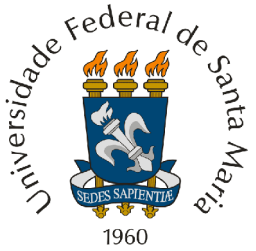

UFSM

Dissertação de Mestrado

UTILIZAÇÃO DE INFORMAÇÕES CONTEXTUAIS EM UM MODELO DE CONTROLE DE ACESSO A INFORMAÇÕES MÉDICAS

Gerson Antunes Soares

PPGEP

Santa Maria, RS, Brasil

2007

UTILIZAÇÃO DE INFORMAÇÕES CONTEXTUAIS EM UM MODELO DE CONTROLE DE ACESSO A INFORMAÇÕES MÉDICAS

por

Gerson Antunes Soares

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Engenharia de Produção, Área de Concentração em Tecnologia da Informação, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Engenharia de Produção**.

Orientador Prof. Dr. Raul Ceretta Nunes

Santa Maria, RS, Brasil

2007

Soares, Gerson Antunes, 1971
S676u

Utilização de informações contextuais em um modelo de controle de acesso a informações médicas / por Gerson Antunes Soares; orientador Raul Ceretta Nunes. Santa Maria, 2007
84 p.: il., tabs

Dissertação (Mestrado) – Universidade Federal de Santa Maria, Centro de Tecnologia. Programa de Pós-Graduação em Engenharia de Produção, RS, 2007.

1. Tecnologia da Informação 2. Prontuário Eletrônico do Paciente 3. Modelo de controle de acesso 4. Segurança e autorização I. Nunes, Raul Ceretta. II. Título.

CDU: 004.78

Catalogação na Fonte: Cristiane Oliveira dos Santos – CRB 10/1617

Endereço: Rua Aníbal Lopes da Silva, n. 515, bairro Santa Rita, Cruz Alta, RS, 98050-050
Fone (0xx)55 33229353; e-mail: gerson@inf.ufsm.br

Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Engenharia de Produção

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

UTILIZAÇÃO DE INFORMAÇÕES CONTEXTUAIS EM UM MODELO DE CONTROLE DE ACESSO A INFORMAÇÕES MÉDICAS

elaborada por
Gerson Antunes Soares

como requisito parcial para obtenção do grau de
Mestre em Engenharia de Produção

COMISSÃO EXAMINADORA:

_____
Dr. Raul Ceretta Nunes –UFSM - Brasil
(Presidente/Orientador)

_____
Dra. Elena Ferrari –Uninsubria – Itália

_____
Dra. Roseclea Duarte Medina-UFSM - Brasil

Santa Maria, 17 de Janeiro de 2007.

Ao meu pai

Jurandi Gomes Soares,

à minha mãe

Maria Antunes Soares

e aos meus amores

Daiana e Bárbara

Agradecimentos

Ao longo destes dois anos de pesquisa no mestrado em engenharia de produção da UFSM, tenho muito a quem agradecer.

Primeiramente a Deus, pela vida.

A CAPES pelo fomento a pesquisa, fundamental para o desenvolvimento dos trabalhos.

A todos os colegas do GMICRO que conviveram e trabalharam durante este tempo, e à equipe do CPD que disponibilizou as informações necessárias à implementação.

Ao meu amigo e orientador Professor Dr. Raul Ceretta Nunes, pela dedicação e auxílio durante as atividades de pesquisa.

Às Professoras Dra. Elena Ferrari e Dra. Bárbara Carminati pela acolhida na Itália e pelas orientações em modelagem de controle de acesso.

À amiga Cecília e sua família que acolheram-me em Santa Maria durante o período do mestrado.

Em especial aos meus pais Jurandi e Maria pelo apoio e compreensão ao longo do curso, incentivando-me sempre em todos os momentos.

Enfim, agradeço a todos os demais que deram a sua contribuição para minha formação profissional.

Sumário

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

AM	*Access Mode*
AMM	Associação Médica Mundial
CAAC	*Context-Aware Access Control*
CABAC	*Contextual Attribute-Based Access Control*
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CASPEr	*Context Aware Security Policy Enforcement*
CBAC	*Context-Based access Control*
CC	*Context Condition*
CE	*Credential Expression*
CFM	Conselho Federal de Medicina
CI	*Contextual Information*
CIBAC	*Contextual Information-Based Access Control*
CMU	*Couverture Maladie Universelle*
CPD	Centro de Processamento de Dados
CSAC	*Context Sensitive Access Control*
CS-RBAC	*Context-Sensitive Role-Based Access Control*
CT	*Context Type*
C-TMAC	*Contextual Team-Access Control*
DAC	*Discretionary Access Control*
DRIVE-RBAC	*Drug in Virtual Enterprise Role-Based Access Control*
EPR	*Electronic Patient Record*
E-RBAC	*Enviroment Role-Based Access Control*
GMICRO	Grupo de Microeletrônica
GTRBAC	*Generalized Temporal Role-Based Access Control*
HUSM	Hospital Universitário de Santa Maria
IEC	*International Electrotechnical Commission*
INAMPS	Instituto Nacional de Assistência Médica da Previdência Social
IP	*Internet Protocol*
ISSO	*International Standards Organization*
InCor	Instituto do Coração
LDAP	*Lightweight Directoty Access Protocol*
MAC	*Mandatory Access Control*
MACA	*Middleware* de Autenticação e Controle de Acesso
OASIS	*Open Architecture for Securely Interworking Services*
OCDE	Organização de Cooperação e de Desenvolvimento Econômico
OMG	*Object Management Group*
ONU	Organização das Nações Unidas
PEP	Prontuário Eletrônico do Paciente
PDP	Ponto de Decisão de Políticas
POMR	*Problem-Oriented Medical Record*
PP	Prontuário do Paciente
RBAC	*Role-Based Access Control*
RBPEAC	*Role-Based Policy-Enforced Access Control*
RCP	Repositório de Comportamento de Propriedades
RPC	*Remote Procedure Call*

SGCA	Sistema de Gerenciamento e Controle de Aplicações
SGBD	Sistema Gerenciador de Banco de Dados
SIE	Sistema de Informações Educacionais
SIH	Sistema de Informações Hospitalares
SOAP	*Simple Object Access Protocol*
SQL	*Structured Query Language*
SER	Separação de Responsabilidade Estática
TCM	*Tees Confidentiality Model*
TI	Tecnologia da Informação
TRBAC	*Temporal Role-Based Access Control*
UDDI	*Universal Description, Discovery and Integration*
UFSM	Universidade Federal de Santa Maria
UTI	Unidade de Terapia Intensiva
WSDL	*Web Service Description Language*
XACML	*eXtensible Access Control Markup Language*
XML	*Extensible Markup Language*
XORBAC	*eXtended Object Role-Based Access Control*

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria

UTILIZAÇÃO DE INFORMAÇÕES CONTEXTUAIS EM UM MODELO DE CONTROLE DE ACESSO A INFORMAÇÕES MÉDICAS

AUTOR: GERSON ANTUNES SOARES
ORIENTADOR: DR. RAUL CERETTA NUNES
Data e Local da Defesa: 17 de janeiro de 2007, Santa Maria.

Este trabalho apresenta uma abordagem sobre a utilização de informações contextuais em um modelo de controle de acesso a informações de prontuários eletrônicos de paciente (PEP).

O PEP registra informações sobre a saúde do paciente e a assistência a ele prestada, e tem caráter legal, sigiloso e científico, podendo incluir também conteúdos administrativos e financeiros relacionados a procedimentos ou tratamentos realizados. Resumidamente, pode-se dizer que o PEP guarda os documentos sobre o estado de saúde e os cuidados recebidos por um indivíduo ao longo da sua vida. Entretanto, a disponibilização de informações clínicas em redes de computadores levanta questionamentos sobre a privacidade dos pacientes e a integridade e confidencialidade dos dados. O controle de acesso é um ponto chave para manter tais requisitos.

O principal objetivo no desenvolvimento deste modelo de controle de acesso é prover diferentes formas de acesso a informações em um ambiente hospitalar, propiciando a adequação com a legislação pertinente. A abordagem proposta neste trabalho permite a aplicação de políticas e regras de acesso mais específicas, agregando mais funcionalidade aos sistemas de controle de acesso.

O foco de discussão desta dissertação trata da utilização de informações médicas no âmbito do Hospital Universitário de Santa Maria, e visa à integração do modelo com módulos em desenvolvimento no centro de processamento de dados da instituição.

Palavras-chave: Modelo de controle de acesso, prontuário eletrônico do paciente, informações contextuais, segurança e autorização.

ABSTRACT

Master Dissertation
Program of Under-Graduate Studies in Production Engineering
Federal University of Santa Maria

USE OF CONTEXTUAL INFORMATION IN A MODEL OF ACCESS CONTROL TO MEDICAL INFORMATION

AUTHOR: GERSON ANTUNES SOARES
ADVISER: RAUL CERETTA NUNES, DR.
Date and Local: January, 17th of 2007, Santa Maria.

This work presents a boarding on the use of contextual information in a model of access control to electronic patient record (EPR).

The EPR registers information on the health of the patient and the assistance given it, and has legal, secret and scientific character, being able to also include administrative and financial contents related the carried through procedures or treatments. In summary, can be said that the EPR keeps to the documents on the state of health and the cares received for an individual throughout its life. However, the availability of clinical information in computer networks raises questionings on the privacy of the patients and the integrity and confidentiality of the data. The access control is a point key to keep such requirements.

The main objective in the development of this modelof access control is to provide different forms of access to information in a hospital environment, propitiating the adequacy with the pertinent legislation. To boarding proposal in this work allows to the application of politics and more specific rules of access, adding more functionality to the systems of access control.

The focus of quarrel of this work deals with the use of medical information in the scope of the University Hospital of Santa Maria, and aims at to the integration of the model with modules in development in the data processing center of the institution.

***keywords**: Model of access control, electronic patient record, contextual information, security and authorization.*

Capítulo 1
INTRODUÇÃO

A evolução das tecnologias de comunicação e computação vem incrementando a utilização de sistemas computacionais em diversos domínios, tal como negócios, saúde e educacional. Especialmente na área da saúde, a disponibilização de informações clínicas em redes de computadores, tal como o prontuário eletrônico do paciente (PEP)[1], necessita manter a privacidade dos pacientes, a confidencialidade dos dados e a integridade da informação (CFM, 2002). Na prática, tais requisitos podem ser atendidos através do uso de mecanismos de controle de vulnerabilidades, de métodos fortes de autenticação, de restrições de acesso, dentre outros (ISO/IEC, 1999). Sendo o acesso um ponto chave para manter a segurança (privacidade, confidencialidade e integridade) da informação, o modelo de controle de acesso necessita refletir os requisitos da aplicação.

Existe uma série de modelos de controle de acesso disponíveis, dentre os quais os mais conhecidos são o MAC (*Mandatory Access Control*), o DAC (*Discretionary Access Control*) e o RBAC (*Role-Based Access Control*) (SAMARATI, 2001). O MAC é direcionado para aplicações militares enquanto o DAC e o RBAC são direcionados para aplicações civis. Diferentemente do MAC e DAC, o RBAC possibilita que o controle de acesso considere as funções que um usuário pode realizar dentro de uma organização, tornado-se assim o modelo base mais utilizado atualmente. O RBAC (FERRAIOLO, 2001) introduz o conceito de *role* (função, papel, perfil ou cargo). Tal conceito permite definir o perfil de cada usuário de forma a especificar regras de acesso baseadas em diferentes perfis. Por generalidade, o RBAC não especifica como cada perfil deve ser utilizado para atender requisitos distintos, ficando isto a cargo do utilizador.

---

[1] De acordo com o Conselho Federal de Medicina do Brasil (CFM, 2002), um prontuário médico é um "documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo". Quando em sua versão eletrônica é dado o nome de Prontuário Eletrônico do Paciente, ou PEP.

O acesso a informações médicas presentes no PEP deve ser realizado por um grupo heterogêneo de usuários que, para garantir a integridade do prontuário, devem ter permissões de acesso distintas (MOTTA, 2003b), o que pode ser alcançado com mecanismos de controle de acesso baseados em *perfis de usuários*. Entretanto, em se tratando de acesso ao PEP, além da separação de usuários em múltiplos perfis, o mecanismo de controle de acesso também deve considerar *informações de ambiente*, tais como questões temporais, número de acessos, localidade do recurso ou do usuário, entre outras, bem como as *características dinâmicas da informação* (SOARES, 2005), uma vez que seu conteúdo pode ser alterado ao longo do tempo (COVINGTON, 2006). Observe que o conjunto de informações de ambiente, neste trabalho chamado *contexto*, e sua dinamicidade são aspectos importantes para a eficácia do mecanismo de controle de acesso. No ambiente hospitalar a aceitação ou negação do acesso deve no mínimo considerar as freqüentes mudanças de turnos (*aspectos temporais*) e de funções (*perfil do usuário*), buscando contextualizar o acesso. Além disto, o mecanismo de controle de acesso deve considerar a mudança de contexto ao longo do tempo, o que se reflete na alteração dinâmica das permissões para um dado usuário.

O modelo de controle de acesso baseado em regras temporais, ou TRBAC (BERTINO, 2001), resolve parcialmente o problema ao incluir regras que controlam a validade temporal. Além disto, por ser um modelo conceitual, assim como o RBAC, o TRBAC não determina como estas regras podem ser utilizadas de uma maneira mais transparente ao usuário, ou mesmo como estas regras podem ser gerenciadas.

Para atender aos requisitos da área médica, o *Middleware* de Autenticação e Controle de Acesso - MACA (MOTTA, 2003a) baseia-se num modelo de autorização contextual para controle de acesso baseado em perfis[2] de usuários (MOTTA, 2002). A idéia chave do modelo é decidir pela autorização positiva ou negativa de acordo com as regras de autorização que relacionam as informações sobre o contexto em que cada autorização está sendo solicitada. Além disto, o modelo trata a *separação de responsabilidades* no âmbito do PEP, conforme exigido pela legislação brasileira (CFM, 2002), e a *hierarquia dos perfis*. Entretanto, associações entre autorizações e perfis, ou ativação dinâmica de mais de um perfil, são as potenciais causas da ocorrência de conflitos de autorização. O MACA estabelece contribuições significativas para solucionar o controle de acesso ao PEP, mas não resolve apropriadamente a detecção e tratamento de conflitos que possam resultar em possíveis

[2] O artigo original refere-se a controle de acesso baseado em *papéis*, mas para coerência deste trabalho chamamos controle de acesso baseado em *perfis*, pois ambos derivam de *role-based access control*.

violações da política de separação de responsabilidades, nem trata a delegação de atribuições, que no âmbito hospitalar é uma prática bastante utilizada.

Neste trabalho, propõe-se um modelo dinâmico de controle de acesso baseado em contexto, o qual pode ser enquadrado como extensão ao modelo de controle de acesso baseado em perfis (RBAC). O modelo considera informações sobre os elementos inseridos no ambiente como sendo *propriedades* do contexto e assume o conjunto de idéias, situações, eventos e informações necessárias para o correto entendimento do ambiente, como sendo o contexto. Sendo uma extensão do RBAC/TRBAC, o modelo possibilita o acesso diferenciado para perfis distintos de usuários, ao mesmo tempo em que considera requisitos como temporalidade e hierarquia de privilégios. Sendo o contexto para autorização de acesso definido a partir de propriedades que representam as informações dinâmicas do ambiente, a lógica de controle de acesso pode ser fixada através de *condições de contexto* (regras), possibilitando que a concessão de autorização possa variar de acordo com a dinamicidade da propriedade incluída na condição de contexto. Como resultado, tem-se um modelo de autorização que possibilita a implementação facilitada de um controle de acesso dinâmico, baseado em informações contextuais, onde a delegação de atribuições pode ser tratada de maneira diferenciada, ou seja, através da análise das relações entre as propriedades de uma condição de contexto.

1.1 Motivação

O PEP não apenas revela muitos dados privativos dos pacientes que devem ser mantidos em sigilo, mas principalmente é a base de decisões que tem um profundo impacto no seu bem-estar (MARIN, 2003). Mais ainda, os dados contidos no PEP também fornecem matéria-prima para processos de tomada de decisão por instituições de saúde, governos e outras agências sem os quais os sistemas de saúde simplesmente não funcionariam (WECHSLER et al., 2003). Portanto, os profissionais de informática em saúde, ao influenciarem na construção, manutenção, armazenamento, acesso e manipulação de PEP's, desempenham um papel distinto dos de outros profissionais de informática.

Observa-se ainda que a moderna sociedade da informação utiliza um conjunto muito amplo de informações de indivíduos e instituições para propiciar atendimento à saúde de pacientes, planejar a alocação de recursos, regular as ações de operadoras de planos de saúde, planejar a gestão de serviços de saúde, etc. Estas informações são obtidas a partir de formulários em papel, bancos de dados isolados e por meio de vínculos entre bancos de dados

pertencentes a instituições diferentes (RODRIGUES, 2001). Por outro lado, esta ampla disponibilidade de dados propicia o risco de acesso, uso indevido de informações e a quebra de privacidade de indivíduos e instituições.

Diante desta exposição, surge a motivação para provar e validar um modelo de controle de acesso a informações médicas, mais especificamente a informações contidas em prontuários eletrônicos de paciente, que forneça uma abordagem mais realista às características e necessidades de acesso para diferentes usuários e situações.

1.2 Metodologia

A metodologia utilizada acerca da disponibilização de informações médicas teve cunho teórico-reflexivo com bases no mapeamento e análise da literatura sobre Prontuários Eletrônicos, com especial foco no tratamento da informação, na Legislação pertinente e na utilização das Tecnologias da Informação na área da saúde.

O processo de software adotado para a implementação do modelo e da arquitetura proposta foi o *desenvolvimento evolucionário* (SOMMERVILLE, 1996) que prevê que as atividades de especificação, projeto, implementação e validação ocorram simultaneamente. Com base em uma especificação preliminar, um protótipo inicial é projetado e implementado, para depois ser validado. O objetivo da validação é observar as deficiências do software em atender os requisitos previamente estabelecidos, de modo que o procedimento seja refinado e o ciclo se repita até que se atenda aos requisitos. Neste trabalho os requisitos gerais para o problema de controle de acesso ao Prontuário Eletrônico são estabelecidos e apresentados no capítulo 4.

A aplicação prática da implementação do modelo de controle de acesso utilizando informações contextuais se dá através da prototipação de módulos funcionais agregados a aplicações desenvolvidas pelo Centro de Processamento de Dados da Universidade Federal de Santa Maria (CPD-UFSM), e tem por objetivo prover o controle de acesso a informações utilizadas pelo Hospital Universitário de Santa Maria (HUSM).

As ferramentas de âmbito acadêmico utilizadas no desenvolvimento deste trabalho estão descritas no capítulo 5.

1.3 Contribuições da dissertação

O estudo realizado nesta pesquisa acerca da utilização de informações contextuais para prover o controle de acesso a informações médicas apresenta as seguintes contribuições:

- modelar as regras da política de segurança de uma forma mais condizente com a linguagem natural, possibilitando melhora na produtividade da gerência da política de segurança;
- incluir a possibilidade da delegação de atribuições de acordo com a normatização das atividades da área da saúde, possibilitando a melhor aceitação do sistema de tecnologia de informação junto a equipe de saúde;
- estabelecer um controle de acesso mais versátil aos módulos desenvolvidos pelo CPD-UFSM para atender ao Hospital Universitário.

1.4 Organização da Dissertação

O trabalho está dividido em seis capítulos. No capítulo 2 será apresentada uma revisão bibliográfica sobre o prontuário eletrônico do paciente e atividades relacionadas com o armazenamento e proteção de registros médicos. Também neste capítulo são abordados os preceitos legais pertinentes ao assunto. O capítulo 3 destaca os modelos de controle de acesso estudados e uma visão geral do modelo adotado pelo CPD-UFSM para prover acesso ao módulo SIE (Sistema de Informações Educacionais). No capítulo 4, são apresentadas a proposta e a especificação do modelo de controle de acesso baseado em informações contextuais. No capítulo 5 são apresentados detalhes sobre a implementação e testes. No último capítulo, apresentam-se as conclusões, indicando os objetivos alcançados e as principais contribuições para a área de conhecimento em questão, bem como algumas perspectivas para trabalhos futuros.

Capítulo 2

REVISÃO SOBRE LEGISLAÇÃO, ARMAZENAMENTO E PROTEÇÃO A REGISTROS MÉDICOS

Neste capítulo, apresenta-se uma revisão teórica e descritiva sobre a legislação vigente e questões sobre armazenamento e proteção a registros médicos, com destaque principal para a proteção ao acesso a registro médico informatizado, que servirá como fundamentação para o desenvolvimento desta dissertação.

2.1 Conceitos sobre Prontuário Eletrônico do Paciente

De acordo com (MASSAD, 2003) o prontuário do paciente é um elemento crucial no atendimento à saúde dos indivíduos, devendo reunir as informações necessárias para garantir a continuidade dos tratamentos prestados ao paciente.

O prontuário do paciente foi desenvolvido por médicos e enfermeiros para possibilitar que estes pudessem lembrar, de uma forma sistemática, os fatos e eventos clínicos sobre cada indivíduo de forma que todos os demais profissionais envolvidos no processo de atenção de saúde pudessem também ter as mesmas informações (SLEE, 2000). Desta forma, o prontuário representa o mais importante veículo de comunicação entre os membros da equipe de saúde responsável pelo atendimento.

Ao considerar o conteúdo do prontuário do paciente, vale destacar que todo e qualquer atendimento em saúde pressupõe o envolvimento e a participação de múltiplos profissionais: médicos, enfermeiros, nutricionistas, psicólogos, fisioterapeutas entre outros. Além disso, freqüentemente as atividades de atendimento ao paciente acontecem em diferentes locais, tais como: sala de cirurgia, enfermarias, ambulatórios, unidade de terapia intensiva (UTI) ou consultórios.

Para a realização destas atividades, são necessárias múltiplas informações de diferentes fontes. Por outro lado, os procedimentos realizados pelos profissionais individualmente também geram outras tantas informações, que vão garantir a continuidade do processo de cuidado. São diferentes fontes de dados, gerando conseqüentemente uma grande

variedade de informações. Tais dados necessitam ser agregados e organizados de modo a produzir um único documento que servirá de apoio para tomada de decisões sobre o tipo de tratamento ao qual o paciente deverá ser submetido, orientando todo o processo de atendimento à saúde de um indivíduo ou de uma população.

Vale ressaltar que o dado clínico é muito heterogêneo para ser introduzido em sistemas tradicionais de informação. Por este motivo o Prontuário deve permitir que seus criadores e usuários possam intervir para resolver problemas de ordem clínica, administrativa ou de gestão em organizações de saúde, garantindo que todos possam agir coerentemente sobre as decisões a serem tomadas em relação ao paciente ao qual o prontuário se refere.

