MACA Administrativo – Manual do Usuário

Gustavo Motta

Versão: 3.2.2

São Paulo, setembro de 2005

APRESENTAÇÃO

O objetivo deste manual é mostrar como utilizar o MACA AD para definição de políticas de controle de acesso e o MACA AD Web para criação de contas de usuários. Apresenta conceitos básicos de controle de acesso, com ênfase no controle de acesso baseado em papéis do NIST, modelo adotado pelo MACA. Descreve ainda a arquitetura de software onde o MACA está implementado. Ilustra através de um tutorial o processo de definição de uma política de acesso para uma aplicação didática, o "Sistema de Gerência de Pedidos". Ao final, esperamos que os futuros usuários do MACA AD tenham autonomia para administração de políticas de controle de acesso usando esta ferramenta.

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

SUMÁRIO

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

LISTA DE FIGURAS

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

LISTA DE TABELAS

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

1 Introdução

O objetivo do MACA (***M****iddleware* de **A**utenticação e **C**ontrole de **A**cesso) é prover os serviços de autenticação de usuário e controle de acesso para aplicações legadas ou' em desenvolvimento, independente de plataforma e linguagem de programação, através de uma API padronizada.

O MACA implementa um modelo de autorização contextual para o controle de acesso baseado em papéis (CABP) definido pelo NIST. O CABP tem características adequadas para definição e administração viável de políticas de acesso, particularmente em aplicações corporativas emergentes, que demandam um controle com granularidade fina para um grande número de usuários e recursos.

A arquitetura de software do MACA baseia-se em padrões de processamento aberto e distribuído a fim de alcançar interoperabilidade e portabilidade para segurança. Adota o serviço de diretórios LDAP como uma base de informações de gerenciamento de segurança (BIGS); o CORBA *Security Service* (CSS) para autenticação de usuários e o serviço de decisão para acesso a recursos (RAD – *Facility*), do CORBA *horizontal facilities*, como soluções de *middleware* para autenticação de usuários e solicitação de autorizações de acesso, respectivamente, por parte das aplicações clientes. Esta solução viabiliza a administração da política de autorização e o controle de acesso de modo unificado e consistente, a partir de diferentes sistemas, em plataformas e linguagens de programação distintas, mas de forma padronizada.

Três componentes principais integram esta arquitetura: o servidor de autenticação e controle de acesso (MACA CS); o módulo para administração da política de autorização de acesso e gerência de contas de usuários (MACA AD); e aplicações clientes que solicitam autorizações de acesso e autenticação de usuários. Este manual descreve de forma prática como utilizar o MACA AD para configuração de uma política de autorização de acesso. A fim de facilitar seu uso, as subseções seguintes descrevem sucintamente os conceitos básicos de controle de acesso e do CABP, bem como a arquitetura do software do MACA.

1.1 Conceitos Básicos de Controle de Acesso

O controle de acesso vai limitar as ações ou operações que um usuário legítimo de um sistema computacional pode realizar, com base nas autorizações aplicáveis ao mesmo no momento do acesso. Uma autorização estabelece as permissões[1] de acesso que um sujeito[2] pode exercer em um determinado recurso computacional. Procura restringir o uso não autorizado dos recursos computacionais para evitar violações de segurança. A restrição do que pode ou não ser acessado é imposta diretamente às ações do usuário.

[1] Os termos direitos de acesso, privilégios, permissões e autorizações são usados neste texto indistintamente.
[2] Um sujeito pode ser um usuário humano ou algum agente autônomo que atua em benefício deste.

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

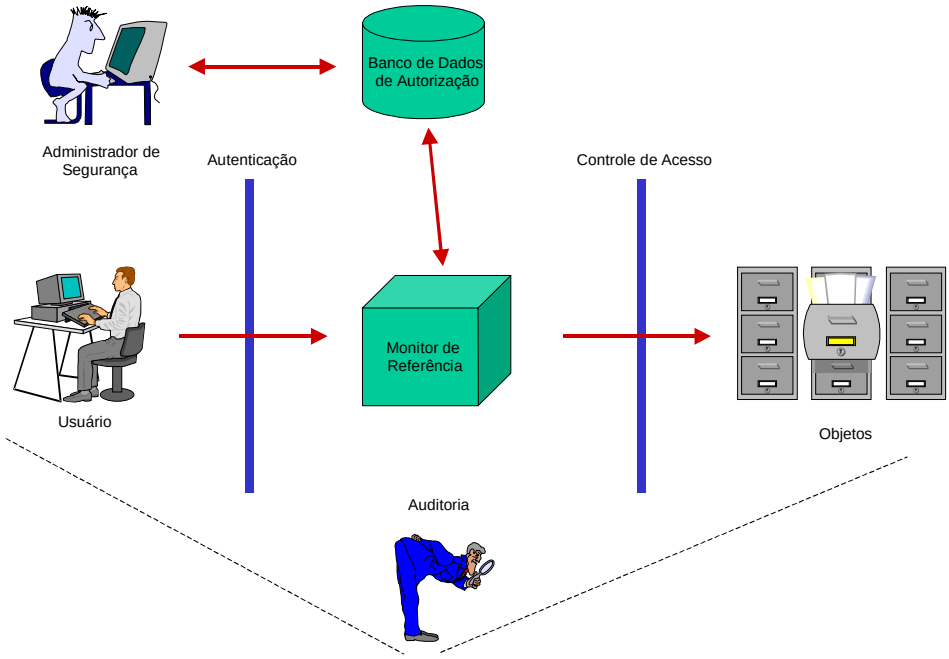


Figura 1 – Esquema do controle de acesso e outros serviços de segurança

Em geral, o controle de acesso exige a autenticação prévia do usuário que deseja usar os objetos protegidos (Figura 1). A autenticação estabelece a identidade do usuário para o sistema de segurança, tipicamente através de um identificação pessoal (nome para *login*) e senha. Quando necessária uma autenticação mais robusta, pode-se adicionalmente empregar cartões de identificação, certificados digitais ou dados biométricos do usuário. O controle de acesso é imposto pelo monitor de referência que intermedeia todas as tentativas do usuário de acessar os objetos protegidos. O monitor de referência consulta uma base de dados de autorização para determinar se um usuário que deseja realizar uma operação tem a permissão ou não realizá-la. A auditoria registra dados sobre a atividade no sistema e os analisa para descobrir violações de segurança e diagnosticar suas causas. O administrador de segurança é o responsável pela configuração e gerência das autorizações, de acordo com política de controle de acesso adotada.

Dentre os modelos de controle de acesso existentes, destacam-se o controle de acesso discricionário (CAD), o controle de acesso compulsório (CAC) e o controle de acesso baseado em papéis (CABP).

1.1.1 Controle de Acesso Discricionário

O CAD controla o acesso a um objeto protegido com base na identidade do usuário (ou grupos de usuários) e nas autorizações que especificam, para cada objeto, através de uma lista de controle de acesso, os privilégios que cada usuário (ou grupo) tem (e. g., ler, escrever, executar, etc.). O proprietário do objeto pode, a seu arbítrio, conceder ou revogar privilégios de acesso para outros usuários

(ou grupos), o que torna este enfoque bastante flexível e amplamente utilizado em sistemas operacionais e SGBDs. Entretanto, por sua natureza assimétrica e descentralizada, o CAD dificulta a administração dos privilégios de acesso que um usuário possui. É preciso examinar a lista de controle de acesso de cada objeto num sistema para determinar os privilégios de acesso de um usuário. Outra dificuldade ocorre quando se pretende remover parcial ou totalmente os privilégios de um usuário. Além de ser necessário visitar todas as listas de controle de acesso, o proprietário do objeto deve conceder o privilégio de modificação da lista para quem administra a política de controle de acesso. Assegurar isto em larga escala numa organização que tem um grande número de usuários e sistemas distribuídos e heterogêneos não é trivial.

1.1.2 Controle de Acesso Compulsório

O CAC confina o fluxo da informação numa única direção numa hierarquia de acesso. Está baseado na classificação de sujeitos e objetos. Por exemplo, um usuário da classe *secreto* pode ler qualquer objeto de uma classe igual ou inferior a sua, mas quando grava informações lidas ou criadas, estas só podem ser de uma classe igual ou superior a dele. Informações sensíveis lidas por uma pessoa da classe *secreto* não podem ser passadas para pessoas de uma classe de acesso menos privilegiada. No CAD, este tipo de controle não pode ser realizado. Já o CAC provê mais segurança para os dados, lidando com requisitos de segurança mais específicos, tais como uma política de controle do fluxo da informação. No entanto, implementar mecanismos que satisfaçam este modelo é uma tarefa difícil. Ademais, por ser excessivamente rígido, projetado para uso em ambientes militares, não possui a flexibilidade para suportar as situações excepcionais necessárias para um adequado controle de acesso às informações em ambientes corporativos.

1.1.3 Controle de Acesso Baseado em Papéis

O CABP permite regular o acesso dos usuários aos recursos protegidos com base nos papéis que eles exercem numa organização. Os papéis denotam funções que descrevem a autoridade e a responsabilidade concedidas a um usuário para o qual um papel foi associado. Neste caso, autorizações não são associadas diretamente a usuários, mas sim a papéis, de acordo com as atribuições pertinentes. Papéis são associados a usuários segundo as funções que eles exercem. Por exemplo, num hospital, se um usuário é um médico e tem o cargo de diretor clínico, ele terá os papéis *Médico* e *Diretor Clínico* associados. Consequentemente, seus direitos de acesso são os definidos para estes papéis, de acordo com a necessidade de saber/fazer inerente a autoridade e responsabilidade de cada papel.

Ademais, o CABP favorece a administração da política de acesso, pois permite coloca-la na perspectiva e um modelo organizacional. Usuários podem facilmente ser remanejados de um papel para outro e novas autorizações podem ser concedidas para papéis, refletindo as necessidades da organização. Como privilégios não são concedidos diretamente para usuários, mas a papéis, a rotatividade de pessoal tem um baixo impacto na administração da política de autorização, que é realizada

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

de forma unificada através de papéis administrativos. Neste caso, os procedimentos para remoção de privilégios ou bloqueio de contas de acesso quando o vínculo de um usuário com a organização se encerra podem ser feitos com facilidade. Isto é particularmente útil em organizações onde o número de usuários com vínculo temporário não é desprezível, como no caso dos hospitais escola.

