaration>
    <Class IRI="#transactionType"/>
</Declaration>
<Declaration>
    <Class IRI="#trustLevel"/>
</Declaration>
<Declaration>
```

```
    <ObjectProperty IRI="#canBeUsedBy"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#hasEncriptionLevel"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#hasMinimumEducationLevel"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#hasMinimumRank"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#hasMinimumRole"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#hasOperationalThreatLevel"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#hasTrustLevel"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#usesApplication"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#usesAuthenticationType"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#usesConnectionType"/>
  </Declaration>
  <Declaration>
    <ObjectProperty IRI="#usesMachineType"/>
  </Declaration>
  <Declaration>
    <DataProperty IRI="#value"/>
  </Declaration>
  <Declaration>
    <DataProperty IRI="#weight"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Admin"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Aes"/>
  </Declaration>
  <Declaration>
```

```
    <NamedIndividual IRI="#Auditable"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Brazil"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Browser"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Client"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Database"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Desktop"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#E-3"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Elevated"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#FileShare"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Graduation"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#HighRiskKnowledge"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#HighTrustLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Internet"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Iraq"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Jwics"/>
</Declaration>
<Declaration>
```

```
    <NamedIndividual IRI="#LowRiskKnowledge"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#LowTrustLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Masters"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#MediumTrustLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#MoreThan10000Km"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#MoreThan1000Km"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#MoreThan5000km"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#MoreThanOnePerson"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#NeededNow"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#NeededSoon"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#NoAccessLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#NoPreviousViolations"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#NoRiskKnowledge"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Norway"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Operator"/>
  </Declaration>
  <Declaration>
```

```
    <NamedIndividual IRI="#Pda"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Perishable"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Phd"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Pki"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Query"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#ReadOnly"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#SecretClassificationLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Server"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Severe"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#SinglePerson"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Ssl"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#SuportTeam"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#TeamLeader"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#TopSecretClassificationLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#Until1000km"/>
</Declaration>
<Declaration>
```

```
    <NamedIndividual IRI="#UsernameAndPassword"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Wep"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Wired"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#Wireless"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#YesAccessLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#YesPreviousViolations"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#accessLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#application"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#audianceSize"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#auditableOrNonAuditable"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#authenticationType"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#classificationLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#clearanceLevel"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#connectionType"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#currentLocation"/>
  </Declaration>
  <Declaration>
```

```
    <NamedIndividual IRI="#distanceFromRequesterToSource"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#educationLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#encryptionLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#machineType"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#network"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#networkClassificationLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#normalAuthenticationType"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#operationalEnvironmentThreatLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#perishableNonPerishable"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#permissionLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#previousViolations"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#qopEncryptionLevel"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#rank"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#riskKnowledge"/>
</Declaration>
<Declaration>
    <NamedIndividual IRI="#role"/>
</Declaration>
<Declaration>
```

```
    <NamedIndividual IRI="#secureAuthenticationType"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#specificMissionRole"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#timeSensitivityOfInformation"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#transactionType"/>
  </Declaration>
  <Declaration>
    <NamedIndividual IRI="#trustLevel"/>
  </Declaration>
  <SubClassOf>
    <Class IRI="#accessLevel"/>
    <Class IRI="#characteristicsOfRequester"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#application"/>
    <Class IRI="#characteristicsOfItComponents"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#audienceSize"/>
    <Class IRI="#situationalFactors"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#auditableOrNonAuditable"/>
    <Class IRI="#situationalFactors"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#authenticationType"/>
    <Class IRI="#characteristicsOfItComponents"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#classificationLevel"/>
    <Class IRI="#characteristicsOfInformationRequested"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#clearanceLevel"/>
    <Class IRI="#characteristicsOfRequester"/>
  </SubClassOf>
  <SubClassOf>
    <Class IRI="#connectionType"/>
    <Class IRI="#characteristicsOfItComponents"/>
```