De acordo com (PINTO, 2006) o prontuário do paciente é um documento que contém registradas todas as informações concernentes a um paciente, sejam elas de caráter de identificação, socioeconômico, de saúde (radiografias, receitas, resultados de exames, diagnósticos de especialistas, notas de evolução redigidas por pessoal de enfermagem com relação ao progresso observado) ou administrativo, dentre outros. Na verdade, trata-se da memória escrita (ou armazenada) da história da pessoa doente, sendo, portanto, indispensável para a comunicação intra e entre a equipe de saúde e o paciente. Tornando-se um documento primordial para garantir a continuidade, a segurança, a eficácia e a qualidade do tratamento do indivíduo, bem como da gestão das organizações hospitalares.

2.2 Aspectos Legais

A questão mais complexa a ser definida nas políticas de segurança da informação em saúde diz respeito ao controle de acesso, ou seja, quem tem direito de acesso aos dados de saúde. A definição desta política implica na participação de todos os envolvidos no processo saúde, onde o Governo desempenha o papel de regulador e direcionador da discussão. Em geral, esta é uma discussão de longo prazo, conforme visualizado pela experiência internacional (VARGA, 1980).

Cientes desta complexidade, a preocupação primordial deste trabalho visa à adequação com a legislação pertinente, sem ferir seus aspectos legais nem reduzir ou maximizar a importância de sistemas de controle de acesso. Além disto, com a crescente disponibilização de informações em meio eletrônico, bem como a utilização de tele medicina em diagnósticos e/ou tratamentos à distância, torna-se necessário verificar, *a priori*, se o modelo de controle de acesso atenderá as especificações da legislação e a normatização por ela exigida.

2.2.1 Padrões Internacionais

No contexto mundial, desde 1990, a Organização das Nações Unidas (ONU), por intermédio do seu Alto Comissariado, exige respeito aos princípios de confidencialidade, não-discriminação em relação aos dados pessoais, segurança dos arquivos, declarações e legitimidade das informações. Por exemplo, questões éticas não devem constar nos prontuários, salvo se realmente necessárias. Por outro lado, a Organização de Cooperação e de Desenvolvimento Econômico (OCDE) recomenda aos seus Estados Membros que limitem a coleta dos dados apenas aos que forem considerados úteis e sem constrangimentos aos indivíduos.

No contexto europeu, desde 1995, foram estabelecidas ações para harmonizar as normas. Na França, a Lei n° 78-17 de 06 de janeiro de 1978 - relativa à informática, aos arquivos e liberdades, diz respeito apenas às questões de saúde (VARGA, 1980); a Lei nº. 94-548 de 01 de julho 1994 é mais específica em relação aos dados nominativos concernentes a pesquisa médica; e a Lei n° 99-461 de 27/07/1999, denominada *Couverture Maladie Universelle* (CMU), também trata sobre PEP's.

A Associação Médica Mundial (AMM), fundada em 1947, tem emitido uma série de resoluções e declarações (KFOURI NETO, 2003). Em 1948, a AMM adotou a Declaração de Genebra, um juramento do médico, que foi posteriormente adotado no Código Internacional de Ética da AMM. Essa declaração lista diversas responsabilidades, incluindo o dever do respeito aos segredos que são confiados ao médico, mesmo após a morte do paciente.

Em 1964, a AMM adotou uma declaração detalhada de princípios éticos para a pesquisa médica que ficou conhecida como Declaração de Helsinque (VARGA, 1980). Esta declaração sofreu revisões em 1975 e 2000. Nesta declaração, a privacidade e consentimento informado são considerados centrais para a preservação da integridade e dignidade de indivíduos humanos. Ao considerar os benefícios e ônus devido ao uso de computadores na medicina, a AMM, em 1973, adotou resoluções que reafirmaram a importância vital da manutenção do segredo médico para a proteção da privacidade de indivíduos como base para a relação de confiança entre o médico e o paciente.

Atualmente, na sua versão revisada, a Declaração sobre o Uso de Computadores na Medicina busca harmonizar o dever de respeitar a confidencialidade, como proclamada na Declaração de Genebra, com a pesquisa médica que pode ser facilitada com o processamento eletrônico dos dados. A declaração estabelece que não se caracteriza em uma quebra de confidencialidade liberar ou transferir informações confidenciais sobre a atenção à saúde

necessárias para o propósito de se conduzir pesquisa científica, desde que as informações liberadas não identifiquem, direta ou indiretamente, qualquer paciente individual em qualquer relatório de tal publicação.

Não é objetivo deste trabalho realizar uma análise comparativa das resoluções acima citadas. Elas levantam, entretanto, uma série de questões que devem ser abordadas por leis de proteção à privacidade.

2.2.2 Legislação Brasileira

A Constituição Federal Brasileira (BRASIL, 1988), em seu Artigo 5º, assegura à todos os brasileiros a inviolabilidade do direito à segurança, abrangendo entre outros os seguintes itens:

1) é inviolável o sigilo de dados;

2) é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

3) são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

4) todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

No artigo 196, a Constituição estabelece que “A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação”.

Deste modo, subentendem-se os direitos individuais à privacidade. Mas a mesma Constituição prevê situações onde o interesse público pode tornar relativo o sigilo absoluto de certos dados, principalmente na área da saúde, em função de políticas sociais e econômicas que visem à redução do risco de doenças e de outros agravos, ou por necessidade de exercício profissional.

O Conselho Federal de Medicina (CFM) está empenhado no contexto legal e ético do prontuário do paciente, tendo aprovado a Resolução CFM no. 1.331/89, que trata da temporalidade do PEP, e as portarias de nº. 1.638/2002 e nº. 1.639/2002 que normalizam o uso de sistemas informatizados, a guarda e o manuseio de prontuários. Portanto, todos os

aspectos legais do PEP vêem ao encontro da autenticidade, integridade, confidencialidade, privacidade, auditagem, assinatura eletrônica e guarda de documentos. Estes documentos configuram-se em referências balizadoras sobre o tema, comportando alguns aspectos diretamente relacionados ao assunto:

- Resolução nº. 1.331/89: Art. 1º - O prontuário médico é documento de manutenção permanente pelos estabelecimentos de saúde;
- Resolução nº. 1.605/00: Art. 1º - O médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica; Art. 2º - Nos casos do art. 269 do Código Penal, onde a comunicação de doença é compulsória, o dever do médico restringe-se exclusivamente a comunicar tal fato à autoridade competente, sendo proibida a remessa do prontuário médico do paciente.

Considerado todo o exposto, fica evidente que a relação física médico-paciente necessita de aprimoramento na sua regulamentação, pois já estão inseridos novos elementos que vão permeá-la daqui para frente - as ciências da informação, da computação e da comunicação, sob as mais variadas formas, metodologias e tecnologias – e o sigilo das informações recebidas e transmitidas deve ser mantido por mecanismos de total segurança (CASTRO et al., 2004), pois os prontuários eletrônicos dos pacientes assistidos não podem ser violados, tendo em vista o respeito e a garantia do sigilo, da privacidade e do segredo profissional, de forma a que os novos sistemas de informações que utilizam os meios modernos de controle de acesso não se revelem tão inseguros quanto os baseados nas velhas pastas, fichas e papéis.

Sabe-se que não existe sistema impossível de ser burlado e que impeça de forma permanente e completa o acesso indevido aos dados computadorizados. Então, do mesmo modo que é importante estabelecer mecanismos de segurança para acesso aos dados armazenados, definindo quem pode, quando pode e como pode ter acesso às informações de um paciente contidas em prontuário eletrônico; fundamental é dispor, além de aplicativos de controle e monitoração, sistemas de auditoria que permitam saber quem, quando e de onde foi acessado o prontuário, mesmo que não tenha sido extraído nenhum relatório.

2.3 Necessidade de Utilização do PEP em Hospitais Universitários

Dentro do cenário atual, o Prontuário de Pacientes é o documento básico de um hospital, e permeia toda a sua atividade assistencial, de pesquisa, ensino e atividades administrativas. É o elemento de comunicação entre os vários setores do hospital e entre os

diferentes atores envolvidos, e depositário de um conjunto muito grande e rico de informações, capazes de gerar conhecimento.

Portanto, o Prontuário de Pacientes deve suprir os diversos atores envolvidos no processo, com as informações necessárias quando, onde e como o usuário necessitar, nas mais diversas atividades. Essas necessidades incluem o apoio à equipe médica, para a tomada de decisão diagnóstica e terapêutica; o suporte aos pesquisadores, na busca de dados para pesquisas relevantes; aos professores, nas atividades didáticas, nas quais a técnica de estudo de casos é muito utilizada; aos administradores, nas tarefas de faturamento e emissão de relatórios gerenciais e para prover o suporte legal, quando necessário.

Não existe uma definição, na legislação brasileira, a respeito do conteúdo obrigatório do PEP. Entretanto, o Instituto Nacional de Assistência Médica da Previdência Social (INAMPS), mediante a Ordem de Serviço 5/83, enumera o seguinte conteúdo: capa, anamnese e exame físico, exames complementares, sumário de baixa, termo de responsabilidade, folha de identificação, evolução clínica, gráfico de sinais vitais, plano terapêutico, histórico de enfermagem e outros documentos apropriados para casos particulares (controle de anestesia, relatório cirúrgico, evolução obstétrica, entre outros).

De acordo com (SHORTLIFFE, 1990), pode-se classificar os propósitos do Prontuário do Paciente em três (3) grandes grupos: assistência ao paciente, suporte financeiro e legal e pesquisa clínica.

Esses propósitos não são imutáveis e devem alterar-se com a introdução das novas tecnologias de informação.

Ainda de acordo com (SHORTLIFFE, 1990), entre as deficiências encontradas em prontuários convencionais (não eletrônicos), pode-se destacar o seguinte:

• aspectos pragmáticos: as informações contidas no Prontuário do Paciente devem estar disponíveis onde, quando e como elas são necessárias, para qualquer membro da equipe responsável pelo atendimento do paciente, mas nem sempre isto é possível, pois o Prontuário pode não ser localizado, pode não conter a informação desejada, ou essa informação estar ilegível ou incompleta;

• redundância de informações: informações duplicadas são comuns, anotadas por diferentes profissionais em diferentes momentos, em diferentes procedimentos. Embora possa haver motivos para anotações de diferentes formas e em diferentes localizações do Prontuário, o processo acelera o seu crescimento físico e dificulta a tarefa de consulta;

• influência na pesquisa clínica: a pesquisa clínica e epidemiológica retrospectiva, realizada em Prontuários, é de fundamental importância para a Medicina. É tediosa e muito

trabalhosa a busca de informações para pesquisas retrospectivas em prontuários convencionais e, por essa razão, o conhecimento médico existente nas anotações e teoricamente possível de ser extraído delas, perde-se de forma irreversível;

• a natureza passiva do Prontuário do Paciente (PP): o sistema manual tradicional apresenta uma característica que só foi identificada após o advento do Prontuário Eletrônico; a sua natureza é passiva e as informações permanecem arquivadas até que sejam solicitadas por alguém. São insensíveis às características dos dados armazenados nas suas páginas, tais como legibilidade, exatidão ou implicações para o atendimento ao paciente.

Portanto, o Prontuário de Pacientes (PP) é o documento básico dentro de um Sistema de Informações Hospitalares (SIH), e seu armazenamento na forma tradicional, em papel, acarreta inúmeros problemas para a adequada recuperação e utilização das informações neles contidas, principalmente em se tratando de hospitais universitários.

A utilização adequada da Tecnologia da Informação (TI) permite o desenvolvimento de Prontuários Eletrônicos de Pacientes (PEP), que atendam mais prontamente às necessidades dos diversos usuários. A definição do conteúdo e do formato das informações relevantes que devem ser armazenadas são etapas fundamentais na consecução deste desejado cenário.

A informação representa dados em uso e este uso implica usuários e, portanto, o sistema deve identificar quem necessita qual informação e quando, onde e como a informação é necessária. A concepção de um Sistema de Informação, portanto, não pode ser conduzida, unicamente, por profissionais de informática. Essa tarefa demanda alto nível de participação e de controle dos usuários finais. As necessidades e exigências do usuário devem dirigir os esforços de construção do Sistema de Informação. Neste sentido, a elaboração de um modelo de controle de acesso, que atenda a linguagem natural e facilite a interação entre os profissionais da saúde e a informação por estes manipulada, pode propiciar uma integração maior entre tecnologia e a atividade fim.

A evolução na direção do prontuário eletrônico é tanto desejável quanto inevitável, principalmente em ambientes universitários. Até o momento, no entanto, muitos profissionais médicos têm sido lentos na adoção do computador como ferramenta clínica, apesar do uso crescente desta em atividades administrativas.

Apesar da vontade e da inevitabilidade, grande parcela de incerteza ronda o *status* legal do prontuário eletrônico. A história nos ensina que as mudanças nos paradigmas legais ocorrem, geralmente, por pressão de situações já criadas e adotadas por consenso da sociedade.

Uma vez que modelos sólidos de controle possam atender estes requisitos, a utilização de prontuários eletrônicos pode passar a sofrer a influência do consenso. Por este motivo o capítulo que se segue visa explanar sobre modelos de controle de acesso que atendam as peculiaridades de acesso ao PEP.

Capítulo 3
MODELOS DE CONTROLE DE ACESSO

O controle de acesso ao PEP, em nenhuma circunstância, deve prejudicar o atendimento ao paciente por negar acesso legítimo às informações e aos serviços requisitados pelo pessoal médico. No entanto, as informações do prontuário devem permanecer sigilosas, exceto quando em atendimento à vontade do paciente ou a determinações legais.

Este capítulo traz considerações sobre modelos de controle de acesso que possam vir a atender esta premissa. O problema é que não existe um modelo claro sobre a política de autorização e controle de acesso a ser adotada para o PEP, isto é, como determinar quem tem direito a acessar certas classes de informações, com quais privilégios e em quais condições.

É indesejável impor um controle de acesso tão restrito que impeça um médico, em uma sala de emergência, de acessar o prontuário de um paciente gravemente doente. Neste caso, a circunstância da emergência deve ser considerada uma exceção, sobrepondo-se a restrições de acesso estabelecidas. O controle de acesso nos sistemas computacionais normalmente segue as seguintes diretrizes (SANDHU, 1994):

- Modelo Discricionário (DAC);
- Modelo Obrigatório (MAC);
- Modelo Baseado em Perfis (RBAC).

Além destas diretrizes de controle de acesso, que podem ser complementares entre si, também tratamos neste capítulo alguns modelos de controle de acesso pesquisados por Motta (2002) para atender a utilização do PEP no InCor, e outros modelos relacionados especificamente à utilização de contextos.

3.1 Modelos Discricionário e Obrigatório

As políticas de controle do modelo DAC (*Discretionary Access Control*) são baseadas na identidade dos usuários. As autorizações especificam para cada usuário (ou grupo de usuários) e para cada objeto do sistema os modos de acesso permitidos. Enquanto que as políticas de controle do modelo MAC (*Mandatory Access Control*) são baseadas na

classificação dos *subjects* e *objects* do sistema. Para cada objeto e usuário do sistema é associado um nível de segurança.

O nível de segurança associado ao objeto reflete o nível de importância da informação contida no objeto, classificando o objeto quanto ao dano potencial que um acesso não autorizado traria. O nível de segurança associado ao usuário, também chamado de *clearance*, reflete o nível de confiabilidade do usuário em não expor a informação a um usuário que não esteja autorizado para tal (SANDHU, 1994). De maneira geral, o acesso de um usuário a um objeto é verificado em função do relacionamento entre os níveis de segurança deles, levando-se em conta o tipo de acesso solicitado.

3.2 Role-Based Access Control (RBAC)

As políticas de controle de acesso deste modelo são baseadas nas atividades que os usuários desempenham no sistema (perfis). Esta estratégia torna necessária a identificação dos perfis dentro do sistema. Um perfil pode ser visto como um conjunto de ações e responsabilidades associadas a uma atividade de trabalho (SANDHU, 1994).

Uma grande vantagem decorre desta abordagem: em vez da atribuição de direitos de acesso de forma individualizada a cada usuário, esta atribuição é feita aos perfis. Em uma segunda etapa, os usuários são associados a perfis em função das atividades desempenhadas no sistema. Assim o modelo RBAC oferece um controle mais flexível do que os modelos discricionário e obrigatório para o estabelecimento de políticas de autorização. Como pode ser visto, no modelo de acesso discricionário os direitos de acesso são mapeados individualmente a usuários ou a grupos de usuários, um esquema pouco flexível e que limita bastante o gerenciamento das permissões de acesso. Já no modelo obrigatório, ocorre o uso de um esquema de classificação em níveis de segurança, também muito rígido para as necessidades da maioria das organizações.

Um importante conceito também empregado pelo RBAC é a hierarquia de perfis. Em um cenário típico de uma organização, indivíduos que desempenham diferentes funções podem executar tarefas em comum. Neste sentido, a hierarquia entre perfis simplifica bastante a descrição de direitos de usuários, pois evita a necessidade de especificar de forma repetida operações em comum. Ainda, este relacionamento hierárquico pode ser balizado pela estrutura hierárquica das próprias organizações, permitindo que a política de segurança seja descrita de maneira extremamente natural. Em uma hierarquia de perfis, um perfil pode "conter" outros perfis. No RBAC, um perfil hierarquicamente superior pode conter um ou

mais perfis hierarquicamente inferiores. Isto significa que um perfil superior tem todos os privilégios e pode executar todas as operações que os perfis de níveis inferiores contêm.

O RBAC ainda apresenta outra peculiaridade, segundo Ferraiolo et al. (2001) no controle de acesso discricionário o número de associações gerenciáveis é da ordem de $\sum_{i=1}^{n}$ ($|U_i| . |A_i|$), enquanto que no RBAC ele é reduzido para $\sum_{i=1}^{n}$ ($|U_i| + |A_i|$), onde U_i é o conjunto de indivíduos com função organizacional i, A_i é o conjunto de autorizações necessárias para a função e n é o número de funções existentes.

Segundo (MOTTA, 2002), isto viabiliza a administração de uma política de acesso detalhada, com granularidade fina, para um número maior de usuários e recursos, abrangendo coerentemente todos os sistemas que possam vir a compor o PEP. FERRAIOLO et al. (2001) ainda sugerem o princípio do privilégio mínimo, que ao invés de se adotar uma política abrangente, liberando o acesso aos PEP's para todos os usuários com perfil "Médico", pode-se aplicar uma política pormenorizada, onde a liberação de acesso se daria somente aos médicos com vínculo assistencial com o paciente em questão. Isto reduziria a quantidade de prontuários passíveis de acesso sem necessidade e, como visto anteriormente, sem legalidade.

Outro ponto interessante é que os procedimentos para remoção de privilégios ou bloqueio de contas de acesso ao PEP, quando o vínculo de um usuário se encerra, podem ser feitos de forma confiável e sem muito esforço (MOTTA, 2002), mesmo quando uma alta rotatividade de pessoal é observada. Isto é bastante útil em hospitais escola, onde o número de usuários com vínculo temporário pode ser considerável.

3.3 Modelos Derivados do RBAC

Após a concepção do RBAC, muitos modelos surgiram para suprir algumas características não vislumbradas anteriormente, ou mesmo para atender peculiaridades específicas de algumas aplicações.

Em (MOTTA, 2003a) têm-se uma sumarização de alguns destes modelos, onde o autor trata da caracterização e diferenciação quanto à utilização de regras contextuais, implementação e a aplicabilidade no âmbito do PEP.

Julgando estas informações necessárias e totalmente relevantes para o escopo deste trabalho, transcrevemos algumas destas características que são demonstradas através da tabela 3.1.

Tabela 3.1 – Sumário das características dos modelos derivados do RBAC.

Modelos	Características		
	Regras contextuais	Implementação	Aplicação ao PEP
E-RBAC (COVINGTON et al., 2003)	Usadas para ativação/desativação de perfis ambientais	Protótipo desenvolvido na plataforma Java 2 SE	Não relatada
C-TMAC (GEORGIADIS et al., 2001)	Vinculadas a equipes e definidas como cláusulas *where* da linguagem SQL	Protótipo desenvolvido na plataforma Oracle e implementado em PL/SQL	Sim, em caráter experimental.
CS-RBAC (KUMAR et al., 2002)	Definidas em perfis que relacionam os contextos de usuário e de objeto, que são fixos	Protótipo desenvolvido nas tecnologias JSP e servlets e disponibilizado na plataforma Tomcat	Não relatada
TCM (LONGSTAFF et al., 2003)	Não utiliza	Protótipo desenvolvido com base em SQL e XML na plataforma .NET/C#	Sim, num estudo de caso contemplando requisitos de confidencialidade para informações clínicas de pacientes na Grã-Bretanha.
DRIVE-RBAC (WILIKENS et al., 2002)	Usadas para ativação/desativação de perfis em sessões de um usuário específico, de acordo com o estado de um conjunto fixo de variáveis contextuais	Não relatada	Sim, em um estudo de caso para um sistema de suprimento de drogas integrado ao PEP
RBPEAC (LIN et al., 2000)	Definidas nas autorizações por meio de expressões em Prolog	Disponibilidade de bibliotecas para as plataformas Windows NT 4.0 e HP-UX 11.0	Não relatada
XORBAC (NEUMANN et al., 2003)	Definidas como um conjunto de condições (restrição contextual) que determinam a validade de uma autorização	Disponibilidade de um produto acabado, implementado para as plataformas Unix-like e Windows, para uso sem fins comerciais	Não relatada
OASIS (BACON et al., 2002)	Definidas como regras (cláusulas de Horn) que determinam as condições para ativação/desativação dinâmica de perfis	Protótipo desenvolvido em Java com web services usando SGBD PostgreSQL como suporte	Sim, em um estudo de caso contemplando requisitos de confidencialidade
GTRBAC (JOSHI et al., 2003)	Usadas de forma generalizada para impor restrições (temporais) nas entidades e relações que compõem o modelo	Protótipo com funcionalidade reduzida desenvolvido na plataforma Oracle com implementação em PL/SQL	Sim, nos exemplos apresentados nos trabalhos que descrevem o modelo

3.3.1 Modelo E-RBAC

O modelo E-RBAC (*Environment Role-Based Access Control*) foi desenvolvido por (COVINGTON et al., 2003 apud MOTTA, 2003a) para ser aplicado em uma arquitetura de sistema para "residências inteligentes". O E-RBAC estende o RBAC básico com a introdução de um novo tipo, denominado perfil ambiental. Entretanto, diferentemente dos perfis tradicionais do RBAC, o perfil ambiental não possui usuários associados, mas sim autorizações e uma regra que estabelece as condições de ativação/desativação automática do perfil, com base em um conjunto de informações ambientais (por exemplo: horário, temperatura, nível de ruído, localização do usuário, etc), estas informações são capturadas por sensores distribuídos pela residência.