Como o CABP é viável identificar, a partir de um usuário, todas as suas autorizações e, por outro lado, a partir das autorizações, identificar todos os usuários. A administração da política de acesso pode ser unificada em papéis administrativos, não cabendo necessariamente esta atividade ao proprietário do objeto. Outro aspecto interessante é que o CABP é politicamente neutro, podendo suportar os modelos CAC ou CAD, dentre outros. Assim, o CABP permite uma administração unificada da política de acesso, mas com flexibilidade.

O Padrão para CABP do NIST

O padrão NIST para CABP (Figura 2) possui quatro conjuntos de entidades principais: *U* (usuários), *P* (papéis), *A* (autorizações) e *S* (sessões). Especifica que uma autorização é um relacionamento *n* para *m* entre os recursos protegidos (objetos) e respectivas formas de acesso (operações), mas deixa em aberto a representação de usuários, papéis, objetos e operações, bem como a interpretação de autorizações, cabendo estas tarefas a modelos mais detalhados. Estas entidades possuem os seguintes relacionamentos: usuário-papel *UP*; papel-autorização *PA*; hierarquia de papéis *HP* e sessões. As relações *UP* e *PA* especificam associações *n* para *m* entre usuários e papéis; e entre papéis e autorizações, respectivamente. *HP* define uma relação de ordem parcial entre papéis, dispondo-os em hierarquias a fim de melhor representar as linhas de autoridade e responsabilidade de uma organização. Uma sessão se relaciona com um único usuário por vez, mas permite que ele assuma (ative) múltiplos papéis simultaneamente, desde que estes papéis estejam associados ao usuário na relação *UP*. Por outro lado, um usuário pode ter várias sessões ao mesmo tempo.

Aos relacionamentos do padrão, podem-se estabelecer restrições para minimizar as chances de fraude ou dano acidental pela demasiada concentração de poder numa única pessoa. Uma restrição típica é limitar o número máximo de papéis de um usuário. Outra é a *separação de responsabilidades* (SR), que distribui a responsabilidade para realização de uma ação por múltiplos usuários, de modo que uma pessoa não seja poderosa o suficiente para efetuá-la sem um conluio. A SR é definida através de papéis mutuamente exclusivos, tanto na relação *UP*, quanto na relação *PA*. Em *UP*, dois ou mais papéis mutuamente exclusivos não podem ter usuários em comum associados. Já em *PA*, define-se a separação de responsabilidades proibindo-se a associação de uma mesma autorização a

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

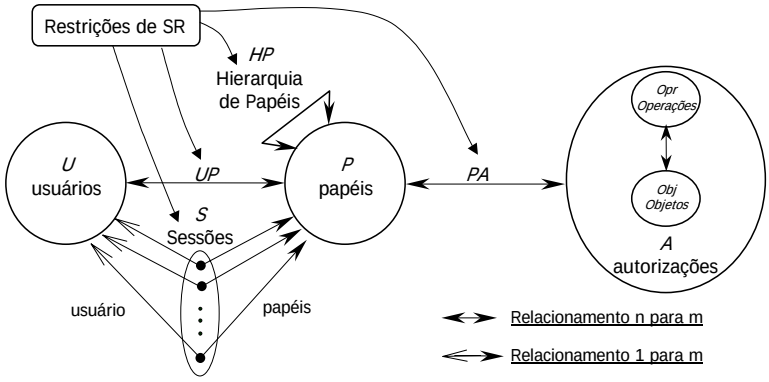


Figura 2 – Padrão NIST de referência para CABP

papéis mutuamente exclusivos. A idéia é adotá-la para reduzir a possibilidade de um usuário assumir papéis onde ocorram conflitos de interesse. Quando a restrição é imposta no momento em que estas relações são estabelecidas, ela é denominada de *separação de responsabilidades estática* (SRE). A *separação de responsabilidades dinâmica* (SRD) ocorre quando potenciais conflitos de interesse são detectados no momento em que um usuário tenta ativar mais de um papel simultaneamente, independente das sessões que abriu. A SRD admite um usuário possuir vários papéis conflitantes, desde que não sejam ativados ao mesmo tempo.

1.2 Arquitetura de Software do MACA

A arquitetura onde os componentes do MACA estão implementados é apresentada na Figura 3. É um modelo cliente-servidor multicamada com os seguintes componentes principais: um servidor LDAP, encarregado de manter a base de gerência de informações de segurança; um servidor de segurança (MACA CS), encarregado de oferecer serviços de autenticação de usuário, de decisão de acesso a recursos, dentre outros; e finalmente as aplicações cliente que requisitam estes serviços de segurança.

Nesta arquitetura, as aplicações cliente são protegidas pela *intranet* da instituição que as mantém. Isto é, a *intranet* limita o acesso apenas para terceiros confiáveis através de conexões seguras (uma rede privada virtual, por exemplo). Entretanto, tanto dos acessos externos, quanto os internos, são regulados pela política de segurança armazenada na BIGS e estabelecida pela instituição mantenedora das aplicações.

1.2.1 Base de Informações de Gerência de Segurança

A BIGS mantém num servidor LDAP configurações de segurança, tais como, autorizações de acesso, papéis, representações dos recursos protegidos e dos usuários, dados para autenticação, relacionamentos usuários-papéis, papéis-autorizações, etc. Todo acesso à BIGS deve ser realizado através do protocolo LDAP sobre TLS (*Transport Layer Security*) para assegurar confidencialidade e integridade na comunicação. Adicionalmente, TLS pode assegurar autenticação mútua entre clientes LDAP e o

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

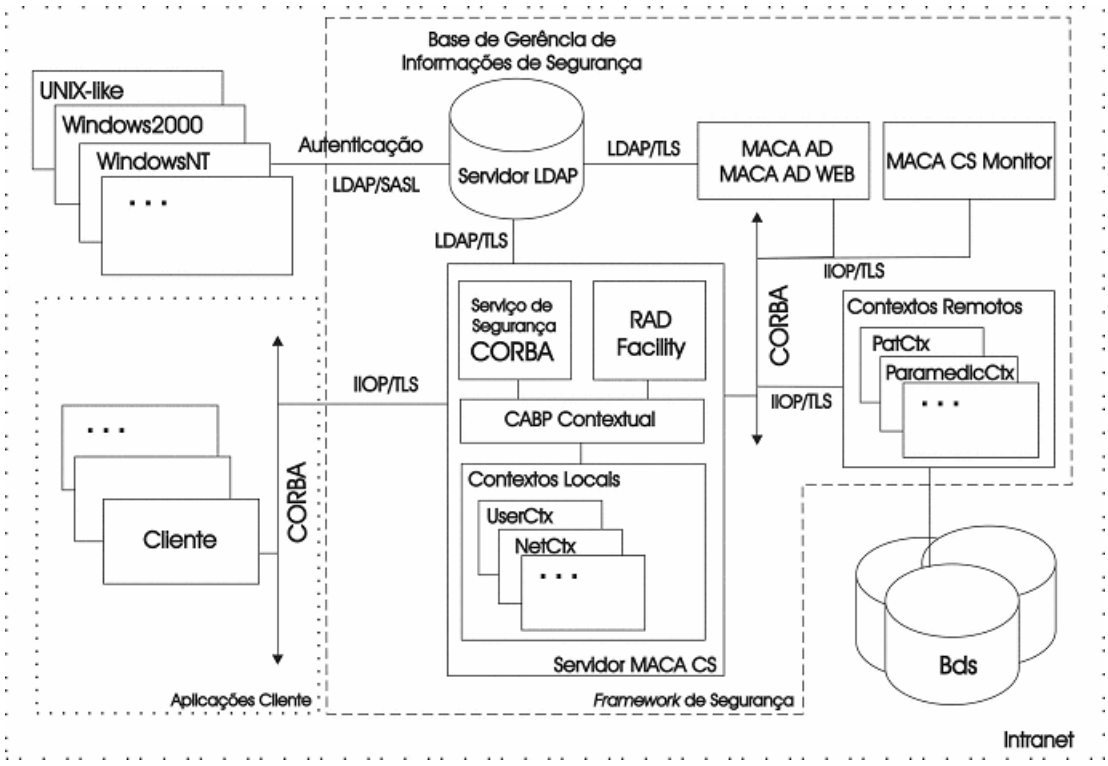


Figura 3 – Arquitetura de Software do MACA

servidor LDAP. Ademais, autenticação via sistemas operacionais e gerenciadores de bancos de dados mais populares podem efetuadas com segurança junto ao servidor LDAP através do protocolo SASL. Esta solução viabiliza a autenticação unificada de usuários numa organização, independente de sistema operacional ou aplicação.

1.2.2 MACA AD e MACA AD WEB

A administração da política de segurança é realizada na BIGS com o MACA AD (Figura 3) e apenas por usuários privilegiados através de interações seguras e com autenticação e controle de acesso adequados. De modo similar, o MACA AD WEB permite a gerência de contas de usuários via *web* com flexibilidade para definição dos atributos armazenados em cada conta no LDAP. O servidor LDAP deve ser protegido fisicamente e todos os acesso não locais devem ser desabilitados. A localização unificada das políticas de segurança facilita a administração, mas introduz uma sobrecarga adicional, visto que todos os clientes LDAP usam um único servidor. Ademais, um servidor central introduz um único ponto de falha e abre oportunidades de ataques para colocá-lo fora de serviço. Como LDAP é um serviço de diretório distribuído e a maioria das implementações disponíveis têm mecanismo de réplica automático, é viável construir um servidor logicamente centralizado e tolerante a falhas, embora fisicamente distribuído e redundante.