```
</SubClassOf>
<SubClassOf>
   <Class IRI="#currentLocation"/>
   <Class IRI="#environmentalFactors"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#distanceFromRequesterToSource"/>
   <Class IRI="#characteristicsOfItComponents"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#educationLevel"/>
   <Class IRI="#characteristicsOfRequester"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#encryptionLevel"/>
   <Class IRI="#characteristicsOfInformationRequested"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#machineType"/>
   <Class IRI="#characteristicsOfItComponents"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#network"/>
   <Class IRI="#characteristicsOfItComponents"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#networkClassificationLevel"/>
   <Class IRI="#characteristicsOfInformationRequested"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#normalAuthenticationType"/>
   <Class IRI="#authenticationType"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#operationalEnvironmentThreatLevel"/>
   <Class IRI="#environmentalFactors"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#perishableNonPerishable"/>
   <Class IRI="#characteristicsOfInformationRequested"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#permissionLevel"/>
   <Class IRI="#characteristicsOfInformationRequested"/>
</SubClassOf>
```

```
<SubClassOf>
   <Class IRI="#previousViolations"/>
   <Class IRI="#characteristicsOfRequester"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#qopEncryptionLevel"/>
   <Class IRI="#characteristicsOfItComponents"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#rank"/>
   <Class IRI="#characteristicsOfRequester"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#riskKnowledge"/>
   <Class IRI="#heuristics"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#role"/>
   <Class IRI="#characteristicsOfRequester"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#secureAuthenticationType"/>
   <Class IRI="#authenticationType"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#specificMissionRole"/>
   <Class IRI="#situationalFactors"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#timeSensitivityOfInformation"/>
   <Class IRI="#situationalFactors"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#transactionType"/>
   <Class IRI="#situationalFactors"/>
</SubClassOf>
<SubClassOf>
   <Class IRI="#trustLevel"/>
   <Class IRI="#heuristics"/>
</SubClassOf>
<ClassAssertion>
   <Class IRI="#role"/>
   <NamedIndividual IRI="#Admin"/>
</ClassAssertion>
<ClassAssertion>
```

```
    <Class IRI="#encryptionLevel"/>
    <NamedIndividual IRI="#Aes"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#auditableOrNonAuditable"/>
    <NamedIndividual IRI="#Auditable"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#currentLocation"/>
    <NamedIndividual IRI="#Brazil"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#application"/>
    <NamedIndividual IRI="#Browser"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#application"/>
    <NamedIndividual IRI="#Database"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#machineType"/>
    <NamedIndividual IRI="#Desktop"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#rank"/>
    <NamedIndividual IRI="#E-3"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#operationalEnvironmentThreatLevel"/>
    <NamedIndividual IRI="#Elevated"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#application"/>
    <NamedIndividual IRI="#FileShare"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#educationLevel"/>
    <NamedIndividual IRI="#Graduation"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#riskKnowledge"/>
    <NamedIndividual IRI="#HighRiskKnowledge"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#trustLevel"/>
```

```
    <NamedIndividual IRI="#HighTrustLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#network"/>
    <NamedIndividual IRI="#Internet"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#currentLocation"/>
    <NamedIndividual IRI="#Iraq"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#networkClassificationLevel"/>
    <NamedIndividual IRI="#Jwics"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#riskKnowledge"/>
    <NamedIndividual IRI="#LowRiskKnowledge"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#trustLevel"/>
    <NamedIndividual IRI="#LowTrustLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#educationLevel"/>
    <NamedIndividual IRI="#Masters"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#trustLevel"/>
    <NamedIndividual IRI="#MediumTrustLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#distanceFromRequesterToSource"/>
    <NamedIndividual IRI="#MoreThan10000Km"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#distanceFromRequesterToSource"/>
    <NamedIndividual IRI="#MoreThan1000Km"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#distanceFromRequesterToSource"/>
    <NamedIndividual IRI="#MoreThan5000km"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#audienceSize"/>
    <NamedIndividual IRI="#MoreThanOnePerson"/>
```