O acesso para a execução de uma operação é concedido a um usuário quando este possui um perfil tradicional e todos os perfis, do conjunto de perfis ambientais, estão ativos no momento da requisição de autorização (MOTTA, 2003a). As regras contextuais são suportadas pelo modelo na definição das condições de ativação/desativação dos perfis ambientais. Segundo (MOTTA, 2003a) um protótipo do modelo foi desenvolvido na plataforma Java 2 SE (SUN MICROSYSTEMS, 2003) e não há relatos sobre sua aplicação no âmbito do controle de acesso ao PEP.

3.3.2 Modelo C-TMAC

O modelo C-TMAC (*Contextual Team-Access Control*) foi desenvolvido por (GEORGIADIS et al., 2001 apud MOTTA, 2003a) para gerir políticas de acesso em ambientes colaborativos. Segundo MOTTA (2003a) o C-TMAC estende o RBAC básico com a introdução de equipes, contextos e relacionamentos usuário-equipe e equipe-contexto.

O modelo foi especificado sem suporte a hierarquia de perfis. Os autores ainda relatam a utilização de separação de responsabilidade estática[3] (SRE) (GLIGOR et al., 1998), que atua na relação usuário-perfil e na hierarquia de perfis para evitar usuários comuns entre perfis e equipes específicas. As regras contextuais são suportadas pelo C-TMAC associadas a equipes e utilizadas como critério de filtragem de autorizações possíveis para os perfis ativos de membros de cada equipe. Um protótipo foi desenvolvido na plataforma Oracle

[3] Segunda a definição de Gligor et al. (1998), uma separação de responsabilidade estática é um conjunto de pares de perfis conflitantes, onde nenhum usuário pode estar associado a mais do que um perfil de cada par. Ainda segundo os autores, existe a separação de responsabilidade dinâmica (SRD), que é dependente da ativação de perfis pelos usuários.

(FERNANDES, 2002), com implementação em SQL (CELKO, 1999), para uma aplicação em intranets na área da saúde. Nesta implementação as autorizações são definidas como visões ou consultas a bancos de dados relacionais e as regras contextuais são modeladas como cláusulas *where* da linguagem SQL, aplicadas para filtrar as requisições (consultas) de autorização.

3.3.3 Modelo CS-RBAC

O CS-RBAC (*Context-Sensitive Role-Based Access Control*) foi desenvolvido por (KUMAR et al., 2002 apud MOTTA, 2003a) e estende o RBAC básico através da introdução dos conceitos de contextos de perfis e de filtros contextuais. O modelo foi especificado sem hierarquias de perfis e sem restrições de separação de responsabilidades. Segundo (MOTTA, 2003a) existem apenas dois contextos (de usuário e de objeto) e que estes estão fixos na linguagem usada para expressar os filtros contextuais. Um protótipo do modelo foi disponibilizado na plataforma Tomcat (APACHE, 2003) para utilização em um estudo de caso de *web services* (NEWCOMER, 2002). Não existem relatos sobre a aplicação do modelo para controlar o acesso ao PEP.

3.3.4 Modelo TCM

O TCM (*Tees Confidentiality Model*) foi desenvolvido por (LONGSTAFF et al., 2003 apud MOTTA, 2003a) e estende o RBAC básico com a introdução dos conceitos de coleções e de identidades. As coleções possuem elementos que podem ser membros das coleções ou outras coleções. A capacidade de conter subcoleções às tornam hierarquicamente modeláveis.

O modelo TCM suporta hierarquias gerais para perfis, identidades e objetos por meio de coleções, não suporta restrições, nem regras contextuais. Uma implementação piloto foi desenvolvida em SQL e XML (W3 CONSORTIUM, 2000), na plataforma .NET/c# (LIMA, 2002), para demonstrar a aplicação do modelo em um estudo de caso que contemplava requisitos de uma política proposta para prover o controle de acesso a informações clínicas de pacientes na Grã-Bretanha.

3.3.5 Modelo DRIVE-RBAC

O modelo DRIVE-RBAC foi desenvolvido por (WILIKENS et al., 2002 apud MOTTA, 2003a) para utilização no projeto DRIVE (*Drug in Virtual Enterprise*). De acordo com (MOTTA, 2003a) o DRIVE-RBAC estende o RBAC básico com a modificação do

conceito de usuário, a introdução de propriedades dinâmicas baseadas em contextos e em eventos para ativação/desativação de perfis, o que pode tornar o modelo mais flexível. Os autores utilizam o estado da arte do RBAC para demonstrar a integração do conceito com características de sistemas de saúde, mas a idéia de contexto se dá no sentido de autenticação de usuários, onde parâmetros como "localização" são utilizados para garantir níveis de autenticidade do usuário. Um usuário não refere-se a apenas um único indivíduo, mas uma categoria de indivíduos agrupados segundo alguns critérios específicos.

Segundo (MOTTA, 2003a), o DRIVE-RBAC suporta hierarquias gerais para perfis e usuários. Os autores relatam a existência de separação de responsabilidades estática e dinâmica, porém não demonstram como está integrada ao modelo. As regras contextuais são usadas para ativação/desativação de perfis em sessões de usuários específicos, de acordo com um conjunto fixo de variáveis disponíveis nos contextos de tempo; de local de acesso do usuário; e da circunstância no momento do acesso. Entretanto, não há relatos sobre a existência de uma implementação do modelo, os autores apenas descrevem sua integração a uma arquitetura e apresentam um estudo de caso para um sistema de suprimento de drogas para o PEP.

3.3.6 Modelo RBPEAC

O RBPEAC (*Role-Based Policy-Enforced Access Control*) foi desenvolvido por (LIN et al., 2000 apud MOTTA, 2003a) para estender o RBAC básico com a introdução de regras lógicas às autorizações de acesso e pela definição de políticas para a atribuição dinâmica de usuários a perfis. Estas regras são expressas na linguagem de programação Prolog (CLOCKSIN, 1984) e são avaliadas durante uma requisição de acesso. Se o resultado da avaliação é verdadeiro, a autorização é positiva, caso contrário, ela é negativa.

Este modelo não suporta hierarquia de perfis nem separação de responsabilidades. O modelo ainda suporta regras por meio de expressões em Prolog nas autorizações, com os contextos definidos nas variáveis e nas relações disponíveis na linguagem. Não há relatos da aplicação no âmbito do PEP.

3.3.7 Modelo XORBAC

O modelo XORBAC (*eXtended Object Role-Based Access Control*) foi desenvolvido por (NEUMANN, 2003 apud MOTTA, 2003a) para a utilização em aplicações web e estende o RBAC básico com a introdução de restrições contextuais para determinar uma autorização

de acesso. Uma restrição contextual é formada por condições contextuais que definem uma relação booleana entre valores de atributos contextuais.

De acordo com (MOTTA, 2003a) o XORBAC suporta hierarquia de perfis com herança de autorizações e separação estática de responsabilidades pela definição de perfis ou de autorizações mutuamente exclusivas. As regras contextuais determinam as condições em que as autorizações podem ser válidas. Não existem relatos da utilização do modelo XORBAC em aplicações ao PEP nem em aplicações da área da saúde.

3.3.8 Modelo OASIS

O OASIS (*Open Architecture for Securely Interworking Services*) foi desenvolvido por (BACON et al., 2002 apud MOTTA, 2003a) para atender os requisitos dependentes de contexto vislumbrados em sistemas como o PEP. O modelo estende o RBAC básico com a introdução dos conceitos de designação, perfis parametrizados com ativação condicionada por regras e regras de autorização. Uma regra de autorização, de acordo com (MOTTA, 2003a), impõe restrições contextuais que devem ser satisfeitas para associar dinamicamente uma autorização a um perfil, sendo definida através de uma cláusula de Horn (HORN, 1951). As cláusulas de Horn estabelecem todas as condições que devem ser satisfeitas para que um usuário possa ativar um perfil em uma sessão particular.

O modelo não suporta hierarquia de perfis e a separação de responsabilidade dinâmica pode ser configurada por meio de regras de ativação de perfis. Regras contextuais podem ser definidas nos perfis como condição para ativação/desativação pelo usuário, ou na relação perfil-autorização, como condição para a vinculação de um perfil a uma autorização. Os autores relatam a implementação de um protótipo em Java com web services, utilizando o SGBD do PostgreSQL (MONJIAN, 2000) para suporte às regras e para armazenar os dados persistentes do modelo. O protótipo foi utilizado em uma aplicação para contemplar requisitos de política de confidencialidade proposta para controlar o acesso a informações clínicas de pacientes na Grã-Bretanha.

3.3.9 Modelo GTRBAC

O GTRBAC (*Generalized Temporal Role-Based Access Control*) foi desenvolvido por (JOSHI et al., 2003) para generalizar o modelo TRBAC (*Temporal Role-Based Access Control*) proposto pro (BERTINO et al., 2001) e estende o RBAC básico com a introdução de

uma linguagem que especifica várias restrições temporais em perfis. O modelo suporta hierarquia de perfis dependente de restrições temporais.

É relatado por (BERTINO et al., 2001) o desenvolvimento de um protótipo do TRBAC na plataforma Oracle, e aguarda-se uma implementação completa da especificação do GTRBAC em SQL ou XML. Os autores relatam a aplicação do modelo ao PEP somente nos exemplos demonstrados em seus trabalhos, não havendo estudos de caso mais elaborados.

3.4 MACA

O MACA (*Middleware* de Autenticação e Controle de Acesso) foi desenvolvido por (MOTTA 2003a) para estender o RBAC básico com a introdução de autorizações contextuais. Estas autorizações incorporam uma expressão lógica, denominada regra de autorização, que relaciona informações de contexto em uma tentativa de acesso, e adicionalmente, esta autorização pode ser do tipo forte ou fraca, onde autorizações do tipo forte estabelecem políticas restritas, que não podem ser revogadas; e as autorizações do tipo fraca são utilizadas em políticas mais permissivas.

A idéia chave do modelo é decidir pela autorização positiva ou negativa de acordo com as regras de autorização que relacionam as informações sobre o contexto em que cada autorização está sendo solicitada. Além disto, o modelo trata a separação de responsabilidades no âmbito do PEP, e a hierarquia de perfis, conforme exigido pela legislação brasileira (CFM, 2002).

Entretanto, associações entre autorizações e perfis ou ativação dinâmica de mais de um perfil são as potenciais causas da ocorrência de conflitos de autorização (MOTTA, 2003a). O MACA estabelece contribuições significativas para solucionar o controle de acesso ao PEP, mas não resolve apropriadamente a detecção e tratamento de conflitos que possam resultar em possíveis violações da política de separação de responsabilidades, nem trata a delegação de atribuições, que no âmbito hospitalar é uma prática bastante utilizada (MOTTA, 2003a). O MACA foi desenvolvido através de uma implementação integrada ao serviço de diretórios LDAP (*Lightweight Directoty Access Protocol*) (YEONG et al., 1995) com linguagem de programação Java e padrões de segurança da arquitetura CORBA (OMG, 2001) para prover acesso ao PEP do Instituto do Coração (InCor) de São Paulo.

3.5 CSAC

Assim como em (MOTTA, 2003a), Hulsebosch et al. (2005) também apresentam um modelo de controle de acesso sensível a contextos, o CSAC (*Context Sensitive Access Control*), o qual utiliza regras e informações contextuais. Entretanto, também não definem precisamente o escopo do termo utilizado. As regras definidas por (HULSEBOSCH et al., 2005) são bem modeladas, porém a utilização do termo ”contexto” reporta-se apenas ao sentido do ambiente a que a política de controle de acesso está inserida. Observa-se que se os contextos forem adequadamente modelados, fazendo parte do modelo, as relações contextuais podem ser melhor exploradas.

A arquitetura do CSAC reflete as regras de negócio através de uma versão simplificada de outros modelos sensíveis a contexto, e as operações não envolvem somente o acesso, propriamente dito, mas também algumas informações de outros recursos, como mecanismos de autenticação e *logs* de acesso. Os autores relatam a implementação de um protótipo para utilização em um portal web em linguagem java.

3.6 CAAC e CASPEr

Após o MACA, Hu e Weaver (2004) descrevem o CAAC (*Context-Aware Access Control*) como sendo uma extensão ao RBAC básico. O modelo associa permissões de acesso com o conceito “ciente de contexto” (SCHILIT, 1994 apud DEY, 1999). Cada requisição é avaliada dinamicamente de acordo com o contexto atual do pedido de acesso. Assim o modelo é capaz de tomar decisões sobre autorizações baseadas em informações de contexto e perfis. Além disso, os administradores têm a flexibilidade de especificar políticas sensíveis a contextos. O mecanismo de autorização pode especificar cada política “ciente de contexto” automaticamente porque não é limitada estaticamente a nenhuma aplicação. Entretanto, cada tipo de definição de contexto é independente da especificação das regras de acesso.

Neste modelo de controle de acesso ciente de contexto, uma política de acesso especifica quais perfis têm permissões sob algumas situações contextuais (HU, 2004). Embora as políticas de acesso sejam usadas principalmente para que o mecanismo de autorização possa tomar decisões sobre o controle de acesso, estas políticas necessitam também ser verificadas sob domínios de confiança. Estes domínios de confiança são garantidos através de mecanismos de autenticação de usuário, onde o nível de acesso é estabelecido de acordo com o nível de confiabilidade da autenticação do usuário.

Em (HAN, 2005) é apresentado o modelo CASPEr (*Context Aware Security Policy Enforcement*) que estabelece que as políticas de segurança devem ser ajustadas dinamicamente de acordo com a informação relevante no contexto. A política de segurança de um sistema consiste em diversas regras, que são estabelecidas de acordo com um contexto específico de uma entidade; as decisões de acesso são tomadas e reforçadas através do conceito “ciente de contexto”.

Os autores relatam que o CAAC foi implementado em um protótipo como portal web denominado Ceberus (HU, 2004) e existem trabalhos em que o modelo é nomeado como CBAC (*Context-Based access Control*), já o modelo CASPEr (HAN, 2005) sugere uma implementação utilizando diversas linguagens em extensão ao CAAC, mas o autor relata apenas exemplos desta implementação, demonstrando interações entre as linguagens sem apresentar uma aplicação.

3.7 CABAC

O modelo CABAC (*Contextual Attribute-Based Access Control*) é apresentado por (COVINGTON, 2006) para introduzir o conceito de atributos contextuais, que descrevem o usuário e os vários aspectos de seu ambiente móvel, sem necessariamente divulgar informações que possam identificar o usuário pessoalmente. O autor descreve que os novos paradigmas computacionais, tais como a mobilidade, fornecem alguns cenários que podem não apresentar a confiabilidade necessária aos mecanismos de segurança. Esta abordagem difere dos trabalhos precedentes enfatizando a importância dos atributos contextuais, uma vez que estes podem ser estruturados para descrever exatamente a entidade a que são relacionados (COVINGTON, 2006).

Este modelo, segundo o autor, não é uma extensão de modelos existentes de controle de acesso, porque não é necessário estabelecer “atores específicos” ao sistema; e a política de acesso é fortemente definida através de situações onde os atributos contextuais servem como a fundamentação do modelo.

3.8 SGCA / SIE

O SIE (Sistema de Informações Educacionais) implementado pelo CPD/UFSM utiliza um sistema de gerenciamento e controle de aplicações denominado SGCA. O SGCA é uma ferramenta utilizada para controlar o acesso dos usuários às aplicações do sistema, armazenando senhas e garantindo que cada usuário tenha acesso somente às aplicações e

registros que lhe forem repassados. Como um dos objetivos deste trabalho é agregar funcionalidades aos módulos do SIE que atendem o HUSM (Hospital Universitário de Santa Maria), utilizaremos os conceitos básicos do SIE para demonstrar como ele está estruturado e posteriormente, estabeleceremos a solução proposta para o que chamaremos de SIE-Saúde, o SIE que comporta o PEP e demais serviços inerentes ao hospital universitário.

No SIE, toda e qualquer pessoa que acessa o sistema é chamada pelo SGCA de *Usuário* (uma analogia ao termo perfil do RBAC). Um Usuário possui uma senha que, por definição, é pessoal e intransferível. Um Usuário do sistema normalmente está vinculado a um registro do *Cadastro Único de Pessoas*, sendo que uma mesma pessoa pode pertencer a vários perfis cadastrados no SGCA.

As Aplicações, normalmente programas executáveis, são os programas aos quais os Usuários terão (ou não) acesso. São exemplos de Aplicações para o SIE-Saúde: “Serviço de Informações Cadastrais”; “Serviço de Prescrição Médica”; “Serviço de Agendamento e Internação”; “Serviço de Pesquisa Clínica”, entre outros.

Um conjunto de Aplicações cadastradas no SGCA, inclusive ele próprio, forma um *Subsistema* ou *Módulo*, e um conjunto de Aplicações, normalmente pertencentes a um mesmo subsistema, formam um *Grupo*. Uma vez definidas as Aplicações que compõem um Grupo, pode-se definir quais Usuários fazem parte de quais Grupos. Quando um Usuário é adicionado a um Grupo, ele passa a ter acesso a todas as Aplicações que compõem este Grupo.

As restrições no SIE são modeladas como *Restrições de Funcionalidade* (ou Ações) e *Restrições de Dados*. As Restrições de Funcionalidade definem o quê os Usuários podem (ou não) fazer quando estão executando uma Aplicação. São exemplos de Restrições de Funcionalidade: “Inserir”, “Alterar”, “Excluir”, etc. O universo de Restrições de Funcionalidade válidas pode ser diferente para diferentes Aplicações e está restrito ao conjunto de Restrições previamente estabelecido.

As Restrições de Dado definem quais registros de quais tabelas do banco de dados os Usuários podem acessar quando estão executando uma determinada Aplicação. São exemplos de Dados no SIE-Saúde: “Dados de Identificação do Paciente”, “Dados Demográficos”, “Prescrição”, “Agendamento”, “Internação”, etc.

O SIE utiliza o controle de acesso discricionário, o que faz com que quando uma permissão é adicionada ou removida do Perfil de um Usuário em um Grupo, ela seja também adicionada ou removida em todos os seus subgrupos.

3.8.1 Quanto às Aplicações e Restrições

Existem basicamente dois tipos de Aplicações no SIE. *Aplicações de Menu*, utilizadas para definir uma forma de apresentação hierárquica entre as Aplicações, de maneira a facilitar a sua localização dentro do Sistema. E as Aplicações propriamente ditas, que são *extensões dos arquivos executáveis* através das quais estes arquivos se tornam disponíveis para acesso através do SGCA.

Um mesmo arquivo executável pode dar origem a várias Aplicações dentro do SGCA, e as autorizações de acesso dos Usuários são definidas sempre em função destas Aplicações. Diferentes Aplicações podem ter diferentes configurações, mesmo estando relacionadas a um mesmo arquivo executável. Dentre estas configurações disponíveis para as Aplicações está a definição de Restrições, que são, na verdade, tipos de controles de acesso que podem ser efetuados dentro de cada Aplicação.

As Restrições de Funcionalidade dizem respeito a quais ações serão controladas pelo SGCA quando os Usuários estiverem executando uma determinada Aplicação, enquanto às Restrições de Dado dizem respeito a quais tipos (ou conjuntos) de registros serão controlados pelo SGCA. Por utilizar um controle discricionário o SIE não suporta delegação de atribuições, que são vislumbradas no âmbito do SIE-Saúde, e nem regras dinâmicas, que podem ser manipuladas contextualmente.

No Capítulo 4 descreve-se a solução proposta para resolver os problemas observados quanto ao controle de acesso a informações médicas, bem como a sua integração com o SIE-Saúde.

Capítulo 4
ESPECIFICAÇÃO DA UTILIZAÇÃO DE INFORMAÇÕES CONTEXTUAIS

Neste capítulo destaca-se a forma como as informações contextuais são utilizadas no âmbito do SIE-Saúde e define-se precisamente o que significa *contexto* em conformidade com outros trabalhos, bem como esclarece seus relacionamentos de forma genérica, ou seja, independente do domínio da aplicação. Inicialmente apresentamos a terminologia a cerca do termo contexto e explicamos de forma textual os conceitos, para então apresentar a especificação formal dos termos utilizados no modelo de controle de acesso, denominado a partir de agora como CIBAC (*Contextual Information-Based Access Control*). Salienta-se que embora a exemplificação utilizada neste capítulo seja direcionada para a área da saúde, foco principal desta dissertação, as proposições podem ser utilizadas também em outros domínios.

4.1 Conceitos Básicos

De acordo com Dey e Abowd (1999), contexto é qualquer informação relevante que possa ser utilizada para caracterizar a situação de uma entidade. Uma entidade pode ser uma pessoa, um lugar, ou um objeto, relevantes para a interação entre o usuário e a aplicação. Uma aplicação que utiliza informações de contexto é uma “aplicação ciente de contexto”.

O primeiro trabalho a utilizar o termo “ciente de contexto” foi o de Schilit e Theimer (1994), os quais se referiam a contexto como localização, identidades de pessoas e objetos e mudanças desses objetos (DEY, 1999). Outras abordagens definem contexto como o ambiente ou situação em que uma determinada interação ocorre. Tanto a definição de Shilit (1994) (os principais aspectos do contexto são: onde você está, quem está com você, e quais recursos estão próximos) quanto à de Pascoe (1998) (contexto é o subconjunto de estados físicos e conceituais de interesse de uma entidade particular) são muito específicas, já que contexto é toda situação relevante a uma aplicação e seu conjunto de usuários.

Do ponto de vista prático, aplicações cientes de contexto devem ser capazes de adquirir informações de contexto de modo automatizado, disponibilizando-as em um ambiente computacional em tempo de execução. Deste modo, os desenvolvedores deste tipo

de aplicação, como por exemplo controle de acesso ciente de contexto, têm a tarefa de decidir se as informações obtidas são realmente relevantes e decidir sobre como manipulá-las. Mas para tal é necessário definir o que são informações contextuais e o que é contexto.

Dey e Abowd (1999) definem informação de contexto como qualquer informação que possa ser usada para caracterizar a situação de uma entidade. Em outras palavras, se uma informação pode ser usada para caracterizar a situação de um participante em uma interação, então tal informação pode ser considerada uma informação contextual. RYAN et al. (1997) sugerem tipos de informações de contexto como localização, ambiente, identidade e tempo.

O significado de informação contextual leva a uma definição de contexto como sendo um encadeamento de informações sobre um ambiente, ou o conjunto de idéias, situações, eventos e informações necessárias para o correto entendimento do ambiente. Onde ”informação” pode ser reconhecida como uma ”propriedade de um elemento”. Assim, definimos um contexto como **um encadeamento de propriedades de um elemento em um ambiente**. Observa-se que um ”elemento” pode ser um usuário, um dispositivo ou um recurso, tornando assim o contexto uma definição aplicável a diferentes domínios.

No CIBAC, as informações contextuais são modeladas de acordo com a política adotada, e por este motivo as definimos como **propriedades**, pois fornecem os dados necessários a caracterização de um contexto. Cada propriedade distinta pode, por sua vez, ser agrupada diretamente nos contextos a que se referem, isto é, um ”contexto” pode ser definido a partir de um conjunto de informações sobre determinados elementos, e as informações (propriedades) podem servir a mais de um contexto.