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

1.2.3 MACA CS

Cabe ao servidor de segurança (Figura 3) oferecer autenticação, autorização e controle de acesso às aplicações clientes, dentre outros serviços de segurança. O RAD – *Facility* oferece interfaces padronizadas que permitem o controle de acesso detalhado, ao nível da aplicação, mas de uma forma em que a lógica do controle de acesso é separada da lógica da aplicação, com transparência em relação ao modelo de decisão efetivamente implementado. Este *framework* é adequado para suportar o modelo de autorização do MACA, pois prevê o tratamento dos fatores dinâmicos que influenciam a lógica de autorização e possibilita a combinação de diferentes políticas de controle de acesso. O Serviço de Segurança CORBA oferece interface padrão para autenticação de usuários e faz o controle de acesso transparente para as operações definidas nos objetos CORBA. O módulo "CABP Contextual" implementa o modelo de autorização do MACA, sendo utilizado como política de autorização de acesso pelo CSS e pelo RAD – *Facility*. Todas as interações entre objetos CORBA cliente e o servidor de segurança devem ocorrer via IIOP (*Internet Inter-ORB Protocol*) sobre TLS.

1.2.4 Implementação

Os módulos MACA CS e MACA AD foram implementados em Java e o MACA AD WEB foi desenvolvido em Java/JSP. O MACA AD WEB permite a um administrador de contas criar, consultar, atualizar e remover contas usuários. O MACA AD permite a um administrador de autorizações estabelecer políticas de acesso através da definição de papéis, recursos e autorizações. O módulo "CABP Contextual" implementa o serviço de autenticação de usuários com *login* e senha, o gerenciador de sessões de usuários e o serviço de autorização de acesso. Ainda provê um interpretador para regras para autorização contextuais. Tais regras permitem que a política de acesso seja estabelecida com base em variáveis ambientais que denotam informações sobre usuário corrente, data/hora e local do acesso, e outras que podem ser livremente programadas e incorporadas para especificação de políticas de autorização mais complexas. Os contextos locais são implementados em Java e compartilham o mesmo espaço de endereçamento do módulo "CABP Contextual". Contextos remotos são acessados por clientes Java/CORBA via IIOP sobre TLS. Contextos são bibliotecas dinâmicas carregadas em tempo de execução através do mecanismo de extensão de Java.

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

2 Política de Acesso para o Sistema de Gerência de Pedidos

Este capítulo apresenta os requisitos de controle de acesso para um sistema de gerência de pedidos – SGP. No capítulo seguinte, o MACA AD é utilizado para execução da política de acesso apresentada. A seção 2.1 descreve o SGP e a seção 2.2 especifica os requisitos de acesso.

2.1 Cenário do Sistema de Gerência de Pedidos

Este sistema tem por objetivo gerenciar os pedidos de uma empresa que tem vendedores espalhados por todo o país. Pedidos são solicitados diretamente por vendedores credenciados pela empresa utilizando o SGP. Um vendedor poderá modificar ou remover um pedido que antes que este seja faturado para o cliente. Cada pedido é formado por um conjunto de itens que o cliente deseja adquirir. Os itens devem constar no conjunto de produtos que a empresa comercializa. Vendedores sêniores são uma categoria que tem autonomia para conceder descontos e manipular quaisquer pedidos. Pedidos são faturados por faturistas.

2.1.1 Modelo de Objetos

O modelo de objetos com as classes e operações do SGP é ilustrado na Figura 4. Abaixo segue uma descrição sucinta do modelo:

- **Produtos**: representa o conjunto dos produtos comercializados via SGP, com as seguintes operações disponíveis:
  - **Inclusão**: inclui um novo produto;
  - **Consulta**: permite a visualização dos produtos disponíveis;
  - **Exclusão**: remove um produto existente;
  - **Alteração**: modifica o conteúdo de um produto disponível;
- **Clientes**: representa o conjunto dos clientes da empresa, com as seguintes operações disponíveis:
  - **Inclusão**: inclui um novo cliente;
  - **Consulta**: permite a visualização dos clientes disponíveis;
  - **Exclusão**: remove um cliente existente;
  - **Alteração**: modifica o cadastro de um cliente disponível;

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

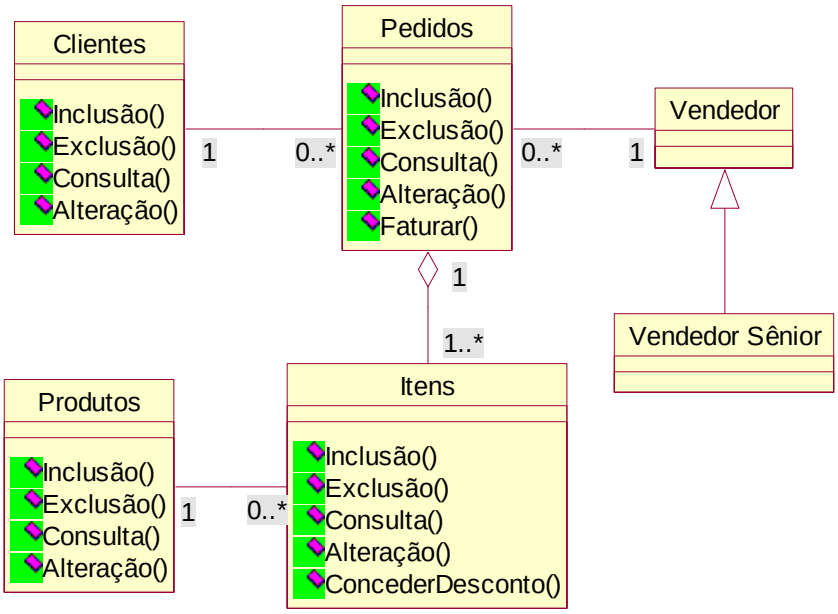


Figura 4 – Diagrama de classes do SGP

- **Pedidos**: representa o conjunto dos pedidos para fornecimento de produtos, com as seguintes operações e dados disponíveis:
  - **Inclusão**: inclui um novo pedido;
  - **Consulta**: permite a visualização dos pedidos disponíveis;
  - **Exclusão**: remove um pedido existente;
  - **Alteração**: modifica o conteúdo de um pedido disponível;
  - **Faturar**: emite fatura correspondente a um pedido selecionado;
  - **Itens**: representa o conjunto de itens de produtos de um pedido;
    - **Inclusão**: inclui um novo item no pedido;
    - **Consulta**: permite a visualização dos itens de um pedido;
    - **Exclusão**: remove um item de um pedido;
    - **Alteração**: modifica o conteúdo de um item num pedido;
    - **ConcederDesconto**: permite a especificação de um percentual de desconto para um item de um pedido;
- **Vendedor**: representa um vendedor que gerencia pedidos;

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- **Vendedor Sênior**: especialização de **Vendedor** que tem privilégios de acesso especiais.

2.2 Requisitos de Controle de Acesso

Todo o acesso ao SGP só poderá ser realizado por usuários autenticados e devidamente autorizados. Têm direito de acessá-lo os seguintes profissionais: vendedores, vendedores seniores, faturistas, gerentes de produto. Os privilégios de acesso no SGP para cada um destes profissionais são detalhados[3] a seguir:

- **Vendedor**: pode consultar os cadastros de produtos e clientes, mas está proibido de realizar qualquer modificação neles. Está autorizado a criar novos pedidos e a consultá-los, mas só pode remover ou alterar os pedidos criados sob sua responsabilidade. Um vendedor não pode conceder descontos superiores a 10% ou emitir faturas;

- **Vendedor Sênior**: pode consultar o cadastro de produtos, mas está proibido de realizar qualquer modificação nele. Pode consultar e alterar o cadastro de clientes, mas não pode incluir ou remover clientes. Está autorizado a criar novos pedidos, podendo consultar, remover ou alterar pedidos independente de quem os criou. Vendedores seniores não podem conceder descontos superiores a 40% ou emitir faturas;

- **Faturista**: está autorizado a consultar e faturar pedidos. Adicionalmente poderá consultar os cadastros de produtos e clientes. Pedidos somente podem ser faturados nos dias de semana, no horário de expediente: das 8 às 18 horas;

- **Gerente de Produto**: tem controle total sobre os cadastros de produtos e clientes e poderá consultar o cadastro de pedidos.

Para reduzir a possibilidade de fraude, um mesmo usuário que atue como gerente de produto não poderá atuar como vendedor e vice-versa. Adicionalmente, os usuários do GSP têm o direito de alterar a própria senha.

[3] Omissões são tratadas como negação de acesso para o recurso.

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

3 Usando o MACA AD e MACA AD Web para Execução da Política de Acesso do Sistema de Gerência de Pedidos

Este capítulo mostra como usar o MACA AD para executar a política de acesso especificada para o SGP. O processo adotado para implementá-la baseou-se nas seguintes etapas:

1. Definição dos recursos a serem protegidos: nesta fase, uma representação abstrata dos recursos do SGP é definida e armazenada no servidor LDAP. A equipe responsável pela política de acesso deverá, em conjunto com a equipe que desenvolveu a aplicação, definir os nomes dos recursos e respectivos privilégios de acesso. Os nomes dos recursos e privilégios são utilizados pela aplicação na solicitação de autorizações de acesso ao servidor MACA CS (ver Figura 3);
2. Definição dos papéis desempenhados na instituição: análise das funções organizacionais exercidas pelos usuários para definição dos respectivos papéis. As linhas de autoridade e responsabilidade de cada papel definirão sua disposição hierárquica;
3. Configuração das autorizações de acesso: atribuição das autorizações para cada papel de acordo com a política de acesso especificada para cada recurso protegido;
4. Cadastramento das contas usuários: identificação e cadastramento no servidor LDAP das contas de usuários, atribuição dos respectivos papéis de acordo com suas funções e responsabilidades e configuração da política de senhas;
5. Testes e validação: fase em que se busca encontrar falhas na implementação da política de acesso, tanto do ponto de vista lógico, quanto operacional. A aplicação protegida só será liberada após a validação do funcionamento da política de acesso especificada.

Antes de prosseguir com a implementação da política de acesso do SGP, é importante conhecer os papéis administrativos MACA AD vistos na seção 3.1

3.1 Papéis Administrativos do MACA AD

Papéis administrativos são papéis privilegiados que habilitam usuários a utilizarem o MACA AD e MACA AD Web para administração da política de autorização. Dois papéis estão disponíveis:

- **Administrador de Contas**: um usuário com este papel pode criar, consultar, modificar ou excluir contas de usuários. Ainda pode atribuir ou remover papéis e gerenciar senhas. Entretanto, não pode alterar o próprio papel ou o seu login;

- **Administrador de Autorizações**: um usuário com este papel pode criar, consultar, modificar ou excluir recursos e autorizações. Entretanto, tem permissão apenas de consulta em contas de usuários, ficando proibido de modificá-las.