```
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#timeSensitivityOfInformation"/>
   <NamedIndividual IRI="#NeededNow"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#timeSensitivityOfInformation"/>
   <NamedIndividual IRI="#NeededSoon"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#accessLevel"/>
   <NamedIndividual IRI="#NoAccessLevel"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#previousViolations"/>
   <NamedIndividual IRI="#NoPreviousViolations"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#riskKnowledge"/>
   <NamedIndividual IRI="#NoRiskKnowledge"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#currentLocation"/>
   <NamedIndividual IRI="#Norway"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#role"/>
   <NamedIndividual IRI="#Operator"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#machineType"/>
   <NamedIndividual IRI="#Pda"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#perishableNonPerishable"/>
   <NamedIndividual IRI="#Perishable"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#educationLevel"/>
   <NamedIndividual IRI="#Phd"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#secureAuthenticationType"/>
   <NamedIndividual IRI="#Pki"/>
</ClassAssertion>
```

```
<ClassAssertion>
   <Class IRI="#transactionType"/>
   <NamedIndividual IRI="#Query"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#permissionLevel"/>
   <NamedIndividual IRI="#ReadOnly"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#classificationLevel"/>
   <NamedIndividual IRI="#SecretClassificationLevel"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#machineType"/>
   <NamedIndividual IRI="#Server"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#operationalEnvironmentThreatLevel"/>
   <NamedIndividual IRI="#Severe"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#audienceSize"/>
   <NamedIndividual IRI="#SinglePerson"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#qopEncryptionLevel"/>
   <NamedIndividual IRI="#Ssl"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#specificMissionRole"/>
   <NamedIndividual IRI="#SuportTeam"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#role"/>
   <NamedIndividual IRI="#TeamLeader"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#classificationLevel"/>
   <NamedIndividual IRI="#TopSecretClassificationLevel"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#distanceFromRequesterToSource"/>
   <NamedIndividual IRI="#Until1000km"/>
</ClassAssertion>
<ClassAssertion>
```

```
    <Class IRI="#normalAuthenticationType"/>
    <NamedIndividual IRI="#UsernameAndPassword"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#qopEncryptionLevel"/>
    <NamedIndividual IRI="#Wep"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#connectionType"/>
    <NamedIndividual IRI="#Wired"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#connectionType"/>
    <NamedIndividual IRI="#Wireless"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#accessLevel"/>
    <NamedIndividual IRI="#YesAccessLevel"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#previousViolations"/>
    <NamedIndividual IRI="#YesPreviousViolations"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#accessLevel"/>
    <NamedIndividual IRI="#accessLevel"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#application"/>
    <NamedIndividual IRI="#application"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#audienceSize"/>
    <NamedIndividual IRI="#audianceSize"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#auditableOrNonAuditable"/>
    <NamedIndividual IRI="#auditableOrNonAuditable"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#authenticationType"/>
    <NamedIndividual IRI="#authenticationType"/>
</ClassAssertion>
<ClassAssertion>
    <Class IRI="#classificationLevel"/>
```

```
    <NamedIndividual IRI="#classificationLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#clearanceLevel"/>
    <NamedIndividual IRI="#clearanceLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#connectionType"/>
    <NamedIndividual IRI="#connectionType"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#currentLocation"/>
    <NamedIndividual IRI="#currentLocation"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#distanceFromRequesterToSource"/>
    <NamedIndividual IRI="#distanceFromRequesterToSource"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#educationLevel"/>
    <NamedIndividual IRI="#educationLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#encryptionLevel"/>
    <NamedIndividual IRI="#encryptionLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#machineType"/>
    <NamedIndividual IRI="#machineType"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#network"/>
    <NamedIndividual IRI="#network"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#networkClassificationLevel"/>
    <NamedIndividual IRI="#networkClassificationLevel"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#normalAuthenticationType"/>
    <NamedIndividual IRI="#normalAuthenticationType"/>
  </ClassAssertion>
  <ClassAssertion>
    <Class IRI="#operationalEnvironmentThreatLevel"/>
    <NamedIndividual IRI="#operationalEnvironmentThreatLevel"/>
```