Para agrupar informações de contexto relevantes à aplicação, pode-se utilizar uma categorização por tipos de contexto, que auxilia desenvolvedores a construírem aplicações cientes de contexto. Deste modo, a combinação de informações relevantes sobre um dado elemento, por exemplo um usuário, caracteriza-se como um **contexto**.

Na área da saúde o conceito de tipo de contexto auxilia a especificação de regras de acesso cientes de contexto e afinadas com a política de acesso utilizada. Por exemplo, médicos plantonistas na emergência devem ser autorizados a acessar dados sobre pacientes em atendimento na emergência, mas não sobre pacientes internados em outras unidades do hospital, a menos que ele seja também o médico de um determinado paciente.

Do ponto de vista do acesso, uma autorização de acesso deve considerar regras ambientais (pacientes internados, local do acesso, etc) associadas a operações (visualização de dados, prescrição de laudos, etc), bem como requisitos temporais (período de plantão, tempo

de internação, etc). Observe que a existência destas regras de acesso define uma política de segurança, que determina quais os tipos de contextos são ou não necessários para a elaboração de uma condição de contexto, uma expressão que deve ser verificada para concessão da autorização de acesso.

Como toda regra de acesso se reporta a informações, e neste trabalho informações são modeladas como propriedades, um exemplo de contexto para um médico plantonista na emergência pode ser modelado como:

- Tipo de Contexto: Usuário;
- Elemento: Médico;
- Propriedade: Função, com valor de propriedade = plantonista;
- Propriedade: Local, com valor de propriedade = emergência.

Observe que cada propriedade, ou informação, possui comportamento específico. Por exemplo, o valor de uma propriedade denominada “Local” deve ser atualizado no momento de uma requisição de acesso, e pode ter como base os endereços IP’s dos equipamentos e a localização dentro da instituição. Note que a existência de tal propriedade não se restringe a um único elemento, uma vez que esta pode estar relacionada a *n* tipos de contexto.

Em síntese, para conseguir uma separação lógica das propriedades que podem ser utilizadas por diferentes sistemas, utilizamos a noção de contexto e de tipos de contexto. Por exemplo, uma dada aplicação pode conter dois tipos de contextos, um Contexto de Objeto e um Contexto de Sujeito (ou usuário), e manipular as informações de cada contexto de maneira a obter políticas de acesso mais complexas. Neste sentido, quando modela-se a política de acesso através de contextos é possível prever a detecção de regras conflitantes, uma vez que uma autorização baseada em uma mesma informação, ou propriedade, não pode assumir valores diferentes.

Outro ponto interessante abordado pelo CIBAC é que, em um ambiente hospitalar pode ser comum a delegação de atribuições a médicos ou especialistas de outras áreas da saúde, a fim de prover assistência a um determinado paciente. Quando tratamos a questão da delegação como sendo uma informação contextual e geramos regras para que esta delegação seja coerente, fica facilitada a modelagem de dados temporais, locais, e relacionados a uma dada assistência, o que facilita a adequação do controle de acesso à legislação pertinente.

4.2 Definições

Visando a especificação do modelo CIBAC, nesta subseção apresentam-se as definições formais que norteiam a utilização do termo contexto. Nestas definições cada informação de contexto é apresentada na forma de propriedade.

- (**Propriedade de Contexto**). Uma Propriedade de Contexto é um par (P, V), onde P é o nome da propriedade e V é o valor da propriedade P. Observa-se que como uma propriedade de contexto é aplicável a um dado elemento (usuário, dispositivo ou recurso), pode-se dizer que todo par (P, V) $\in$ D, onde D é um domínio.
- (**Contexto**). Um contexto CTX é um conjunto de propriedades de contexto (P, V). Note que um dado contexto CTX pode também ser formado por outros diferentes contextos. Por exemplo, CTX1 = {(P11,V11), (P12,V12)} e CTX2 = {(P21,V21), (P22,V22)}, mas CTX3 = (CTX1,CTX2).
- (**Condição de Contexto**). Uma Condição de Contexto ContextCond é uma fórmula booleana em forma de tupla, tal como (CT, P, $\oplus$, V), onde CT é o tipo de contexto, P é o nome da propriedade, $\oplus$ é um operador (por exemplo, <, >, =) e V é o valor que a propriedade assume.
- (**Tipo de Contexto**). Um Tipo de Contexto é uma classificação dada de acordo com as características das informações de cada contexto, ou seja, possibilita agrupar propriedades contextuais de acordo com a natureza de cada informação (por exemplo, sujeito ou objeto).
- (**Autorização**). Uma Autorização é uma tupla (CE, O, AM, CC), onde CE representa as expressões credenciais do usuário[4], O é o objeto, ou objetos, a ser acessado, AM é o modo de acesso e CC é o resultado da avaliação sobre uma condição de contexto.

Segundo Kudo e Hada (2000), uma autorização deve apresentar pelo menos três parâmetros básicos: sujeito, objeto e ação. Um sujeito pode ser um identificador de usuário ou um grupo de usuários; um objeto pode ser um documento completo (como uma aplicação) ou partes de um documento; e uma ação pode assumir a execução de escrita (gravação), leitura, criação, entre outras, como por exemplo uma delegação.

Observa-se que a contribuição deste trabalho caracteriza-se pela inserção da condição de contexto (CC) como regra de autorização e pela manipulação das informações de contexto

[4] Por definição (FERRAIOLO, 2001), Expressões Credenciais são os atributos do sujeito necessários para se prover a segurança, como por exemplo, perfil do usuário, a autenticação deste perfil, login, senha, entre outros.

(CI) na forma de propriedades de contexto. Os demais termos são originários da definição de autorização do modelo de referência RBAC.

4.3 Arquitetura do Sistema

A arquitetura do sistema de controle de acesso proposto foi dividida em módulos funcionais, conforme mostra a figura 4.1, e separa o mecanismo de controle de acesso dos mecanismos de atualização. Entende-se por mecanismo de atualização todo e qualquer mecanismo ou aplicação que possibilite um *update* ao sistema, isto é, no CIBAC consideramos módulos de imposição de políticas como sendo um mecanismo de atualização, pois fornecem as informações necessárias sobre as regras e as propriedades que devem ser manipuladas pelo controle de acesso.

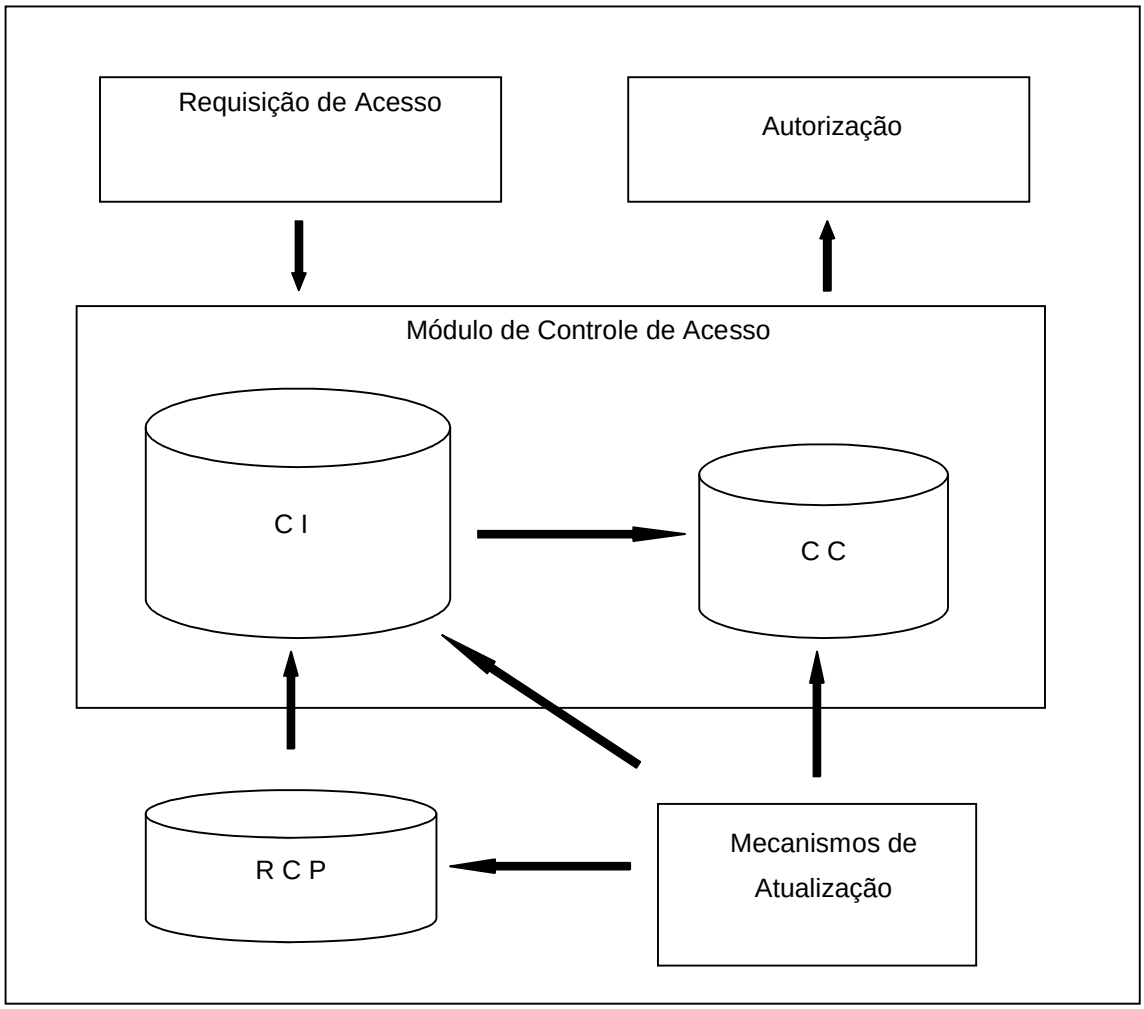

Fig. 4.1 - Arquitetura do CIBAC

A separação dos mecanismos possibilita uma abordagem genérica ao modelo, não restringindo-o a apenas um tipo de aplicação. Observe que esta separação possibilita determinar claramente as políticas e regras para o controle de acesso de cada sistema, bem como o agrupamento destas informações na forma de Contextos, pois isola a lógica da política de controle de acesso dos mecanismos de imposição da política (regras).

Com esta organização, no CIBAC os mecanismos de atualização podem estabelecer alterações no *Repositório de Comportamento de Propriedades* (RCP), nas Informações de Contextuais (CI) e nas Condições de Contexto (CC), possibilitando que cada nova informação, por exemplo uma nova propriedade, seja atualizada e acrescentada em todos os níveis necessários, o que contribui para manter a integridade da informação.

O Módulo de Controle de Acesso verifica as regras necessárias para o acesso, contidas nas condições de contexto (CC) e confronta os dados com as informações de contexto do sistema (CI), liberando ou não o acesso. Em cada requisição de acesso são necessárias informações relativas às credenciais do usuário, objeto e modo de acesso. Assim as atualizações necessárias ao funcionamento do sistema são reportadas diretamente às *Políticas de Acesso* (CC), *Contexto* (e seus *Tipos de Contexto*) (CI) e ao *Repositório de Comportamento de Propriedades* (RCP), o que possibilita mapearmos cada informação, ou comportamento de cada propriedade, de acordo com a modelagem previamente determinada para a aplicação.

A dinamicidade do sistema é garantida pela variabilidade dos valores de determinadas propriedades, o que ocorre de acordo com o comportamento pré-determinado para cada uma delas. Este comportamento é estabelecido através do RCP, que determina como uma propriedade deve “comportar-se” diante de uma ocorrência específica, possibilitando desta forma a alteração ou não do valor contido na propriedade.

Na política de acesso é inserida uma Condição de Contexto, conforme definido na subseção 4.2. Esta condição nada mais é do que uma regra da política de acesso que determina quais situações podem prover o acesso a determinados recursos. Como tanto a condição contextual como as propriedades nos tipos de contexto se referem as mesmas informações, a manipulação destes dados pode ser tratada da mesma forma, ou seja, uma propriedade (informação), considerada por uma regra de acesso em uma condição de contexto, deve ser a mesma indicada no contexto especificado pela política.

Digamos que uma propriedade com nome *Tempo* é necessária para, em conjunto com outras propriedades, prover acesso a um determinado objeto. Esta mesma propriedade é

referenciada na *Condição de Contexto*, na forma de regra para a autorização de acesso, e no *Contexto* na forma de informação de contexto (CI), relacionada com o tipo de contexto e o objeto em questão. Além de possuir referência no repositório de comportamento de propriedades (RCP), o que garante a dinamicidade da mesma, uma vez que pode-se determinar como e em que situações o valor da propriedade deve sofrer alterações.

Note que a arquitetura utilizada no CIBAC possibilita agregar novas funcionalidades ao RBAC, assim como em (MOTTA, 2003a) e (HULSEBOSCH, 2005), pois todos os modelos baseados em regras utilizam um conjunto de políticas de acesso. Por outro lado, o CIBAC possibilita o armazenamento das informações contextuais de forma mais transparente, facilitando a implementação do mecanismo de controle de acesso.

Isto possibilita um ajuste dinâmico das regras estáticas, através da manipulação das informações contextuais. Uma abordagem parecida já foi utilizada por (ZHANG, 2004), que possibilitava o acesso através de interações dinâmicas entre entidades participantes.

4.4 Módulo de Controle de Acesso

No CIBAC o módulo de controle de acesso considera as informações de um ambiente como propriedades de um determinado contexto e as relaciona como itens de regras de acesso, possibilitando a criação de condições de contexto relativas ao acesso desejado. Observe que a modelagem de tais relações torna o controle de acesso a determinados objetos ou recursos uma tarefa mais prática, uma vez que as informações necessárias à uma dada ação, por exemplo delegação, podem ser tratadas como propriedades de um contexto, seja este de um sujeito ou de um objeto, dependendo apenas de como a regra de acesso é modelada.

Esta subseção apresenta a codificação e as descrições XML do CIBAC, além da descrição detalhada do funcionamento do modelo de controle de acesso baseado em informações contextuais.

4.4.1 Codificação XML

O XML provê uma representação estruturada dos dados (metadados) e não possui elementos nem marcas predefinidas, logo não especifica como os autores devem utilizar esses metadados. Assim, existe total liberdade para utilizar qualquer método disponível, desde simples atributos, até a implementação de padrões mais complexos (ALMEIDA, 2002), o que possibilita o relacionamento facilitado das definições propostas. A seguir exemplificamos como uma Política de Acesso pode ser descrita no CIBAC utilizando a linguagem XML. Para

tal explica-se como representar uma condição de contexto e um tipo de contexto, elementos chaves da política de acesso.

Condição de Contexto

De acordo com os modelos de controle de acesso existentes, para descrever uma política eficiente costuma-se utilizar regras que consideram objetos e modos de acesso. Entretanto, no CIBAC as regras consideram também expressões credenciais dos usuários, resultando em uma avaliação sobre uma determinada condição de contexto. Por exemplo, suponha que um determinado arquivo de paciente só pode ser acessado, ou tenha seu acesso liberado, se uma das duas condições seguintes for satisfeita: 1) um usuário com função de enfermeira acessa os dados a partir das 10:00h; ou 2) o objeto em questão deve estar no setor de emergência com um contador de acessos com valor inferior a 20 ocorrências. Esta "regra" ou "condição de contexto" pode ser codificada em XML conforme ilustra a figura 4.2.

```
<ContextCond>
.  <Clause>
.    <Context Type="Sujeito">
.      <Property Name="Tempo"/>
.      <Operator OP=">"/>
.      <Value V="10:00"/>
.    </Context>
.    <Context Type="Sujeito">
.      <Property Name="Função"/>
.      <Operator OP="="/>
.      <Value V="Enfermeira"/>
.    </Context>
.  </Clause>
.  <Clause>
.    <Context Type="Objeto">
.      <Property Name="Contador"/>
.      <Operator OP="<"/>
.      <Value V="20"/>
.    </Context>
.    <Context Type="Objeto">
.      <Property Name="Local"/>
.        <Operator OP="="/>
.      <Value V="Emergência"/>
.    </Context>
.  </Clause>
</ContextCond>
```

Fig. 4.2 - Exemplo Elemento XML - ContextCond

Observe que um elemento `ContextCond` é dividido em cláusulas (`Clause`), como as cláusulas de Horn (HORN, 1951) utilizadas no modelo OASIS (BACON et al., 2002), que contém as possíveis regras de liberação de acesso baseadas em informações contextuais. Estas

cláusulas contêm os tipos de contextos utilizados, neste caso `Sujeito` e `Objeto` com suas respectivas propriedades e valores, e um operador que determina a condição efetiva da regra.

Como uma condição de contexto pode definir várias regras de acesso para uma determinada ação (seção 4.2), na definição agrupa-se estas regras em cláusulas. Cada cláusula contém expressões que configuram-se efetivamente nas regras de acesso. Observa-se que cada condição de contexto deve possuir um agrupamento de elementos de uma tupla, ou no caso das cláusulas, vários agrupamentos. Deste modo, cada tupla é traduzida em forma de regra de acesso. Com base no exemplo apresentado, podemos traduzir uma tupla (CT, P, ⊕, V) por uma das expressões da primeira cláusula onde: CT é o tipo de contexto (<Context Type = “Sujeito”>), P é o nome da propriedade (<Property Name =“Tempo”>), ⊕ é o operador da regra (<Operator OP=“>”>) e V é o valor da propriedade (<Value V=“10:00”>).

A condição de contexto definida na figura 4.2 é confrontada com o Contexto do Sistema no momento da requisição de acesso. O Contexto do Sistema, com suas informações de contexto, é armazenado e agrupado de acordo com seus tipos de contextos.

Consideram-se as cláusulas da Condição de Contexto como uma operação ”OR”, determinando que: ou uma ou outra condição é suficiente para liberar o acesso de determinado sujeito à determinado recurso; e um conjunto de expressões em cada cláusula é considerado como uma operação ”AND”, ou seja, a cláusula só é verdadeira se todas as expressões em seu interior forem verdadeiras.

Esta consideração permite a manipulação da política de acesso de forma mais rígida ou de forma mais permissiva. Isto ocorre de acordo com a quantidade de cláusulas utilizadas para a concessão de um acesso, isto é, se para um determinado acesso só existe a possibilidade de uma única regra de acesso, esta regra é mapeada em uma única cláusula, excluindo a possibilidade de um “OR”. Desta forma o acesso só será concedido se, e somente se, esta única regra for satisfeita.

Tipo de Contexto

No CIBAC uma informação contextual é definida por um conjunto de propriedades pertencentes a um dado tipo de contexto, ou seja, considera-se o tipo de contexto, suas propriedades e seus respectivos valores. Entretanto, como um tipo de contexto representa uma classe de contextos, no CIBAC cada informação contextual pertence a um tipo de contexto e cada tipo de contexto possui seu respectivo *target*. *Target* é o identificador de um objeto específico ou de um conjunto de objetos, e é utilizado na codificação XML para se efetuar uma separação entre os elementos inseridos em cada tipo de contexto.

A figura 4.3 exemplifica a representação XML de um tipo de contexto `Objeto`. O elemento específico é o arquivo `Ordem_Médica.doc` e suas informações são descritas pelas propriedades de contexto: `Tempo` e `Contador`. O valor de cada propriedade pode ser alterado de acordo com o repositório de comportamento de propriedades, o que possibilita por exemplo que o valor da propriedade `Contador` seja incrementado em determinadas situações e que o valor da propriedade `Tempo` seja consultado nos momentos em que se determine. Desta forma todas as informações necessárias para o controle de acesso podem ser modeladas como regras na condição de contexto e tratadas de acordo com sua especificação em cada tipo de contexto.

```
<Context Type="Objeto">
.  <Objeto target="Ordem_Médica.doc">
.    <Property Name="Tempo">
.      10:00
.    </Property>
.    <Property Name="contador">
.      12
.    </Property>
.  </Objeto>
</Context>
```

Fig. 4.3 - Exemplo Elemento XML – Context Type

Por exemplo, considere a descrição da figura 4.3. Como o Contexto é do tipo Objeto e as informações referentes ao arquivo `Ordem_Médica.doc` (objeto alvo) são agrupadas no próprio objeto especificado, os valores das propriedades podem ser facilmente localizados quando a propriedade for consultada ou requerida por uma regra em uma Condição de Contexto. Além disto, observe que com este tipo de representação as informações podem ser tratadas da mesma forma (como propriedades), tanto no Contexto propriamente dito como na Condição de Contexto referenciada pela política de acesso. Assim, um Contexto pode ser compreendido como um conjunto de elementos `Context Type`, e uma Condição de Contexto inserida em uma política de acesso pode ser compreendida como um elemento `ContextCond`, habilitando o uso de algoritmos baseados em informações contextuais no mecanismo de controle de acesso.

4.4.2 Requisitos para o CIBAC

Para a utilização do Modelo de Controle de Acesso Baseado em Informações Contextuais (CIBAC) no âmbito do SIE-Saúde é necessário estabelecer os requisitos gerais que norteiam a sua especificação. Esta seção detalha alguns destes requisitos.

Um dos requisitos que julgamos de suma importância é a utilização da **hierarquia de perfis** de acordo com a estrutura organizacional do HUSM. Cabe ressaltar que a construção de uma hierarquia de perfis configura-se em um processo contínuo que evolui de acordo com as necessidades da organização e com as circunstâncias encontradas no ambiente em que se insere.

Esta hierarquia é demonstrada através da tabela 4.1 e sugere, implicitamente, alguns níveis de acesso que podem ser relacionados a cada nível hierárquico.