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

3.2 Definindo os Recursos do SGP

No MACA, a definição de nomes de recursos é hierarquizada numa estrutura em árvore. De comum acordo com os desenvolvedores do SGP, chegou-se ao seguinte resultado para os nomes dos recursos:

- **SGP** Tipo: aplicação - Formas de acesso: execução
  - **Clientes** Tipo: tabela - Formas de acesso: consulta, inclusão, alteração, exclusão
  - **Produtos** Tipo: tabela - Formas de acesso: consulta, inclusão, alteração, exclusão
  - **Pedidos** Tipo: tabela - Formas de acesso: consulta, inclusão, alteração, exclusão
    - **Itens** Tipo: tabela - Formas de acesso: consulta, inclusão, alteração, exclusão
      - **ConcederDesconto** Tipo: método - Formas de acesso: execução
    - **Faturar** Tipo: método - Formas de acesso: execução

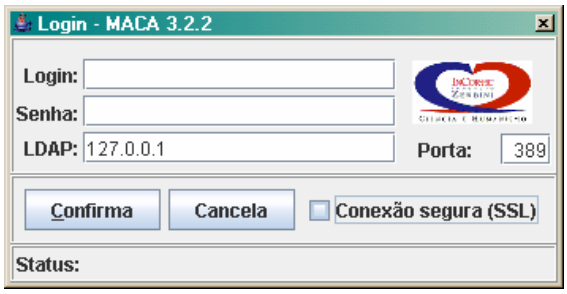
Cada recurso tem um tipo associado com respectivas formas de acesso. Por exemplo, o recurso "SGP" é do tipo aplicação e sua única forma de acesso é "execução". Já "Pedidos" é do tipo tabela, sendo composto por "Itens" e "Faturar". "Faturar" representa uma ação que pode ser executada sobre um pedido, sendo portando do tipo método, com forma de acesso "execução".

3.2.1 Cadastrando os Recursos do SGP com o MACA AD

Uma vez estabelecidos os nomes, tipos e formas de acesso dos recursos do SGP, pode-se utilizar o MACA AD para cadastrá-los. Entretanto, certifique-se que você possui o papel "Administrador de Autorizações" associado e efetue os seguintes passos:

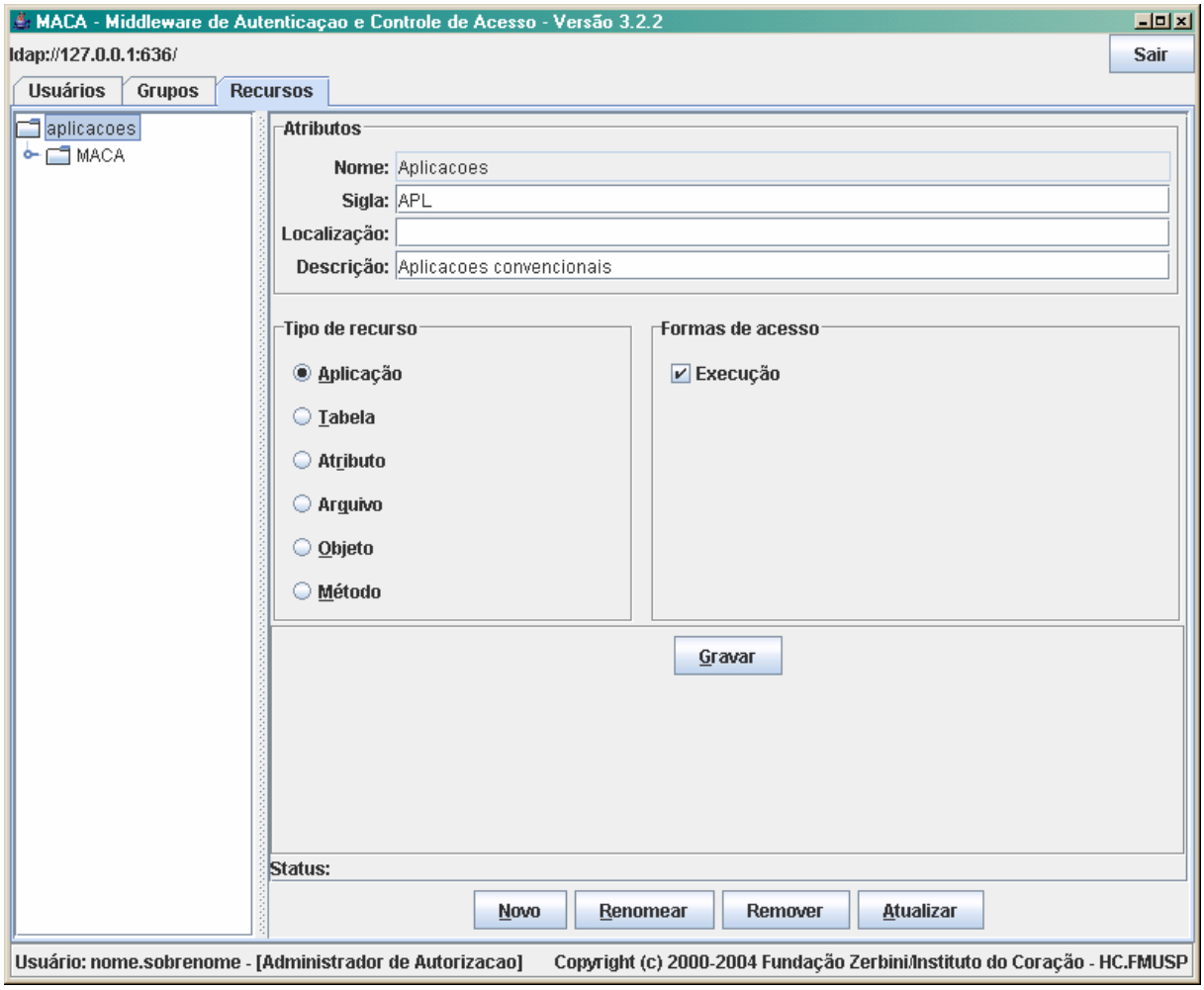
1. Faça um clique duplo no ícone do MACA AD 

para executá-lo;
2. Quando sua janela abaixo aparecer, entre com o seu nome de *login*, a senha, seleciono o papel "Administrador de Autorização" e pressione o botão "Confirma". Antes, verifique se o nome do servidor LDAP está correto e se ele está configurado para aceitar conexões seguras via SSL. Em caso afirmativo, marque a opção "Conexão segura (SSL)" para que toda comunicação entre o MACA AD e o servidor LDAP seja garantida quanto a sua confidencialidade e integridade.

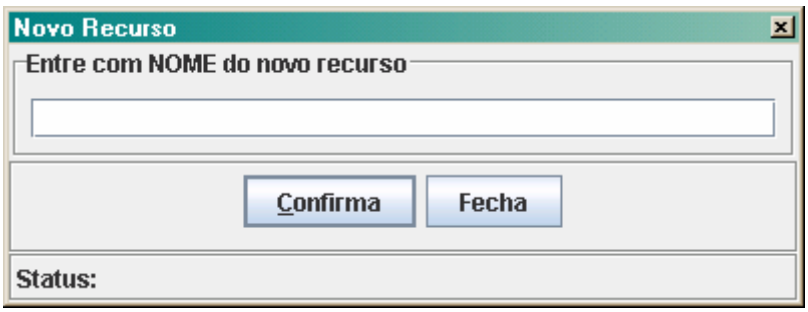


www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

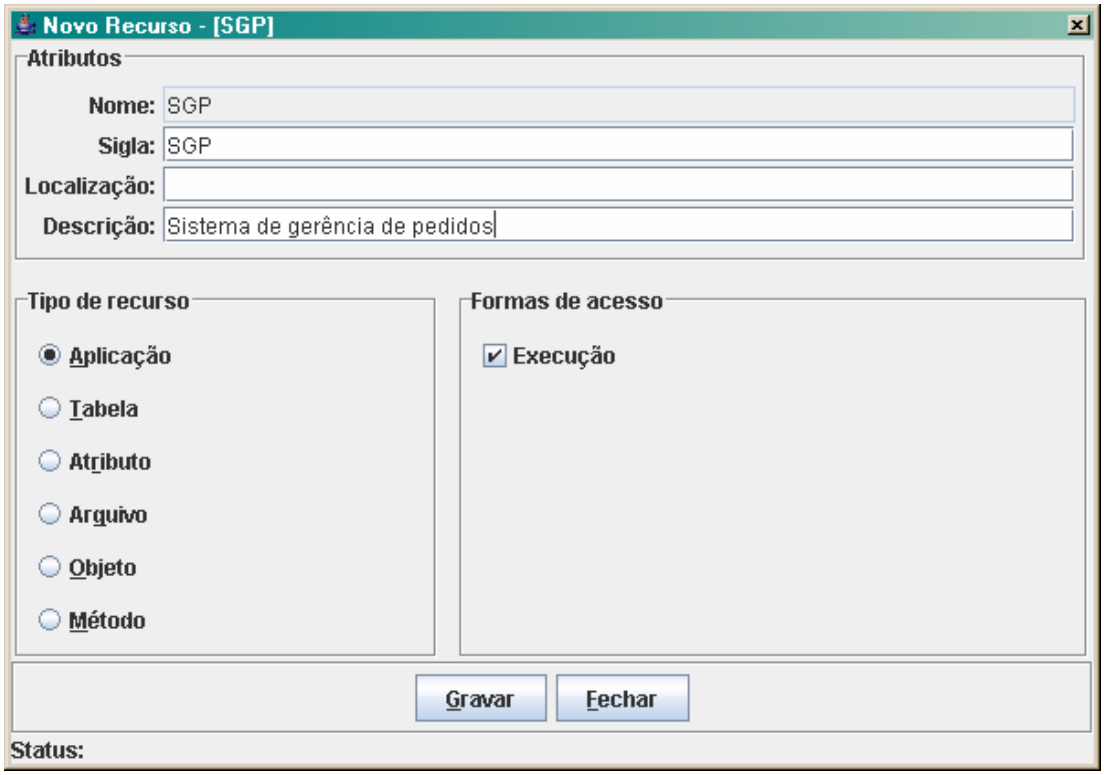
3. Na janela principal do MACA AD (abaixo), selecione a pasta intitulada “Recursos” e selecione o recurso “Aplicacoes” no painel do lado esquerdo;