```
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#perishableNonPerishable"/>
   <NamedIndividual IRI="#perishableNonPerishable"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#permissionLevel"/>
   <NamedIndividual IRI="#permissionLevel"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#previousViolations"/>
   <NamedIndividual IRI="#previousViolations"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#qopEncryptionLevel"/>
   <NamedIndividual IRI="#qopEncryptionLevel"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#rank"/>
   <NamedIndividual IRI="#rank"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#riskKnowledge"/>
   <NamedIndividual IRI="#riskKnowledge"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#role"/>
   <NamedIndividual IRI="#role"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#secureAuthenticationType"/>
   <NamedIndividual IRI="#secureAuthenticationType"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#specificMissionRole"/>
   <NamedIndividual IRI="#specificMissionRole"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#timeSensitivityOfInformation"/>
   <NamedIndividual IRI="#timeSensitivityOfInformation"/>
</ClassAssertion>
<ClassAssertion>
   <Class IRI="#transactionType"/>
   <NamedIndividual IRI="#transactionType"/>
</ClassAssertion>
```

```
<ClassAssertion>
   <Class IRI="#trustLevel"/>
   <NamedIndividual IRI="#trustLevel"/>
</ClassAssertion>
<SameIndividual>
   <NamedIndividual IRI="#Client"/>
   <NamedIndividual IRI="#Desktop"/>
</SameIndividual>
<ObjectPropertyAssertion>
   <ObjectProperty IRI="#hasMinimumEducationLevel"/>
   <NamedIndividual IRI="#Admin"/>
   <NamedIndividual IRI="#Masters"/>
</ObjectPropertyAssertion>
<ObjectPropertyAssertion>
   <ObjectProperty IRI="#usesConnectionType"/>
   <NamedIndividual IRI="#Admin"/>
   <NamedIndividual IRI="#connectionType"/>
</ObjectPropertyAssertion>
<ObjectPropertyAssertion>
   <ObjectProperty IRI="#usesMachineType"/>
   <NamedIndividual IRI="#Admin"/>
   <NamedIndividual IRI="#Desktop"/>
</ObjectPropertyAssertion>
<ObjectPropertyAssertion>
   <ObjectProperty IRI="#usesAuthenticationType"/>
   <NamedIndividual IRI="#Browser"/>
   <NamedIndividual IRI="#normalAuthenticationType"/>
</ObjectPropertyAssertion>
<ObjectPropertyAssertion>
   <ObjectProperty IRI="#usesConnectionType"/>
   <NamedIndividual IRI="#Desktop"/>
   <NamedIndividual IRI="#Wired"/>
</ObjectPropertyAssertion>
<DataPropertyAssertion>
   <DataProperty IRI="#value"/>
   <NamedIndividual IRI="#Admin"/>
   <Literal datatypeIRI="&xsd;double">10.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
   <DataProperty IRI="#value"/>
   <NamedIndividual IRI="#Aes"/>
   <Literal datatypeIRI="&xsd;double">9.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
   <DataProperty IRI="#value"/>
```

```
    <NamedIndividual IRI="#Auditable"/>
    <Literal datatypeIRI="&xsd;double">2.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Brazil"/>
    <Literal datatypeIRI="&xsd;double">5.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Browser"/>
    <Literal datatypeIRI="&xsd;double">5.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Database"/>
    <Literal datatypeIRI="&xsd;double">4.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Desktop"/>
    <Literal datatypeIRI="&xsd;double">5.5</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#E-3"/>
    <Literal datatypeIRI="&xsd;double">8.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Elevated"/>
    <Literal datatypeIRI="&xsd;double">5.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Internet"/>
    <Literal datatypeIRI="&xsd;double">9.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Iraq"/>
    <Literal datatypeIRI="&xsd;double">10.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
```

```
    <NamedIndividual IRI="#Jwics"/>
    <Literal datatypeIRI="&xsd;double">9.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#LowTrustLevel"/>
    <Literal datatypeIRI="&xsd;double">9.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#MoreThan10000Km"/>
    <Literal datatypeIRI="&xsd;double">8.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#NeededNow"/>
    <Literal datatypeIRI="&xsd;double">2.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#NeededSoon"/>
    <Literal datatypeIRI="&xsd;double">5.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#NoAccessLevel"/>
    <Literal datatypeIRI="&xsd;double">10.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#NoPreviousViolations"/>
    <Literal datatypeIRI="&xsd;double">0.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#NoRiskKnowledge"/>
    <Literal datatypeIRI="&xsd;double">10.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Norway"/>
    <Literal datatypeIRI="&xsd;double">1.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
```