Tabela 4.1 – Níveis hierárquicos para o SIE-Saúde

<table>
<tr><td rowspan="30">Usuário</td><td rowspan="30">Profissional</td><td rowspan="4">Médico</td><td colspan="4">Residente</td></tr>
<tr><td colspan="4">Cirurgião</td></tr>
<tr><td colspan="4">Anestesista</td></tr>
<tr><td colspan="4">Hematologista</td></tr>
<tr><td rowspan="15">Paramédico</td><td>Enfermeiro</td><td colspan="3">Auxiliar de Enfermagem</td></tr>
<tr><td colspan="4">Psicólogo</td></tr>
<tr><td colspan="4">Fisioterapeuta</td></tr>
<tr><td colspan="4">Biólogo</td></tr>
<tr><td colspan="4">Fonoaudiólogo</td></tr>
<tr><td colspan="4">Dentista</td></tr>
<tr><td colspan="4">Assistente Social</td></tr>
<tr><td colspan="4">Professor de Educação Física</td></tr>
<tr><td colspan="4">Físico</td></tr>
<tr><td colspan="4">Bioquímico</td></tr>
<tr><td colspan="4">Biomédico</td></tr>
<tr><td>Farmacêutico</td><td colspan="3">Auxiliar de Farmácia</td></tr>
<tr><td>Nutricionista</td><td colspan="3">Auxiliar de Nutrição</td></tr>
<tr><td colspan="4">Auxiliar Técnico</td></tr>
<tr><td rowspan="7">Administrador Executivo</td><td colspan="4">Diretor</td></tr>
<tr><td rowspan="6">Técnico Administrativo</td><td rowspan="4">Auxiliar Administrativo</td><td colspan="2">Escriturário</td></tr>
<tr><td colspan="2">Secretário</td></tr>
<tr><td>Auxiliar de Registro de Saúde</td><td>Analista de Registro de Saúde</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Técnico em Informações Médico Hospitalares</td><td colspan="2">Analista de Informações Médico Hospitalares</td></tr>
<tr><td colspan="3">Operador de Teleatendimento</td></tr>
</table>

			Administrador de RH	Analista de RH	Auxiliar de RH
			Administrador Financeiro	Faturista	Analista de Faturamento
				Técnico Contábil	Analista Contábil
		Técnico de Informática	Analista de Informática	Analista de Suporte	
				Analista Desenvolvedor	
			Administrador de Banco de Dados		
		Pesquisador	Pesquisador Clínico		
	Paciente				
	Estudante	Graduando			
		Pós-Graduando			

Cabe ressaltar ainda que esta hierarquia estabelecida para o SIE-Saúde em conformidade com a estrutura organizacional do HUSM não está concluída, tampouco é completa, dada as características de continuidade do processo de implantação.

Outra questão importante considera os aspectos de **organização interna do PEP**. No final da década de 60 Weed (1968) apresentou uma abordagem definida como Registro Médico Orientado ao Problema (POMR – *Problem-Oriented Medical Record*), onde defende-se que todas as anotações, informações terapêuticas, diagnósticos, entre outros, deveriam ser relacionados a um problema de saúde específico, constituindo assim, uma lista de problemas em uma árvore hierárquica na qual cada problema seria um ramo principal. Adotamos esta abordagem no SIE-Saúde por acreditar que ela estabelece um forte relacionamento aos conceitos propostos pelo CIBAC. A lista de problemas pode atuar como uma tabela de conteúdos do PEP, como evidenciado na tabela 4.2.

Tabela 4.2 – PEP com registro médico orientado ao problema adaptado ao SIE-Saúde

PEP's (lista de pacientes)	Paciente 1	Dados de Identificação do Paciente				
		Dados Demográficos				
		Dados Clínicos	Antecedentes			
			Hábitos de Vida			
			Alergias			
			Lista de Problemas	Problema 1	Data Inicial	
					Data Final	
					Diagnóstico	
					Assistente Responsável	
					Local	
					Eventos	Consultas Médicas
						Exames
						Internações
						Procedimentos
						Prescrição/ Medicamentos

				Problema 2	
	Paciente 2				

Como pode ser verificado, esta estrutura ajusta-se facilmente ao legado de Aplicações e Restrições definidas no SIE, e conseqüentemente ao SIE-Saúde, justificando a sua utilização pelo CIBAC. Observa-se também que cada evento, ou tipo de evento, pode ser relacionado a diferentes perfis definidos na tabela 4.1.

Para melhor compreender a utilização do PEP com a abordagem POMR, considere os serviços definidos para o SIE-Saúde e detalhados a seguir:

- *Serviço de Informações Cadastrais*: subdividido em Dados de Identificação do Paciente e Dados Demográficos. Os Dados de Identificação do Paciente são dados capazes de identificar diretamente o paciente em questão (nome, filiação, entre outros). Os dados Demográficos oferecem uma abordagem anônima ao paciente (sexo, idade, características étnicas, entre outros);
- *Serviço de Agendamento e Internação*: Permite manipular os eventos dos Dados Clínicos do Paciente relativos a consultas, exames e internações;
- *Serviço de Prescrição Médica*: Comporta alguns eventos dos Dados Clínicos do Paciente. Mais precisamente Procedimentos e Prescrições médicas relativas à pacientes específicos e Diagnósticos;
- *Serviço de Pesquisa Clínica*: Permite pesquisar Prontuários de Pacientes com base em observações clínicas, como valores medidos em exames, diagnósticos, tipos de prescrições, antecedentes, hábitos de vida, entre outros.

Observe que cada serviço pode ser considerado uma aplicação no SIE-Saúde e que cada evento de manipulação dos dados do PEP pode ser controlado através de regras que consideram a hierarquia de perfis pré-estabelecida.

Outro requisito importante diz respeito à **delegação de atribuições** (ZHANG, 2002) e (ZHANG, 2001), principalmente por se tratar de uma aplicação em ambiente hospitalar. Atluri e Warner (2005) tratam a questão da delegação através da análise de consistências e predicados de delegação condicional, mas não relatam uma implementação desta solução. Por tratar-se de um assunto relevante para o CIBAC, a subseção seguinte trata especificamente a questão das delegações.

4.4.3 Delegação de Atribuições

Para o CIBAC definimos a delegação como uma Restrição de Funcionalidade no SIE-Saúde. Desta forma podemos mapear a ação de "delegar" através de condições de contexto que possibilitem a sua utilização, mantendo a dinamicidade do modelo para criar delegações. Entretanto, concedida a Funcionalidade (ação de delegação realizada com sucesso), o controle de acesso passa a ser discricionário.

Observa-se que desta forma um usuário pode estabelecer (via Condição de Contexto) uma delegação a outro usuário apenas para uma ação específica sobre algum recurso. A cada acesso a nova atribuição é verificada em uma tabela de delegações, onde há, além da descrição do acesso (Funcionalidade), também informações relativas à revogação das delegações (SOHR et al., 2005).

Como uma delegação só pode ser concedida de acordo com níveis hierárquicos, pode-se garantir que a tabela de delegações não sofre nenhuma inconsistência, uma vez que a Funcionalidade já foi confrontada com as condições de contexto do usuário que delega a atribuição. Por exemplo, suponha que um usuário "x" deseja delegar uma dada ação sobre o arquivo `Ordem_Médica.doc` ao usuário "y". A responsabilidade do CIBAC é determinar se esta delegação deve ser permitida. Isto é feito através da consulta às condições de contexto para a ação de delegar. Se o usuário "x" possuir todas as atribuições necessárias para que o acesso à ação de delegar seja concedido ele pode efetuar a delegação, e o usuário "y" passa a fazer parte da tabela de delegações com seus respectivos direitos, considerando a validade dos mesmos também indicada na tabela. Caso a ação seja negada, o usuário "y" não é inserido na tabela de delegações e a delegação então não existirá, tornando inviável alguma concessão de acesso.

4.5 Política e Regras de Controle de Acesso

Para a utilização do SIE-Saúde, no âmbito do Hospital Universitário de Santa Maria, deliberamos a seguinte política de acesso e respectivas regras:

1. Somente usuários autenticados[5] e devidamente autorizados podem acessar o PEP e seus respectivos serviços;
2. São perfis de usuários autorizados a acessar o PEP:

[5] Salientamos que mecanismos de autenticação de usuários não foram abordados por não fazerem parte do escopo deste trabalho, entretanto são vislumbrados em trabalhos relacionados pelo Laboratório de Tolerância a Falhas do GMicro/UFSM.

- Profissionais de saúde que assistem diretamente o paciente (denominados Assistentes), incluindo Médicos e Paramédicos;
- Auxiliares e Analistas de Registro de Saúde, Técnicos e Analistas de Informações Médico Hospitalares;
- Pesquisadores Clínicos e Estudantes;
- Os próprios Pacientes.

3. Profissionais de Saúde e Auxiliares, Técnicos e Analistas, somente podem acessar o Serviço de Informações Cadastrais do paciente, que incluem os Dados de Identificação e os Dados Demográficos anônimos do paciente;

4. Auxiliares e Analistas de Registro de Saúde podem efetuar a manutenção do Serviço de Informações Cadastrais;

5. Os Auxiliares têm permissão para alterar cadastros;

6. Analistas, além de alterar, têm a permissão de criar e excluir cadastros;

7. Os Pesquisadores Clínicos não podem ver dados que identifiquem diretamente um paciente, mas podem ter acesso aos dados demográficos anônimos;

8. Os Pacientes têm acesso aos próprios dados cadastrais, mas não podem criar ou excluir cadastros, incluindo o próprio, nem ver cadastros de terceiros;

9. Médicos Assistentes, ou sob delegação, têm a prerrogativa de criar prescrições médicas;

10. Médicos Assistentes, ou sob delegação, só podem prescrever para pacientes internados, com atendimento na emergência ou com exames, consultas ou internações agendadas, considerando as datas estabelecidas;

11. São condições impostas aos perfis para manipulação de prescrições:

- Médicos Assistentes têm acesso irrestrito para ver prescrições, desde que de seus pacientes assistidos;
- Paramédicos só podem ver prescrições de pacientes por eles assistidos, ou sob delegação, desde que os pacientes estejam internados;
- Médicos e Paramédicos podem ver as prescrições de pacientes em atendimento na emergência, desde que o acesso seja durante seu turno de trabalho e através de computadores lotados neste setor;
- Pacientes podem ver exclusivamente as próprias prescrições.

12. Pesquisadores Clínicos podem realizar pesquisa aos PEP’s com base em observações clínicas;

13. Somente Auxiliares e Analistas de Registro de Saúde podem agendar consultas, exames e internações para pacientes;

14. Somente o Analista de Registro de Saúde pode efetuar os procedimentos formais para a internação de um paciente;

15. A ação de Delegar só é concedida diretamente para Assistentes e somente sobre os Prontuários relativos à sua assistência, com tempo de validade determinado.

4.6 Algoritmos de Decisão de Acesso e de Delegação

O CIBAC estabelece o acesso aos recursos através da análise de restrições pré-definidas na forma de políticas e regras de autorização. Cada regra é estruturada como uma expressão contextual e o conjunto de expressões é agrupado na forma de cláusulas. A interação entre as condições de contexto e os contextos pré-definidos é realizada utilizando-se o algoritmo de decisão de acesso da figura 4.4.

```
1.  Receber requisição de acesso
2.  Selecionar todas as condições de contexto que satisfaçam a requisição de acesso: CE, O e AM
3.  Selecionar todas as cláusulas nas condições de contexto
4.  Determinar flagc = FALSE                                        // flag de cláusula
5.  Percorrer todas as cláusulas até encontrar uma cláusula verdadeira
6.      Selecionar as expressões em cada cláusula
7.      Determinar flage = TRUE                                     // flag de expressão
8.      Percorrer todas as expressões de cada cláusula até encontrar uma expressão falsa
9.          Para cada expressão comparar Tipo de Contexto, Propriedade e Valor com o Contexto
10.         Se o valor da propriedade não satisfaz o operador da regra, determinar flage = FALSE
11.     Se flage == FALSE
12.         Passar para cláusula seguinte
13.     Senão flagc = TRUE                                          // cláusula verdadeira
14. Se flagc == TRUE                                                // existe um cláusula verdadeira
15.     Permitir Acesso
16. Senão Negar Acesso
```

Fig. 4.4 - Algoritmo de Decisão de Acesso.

No algoritmo de decisão de acesso uma condição de contexto (CC) é avaliada testando cláusulas, ou seja, testando o conjunto de expressões (regras de acesso) contidos nas cláusulas. A lógica consiste em encontrar uma cláusula verdadeira, onde todas as expressões internas a ela são verdadeiras, para então autorizar o acesso. Para tal, na linha 2 são separadas todas as regras que satisfazem a expressão credencial do usuário (CE), o objeto a ser acessado (O) e o modo de acesso (AM), e na linha 3 são selecionadas as cláusulas nas condições de contexto. Em seguida, na linha 4, determina-se um flag de controle denominado flag de cláusula (flagc), o qual deve permanecer FALSE até que se encontre uma cláusula verdadeira. De maneira similar, para testar cada expressão nas cláusulas determina-se um flag de

expressão (flage), linha 7, o qual deve permanecer TRUE até que se encontre uma expressão falsa.

Para verificar se o contexto satisfaz uma cláusula e, conseqüentemente, todas as regras de acesso relativas a ela, o algoritmo compara cada regra de acesso (expressão) com as informações apresentadas pelo contexto (linhas 9 e 10). No momento em que o contexto satisfaz uma cláusula, o acesso é concedido (linhas 14 e 15).

Se alguma expressão no interior da cláusula é falsa (teste da linha 11), então toda a cláusula é considerada falsa e é necessário percorrer as demais cláusulas com a finalidade de se determinar o acesso. Quando todas as regras (cláusulas) inerentes à requisição de acesso são percorridas e nenhuma delas é verdadeira o acesso é negado (linha 16).

Observe que o algoritmo de decisão de acesso possibilita tratar as autorizações de acesso baseando-se apenas em informações contextuais, possibilitando uma maior eficiência ao mecanismo de controle de acesso, pois toda informação pode ser modelada na forma de propriedades e sofrer alterações dinamicamente.

Considerando delegações, o CIBAC também pode conceder permissão de acesso via algoritmo de Delegação (figura 4.5). Se a ação sendo requisitada pertencer a tabela de delegações e a delegação for válida, o acesso é permitido.

```
1. Receber requisição de acesso
2. Selecionar todas as informações da requisição de acesso: CE, O e AM
3. Consultar a tabela de delegações
4. Se informações da requisição pertencem à tabela de delegações
5.         Verificar validade da delegação
6.         Se período de delegação ainda é válido
7.                 Permitir Acesso
8.         Senão passar para o Algoritmo de Decisão de Acesso
9. Senão passar para o Algoritmo de Decisão de Acesso
```

Fig. 4.5 - Algoritmo de Delegação

Note que a negação do acesso só é dada através do algoritmo de Decisão de Acesso do CIBAC, mas a permissão pode ser dada também através do algoritmo de Delegação. Isto é possível porque o algoritmo de avaliação da delegação usa uma tabela de delegações montada a partir da avaliação realizada pelo algoritmo de decisão de acesso. Uma delegação só é criada se o algoritmo de decisão de acesso a permitir.

Validação do Algoritmo de Controle de Acesso

Para a validação do algoritmo de controle de acesso do CIBAC, analisa-se três situações distintas (casos de teste): negação de acesso por inexistência de cláusula; concessão

de acesso por existência de cláusula verdadeira; e tratamento de delegações. Para cada uma discute-se a operação do CIBAC e mostra-se que o algoritmo de controle de acesso pode operar corretamente usando apenas regras positivas.

CASO DE TESTE 1: negação de acesso por inexistência de cláusula.

Considere a Política de Controle de Acesso descrita na seção 4.5, e suponha a requisição de acesso[6]: (*Paciente, Cadastro de Consulta, Excluir*). De acordo com a regra 8 da política estabelecida, pacientes não podem criar ou excluir cadastros. Logo não existe condição de contexto que suporte a ação de "excluir" para um perfil "paciente" sobre o serviço "cadastro de consulta", o que resulta na inexistência de uma cláusula a ser testada. No CIBAC, uma condição de contexto CC é formada por uma ou mais cláusulas *C*, ou seja, CC = *C*1 U *C*2 ... U *C*n, e só existe cláusula C em uma condição de contexto CC se e somente se existe uma regra para ser codificada, ou seja, $\exists\ C \in CC \Leftrightarrow \exists$ Ri. Além disto, o teste de cláusulas do algoritmo de controle de acesso nega acessos não previstos na política de acesso e concede acessos apenas se existir cláusula verdadeira na condição de contexto. Portanto, o acesso é negado se não existe de uma cláusula a ser testada.

Note que o CIBAC não considera regras negativas, somente regras positivas, o que permite uma maior agilidade no funcionamento do algoritmo. Porém esta característica implica em uma definição mais abrangente no momento de cadastrar regras nas condições de contexto. Ao invés de escrever uma única regra impedindo pacientes de excluir, deve-se escrever uma ou mais regras dizendo quais os perfis podem possuir a autorização para excluir.

CASO DE TESTE 2: concessão de acesso por existência de cláusula verdadeira.

Suponha a requisição de acesso (*Paciente, Prescrição, Visualizar*). Dado que existe uma condição de contexto que comporta esta situação (regra 11, item quarto: "Pacientes podem ver exclusivamente as próprias prescrições"), se a prescrição pertencer ao paciente em questão, existe uma ou mais cláusulas verdadeiras na condição de contexto que satisfazem a condição de contexto, logo o acesso é concedido.

Observa-se que a inexistência de uma regra positiva para o perfil paciente negaria o acesso à sua própria prescrição, sem a necessidade efetiva de uma regra negativa para isto.

---

[6] Uma requisição de acesso é uma tupla do tipo (*CE, O, AM*), onde *CE* é a expressão credencial de usuário, *O* é o objeto ou serviço desejado, e *AM* é o modo de acesso pretendido.

CASO DE TESTE 3: tratamento de delegações

Como o tratamento de delegação de atribuições no CIBAC assume caráter discricionário, o algoritmo de controle de acesso primeiro testa a tabela de delegações para verificar a existência de uma condição de contexto que comporte a descrição da delegação. Isto funciona como se fosse uma requisição de acesso normal. Caso a delegação exista, sua validade é testada (regra 15: "...tempo de validade determinado") sob a forma de avaliação de regras temporais. Caso a delegação seja válida o acesso é concedido.

Logo, suponha a requisição de acesso (*Médico*, *Prontuário*, *Delegar*). Para se estabelecer uma delegação é necessário que o objeto em questão esteja sob a assistência de quem delega (regra 15: "....somente sobre os Prontuários relativos à sua assistência"). Desta forma o médico pode delegar a outrem uma determinada ação sobre o referido prontuário somente se for o assistente responsável por este prontuário. Além disto, ele deve ainda estabelecer um período de validade para a existência desta delegação de forma discricionária na tabela de delegações. Na avaliação, caso não exista nenhuma regra que satisfaça a condição de contexto para estabelecer esta delegação, o controle de acesso impede a delegação. Observa-se que novamente pode-se utilizar somente de regras positivas para tratamento de delegações.

Capítulo 5
IMPLEMENTAÇÃO DO MODELO CIBAC

Neste capítulo trata-se da implementação do CIBAC e dos ajustes necessários para incorporá-lo ao SIE, a fim de se obter o SIE-Saúde. As principais modificações no SIE são a adição de módulos responsáveis pela parte clínica e a inclusão do CIBAC junto ao SGCA.

Para efetuar a conectividade entre o SIE atual e o SIE-Saúde através de alterações de baixo custo em seu código-fonte, optou-se pela utilização de uma arquitetura baseada em serviços, implementada com *Web Services (ERL, 2004) e* XACML (GRIFFIN, 2006).

Este capítulo discute inicialmente a utilização de *Web Services* e XACML (seção 5.1) e a arquitetura CIBAC/SIE-Saúde (seção 5.2). Em seguida apresenta detalhes de como informações contextuais podem ser modeladas num banco de dados (seção 5.3), para então abordar a dinâmica de requisições e respostas (seção 5.4) e de tratamento de delegações (seção 5.5). Por fim, mostra-se os principais resultados da avaliação da implementação (seção 5.6).

5.1 Sobre a Escolha de *Web Services* e XACML

Um *Web Service* é uma aplicação de software que contém interfaces e ligações capazes de ser definidas, descritas e descobertas através do uso de linguagens de marcação, suportando interações diretas com outros agentes de softwares através da troca de mensagens baseadas em XML, via protocolos de comunicação Internet (WEB, 2006).

A vasta aceitação dos *Web Services* resultou na criação de novas tecnologias que se tornaram padrões de fato, dentre elas as mais importantes são a Linguagem de Descrição de *Web Services* (WSDL), que descreve a interface e o protocolo de comunicação, e o *Simple Object Access Protocol* (SOAP), um protocolo baseado em XML para uma Chamada de Procedimento Remoto (RPC). Também foi definido um sistema de registro chamado *Universal Description, Discovery and Integration* (UDDI), responsável por armazenar documentos WSDL, permitindo que serviços possam ser publicados e encontrados (ERL, 2005). Um UDDI especifica um padrão bem aceito para estruturar registros que armazenam

descritores de serviços. O registro é baseado em XML e independente de plataforma, podendo ser utilizado para buscas manuais ou através de uma API padronizada (UDDI, 2006).

Como toda a comunicação entre serviços é baseada na troca de mensagens, a especificação do Protocolo Simples de Acesso à Objetos (SOAP) tem como principal objetivo a definição de um formato de mensagem padronizado, o qual consiste em um documento XML capaz de armazenar tanto os dados de um documento, quanto os de uma RPC (ERL, 2004). Assim, o uso de SOAP, que utiliza o protocolo HTTP para o transporte do seu conteúdo, permitindo que os documentos XML passem através de *firewalls* sem problemas, visto que, por motivos de segurança, muitas vezes os administradores de sistema bloqueiam as portas de comunicação dos seus servidores, exceto a porta 80, usada pelo HTTP.

Com a utilização de *Web Services* e troca de mensagens através do SOAP obtém-se a portabilidade necessária ao CIBAC, uma vez que o modelo possui características genéricas e pode ser utilizado por diversas aplicações.

Quanto à descrição das políticas de controle de acesso, ao invés de utilizar uma linguagem própria utilizada só no CIBAC, optou-se pela linguagem de marcação XACML (*eXtensible Access Control Markup Language*), que define o formato de uma requisição que contém informações sobre o usuário, recurso, ação e ambiente. Isto facilita a especificação de algoritmos para encontrar políticas que se apliquem as requisições, facilitando também a tomada de decisões e a geração de respostas (GRIFFIN, 2006).

Ao criar um arquivo contendo uma política defini-se, através de uma marcação (elemento *Target*) contendo informações relativas a uma requisição, quais os atributos da requisição que devem ser analisados para verificar se uma política é aplicável. Se uma política é aplicável, então avaliam-se as regras existentes nela. Como muitas políticas podem ser aplicáveis a uma determinada requisição e uma política pode conter várias regras, o uso de XACML facilita a especificação de algoritmos para tomada de decisões. No CIBAC uma decisão pode assumir os seguintes estados: permitido, negado, não aplicável ou indeterminado.

No CIBAC, o Ponto de Decisão de Políticas (PDP) é o responsável por receber a requisição XACML, procurar, através do *Target*, todas as políticas aplicáveis, avaliar as regras e usar o algoritmo de decisão para retornar uma resposta XACML. Esta resposta também pode conter informações adicionais para um eventual controle de seção por meio da aplicação requisitante, como por exemplo o tempo de duração da permissão.

Em síntese, o uso de *Web Services* fornece ao CIBAC a portabilidade desejada e o uso do XACML fornece padronização para os algoritmos de decisão.

5.2 Arquitetura CIBAC/SIE-Saúde

A arquitetura CIBAC/SIE-Saúde, com enfoque no serviço de controle de acesso CIBAC e sua integração ao SGCA/SIE, é ilustrada através da figura 5.1. Na figura, o "sistema usuário" representa o SGCA/SIE e os serviços representam o CIBAC.