4. Pressione o botão “Novo” para criar um recurso abaixo de “Aplicacoes”, entre com o nome **SGP**, conforme ilustrado na janela abaixo e pressione o botão “Confirma”;



5. Complemente as informações de acordo com a janela de cadastro abaixo, pressione o botão “Gravar” e em seguida o botão “Fechar”;



6. Agora, selecione no painel esquerdo o recurso “SGP”, pressione o botão “Novo” para criar um recurso abaixo de “SGP”, entre com o nome **Clientes** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
   - No campo “Descrição”, entre com o valor **Tabela de Clientes**;
   - No quadro “Tipo de Recurso”, selecione o item “Tabela”;
   - No quadro “Formas de Acesso”, marque as quatro opções disponíveis;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
7. Faça um clique duplo no recurso “SGP” e veja que o recurso “Clientes” foi criado;
8. Agora, selecione novamente o recurso “SGP”, pressione o botão “Novo”, entre com o nome **Produtos** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
   - No campo “Descrição”, entre com o valor **Tabela de Produtos**;
   - No quadro “Tipo de Recurso”, selecione o item “Tabela”;
   - No quadro “Formas de Acesso”, marque as quatro opções disponíveis;

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- Pressione o botão “Gravar” e em seguida o botão “Fechar”;

9. Selecione novamente o recurso “SGP”, pressione o botão “Novo”, entre com o nome **Pedidos** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
   - No campo “Descrição”, entre com o valor **Tabela de Produtos**;
   - No quadro “Tipo de Recurso”, selecione o item “Tabela”;
   - No quadro “Formas de Acesso”, marque as quatro opções disponíveis;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
10. Faça um clique duplo no recurso “SGP” e selecione o recurso “Pedidos” para que se possa criar o recurso “Itens” abaixo dele. Para isto, pressione o botão “Novo”, entre com o nome **Itens** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
    - No campo “Descrição”, entre com o valor **Tabela de itens de produtos**;
    - No quadro “Tipo de Recurso”, selecione o item “Tabela”;
    - No quadro “Formas de Acesso”, marque as quatro opções disponíveis;
    - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
11. Selecione o recurso “Pedidos”, pressione o botão “Novo”, entre com o nome **Faturar** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
    - No campo “Descrição”, entre com o valor **Emite fatura correspondente a um pedido**;
    - No quadro “Tipo de Recurso”, selecione o item “Método”;
    - No quadro “Formas de Acesso”, marque a opção “Execução”;
    - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
12. Faça um clique duplo no recurso “Pedidos” e selecione o recurso “Itens” para que se possa criar o recurso “ConcederDesconto” abaixo dele. Para isto, pressione o botão “Novo”, entre com o nome **ConcederDesconto** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
    - No campo “Descrição”, entre com o valor **Operação que concede um desconto percentual para um item de pedido**;

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- No quadro “Tipo de Recurso”, selecione o item “Método”;
- No quadro “Formas de Acesso”, marque a opção “Execução”;
- Pressione o botão “Gravar” e em seguida o botão “Fechar”;

Considerando ainda que o usuário vai poder alterar a senha através do SGP, é preciso também configurar este recurso, conforme instruções abaixo:

1. Selecione o recurso “SGP”, pressione o botão “Novo”, entre com o nome **Usuários** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
   - No campo “Descrição”, entre com o valor **Usuários do SGP**;
   - No quadro “Tipo de Recurso”, selecione o item “Tabela”;
   - No quadro “Formas de Acesso”, marque as quatro opções disponíveis;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
2. Faça um clique duplo no recurso “SGP” e selecione o recurso “Usuários” para que se possa criar o recurso “AlterarSenha” abaixo dele. Para isto, pressione o botão “Novo”, entre com o nome **AlterarSenha** e pressione o botão “Confirma”. Na janela do novo cadastro, faça o seguinte:
   - No campo “Descrição”, entre com o valor **Operação que permite a alteração de senha pelo usuário**;
   - No quadro “Tipo de Recurso”, selecione o item “Método”;
   - No quadro “Formas de Acesso”, marque a opção “Execução”;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;

Observações: não se pode renomear ou remover um recurso com recursos filho ou com autorizações associadas.

Agora, com os recursos definidos, vamos proceder a definição dos papéis para cadastramento no MACA.

3.3 Definindo Papéis com o MACA AD

O MACA estrutura como árvore invertida a hierarquia de papéis, de modo que, papéis mais específicos herdam as autorizações dos papéis mais gerais. Analisando o cenário de funcionamento do SGP definido no capítulo 1, chegou-se ao seguinte resultado para hierarquia de papéis:

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

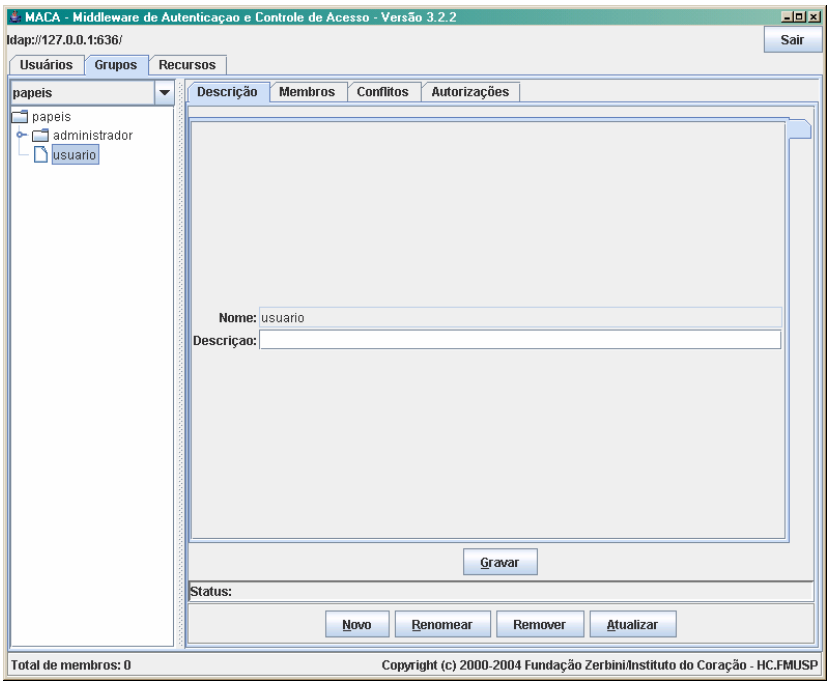
Usuário Descrição: usuário padrão que atue na empresa do SGP.

- **Faturista** — Descrição: responsável pela emissão de faturas e funções correlatas.
- **Gerente** — Descrição: gerente padrão da empresa.
  - **Gerente de Produto** — Descrição: responsável pela administração de produtos da empresa, incluindo sua criação, manutentenção, definição de preços e desativação.
- **Vendedor** — Descrição: responsável pela venda de produtos comercializados pela empresa. Tem controle total sobre os pedidos que cria, porém tem limitações para conceder descontos e não pode modificar o cadastro de clientes.
  - **Vendedor Sênior** — Descrição: tem os mesmos privilégios de vendedor, mas com duas exceções: 1) Tem controle total sobre o cadastro de pedidos, independente de quem foi o criador; 2) Pode realizar alterações no cadastro de clientes.

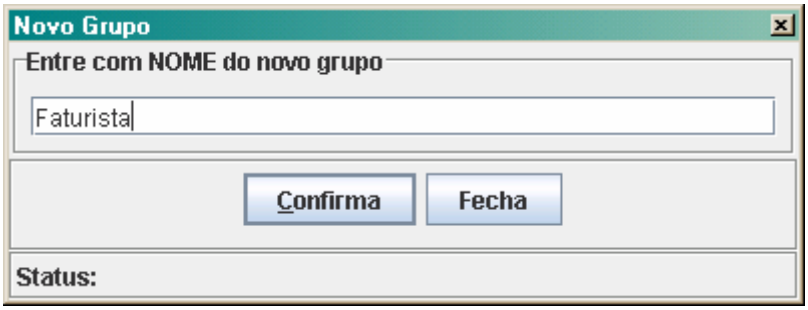
Note que esta é uma possível configuração. Outras poderiam ser definidas baseadas nos requisitos de outras aplicações e de outros setores da empresa, ou em funções dos cargos formais já existentes.