```
    <NamedIndividual IRI="#Operator"/>
    <Literal datatypeIRI="&xsd;double">5.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Pda"/>
    <Literal datatypeIRI="&xsd;double">10.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Perishable"/>
    <Literal datatypeIRI="&xsd;double">9.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Phd"/>
    <Literal datatypeIRI="&xsd;double">2.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Query"/>
    <Literal datatypeIRI="&xsd;double">2.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#ReadOnly"/>
    <Literal datatypeIRI="&xsd;double">9.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#SecretClassificationLevel"/>
    <Literal datatypeIRI="&xsd;double">6.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Severe"/>
    <Literal datatypeIRI="&xsd;double">10.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#SinglePerson"/>
    <Literal datatypeIRI="&xsd;double">2.0</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#value"/>
```

```
    <NamedIndividual IRI="#SuportTeam"/>
    <Literal datatypeIRI="&xsd;double">2.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#TeamLeader"/>
    <Literal datatypeIRI="&xsd;double">7.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#TopSecretClassificationLevel"/>
    <Literal datatypeIRI="&xsd;double">9.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#UsernameAndPassword"/>
    <Literal datatypeIRI="&xsd;double">7.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Wep"/>
    <Literal datatypeIRI="&xsd;double">5.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#Wireless"/>
    <Literal datatypeIRI="&xsd;double">8.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#YesAccessLevel"/>
    <Literal datatypeIRI="&xsd;double">0.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#value"/>
    <NamedIndividual IRI="#YesPreviousViolations"/>
    <Literal datatypeIRI="&xsd;double">10.0</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#accessLevel"/>
    <Literal datatypeIRI="&xsd;double">2.777778</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
```

```
    <NamedIndividual IRI="#application"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#audianceSize"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#auditableOrNonAuditable"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#authenticationType"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#classificationLevel"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#clearanceLevel"/>
    <Literal datatypeIRI="&xsd;double">2.777778</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#connectionType"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#currentLocation"/>
    <Literal datatypeIRI="&xsd;double">8.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#distanceFromRequesterToSource"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
```

```
    <NamedIndividual IRI="#educationLevel"/>
    <Literal datatypeIRI="&xsd;double">2.777778</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#encryptionLevel"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#machineType"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#network"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#networkClassificationLevel"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#operationalEnvironmentThreatLevel"/>
    <Literal datatypeIRI="&xsd;double">8.333333</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#perishableNonPerishable"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#permissionLevel"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#previousViolations"/>
    <Literal datatypeIRI="&xsd;double">2.777778</Literal>
  </DataPropertyAssertion>
  <DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
```

```
    <NamedIndividual IRI="#qopEncryptionLevel"/>
    <Literal datatypeIRI="&xsd;double">2.380952</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#rank"/>
    <Literal datatypeIRI="&xsd;double">2.777778</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#riskKnowledge"/>
    <Literal datatypeIRI="&xsd;double">8.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#role"/>
    <Literal datatypeIRI="&xsd;double">2.777778</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#specificMissionRole"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#timeSensitivityOfInformation"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#transactionType"/>
    <Literal datatypeIRI="&xsd;double">3.333333</Literal>
</DataPropertyAssertion>
<DataPropertyAssertion>
    <DataProperty IRI="#weight"/>
    <NamedIndividual IRI="#trustLevel"/>
    <Literal datatypeIRI="&xsd;double">8.333333</Literal>
</DataPropertyAssertion>
<SubObjectPropertyOf>
    <ObjectProperty IRI="#canBeUsedBy"/>
    <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
</SubObjectPropertyOf>
<SubObjectPropertyOf>
    <ObjectProperty IRI="#hasEncriptionLevel"/>
    <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
```