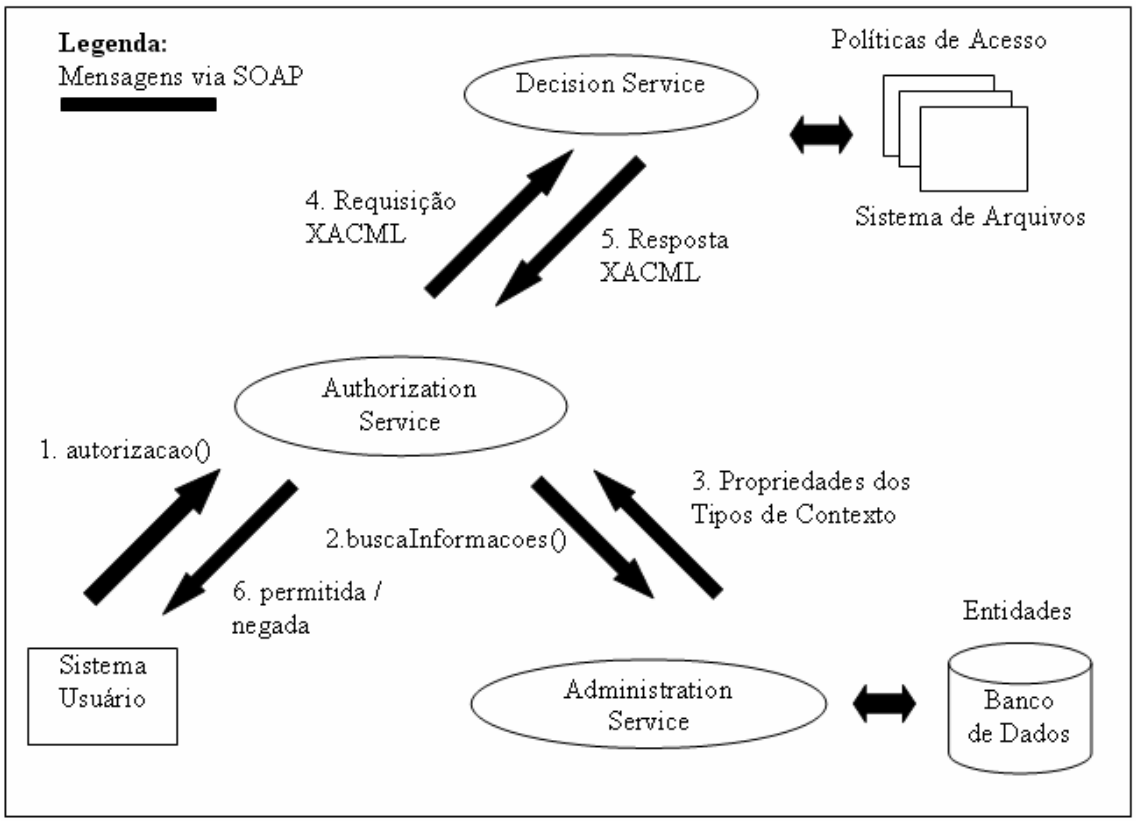

Fig. 5.1 - Arquitetura do CIBAC/SIE-Saúde

Observa-se que para prover as principais funcionalidades do CIBAC criou-se uma arquitetura orientada a serviços. Essa arquitetura é formada pela implementação de três *Web Services* com responsabilidades bem distintas (Serviço de Administração, Serviço de Decisão e Serviço de Autorização), por um banco de informações contextuais (banco de dados) e por um conjunto de políticas de acesso.

É importante destacar que tal modelo, embora usado inicialmente para a área médica, é de uso geral e tem como objetivo armazenar uma variedade de informações, definidas após a instalação do sistema CIBAC.

A descrição de cada serviço, bem como a explicação de seus relacionamentos, são apresentadas nas subseções seguintes.

5.2.1 Serviço de Administração

No CIBAC, as informações contextuais são modeladas como propriedades e armazenadas num banco de dados relacional. O serviço de Administração contempla o acesso ao banco de dados e provê diversas operações para a manipulação destes dados, tais como:

- gravação (inserção ou atualização) de uma delegação, objeto, sujeito, função, tipo de propriedade ou tipo de objeto;
- busca de todas as delegações, objetos, sujeitos, funções, tipos de propriedades e tipos de objetos;
- busca de uma delegação, objeto, sujeito, função, tipo de propriedade ou tipo de objeto usando o `id`, `identificador` ou `nome`, dependendo de qual for a entidade;
- verificação da existência de um objeto, sujeito, função, tipo de propriedade e tipo de objeto baseado em algum parâmetro, como o `identificador` ou `nome` de uma entidade; e
- exclusão de uma delegação, objeto, sujeito, função, tipo de propriedade ou tipo de objeto, usando o `id` de uma entidade.

É importante ainda salientar que para manipular as propriedades dos contextos armazenadas no banco de dados, o Serviço de Administração usa as operações por tipo de contexto, uma vez que estas informações serão acessadas posteriormente, ou seja, para que outros serviços possam utilizar as informações contextuais é necessário que estas estejam armazenadas na forma de propriedades relacionadas aos seus respectivos tipos de contexto, pois é deste modo que os outros serviços do CIBAC manipulam e separam as informações, possibilitando que cada informação seja agrupada de acordo com seu tipo.

Para interagir com este serviço foi criada uma aplicação *Web*, demonstrada através da figura 5.2, para que um usuário administrador pudesse popular o banco de dados com informações relevantes ao sistema. Esta manipulação dos dados também poderia ser feita através de uma interface de usuário do sistema SIE, bastando este se comunicar com o Serviço de Administração.

Fig. 5.2 - Tela de Administração do CIBAC/SIE-Saúde

Do ponto de vista da arquitetura do CIBAC, o resultado de uma consulta a este serviço é a recuperação das informações contextuais de uma dada requisição, as quais irão subsidiar o serviço de decisão.

5.2.2 Serviço de Decisão

O Serviço de Decisão é responsável por gerenciar os arquivos XACML contendo as políticas de acesso, as quais são essenciais ao CIBAC. Estas políticas são armazenadas em um diretório do servidor onde o serviço é executado. A localização de tal diretório é informada ao serviço via parâmetro de inicialização.

Outra responsabilidade deste serviço é receber mensagens SOAP contendo requisições XACML, devidamente instruídas com informações contextuais, e confrontá-las com as diversas políticas previamente cadastradas, seguindo a especificação XACML. Após isso, é gerada uma resposta XACML que é retornada ao requisitante. Para a geração correta da resposta existe uma operação, descrita em seu WSDL, chamada `decisão`.

Para tratar as políticas XACML em conjunto com as requisições e tomar decisões gerando respostas também XACML, foi utilizada a implementação *Sun's* XACML (SUN'S, 2006). *Sun's* XACML é um projeto que fornece um completo suporte a todas as principais características da especificação do XACML, além de ser código aberto e escrito em Java.

Para avaliar se existe alguma política que se aplica a uma dada requisição XACML, este serviço executa um algoritmo de decisão que inicialmente avalia os elementos `Target` das políticas em XACML para verificar se existe uma ou mais políticas aplicáveis a uma dada requisição. Se existe pelo menos uma política aplicável, o algoritmo avalia se existe pelo menos uma cláusula verdadeira que libere o acesso. Uma cláusula só é verdadeira se todas as expressões credenciais (regras) em seu interior forem verdadeiras.

5.2.3 Serviço de Autorização

O Serviço de Autorização desempenha a função de gerente do CIBAC, ou seja, coordena todo o processo de autorização para autorizar ou não um determinado sujeito a executar uma ação que envolve algum objeto (recurso). Para que este serviço retorne uma resposta apropriada, ele utiliza-se dos dois serviços descritos anteriormente.

A função principal do Serviço de Autorização é buscar as informações contextuais (CI) das entidades envolvidas na requisição original (sujeito e objeto), que foram armazenadas através do Serviço de Administração, e montar uma requisição XACML para que esta possa ser utilizada pelo Serviço de Decisão. Logo após, converter a resposta XACML, recebida através do Serviço de Decisão, em uma resposta utilizável pelo sistema usuário.

No SIE-Saúde (sistema usuário), para tomar uma decisão, ao invés de consular sua base de dados, o SCGA comunica-se com o CIBAC, através do Serviço de Autorização. Deste modo o modelo discricionário do SCGA pode ser substituído pelo modelo de controle de acesso baseado em informações contextuais do CIBAC. Além disto, a integração entre o SGCA e o CIBAC demonstrou-se de fácil implementação, em virtude da grande aceitação e suporte à tecnologia *Web Services* pela maioria das plataformas de desenvolvimento.

5.3 Informações Contextuais e o Banco de Dados

Para implementar o modelo CIBAC foram definidos dois tipos de contextos: `sujeitos` e `objetos`, cujas propriedades precisam ser armazenadas em um meio persistente. Para cada um destes tipos foi criada uma tabela no bando de dados com o mesmo

nome, sendo que ambas possuem ligações com suas respectivas tabelas de propriedades. A figura 5.3 ilustra as tabelas contidas no banco de dados.

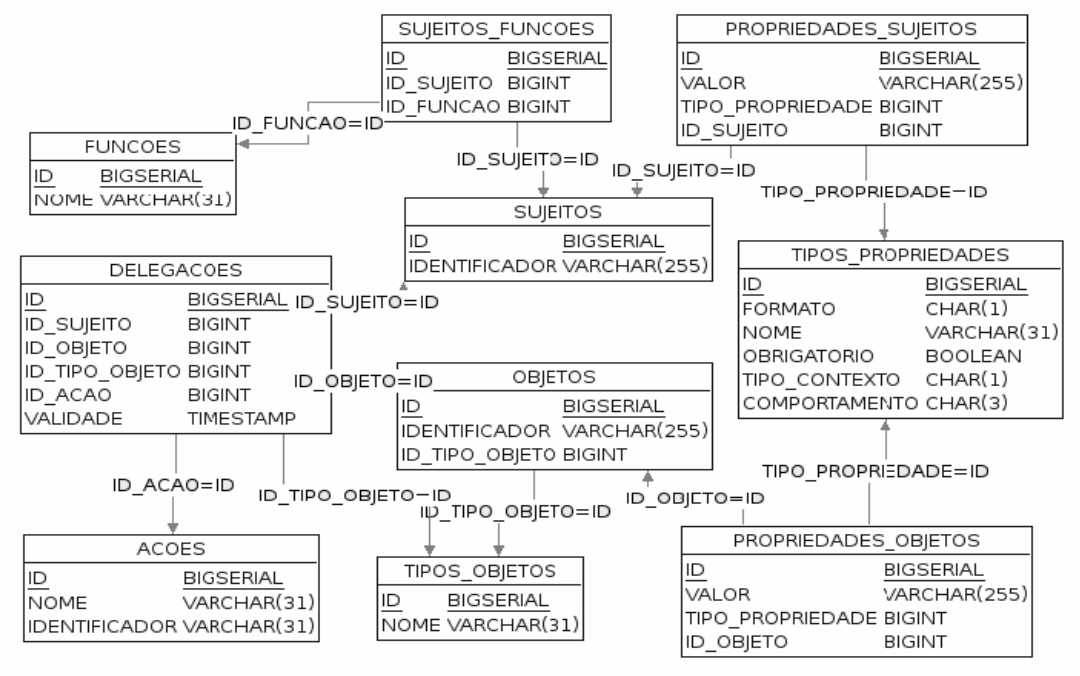

Fig. 5.3 - Tabelas do Banco de Dados

Como a criação de propriedades é dinâmica, foi criada a tabela `Tipos_Propriedades` para armazenar informações sobre elas e seus tipos de contexto. As informações sobre o ambiente também são utilizadas, como a hora do Serviço de Autenticação e o endereço IP do computador do usuário. Por terem características dinâmicas e serem obtidas facilmente através dos computadores utilizados, essas informações não precisam ser armazenadas em um banco de dados, mas sim recuperadas pelo serviço no instante do acesso.

Como os sujeitos possuem funções (ou papéis) desempenhadas dentro de um hospital, foi criada uma tabela `Funcoes`, além de outra tabela para ligar as tabelas `Sujeitos` e `Funcoes`, chamada `Sujeito_Funcoes`. Já os objetos possuem tipos que os classificam em diferentes grupos, logo uma tabela `Tipos_Objetos` foi criada para relacionar objetos a seus tipos.

Conforme demonstrado na figura 5.2, cada tipo de contexto possui um `ID` único, usado apenas pelo banco de dados e pela implementação do CIBAC. No caso do Sujeito este identificador é único, podendo ter valores como CPF ou RG de uma pessoa. Para facilitar a integração com o SIE, na tabela `Tipos_Objetos` do SIE-Saúde utiliza-se o mesmo valor

da chave primária encontrado nas aplicações. Adotou-se esta abordagem por permitir que, por exemplo, um prontuário tenha o mesmo identificador que uma aplicação do SIE, o que os diferenciaria seria o seu tipo: prontuário, aplicação, etc. Facilitando, desta forma, a migração entre o SIE e o SIE-Saúde

De acordo com a modelagem apresentada, cada informação do banco de dados é agregada ao seu contexto na forma de propriedades. Estas propriedades, por sua vez, são armazenadas em tabelas contendo seus valores, sendo os metadados relativos a cada propriedade armazenados na tabela `Tipos_Propriedades`. Na tabela `Tipos_Propriedades` um tipo de contexto relaciona a propriedade a um objeto ou a um sujeito; e contém os seguintes elementos:

- **formato:** forma de representação do valor da propriedade em uma linguagem de programação, como *string*, *int*, *float*;
- **nome:** possui o nome propriamente dito da propriedade, como por exemplo: contador de acesso, médico assistente, entre outros;
- **obrigatório:** determina se o preenchimento do valor da propriedade é obrigatório ou não;
- **tipo de contexto:** relaciona a propriedade a um objeto ou a um sujeito; e
- **comportamento:** determina o comportamento que o valor da propriedade deve assumir, de acordo com características de cada informação, como o incremento do valor na propriedade contador de acesso.

Para dar suporte ao uso de delegações de atribuições no controle de acesso a prontuários médicos, foi criada a tabela `Delegacoes`. Esta tabela armazena uma referência a um sujeito, a ação delegada a ele, e sobre qual objeto (ou tipo de objeto) tal ação pode ser executada, além da validade da delegação criada.

A tabela `Acoes` foi criada para armazenar todas as ações que o CIBAC dá autorizações para serem executadas, limitando-as de acordo com as políticas estabelecidas. O campo nome é usado na criação de políticas, por exemplo, inserir, alterar, excluir, etc. Já o campo identificador serve para criar uma relação com as ações existentes no modelo SIE. Tal campo armazena a chave primária de uma tabela contendo as restrições de funcionalidade (ações existentes).

5.4 Dinâmica de Funcionamento do CIBAC

Para explicar a dinâmica de funcionamento do CIBAC esta seção está dividida em duas subseções: gerência de requisições, onde explica-se como foi implementado o controle para prover ou não uma autorização de acesso; e gerência de delegações, onde explica-se o funcionamento do controle de delegações.

5.4.1 Gerência de Requisições

Uma política de controle de acesso provê a validação de uma requisição de acesso (NBR/ISO/IEC 17799, 2002). Assim, quando o Serviço de Autorização do CIBAC recebe um pedido de autorização, ele recupera as informações de contexto usando o Serviço de Administração e monta uma requisição XACML para o Serviço de Decisão avaliar.

Primeiramente a aplicação do SIE-Saúde se comunica com o SGCA para obter os identificadores dos botões que devem ser habilitados para o usuário corrente. O SGCA então, de posse do identificador do usuário e da aplicação que fez o pedido, se comunica com o Serviço de Autorização através de uma mensagem SOAP. Nessa mensagem o SGCA coloca os identificadores, informa que o objeto em questão é uma aplicação e envia também o endereço IP do computador que abriu a aplicação.

Após o Serviço de Autorização efetuar seu trabalho, ele envia uma mensagem SOAP como resposta para o SGCA. Essa mensagem contém uma *string* informando a decisão resultante, que pode ser: `permitida`, `negada`, `não aplicável` ou `indeterminada`. Uma decisão não aplicável significa que não foi possível encontrar uma política que se aplica aos dados enviados pelo SGCA. Uma decisão do tipo indeterminada é retornada quando ocorre alguma exceção na execução do CIBAC.

Caso a decisão seja `permitida`, são enviados ao SGCA os identificadores de todas as ações que o usuário autenticado possui permissão de executar sobre a aplicação, bem como o tempo de duração desta aplicação, em milissegundos. O SGCA poderá então utilizar esse tempo para garantir as regras temporais de controle de acesso.

Logo após receber a mensagem contendo o pedido de autorização, feita pelo SGCA, o Serviço de Autorização se comunica com o Serviço de Administração para obter as propriedades referentes ao sujeito e ao objeto, bem como as delegações válidas. Para obter estas informações, o Serviço de Administração executa consultas ao banco de dados. Se houver alguma delegação, é feita uma união entre as ações delegadas e as ações permitidas

pelo resultado da avaliação das políticas. Se as políticas negarem a autorização, então somente as ações delegadas serão informadas ao SGCA.

De posse das informações sobre os tipos de contexto, o Serviço de Autorização cria uma requisição XACML com esses dados e envia uma mensagem SOAP para o Serviço de Decisão. Este, por sua vez, verifica todas as políticas que foram carregadas do sistema de arquivos para sua memória, em busca de alguma que seja aplicável à requisição corrente. A resposta do Serviço de Decisão também é no formato XACML.

Ao receber a resposta XACML, o Serviço de Autorização verifica a decisão recebida. Caso exista uma política aplicável, cujo resultado seja permitido, o serviço em questão faz uma união das ações permitidas com as ações delegadas e envia, como resposta, uma mensagem SOAP para o SGCA.

5.4.2 Gerência de Delegações

Um dos grandes benefícios do sistema CIBAC é a possibilidade de um usuário delegar uma ação sobre um objeto para outro usuário. Dentro da área médica esta funcionalidade é de grande valia, pois permite que, por exemplo, um médico responsável por determinado prontuário possa delegar a ação de manipulação do prontuário a outro médico.

Como abordado anteriormente na seção 4.4.2., para o CIBAC delegação é definida como uma Restrição de Funcionalidade no SIE-Saúde. Desta forma a ação “delegar” é mapeada através de condições de contexto que possibilitem a sua utilização.

Avaliada a condição de contexto e concedida a delegação, o controle de acesso às funcionalidades do SIE-Saúde passa a ser discricionário para aquelas ações delegadas. Em outras palavras, no CIBAC quando um usuário estabelece uma delegação a outro usuário para uma ação específica sobre algum recurso, esta nova atribuição é verificada em uma tabela de delegações, onde há a descrição do acesso e também características relativas à revogação da delegação.

Uma vez que a ação a ser delegada é confrontada com as condições de contexto do usuário que delega a atribuição, pode-se garantir que a tabela de delegações não sofre nenhuma inconsistência. Isto é importante porque uma delegação só pode ser concedida de acordo com níveis hierárquicos pré-estabelecidos.

Para que um usuário possa delegar uma ação, foi criada uma aplicação *Web* (figura 5.4) onde existe um formulário para preenchimento e cadastro de delegações. Esta aplicação

também serve para informar ao usuário quais delegações já foram cadastradas, desde que possuam seu prazo de validade ainda ativo.

Fig. 5.4 - Formulário de Controle de Delegações

É importante observar que uma delegação não possui informações sobre o usuário que a criou, pois para o CIBAC não importa quem a cadastrou. Ao invés disto deve-se criar políticas para definir quem pode delegar, quais as ações possíveis, e para quais objetos ou tipos de objeto podem ser destinadas. A verificação se um usuário tem permissão para cadastrar determinada delegação usa o Serviço de Autorização do CIBAC.

Após criada, uma delegação influencia na resposta de um pedido de autorização da seguinte forma: logo após o SGCA fazer um pedido de autorização para o Serviço de Autorização, este serviço verifica os parâmetros recebidos e busca informações contextuais sobre o sujeito e objeto especificado, através da comunicação com o serviço de Administração. Além disto, também são buscadas todas as ações que foram delegadas para o sujeito atual, desde que tais delegações sejam ainda válidas. As ações delegadas e válidas serão imediatamente permitidas e informadas ao SGCA, pois não é necessário avaliar outras políticas, visto que a análise de contexto já foi efetuada para esta ação.

5.5 Testes de Avaliação e Desempenho

Para avaliar a implementação do CIBAC foram efetuados testes de desempenho e de funcionalidade (DOMINGUES, 2002). Testes de desempenho são de grande importância para o sistema, dado que o mesmo deve ser usado continuamente e exige um tempo de resposta pequeno para requisições feitas por diversos usuários, enquanto que os testes funcionais procuram revelar erros em funções, estruturas de dados, no acesso ao banco de dados, dentre outros.

Testes de Desempenho

Para a realização dos testes de desempenho foram utilizados dois computadores, um servidor e outro cliente. O servidor executou todos os serviços do CIBAC, além do banco de dados PostgreSQL 8, usado pelo Serviço de Administração. Já o cliente, efetuou as requisições e contabilizou os resultados e os tempos de execução. Tanto o computador cliente como o computador servidor possuíam a mesma configuração, ou seja, processador Intel® Pentium® 4, de 1.80 GHz e 1 GBytes de RAM. A rede utilizada foi uma Ethernet de 100 Mbps.

Para os testes foram criadas dez políticas XACML, cada uma aplicável a uma determinada função do sujeito e a um tipo de objeto. O banco de dados foi alimentado com informações de contexto e foram cadastradas cinco funções e dois tipos de objetos, combinação usada para gerar as dez políticas.

Estabelecidas as informações necessárias para os testes, o teste de desempenho consiste em realizar lotes de requisições simultâneas, disparadas por um número variado de *threads*, a fim de testar a capacidade do CIBAC para processar requisições. Para cada grupo de *threads* requisitantes (o tamanho do grupo indica o número de requisições simultâneas), foi calculado o tempo médio para atendimento de todas as requisições. O gráfico da figura 5.3 mostra os tempos médios para um número de requisições simultâneas variando de 1 a 50.