Uma vez definidos os papéis e sua hierarquia, pode-se utilizar o MACA AD para cadastrá-los efetuando os seguintes passos:

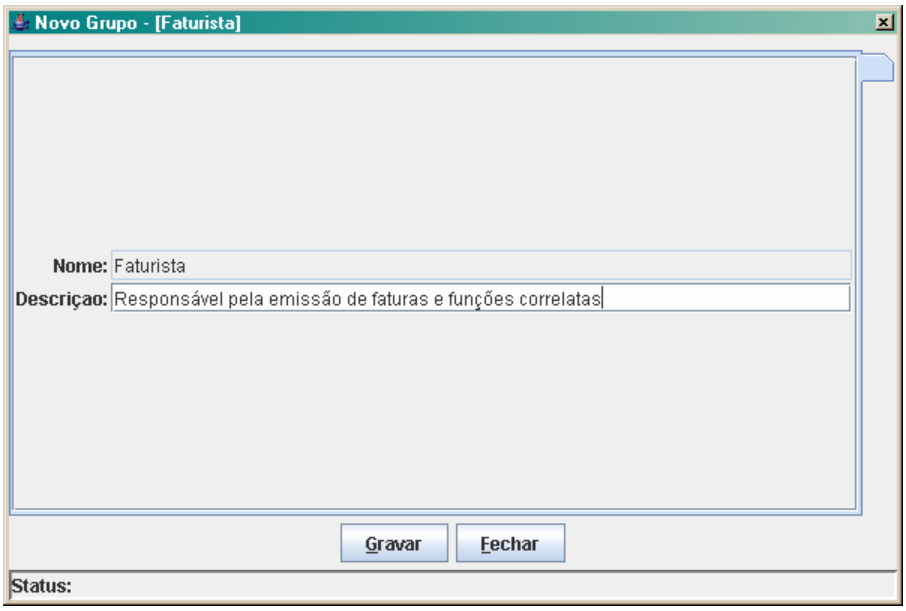
1. Na janela principal do MACA AD (abaixo), selecione a pasta intitulada “Grupos”, selecione grupo “Papeis” e no painel do lado esquerdo, selecione o papel “Usuário”;



2. Para criar um novo papel, abaixo de “Usuario”, seleciona a pasta “Descrição” no painel do lado direito e pressione o botão “Novo”. Entre com nome do novo papel – **Faturista** – tal como indicado na janela abaixo e pressione o botão “Confirma”;



3. Complemente as informações de acordo com a janela de cadastro a seguir, pressione o botão “Gravar” e em seguida o botão “Fechar”;



4. Ainda com o papel “Usuario” selecionado, pressione o botão “Novo”. Entre com o nome **Gerente** e pressione o botão “Confirma”;

5. Na janela do cadastro de novo grupo, preencha o campo “Descrição” com o valor **Gerente padrão da empresa**, pressione o botão “Gravar” e em seguida feche a janela;

6. Novamente, com o papel “Usuario” selecionado, pressione o botão “Novo”. Entre com o nome **Vendedor** e pressione o botão “Confirma”;

7. Na janela do cadastro de novo grupo, preencha o campo “Descrição” com o valor **Responsável pela venda de produtos comercializados pela empresa**, pressione o botão “Gravar” e em seguida feche a janela;

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

8. Faça um clique duplo sobre o papel “Usuario” e selecione o papel “Gerente”. Em seguida, pressione o botão “Novo”, entre com o nome **Gerente de Produto** e pressione o botão “Confirma”;
9. Na janela do cadastro de novo grupo, preencha o campo “Descrição” com o valor **Responsável pela administração de produtos da empresa**, pressione o botão “Gravar” e em seguida feche a janela;
10. Agora, selecione o papel “Vendedor”. Pressione o botão “Novo”, entre com o nome **Vendedor Sênior** e pressione o botão “Confirma”;
11. Na janela do cadastro de novo grupo, preencha o campo “Descrição” com o valor **Vendedor privilegiado**, pressione o botão “Gravar” e em seguida feche a janela;

Observações: não é recomendável definir dois papéis com o mesmo nome; não se pode renomear ou remover um papel com papéis filho, com usuários ou com autorizações associadas.

Com os papéis configurados, pode-se proceder à definição das autorizações de acesso para cada um deles.

3.4 Configurando Autorizações de Acesso para o SGP

A configuração das autorizações de acesso para o SGP deverá satisfazer os requisitos estabelecidos na subseção 2.2. Para cada papel existente, vai-se definir as autorizações necessárias, tomando-se o cuidado de herdar dos papéis mais gerais as autorizações comuns.

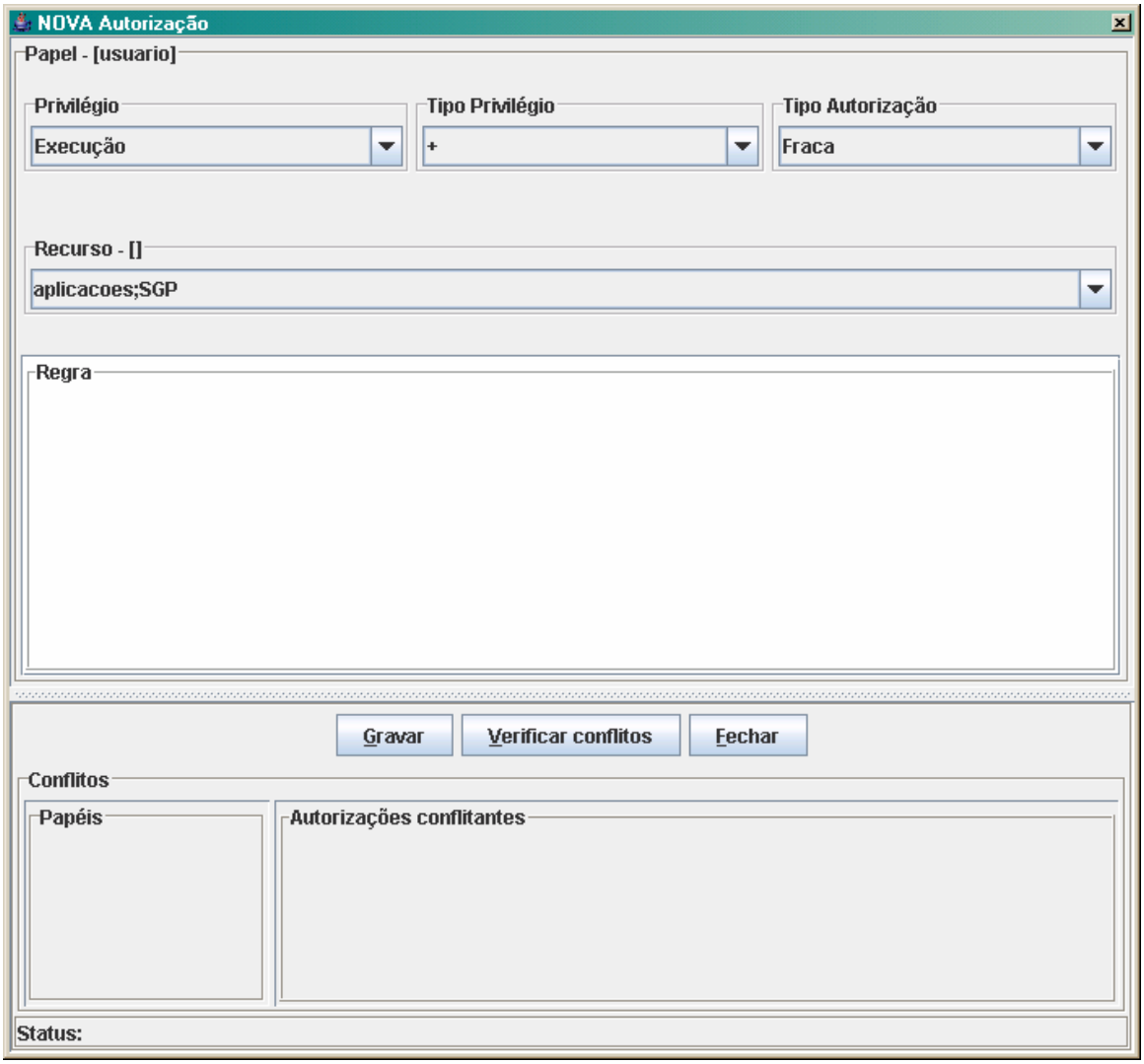
3.4.1 Autorizações do Papel “Usuario”

A política de acesso para o SGP afirma que todos os usuário podem alterar sua senha. Vê-se também que, em todos os papéis, o acesso ao SGP deve ser permitido. Logo, a autorização de acesso para o SGP deve ficar no papel “Usuario” para que possa ser compartilhada pelos seus papéis descendentes. Para configurar estas duas autorizações, faça o seguinte:

12. Na janela principal do MACA AD, selecione pasta intitulada “Grupos”, selecione grupo “Papeis” e no painel do lado esquerdo, selecione o papel “Usuário”;
13. No painel do lado direito, selecione a pasta “Autorizações”. No *comboBox* “Filtros”, utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP** e pressione a tecla ↵ “Enter”;
14. No canto inferior direito da janela, marque a opção “Filtro Ativado”;
15. Pressione o botão “Novo” para criar uma nova autorização. Na janela “NOVA Autorização” ilustrada a seguir, faça o seguinte:

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- No *comboBox* "Recurso", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP** e pressione a tecla ↵ "Enter";
- No *comboBox* "Privilégio", selecione o item **Execução**;
- No *comboBox* "Tipo Privilégio", selecione o item **+**, para indicar que a autorização concede o acesso;
- Pressione o botão "Gravar" e em seguida o botão "Fechar";



16. Note que a autorização recém criada foi incluída no painel do lado direito. Selecione a linha correspondente a ela e pressione o botão "Novo" para criar a autorização que permitirá a um usuário alterar a senha. Na janela "NOVA Autorização", faça o seguinte:

- No *comboBox* "Recurso", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Usuários;AlterarSenha** e pressione a tecla ↵ "Enter";

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- No *comboBox* "Privilégio", selecione o item **Execução**;
- No *comboBox* "Tipo Privilégio", selecione o item **+**;
- Pressione o botão "Gravar" e em seguida o botão "Fechar";

A partir dos requisitos de controle de acesso do SGP, pode-se concluir que todos os papéis têm direito de consultar pedidos, produtos e clientes. Logo, estas autorizações também são definidas para o papel "Usuario". Para configurar estas autorizações, faça o seguinte:

17. Com o papel "Usuario" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP" e pressione o botão "Novo" para criar a autorização que permitirá a um usuário consultar a tabela de clientes. Na janela "NOVA Autorização", faça o seguinte:
    - No *comboBox* "Recurso", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Clientes** e pressione a tecla ↵ "Enter";
    - No *comboBox* "Privilégio", selecione o item **Consulta**;
    - No *comboBox* "Tipo Privilégio", selecione o item **+**;
    - Pressione o botão "Gravar" e em seguida o botão "Fechar";
18. Com o papel "Usuario" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP" e pressione o botão "Novo" para criar a autorização que permitirá a um usuário consultar a tabela de produtos. Na janela "NOVA Autorização", faça o seguinte:
    - No *comboBox* "Recurso", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Produtos** e pressione a tecla ↵ "Enter";
    - No *comboBox* "Privilégio", selecione o item **Consulta**;
    - No *comboBox* "Tipo Privilégio", selecione o item **+**;
    - Pressione o botão "Gravar" e em seguida o botão "Fechar";
19. Com o papel "Usuario" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP" e pressione o botão "Novo" para criar a autorização que permitirá a um usuário consultar a tabela de pedidos. Na janela "NOVA Autorização", faça o seguinte:
    - No *comboBox* "Recurso", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Pedidos** e pressione a tecla ↵ "Enter";
    - No *comboBox* "Privilégio", selecione o item **Consulta**;
    - No *comboBox* "Tipo Privilégio", selecione o item **+**;
    - Pressione o botão "Gravar" e em seguida o botão "Fechar";

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- Na tabela de autorizações criadas para o papel “Usuário”, clique nos cabeçalhos das colunas para ordenar. Por exemplo, um clique sobre o cabeçalho “Recurso” irá classificar a tabela pelo nome do recurso em ordem **ascendente**. Um clique com a tecla *shift* pressionada irá classificar a tabela pelo nome do recurso em ordem **descendente**.