```
    </SubObjectPropertyOf>
    <SubObjectPropertyOf>
        <ObjectProperty IRI="#hasMinimumRole"/>
        <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
    </SubObjectPropertyOf>
    <SubObjectPropertyOf>
        <ObjectProperty IRI="#hasOperationalThreatLevel"/>
        <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
    </SubObjectPropertyOf>
    <SubObjectPropertyOf>
        <ObjectProperty IRI="#hasTrustLevel"/>
        <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
    </SubObjectPropertyOf>
    <SubObjectPropertyOf>
        <ObjectProperty IRI="#usesApplication"/>
        <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
    </SubObjectPropertyOf>
    <SubObjectPropertyOf>
        <ObjectProperty IRI="#usesMachineType"/>
        <ObjectProperty abbreviatedIRI="owl:topObjectProperty"/>
    </SubObjectPropertyOf>
</Ontology>



<!-- Generated by the OWL API (version 3.4.2) http://owlapi.sourceforge.net --
>
```

APÊNDICE B – Parte da Implementação da Classe de Gerenciamento de Contexto de Usuários (User Risk)

```php
<?php

class userClass {

    private $xmlString;
    private $xmlPath;

    function __construct($xmlPath) {
        $this->xmlString = new SimpleXMLElement ( file_get_contents ( $xmlPath ) );
        $this->xmlPath = $xmlPath;
    }

    function changeUserRate($userName, $userRate) {
        $doc = new DOMDocument ();
        $doc->load ( $this->xmlPath );

        $xpath = new DOMXpath ( $doc );
        $nodelist = $xpath->query ( "/users/user/name[. = '$userName']" );
        $oldnode = $nodelist->item ( 0 )->parentNode;

        $parent = new DomDocument ();
        $parent_node = $parent->createElement ( 'user' );

        $parent_node->appendChild ( $parent->createElement ( 'name', $userName ) );
        $parent_node->appendChild ( $parent->createElement ( 'rate', $userRate ) );
        $parent->appendChild ( $parent_node );

        $newnode = $doc->importNode ( $parent->documentElement, true );
        $oldnode->parentNode->replaceChild ( $newnode, $oldnode );

        return new SimpleXMLElement ( $doc->saveXML () );
    }

    function addUser($userName, $userRate) {
        $xmlNode = $this->xmlString->addChild ( 'user' );
        $xmlNode->name = $userName;
        $xmlNode->rate = $userRate;

        return $this->xmlString;
    }
```

APÊNDICE C – Parte da Implementação da Classe de Gerenciamento de Contexto de Arquivos

```php
<?php

class fileClass {

    private  $xmlString;
    private  $xmlPath;

    function __construct($xmlPath){
        $this->xmlString = new SimpleXMLElement(file_get_contents($xmlPath));
        $this->xmlPath = $xmlPath;
    }

    function increaseAccessNumber($filePath) {

        $doc = new DOMDocument();
        $doc->load($this->xmlPath);

        $xpath = new DOMXpath($doc);
        $nodelist = $xpath->query("/files/file/file_path[. = '$filePath']");

        $oldnode = $nodelist->item(0)->parentNode;

        $parent = new DomDocument;
        $parent_node = $parent->createElement('file');
        $parent_node->appendChild($parent->createElement('file_path', $filePath));

        $accessValue = $oldnode->getElementsByTagName('access')->item(0)->nodeValue;
        $accessValue++;
        $parent_node->appendChild($parent->createElement('access', $accessValue));

        $parent->appendChild($parent_node);

        $newnode = $doc->importNode($parent->documentElement, true);
        $oldnode->parentNode->replaceChild($newnode, $oldnode);

        return new SimpleXMLElement($doc->saveXML());
```

APÊNDICE D –Implementação da Classe de Execução de Consultas via SPARQL através do Apache Jena

```php
<?php

class queryOntologyClass {

    private  $sparqlBinPath;
    private  $ontologySourcePath;
    private  $queryPath;

    function __construct($sparqlBinPath, $ontologySourcePath){
        $this->ontologySourcePath = $ontologySourcePath;
        $this->sparqlBinPath = $sparqlBinPath;
    }

    function writeQuery($query){
        file_put_contents($this->queryPath, $query);
    }

    function execQuery(){
        $cmd = $this->sparqlBinPath." --data=$this->ontologySourcePath";
        $cmd.= " --query=$this->queryPath --results JSON";
        $return = shell_exec($cmd);
        if($return)
            return json_decode($return);
        else
            return false;
    }

    function sparqlQuery($query){
        writeQuery($query);
        return execQuery();
    }
```