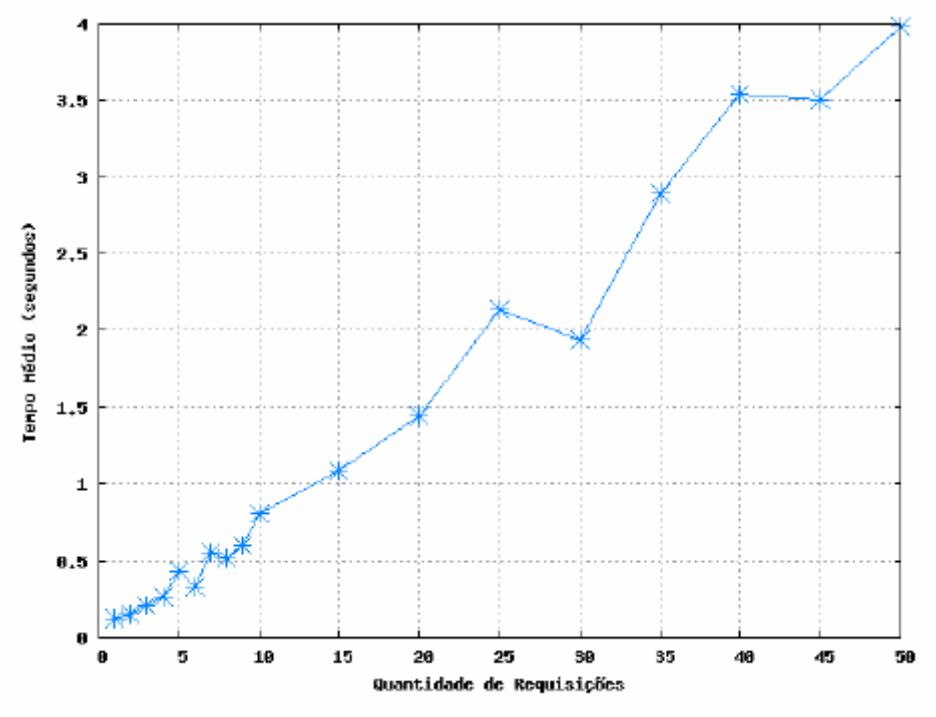

Fig. 5.5 - Tempos Médios de Resposta em Requisições Simultâneas

Como pode-se observar através do gráfico, o tempo médio para atender até 10 requisições simultâneas ficou abaixo de 1 segundo, o que demonstra um desempenho satisfatório, considerando as especificações temporais do SIE-Saúde. Além disto, observa-se um crescimento linear do tempo médio em função da quantidade de requisições simultâneas.

Embora o tempo médio possa aumentar com a adição de novas políticas, devido as funções de verificação de cláusulas, pode-se melhorar o desempenho utilizando um servidor com maior poder de processamento, ou mesmo distribuindo os serviços em computadores distintos.

Testes Funcionais

Para testar a funcionalidade do CIBAC, a geração de casos de teste foi empírica (não automática), mas buscou cobrir as principais funcionalidades do mecanismo de controle de acesso: verificação de informações contextuais no momento da requisição de acesso. Os testes funcionais realizados constituem-se de uma série de requisições, geradas variando-se parâmetros de interesse, e suas respectivas avaliações frente a um conjunto de regras pré-definidas.

Como um teste de funcionalidade visa garantir que não existam diferenças entre os requisitos funcionais (vide requisitos do CIBAC na seção 4.5) e o comportamento do software desenvolvido, os casos de teste tiveram como objeto alvo uma aplicação SIE de “cadastro de

pacientes” e suas regras de acesso. Para esta aplicação, foram definidas três regras de acesso e planejados alguns testes (requisições de interesse), conforme detalhado a seguir.

Considerando que o princípio básico do CIBAC é a utilização de informações contextuais, tais como perfil de usuário, horário de acesso e hierarquia de privilégios, as regras da política de acesso devem ser definidas por modo de acesso.

Deste modo, considerando que na aplicação “Cadastro de Paciente” do SIE a inclusão e exclusão de cadastros possam ser realizados somente entre 8 e 11h da manhã E alterações possam ser realizadas somente entre 8 e 12h da manhã E que apenas médicos e analistas possam manipular o cadastro E que apenas usuários com perfil analista possa excluir cadastros, devemos criar regras específicas para as ações de criar, alterar e excluir cadastros. Assim, definiram-se as seguintes regras para os testes funcionais:

Regra 1 (figura 5.6): os perfis “Médico” e “Analista” só podem realizar a ação “inserir” entre 8 e 11h da manhã.

Regra 2 (figura 5.7): os perfis “Médico” e “Analista” só podem realizar a ação “alterar” entre 8 e 12h da manhã.

Regra 3 (figura 5.8): o perfil “Analista” pode realizar a ação “excluir” entre 8 e 12h da manhã.

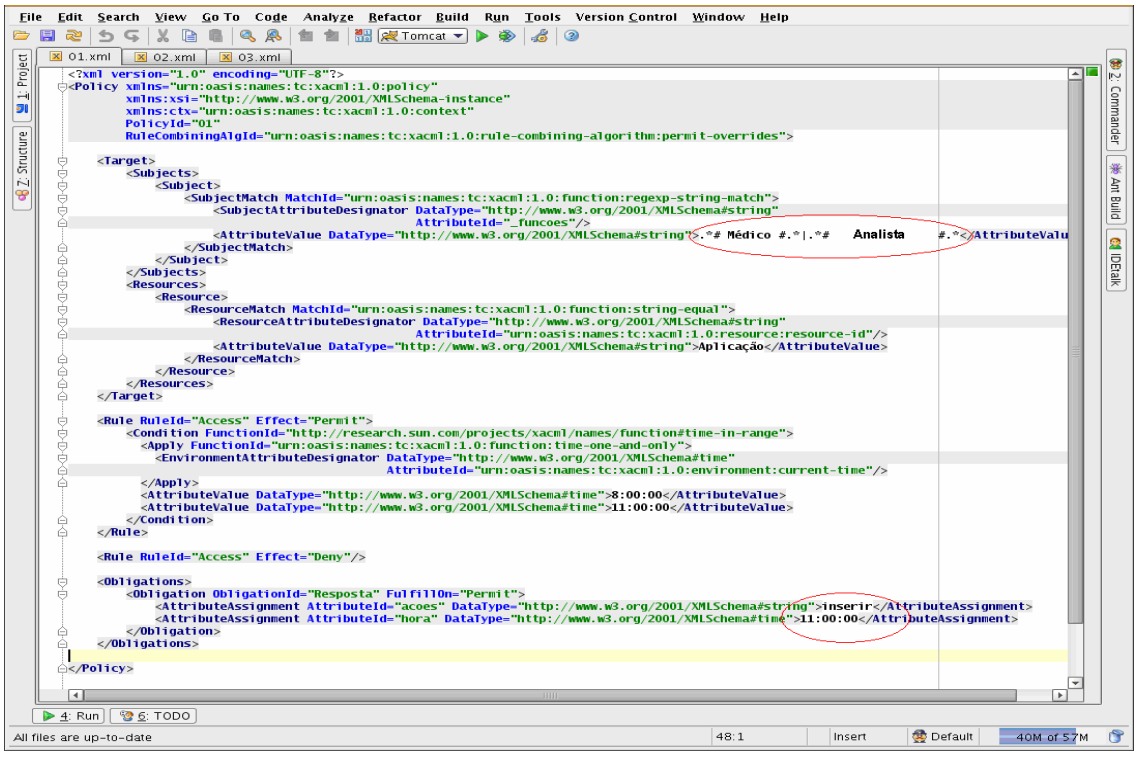

Fig. 5.6 - Regra 1

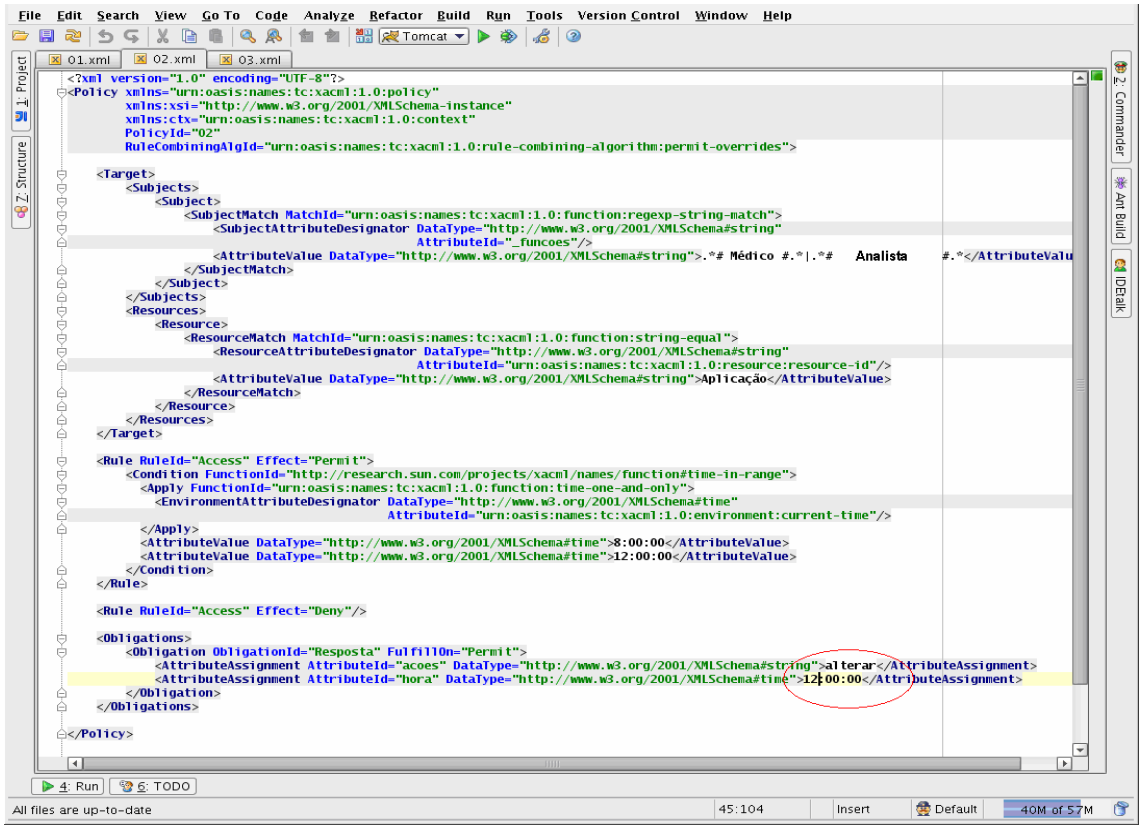

Fig. 5.7 - Regra 2

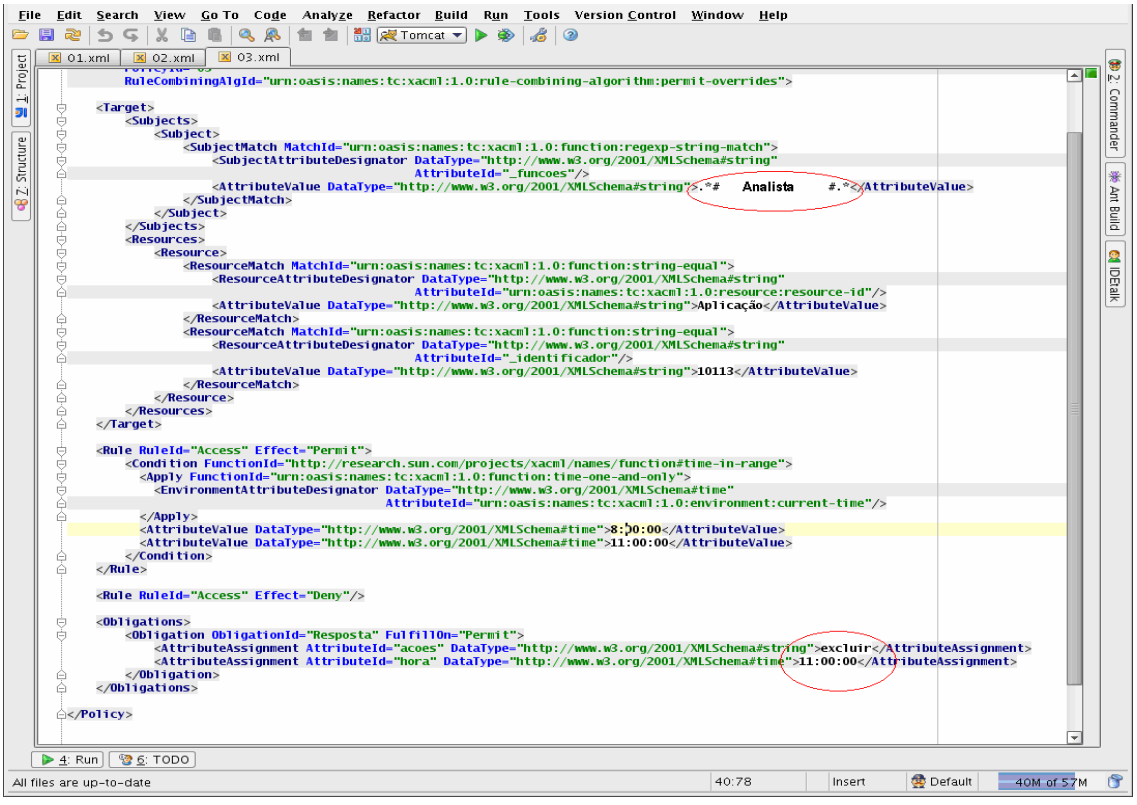

Fig. 5.8 - Regra 3

Com estas três regras básicas foi possível efetuar testes que correspondem aos requisitos básicos do CIBAC e sua funcionalidade.

TESTE 1: neste teste foi efetuada uma requisição de acesso com perfil “Analista” em um horário de acesso inferior ao horário inicial estabelecido pela política, no caso 07h04min. Na política em XACML têm-se três cláusulas que correspondem ao acesso do perfil “Analista”, sendo que todas as cláusulas possuem expressões relativas à propriedade tempo do acesso. Como o valor da propriedade tempo na requisição é inferior ao tempo inicial especificado pela política (08h00min) não existem cláusulas verdadeiras e por este motivo o acesso é negado (vide figura 5.9).

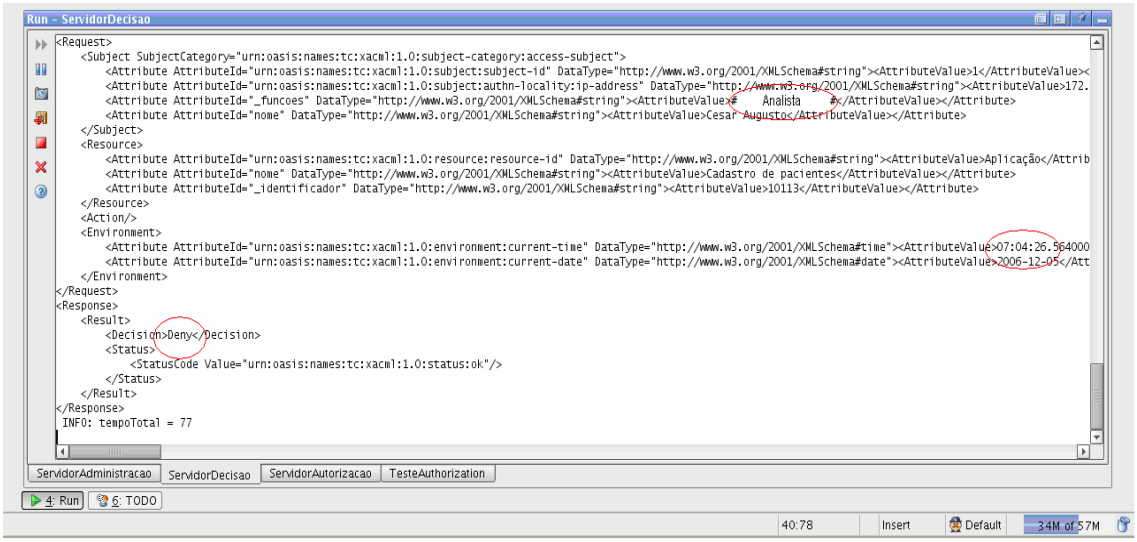

Fig. 5.9 - Decisão de Acesso 1

TESTE 2: neste teste considera-se uma requisição de acesso com o horário correto, 08h43min. Como o horário da requisição neste caso é 08h43min, o acesso é permitido (figura 5.10). Observa-se ainda que o CIBAC retorna os modos de acesso possíveis e o tempo limite para os mesmos, ou seja: excluir – 11h00min, alterar – 12h00min e inserir – 11h00min, agrupando as três cláusulas de acordo com as regras estabelecidas para este perfil.

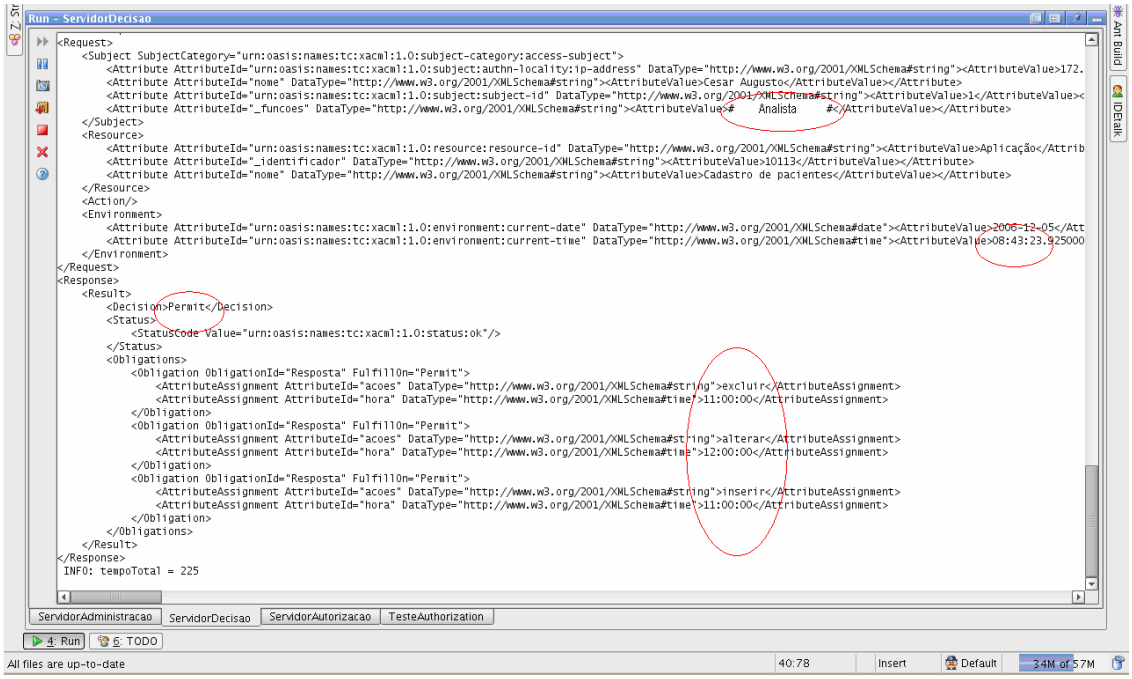

Fig. 5.10 - Decisão de Acesso 2

TESTE 3: neste teste altera-se novamente o horário de acesso. Como o acesso foi solicitado às 11h44min (vide figura 5.11) o CIBAC analisa as informações confrontando-as com a política e concede apenas a permissão para o modo de acesso “alterar”, uma vez que o mesmo pode ser concedido até às 12h00min e esta configura-se como a única cláusula verdadeira de acordo com a propriedade tempo do acesso.

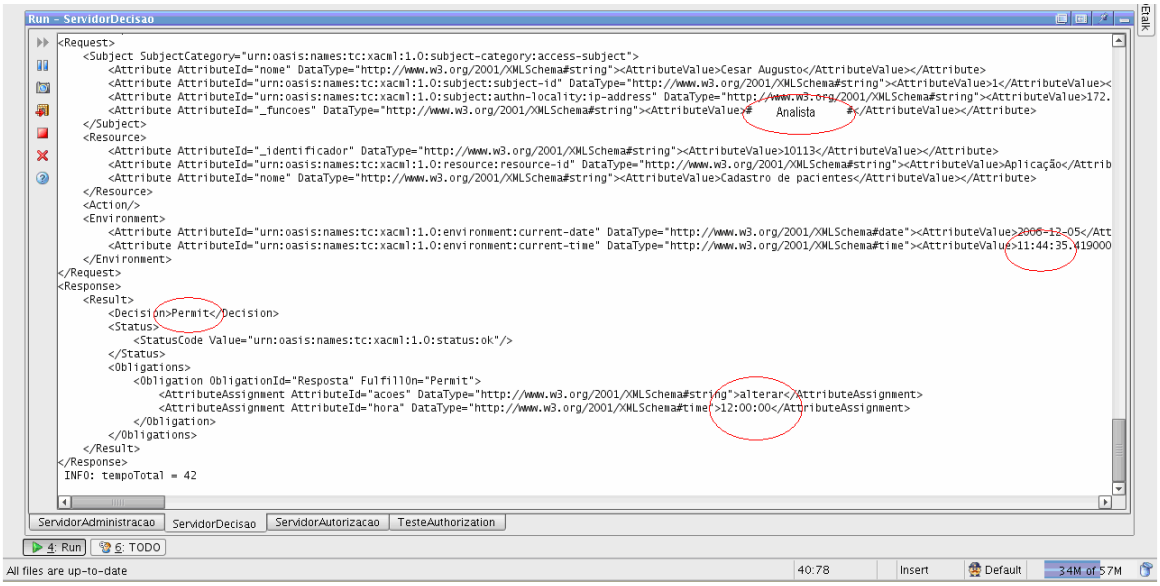

Fig. 5.11 - Decisão de Acesso 3

TESTE 4: neste teste verifica-se a tentativa de acesso após o tempo limite. Neste caso o acesso é negado, pois a requisição de acesso é efetuada às 12h45min (vide figura 5.12) e o acesso à aplicação só poderia ser concedido até às 12h00min. Mais uma vez demonstrando que a inexistência de cláusulas verdadeiras nega o acesso.

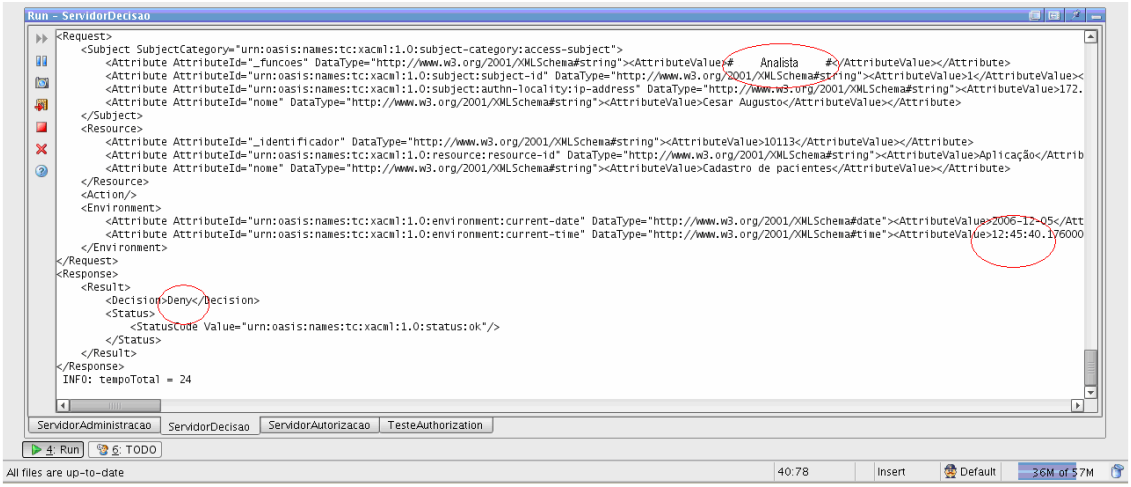

Fig. 5.12 - Decisão de Acesso 4

TESTE 5: este teste avalia uma situação onde um médico requisita permissão para uma ação “excluir”. Como a ação “excluir” só pode ser concedida ao Analista e um usuário Médico tem permissão somente para as ações “alterar” e “inserir”, neste caso somente duas cláusulas são testadas de acordo com a informação do perfil do usuário e a resposta à requisição é relativa somente à estas duas cláusulas (vide figura 5.13), evidenciando a hierarquia de privilégios para o SIE-Saúde.