Agora, qualquer conta com o papel “Usuario” atribuído tem acesso ao SGP, podendo alterar a própria senha. Também tem permissão para consultar os cadastros de clientes, produtos e pedidos. Agora, as autorizações para o papel “Faturista” serão definidas.

3.4.2 Autorizações do Papel “Faturista”

Considerando as autorizações herdadas de “Usuario” pelo papel “Faturista”, basta adicionar a autorização que lhe concede o direito de emitir faturas para satisfazer os requisitos definidos pela política de acesso do SGP. Para configurar esta autorização, faça o seguinte:

20. Com o papel “Faturista” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos” e pressione o botão “Novo” para criar a autorização que permitirá a emissão de faturas. Na janela “NOVA Autorização”, faça o seguinte:

    - No *comboBox* “Recurso”, utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Pedidos;Faturar** e pressione a tecla ↵ “Enter”;
    - No *comboBox* “Privilégio”, selecione o item **Execução**;
    - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
    - Pressione o botão “Gravar” e em seguida o botão “Fechar”;

Agora, usuários com o papel “Faturista” poderão faturar pedidos. Porém, de acordo com os requisitos da seção 2.2, *pedidos somente podem ser faturados nos dias de semana, no horário de expediente: das 8 às 18 horas*. Neste caso, deve-se utilizar uma regra especificando as condições em que o pedido pode ser faturado. Para tanto, é preciso alterar a autorização recém criada, conforme indicado a seguir:

1. Com o papel “Faturista” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos;Faturar” e pressione o botão “Alterar” para criar a autorização que permitirá a emissão de faturas. Na janela “NOVA Autorização”, faça o seguinte:

    - No *comboBox* “Recurso”, utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Pedidos;Faturar** e pressione a tecla ↵ “Enter”;
    - No *comboBox* “Tipo Privilégio”, selecione o item **Regra** e no editor na parte de baixo da janela entre com regra de autorização:

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

Variáveis do contexto `dtCtx`	Tipo	Descrição
dtCtx.ano	Inteiro	Retorna um inteiro correspondente ao ano corrente.
dtCtx.mes	Inteiro	Retorna um inteiro correspondente ao mês corrente.
dtCtx.dia	Inteiro	Retorna um inteiro correspondente ao dia corrente.
dtCtx.hora	Inteiro	Retorna um inteiro correspondente ao hora corrente, numa faixa de 0 até 23.
dtCtx.minuto	Inteiro	Retorna um inteiro correspondente ao minuto corrente.
dtCtx.segundo	Inteiro	Retorna um inteiro correspondente ao segundo corrente.
dtCtx.dia_semana	String	Retorna um string com valor correspondente dia corrente. Os valores possíveis são: “dom”, “seg”, “ter”, “qua”, “qui”, “sex” e “sab”.
dtCtx.fim_de_semana	Conjunto	Retorna um valor do tipo conjunto com os seguintes elementos: “dom” e “sab”.
dtCtx.dia_de_semana	Conjunto	Retorna um valor do tipo conjunto com os seguintes elementos: “seg”, “ter”, “qua”, “qui” e “sex”.

Tabela 1 – Sumário das variáveis do contexto de datas e horário – `dtCtx`

```
exp-abs(umPedido, umCliente, umVendedor) {
  dtCtx.dia_semana in dtCtx.dia_de_semana &
// Testa se o dia de hoje é um dia de semana e
  (dtCtx.hora >= 8 & dtCtx.hora <= 18)
// se hora atual está no intervalo das 8 às 18 horas.
}
```

- Pressione o botão “Gravar” e em seguida o botão “Fechar”;

O que acabou-se de configurar foi uma autorização contextual. Uma autorização contextual será positiva, concedendo o acesso, ou negativa, proibindo o acesso, com base na avaliação de uma expressão lógica, denominada de *regra de autorização*, no momento da solicitação de acesso. Essa expressão é definida em termos de variáveis ambientais (contextos) que, quando avaliadas, resultam em informações sobre o usuário corrente, data/hora do acesso, informações de rede (local do acesso) e outras que podem ser livremente programadas e incorporadas para especificação de políticas de acesso mais complexas. A regra de autorização anteriormente definida utiliza o contexto de data e horário denominado `dtCtx`, que disponibiliza as variáveis contextuais relacionadas na Tabela 1.

Regras relacionam as informações ambientais dos contextos em expressões lógicas que especificam uma política de acesso para um recurso protegido. São definidas numa linguagem de expressões lógicas capaz de acessar as operações implementadas nos contextos e relacioná-las através de operadores aritméticos (+, –, *, /, % - módulo), de conjunto (`in` - pertinência), relacionais (>, <, >=,

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

<=, =, !=) e booleanos (&, |, !). Permite ainda a chamada de funções implementadas nos contextos e a definição de regras parametrizadas, de modo que aplicações que solicitam autorizações de acesso possam passar argumentos para regras. A regra que foi definida é um exemplo de regra parametrizada, pois três argumentos são passados como parâmetro: `umPedido`, valor inteiro denotando o código de identificação do pedido para o qual se pretende emitir uma fatura; `umCliente`, valor inteiro que denota o código de identificação do cliente que fez o pedido que será faturado; `umVendendor` é um string que denota o nome de *login* do vendedor que criou o pedido.

Note que a definição dos parâmetros de uma regra é dependente do recurso a ser protegido e deve ser realizada pelos desenvolvedores da aplicação em conjunto com os responsáveis pela definição da política de autorização. Deve haver um consenso quanto à quantidade, significado, tipo e ordem dos parâmetros. Particularmente, na regra acima, os parâmetros não estão sendo utilizados, mas como foram definidos, têm de constar no cabeçalho da regra.

3.4.3 Autorizações do Papel "Gerente de Produto"

Segundo os requisitos de controle de acesso do SGP, os gerentes de produto têm controle total sobre os cadastros de produtos e clientes e poderá consultar o cadastro de pedidos. Herda indiretamente do papel "Usuario" as autorizações para consulta destes cadastros. Portanto, basta acrescentar as autorizações para inclusão, exclusão e alteração dos cadastros de clientes e produtos, conforme instruções a seguir:

1. Na janela principal do MACA AD, selecione pasta intitulada "Grupos", selecione grupo "Papeis" e no painel do lado esquerdo, faça um clique duplo no papel "Usuário", depois faça um clique duplo no papel "Gerente" e selecione o papel **Gerente de Produto**;
2. No painel do lado direito, selecione a pasta "Autorizações". No *comboBox* "Filtros", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP** e pressione a tecla ↵ "Enter";
3. No canto inferior direito da janela, marque a opção "Filtro Ativado";
4. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Clientes" e pressione o botão "Novo" para criar a autorização que permitirá a inclusão de clientes. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Inclusão**;
   - No *comboBox* "Tipo Privilégio", selecione o item **+**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

5. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Clientes" e pressione o botão "Novo" para criar a autorização que permitirá a exclusão de clientes. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Exclusão**;
   - No *comboBox* "Tipo Privilégio", selecione o item **+**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";
6. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Clientes" e pressione o botão "Novo" para criar a autorização que permitirá a alteração de clientes. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Alteração**;
   - No *comboBox* "Tipo Privilégio", selecione o item **+**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";
7. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Produtos" e pressione o botão "Novo" para criar a autorização que permitirá a inclusão de produtos. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Inclusão**;
   - No *comboBox* "Tipo Privilégio", selecione o item **+**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";
8. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Produtos" e pressione o botão "Novo" para criar a autorização que permitirá a exclusão de produtos. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Exclusão**;
   - No *comboBox* "Tipo Privilégio", selecione o item **+**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";
9. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Produtos" e pressione o botão "Novo" para criar a autorização que permitirá a alteração de Produtos. Na janela "NOVA Autorização", faça o seguinte:

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- No *comboBox* "Privilégio", selecione o item **Alteração**;
- No *comboBox* "Tipo Privilégio", selecione o item **+**;
- Pressione o botão "Gravar" e em seguida o botão "Fechar";

Agora, serão definidas as autorizações do papel "Vendedor".

3.4.4 Autorizações do Papel "Vendedor"

A autorizações de consulta para vendedores já foram definidas para o papel "Usuário", sendo portanto herdadas. Portanto, aqui serão definidas as autorizações para incluir, alterar e excluir pedidos. Para isto, siga as seguintes instruções:

1. Na janela principal do MACA AD, selecione pasta intitulada "Grupos", selecione grupo "Papeis" e no painel do lado esquerdo, faça um clique duplo no papel "Usuário" e depois selecione o papel **Vendedor**;
2. No painel do lado direito, selecione a pasta "Autorizações". No *comboBox* "Filtros", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP** e pressione a tecla ↵ "Enter";
3. No canto inferior direito da janela, marque a opção "Filtro Ativado";
4. Com o papel "Vendedor" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Pedidos" e pressione o botão "Novo" para criar a autorização que permitirá a inclusão de pedidos. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Inclusão**;
   - No *comboBox* "Tipo Privilégio", selecione o item **+**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";
5. Com o papel "Vendedor" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Pedidos" e pressione o botão "Novo" para criar a autorização que permitirá a exclusão de pedidos, desde que criados pelo próprio usuário. Neste caso, utiliza-se uma autorização contextual parametrizada. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Exclusão**;
   - No *comboBox* "Tipo Privilégio", selecione o item **Regra** e no editor na parte de baixo da janela entre com regra de autorização:

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

Variáveis do contexto `userCtx`	Tipo	Descrição
userCtx.login	String	Retorna um string com o nome do usuário corrente.
userCtx.matricula	String	Retorna um string com a matrícula do usuário corrente.
userCtx.area_meio	String	Retorna um string com o campo "area meio" do usuário corrente.
userCtx.papeis_associados	Conjunto	Retorna um valor do tipo conjunto, cujos elementos, do tipo string, representam os papéis associados ao usuário corrente.
UserCtx.<nome do atributo no servidor LDAP>	String	Retorna um string com o valor correspondente ao atributo na conta do usuário corrente no LDAP. Caso seja usando com o operador `=`, então retorna apenas um dos valores armazenados, nos casos em que o campo é multivalorado. Caso seja usando com o operador `in`, então retorna o conjunto com os valores armazenados.