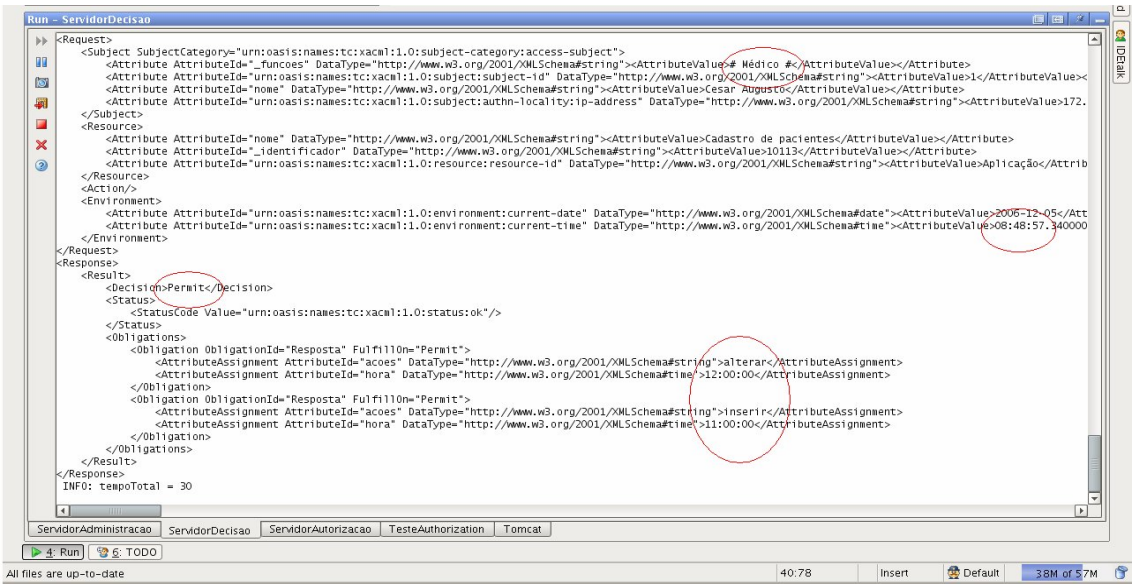

Fig. 5.13 - Decisão de Acesso 5

TESTE 6: este teste avalia o comportamento no caso de requisições com perfis de usuários que não possuem regras explícitas para uma dada ação. Para isto utiliza-se o perfil “Enfermeiro”. Neste caso a resposta do CIBAC (vide figura 5.14) é “não aplicável” pois um usuário com perfil “Enfermeiro” não possui acesso ao “Cadastro de Pacientes”, portanto não existem cláusulas (ou regras) relacionando este perfil com a aplicação “Cadastro de Pacientes”.

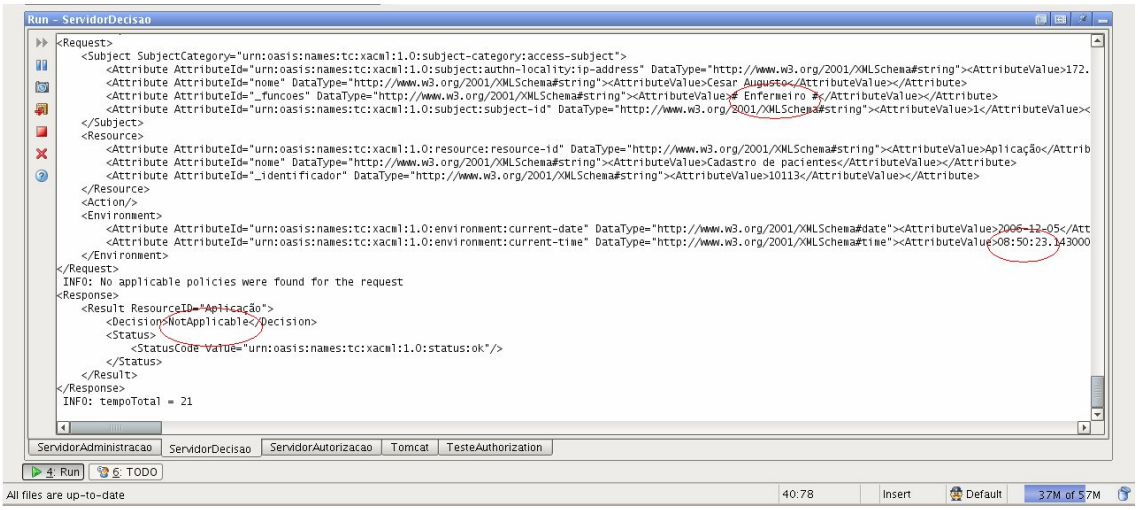

Fig. 5.14 - Decisão de Acesso 6

Durante os testes funcionais observaram-se alguns cenários que podem comprometer o controle de acesso no caso de ataques de intrusão: a correta identificação do usuário e o controle de seção. Entretanto, a cobertura destes cenários está fora do escopo deste trabalho, podendo ser tratados em trabalhos futuros.

Quanto à identificação do usuário, observou-se que o CIBAC trata as informações contextuais segundo as regras da política em questão, mas não trata especificamente a identificação do usuário, sendo este de responsabilidade da aplicação, ou seja, o SIE-Saúde.

Quanto ao controle de seção, o CIBAC possibilita o controle de seção retornando ao SIE-Saúde, além da resposta de acesso, informações relativas ao tempo máximo permitido para o período de acesso (caso existam regras que definam questões temporais). Entretanto, após a verificação no CIBAC, esta informação deve ser utilizada pelo sistema usuário a fim de implementar o controle de seção.

Os testes funcionais realizados demonstram que o CIBAC atende aos requisitos exigidos para suportar o controle de acesso baseado em informações contextuais contidas nas requisições de acesso ao SIE-Saúde.

Capítulo 6
CONCLUSÕES E PERSPECTIVAS

Neste último capítulo são destacadas as principais contribuições obtidas neste trabalho, bem como são sugeridas algumas atividades que poderão ser implementadas em trabalhos futuros.

6.1 Conclusões

Esta dissertação apresentou um modelo de controle de acesso baseado em informações contextuais, denominado CIBAC, o qual fornece autorizações de acesso relacionando informações de diferentes contextos. O modelo agrega novas funcionalidades ao RBAC (*Role-Based Access Control*), que baseia-se principalmente em regras de acesso e perfis de usuários, mas não efetivamente em informações contextuais.

No CIBAC o uso de contextos, definidos através de propriedades, torna o controle de acesso dinâmico e possibilita um melhor mapeamento entre a política de acesso e a implementação das regras utilizadas no âmbito de informações médicas, como no caso do SIE-Saúde. Além disto, possibilita ainda o acesso diferenciado para perfis distintos de usuários, ao mesmo tempo em que considera requisitos como temporalidade e hierarquia de privilégios. Em outras palavras, o principal mérito do CIBAC é possibilitar que as informações necessárias à elaboração das políticas de acesso possam ser armazenadas de uma forma clara e independente.

Como resultado prático a implementação de uma política de acesso complexa que inclui delegações, como a de acesso ao prontuário eletrônico do paciente, pode ser realizada de maneira mais facilitada. As relações contextuais podem ser modeladas de maneira mais simples, uma vez que as informações podem ser tratadas como propriedades de um contexto. Esta facilidade mostrou a sua integração com os módulos do SIE, possibilitando o controle de acesso ao PEP do Hospital Universitário de Santa Maria.

6.2 Perspectivas

Dando continuidade aos trabalhos realizados nesta dissertação, propõem-se algumas atividades que poderão ser realizadas futuramente:

- incluir mecanismos fortes de autenticação ao modelo, que não considerem somente login e senha, agregando mecanismos de identificação mais confiáveis;
- realizar uma especificação mais aprofundada das regras e políticas de controle de acesso que possam abranger os demais níveis hierárquicos da instituição; e
- expandir os módulos de serviço utilizados na arquitetura do CIBAC, com a finalidade de expor a utilização e manutenção do sistema para usuários finais através de interfaces amigáveis.

REFERÊNCIAS

ALMEIDA, Maurício Barcellos. **An introduction to XML, its use on the Internet and some complementary concepts.** Ci. Inf., may/ago. vol. 31, no.2, p.5-13. ISSN 0100-1965. 2002.

APACHE SOFTWARE FOUDATION. **The Apache Jakarta Project : Apache Tomcat.** 2003. Disponível em <http://jakarta.apache.org/tomcat>. Acesso em: novembro de 2005.

ATLURI, V.; WARNER, J. **Supporting Conditional Delegation in Secure Workflow Management Systems.** In: Tenth ACM Symposium on Access Control Models and Technologies. *Proceedings* p. 49-58, 2005.

BACON, J.; MOODY, K.; YAO, W. **A Model of OASIS Role-Based Access Control and its Support for Active Security.** ACM Transaction on Information and System Security, v.5, p.492-540, nov. 2002.

BERTINO, E. ; BONATTI, P. A.; FERRARI, E. **TRBAC: A Temporal Role-Based Access Control Model.** ACM Transaction on Information and System Security, 4(3):191–233. 2001.

BOOCH, G. **Object-Oriented Design with Applications.** Benjamin Cummings, Redwood City, CA. BOO g 94:1. 1991.

BRASIL. **Constituição da República Federativa do Brasil.** 1988.

CASTRO, A. F. de; SILVA, G. M. P. da; SANTOS, S. F. dos. **O controle de documentos mantidos em meio eletrônico e os requisitos da NBR ISO/IEC 17025.** IV Congresso Latino-Americano de Metrologia, Foz do Iguaçu. 2004.

CELKO, J. **Joe Celko's SQL for smarties: advanced SQL programming.** 2. ed. Morgan Kaufmann, 1999.

CFM. **Resolução 1.629/2002 do Conselho Federal de Medicina**. 2002. Disponível em <http://www.arnaut.eti.br/ResoCFM.htm>. Acesso em: dezembro de 2005.

CLOCKSIN, W. F.; MELLISH, C. S. **Programming in Prolog.** 2. ed. Springer-Verlag, 1984.

COVINGTON, M. J.; SASTRY, M. R. **A Contextual Attribute-Based Access Control Model.** Corporate Technology Group. Intel Corporation. January, 2006.

COVINGTON, M. J.; FOGLA, P.; ZHAN, Z.; AHAMAD, M. **A Context-Aware Security for Emerging Applications.** In : 18TH Annual Computer Security Applications Conference, 2003.

DEY, A. K. ; ABOWD, G. D. **Towards a Better Understanding of Context and Contextawareness.** Gvu technical report GIT-GVU-99-22, College of Computing, Georgia Institute of Technology, 1999.

DOMINGUES, André Luis dos Santos. **Avaliação de Critérios e Ferramentas de Teste para programas OO.** Dissertação de Mestrado, Instituto de Ciências Matemáticas e de Computação de São Carlos - Universidade de São Paulo. 2002.

FERNANDES, L. **Oracle 9i para desenvolvedores : curso completo.** Axel Books do Brasil. 2002.

FERRAIOLO, D. F.; SANDHU, R. S.; GAVRILA, S. I. ; KUHN, D. R.; CHANDRAMOULI, R. **Proposed NIST Sstandard for Role-Based Access Control.** Information and System Security, 4(3):224–274. 2001.

GEORGIADIS, C. K.; MAVRIDIS, I.; PANGALOS, G.; THOMAS, R. **Flexible team-based access control using contexts.** In: Sixth ACM Symposium on Access Control Models and Technologies. *Proceedings* p. 21-27, 2001.

GLIGOR, V. D.; GAVRILA, S. I.; FERRAIOLO, D. **On the formal definition of separation-of-duty policies and their composition.** In: IEEE Symposium on Security and Privacy. *Proceedings* p. 172-183, 1998.

HORN, A. **On sentences which are true of direct unions of algebras.** Journal of Symbolic Logic, v. 16, p. 14-21, 1951.

HAN, Yonggang. **Context Aware Security Policy Enforcement: CASPEr.** Master's Thesis of Department of Mathematics and Computer Science. Technische Universiteit Eindhoven. 2005.

HU, J.; WEAVER, A. C. **A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications.** Pervasive Privacy Security, Privacy, and Trust (PSPT2004), Boston, MA, August, 2004.

HULSEBOSCH, R. J.; SALDEN, A. H.; BARGH, M. S.; EBBEN, P. W. G.; REITSMA, J. **Context sensitive access control.** In: Tenth ACM Symposium on Access Control Models and Technologies. *Proceedings* p. 111–119, New York, NY, USA. 2005.

ISO/IEC 15408. **Information Tecnology – Security techniques – Evaluation criteria for IT security.** International Organization for Standardization – ISO and International Electrotechnical Commission – IEC. 1999.

JOSHI, J. B. D.; BERTINO, E.; SHAFIQ, B.; GHAFOOR, A. **Dependencies ans separation of duty constraints in GTRBAC.** In: Eighth ACM Symposium on Access Control Models and Technologies, *Proceedings* p.51-64, 2003.

KFOURI NETO, Miguel. **Responsabilidade Civil do Médico.** 5ª. Ed. Revista dos Tribunais. São Paulo, 2003.

KUDO M. ; HADA S. **XML Access Control Language: Provisional Authorization for XML Documents**. Tokyo Research Laboratory, IBM Research, 2000.

KUMAR, A.; KARNIK, N.; CHAFLE, G. **Context sensitivity in role-based access control.** ACM SIGOPS Operating Systems Review, v.36, n.3, p.53-66, jul. 2002.

LIMA, E.; REIS, E. **C# e .NET : guia do desenvolvedor.** Campus, 358 p., 2002.

LIN, A.; BROWN, R. **The application of security policy to role-based access control and the common data security architecture.** Computer Communications, v.23, p.1584-1593, 2000.

LONGSTAFF, J.; LOCKYER, M.; NICHOLAS, J. **The Tees confidentiality model: an authorisation model for identities and roles.** In: Eighth ACM Symposium on Access Control Models and Technologies, *Proceedings* p. 125-133, 2003.

MARIN, H. F.; MASSAD, E.; AZEVEDO-NETO, R. S. **Prontuário Eletrônico do Paciente: definições e conceitos.** Washington, DC: Organização Pan-Americana de Saúde, 2003.

MASSAD, Eduardo; MARIN, Heimar de Fátima; AZEVEDO-NETO, Raymundo Soares de. **O Prontuário eletrônico do paciente na assistência, informação e conhecimento médico.** São Paulo, ISBN 85-903267-1-3: H. de F. Marin, 213p, 2003.

MONJIAN, B. **PostgreSQL: introduction and concepts.** Addison-Wesley, 462 p. 2000.

MOTTA, G. H. M. B.; FURUIE, S. S. **Um modelo de autorização contextual para o controle de acesso baseado em papéis.** In: II Workshop em Segurança de Sistemas Computacionais (WSeg2002), pages 137–144, Porto Alegre-RS, Brasil. SBC. 2002.

_____. **Um modelo de autorização contextual para o controle de acesso ao Prontuário Eletrônico do Paciente em Ambientes Abertos e Distribuídos.** Tese de doutorado apresentada à Escola Politécnica da Universidade de São Paulo, São Paulo-SP, Brasil. 2003a.

_____. **A contextual role-based access control authorization model for electronic patient record.** IEEE Transactions on Information Technology in Biomedicine, 7(3):202–207. 2003b.

NBR/ISO/IEC 17799**. Tecnologia da informação: Código de prática para a gestão da segurança da informação.** Associação Brasileira de Normas Técnicas ABNT, 55 p. 2002.

NEUMANN, G.; STREMBECK, M. **An approach to engineer and enforce context constraints in an RBAC environment.** In: Eighth ACM Symposium on Access Control Models and Technologies, *Proceedings* p. 65-79, 2003.

NEWCOMER, E. **Understanding web services XML, WSDL, SOAP and UDDI.** Addison Wesley, 368 p. 2002.

OASIS. **eXtensible Access Control Markup Language (XACML) version 1.1.** Committee Specification, August. 2003.

OMG – OBJECT MANAGEMENT GROUP. **CORBA security service specification 1.7.** 2001. Disponível em <http://www.omg.org/cgi-bin/doc?formal/01-03-08>. Acesso em: agosto de 2005.

PASCOE, J. **Adding generic contextual capabilities to wearable computers.** In: International Symposium on Wearable Computers, pp. 92–99, 1998.

PINTO, Virgínia Bentes. **Eletronic Patient Record: Technical Document of Information and Communication of the Health Dominion.** R. Eletr. Bibliotecon. Ci. Inf., Florianópolis, n.21, 1º sem. 2006.

RODRIGUES, R. J.; WINSON, P.; SCHANZ, S. J. **The Regulation of Privacy and Data Protection in the Use of Eletronic Health Information**. in International Perspective in reference source on Regulatory and Legal Issues Releated to Person-Identifiable Health Databases. Washington, DC: Organização Pan-Americana de Saúde, 217 p, 2001.

RYAN, N. S.; PASCOE, J.; MORSE, D. R. **Enhanced reality fieldwork: the context-aware archaeological assistant.** In: Gaffney, V., van Leusen, M., and Exxon, S., editors, Computer Applications in Archaeology, British Archaeological Reports, Oxford. Tempus Reparatum, 1997.

SAMARATI, Pierangela; VIMERCATI, Sabrina De Capitani di. **Access Control: Policies, Models, and Mechanisms.** Foundations of Security Analysis and Design, Tutorial Lectures, LNCS, v.2171, p.137-196, 2001.

SANDHU, R. S.; SAMARATI, P. **Access Control: Principles and Practice.** IEEE Communications, vol. 32, pp. 40-48, Sept. 1994.

SCHILIT, B.; THEIMER, M. **Disseminating active map information to mobile hosts.** In: IEEE Network, v.8, n.5, pp. 22–32, 1994.

SHORTLIFFE, E. H.; PERREAULT, L. E. **Medical informatics: computer applications in Health Care.** New York: Addison-Wesley, 1990.

SLEE, V.; SLEE, D.; SCHMIDT, H. J. **The endangered medical record – ensuring its integrity in the age of informatics.** Saint Paul, Minnesota, Tringa Press, 2000.

SOARES, Gerson Antunes; NUNES, Raul Ceretta. **Controle de Acesso Baseado em Credenciais Hierárquicas Dinâmicas – DHCBAC.** In: II Latin-American Symposium on Dependable Computing - Workshop on Theses and Dissertations, Salvador. *Proceedings* of the LADC Wokshops. Salvador, 2005. p. 77-82. 2005.

SOHR, K.; DROUINEAUD, M.; AHN, G. **Formal Specification of Role-Based Security Policies for Clinical Information Systems.** In: ACM Symposium o Applied Computing, New Mexico – USA. *Proceedings* of the SAC'05, p. 332-339. 2005.

SOMMERVILLE, I. **Software engineering.** 5. ed. Addison-Wesley. 1996.

SUN MICROSYSTEMS. **Java 2 plataform, standard edition.** 5. ed. 2003. Disponível em <http://java.sun.com/j2se/>. Acesso em: junho de 2006.

VARGA, Andrew C. **The Main Issues in Bioethics.** Paulist Press, USA. 1980.

W3 CONSORTIUM. **Extensible Markup Language (XML).** 2. ed., out. 2000 Disponível em <http://www.w3.org/xml/>. Acesso em: maio de 2006.

WECHSLER, Rudolf; ANÇÃO, Meide S.; CAMPOS, Carlos José Reis de; SIGULEM, Daniel. **Computing in medical practice.** Jornal de Pediatria - Sociedade Brasileira de Pediatria. 0021-7557/03/79-Supl.1/S3, 2003.

WEED, L. **Medical Record that guide and teach.** The New England Journal of Medicina, v.278. p. 593-600, 1968.

WILIKENS, M.; FERITI, S.; SANNA, A.; MASERA, M. **A context-related authorization and access control method based on RBAC: a case study from the health care domain.** In: Seventh ACM Symposium on Access Control Models and Technologies, *Proceedings* p. 117-124. 2002.

YEONG, W.; HOWES T.; KILLE, S. **Lightweight directory access protocol. Internet Engineering Task Force.** Mar. 1995. 22 p. Disponível em <http://www.ietf.org/rfc/rfc1777.txt/>. Acesso em: dezembro de 2005.

ZHANG, G.; PARASHAR, M. **Context-Aware Dynamic Access Control for Pervasive Applications.** In: *Proceedings* of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Diego, CA, USA. 2004.

ZHANG, L.; AHN, G.; CHU B. **A Role-Based Delegation Framework for Healthcare Information Systems.** In: Seventh ACM Symposium on Access Control Models and Technologies, *Proceedings* p. 125-134. 2002.

_____. **A Rule-Based Framework for Role-Based Delegation.** In: Sixth ACM Symposium on Access Control Models and Technologies, *Proceedings* p. 153-162. 2001.

Anexo 1

Publicações

SOARES, Gerson Antunes; NUNES, Raul Ceretta; AMARAL, Érico M. H. do. **Um Modelo de Controle de Acesso Baseado em Contexto para Autorizações a Informações Médicas.** In: XXXII Conferência Latino-Americana de Informática, Santiago de Chile, 2006.

SOARES, Gerson Antunes; NUNES, Raul Ceretta. **Controle de Acesso Baseado em Credenciais Hierárquicas Dinâmicas – DHCBAC.** In: II Latin-American Symposium on Dependable Computing - Workshop on Theses and Dissertations, Salvador. *Proceedings* of the LADC Wokshops. Salvador, 2005. p. 77-82. 2005.

SOARES, Gerson Antunes; NUNES, Raul Ceretta; MACHADO, Roger Cavilhas; AMARAL, Érico M. H. do. **Utilização de Agentes em um Modelo de Autorização para Acesso a Dados Médicos em Ambiente de Computação Móvel.** In: III Escola Regional de Redes de Computadores, Santa Cruz do Sul. p.61-66. 2005.

SOARES, Gerson Antunes; MACHADO, Luciano Guilherme; AMARAL, Érico M. H. do; NUNES, Raul Ceretta. **CPAut: um Captive Portal para Autenticação.** In: XX CRICTE – Congresso Regional de Iniciação Científica e Tecnológica em Engenharia, Foz do Iguaçu. 2005.