Tabela 2 – Sumário das variáveis do contexto de usuários– `userCtx`

```
exp-abs(umPedido, umCliente, umVendedor) {
  userCtx.uid = umVendedor
  // Só exclui o pedido se o usuário corrente for
  // o vendedor que criou o pedido
}
```

- Pressione o botão "Gravar" e em seguida o botão "Fechar";
- Esta regra de autorização é parametrizada e afirma que se usuário corrente (variável contextual `userCtx.login`) é o mesmo que criou o pedido (parâmetro `umVendedor`), então a operação é autorizada. Caso contrário, é negada. Esta autorização utiliza o contexto de usuários (`userCtx`), que disponibiliza as variáveis contextuais relacionadas na Tabela 2.

6. Com o papel "Vendedor" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Pedidos" e pressione o botão "Novo" para criar a autorização que permitirá a alteração de pedidos, desde que criados pelo próprio usuário. Neste caso, utiliza-se uma autorização contextual parametrizada. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Alteração**;
   - No *comboBox* "Tipo Privilégio", selecione o item **Regra** e no editor na parte de baixo da janela entre com regra de autorização:

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

```
exp-abs(umPedido, umCliente, umVendedor) {
  userCtx.uid = umVendedor
  // Só altera o pedido se o usuário corrente for
  // o vendedor que criou o pedido
}
```

- Pressione o botão “Gravar” e em seguida o botão “Fechar”;

7. Para gerenciar pedidos, são necessárias autorizações específicas para tabela de itens, que devem ser criadas conforme instruções. Com o papel “Vendedor” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos” e pressione o botão “Novo” para criar a autorização que permitirá a consulta de itens. Na janela “NOVA Autorização”, faça o seguinte:

   - No *comboBox* “Recurso”, utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Pedidos;Itens** e pressione a tecla ↵ “Enter”;
   - No *comboBox* “Privilégio”, selecione o item **Consulta**;
   - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;

8. Com o papel “Vendedor” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos;Itens” e pressione o botão “Novo” para criar a autorização que permitirá a inclusão de itens. Na janela “NOVA Autorização”, faça o seguinte:

   - No *comboBox* “Privilégio”, selecione o item **Inclusão**;
   - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;

9. Com o papel “Vendedor” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos;Itens” e pressione o botão “Novo” para criar a autorização que permitirá a exclusão de itens. Na janela “NOVA Autorização”, faça o seguinte:

   - No *comboBox* “Privilégio”, selecione o item **Exclusão**;
   - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;

10. Com o papel “Vendedor” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos;Itens” e pressione o botão “Novo” para criar a autorização que permitirá a alteração de itens. Na janela “NOVA Autorização”, faça o seguinte:

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- No *comboBox* "Privilégio", selecione o item **Alteração**;
- No *comboBox* "Tipo Privilégio", selecione o item **+**;
- Pressione o botão "Gravar" e em seguida o botão "Fechar";

Para finalizar a configuração "Vendedor", é preciso criar a autorização que permitirá a um vendedor conceder descontos, desde que numa faixa de 0 até 10%. Para isto, siga as instruções a seguir:

1. Com o papel "Vendedor" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Pedidos" e pressione o botão "Novo" para criar a autorização que permitirá a concessão de descontos, desde que não ultrapassem 10%. Neste caso, utiliza-se uma autorização contextual parametrizada. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Recurso", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP;Pedidos;Itens;ConcederDesconto** e pressione a tecla ↵ "Enter";
   - No *comboBox* "Privilégio", selecione o item **Execução**;
   - No *comboBox* "Tipo Privilégio", selecione o item **Regra** e no editor na parte de baixo da janela entre com regra de autorização:

```
exp-abs(umDesconto) {
  umDesconto in 0..10
  // Desconto permitido se for na faixa entre 0 e 10.
}
```

   - Pressione o botão "Gravar" e em seguida o botão "Fechar";

Agora, só falta a definição das autorizações dos vendedores sêniores.

3.4.5 Autorizações do Papel "Vendedor Sênior"

Um vendedor sênior tem as mesmas autorizações de um vendedor, com algumas exceções: pode alterar o cadastro de clientes; pode modificar/excluir pedidos independente de quem os criou e pode conceder descontos numa faixa entre 0 e 40%. Para isto, siga as instruções a seguir:

1. Na janela principal do MACA AD, selecione pasta intitulada "Grupos", selecione grupo "Papeis" e no painel do lado esquerdo, faça um clique duplo no papel "Usuário", depois faça um clique duplo no papel "Vendedor" e selecione o papel **Vendedor Sênior**;
2. No painel do lado direito, selecione a pasta "Autorizações". No *comboBox* "Filtros", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP** e pressione a tecla ↵ "Enter";

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

3. No canto inferior direito da janela, marque a opção “Filtro Ativado”;
4. Com o papel “Vendedor Sênior” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Clientes” e pressione o botão “Novo” para criar a autorização que permitirá a alteração de clientes. Na janela “NOVA Autorização”, faça o seguinte:
   - No *comboBox* “Privilégio”, selecione o item **Alteração**;
   - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
5. Com o papel “Vendedor Sênior” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos” e pressione o botão “Novo” para criar a autorização que permitirá a alteração de pedidos. Na janela “NOVA Autorização”, faça o seguinte:
   - No *comboBox* “Privilégio”, selecione o item **Alteração**;
   - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
   - Note que agora a autorização equivalente herdada foi sobreposta, estando desativada para o papel “Vendedor Sênior”. A desativação é indicada pelo *led*  na coluna “Status”;
6. Com o papel “Vendedor Sênior” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos” e pressione o botão “Novo” para criar a autorização que permitirá a exclusão de pedidos. Na janela “NOVA Autorização”, faça o seguinte:
   - No *comboBox* “Privilégio”, selecione o item **Exclusão**;
   - No *comboBox* “Tipo Privilégio”, selecione o item **+**;
   - Pressione o botão “Gravar” e em seguida o botão “Fechar”;
   - Note também que a autorização equivalente herdada foi sobreposta, estando desativada para o papel “Vendedor Sênior”. A desativação é indicada pelo *led*  na coluna “Status”;
7. Com o papel “Vendedor Sênior” selecionado, selecione a linha correspondente a autorização “Aplicacoes;SGP;Pedidos;Itens;ConcederDesconto” e pressione o botão “Novo” para criar a autorização que permitirá a concessão de descontos, desde que não ultrapassem 40%. Neste caso, utiliza-se uma autorização contextual parametrizada. Na janela “NOVA Autorização”, faça o seguinte:

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- No *comboBox* "Privilégio", selecione o item **Execução**;
- No *comboBox* "Tipo Privilégio", selecione o item **Regra** e no editor na parte de baixo da janela entre com regra de autorização:

```
exp-abs(umDesconto) {
  umDesconto in 0..40
  // Desconto permitido se for na faixa entre 0 e 40.
}
```

- Pressione o botão "Gravar" e em seguida o botão "Fechar";

3.4.6 Separação de Responsabilidades entre os Papéis "Vendedor" e "Gerente de Produto"

A política de acesso para o SGP afirma que para reduzir a possibilidade de fraude, um mesmo usuário que tenha os privilégios de gerente de produto não possa ter todos os privilégios de vendedor e vice-versa. A idéia é que um vendedor não possa alterar um produto, principalmente o seu preço, ao mesmo tempo em que possa criar/alterar um pedido. O modelo de autorização do MACA atende esta questão através das autorizações do tipo **forte**.

Uma autorização forte estabelece uma política de acesso absoluta, que não tolera contradições, prevalecendo portanto sobre qualquer autorização equivalente do tipo **fraca**. Ou seja, uma autorizações do tipo forte não pode ser redefinida em papéis descendentes. Juntamente com as autorizações positivas e negativas, é utilizado para implementação da separação de responsabilidades.

A Separação de Responsabilidades é especificada neste modelo com base nos conflitos existentes entre as autorizações, mas de modo natural e não arbitrário. Isto porque as autorizações positivas e negativas sinalizam conflitos de interesse no acesso a um determinado recurso. Se para um papel, um acesso é autorizado para um recurso e, em outro papel, o mesmo acesso é contradito, então certamente haverá conflitos para um usuário exercendo ambos os papéis. Assim, os conflitos são deduzidos automaticamente segundo a autoridade e a responsabilidade estabelecidas para cada papel através das autorizações associadas.

Quando o tipo de autorização é `forte` em autorizações conflitantes, o tipo de conflito é denominado de *conflito forte*. Caso contrário, o conflito é denominado *conflito fraco*. Dois ou mais papéis que possuam autorizações conflitantes entre si são denominados *papéis conflitantes*. Nota-se que, quando os tipos da autorização são diferentes, não há conflito, pois autorizações fortes prevalecem sobre as autorizações fracas.

Nesse modelo, a separação de responsabilidades ocorre quando um usuário detendo autorizações conflitantes fortes tenta acessar o recurso protegido. **Em um papel, o acesso é concedido e, em outro papel do usuário, ele é proibido. Então, como o conflito é forte, prevalece a au-**

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

torização que proíbe o acesso, pois a concessão da autorização poderia levar o usuário situações de conflitos de interesses.

Entretanto, havendo duas ou mais autorizações fracas conflitantes, prevalecerá aquela autorização que concede o acesso. Pois, o conflito não denota conflitos de interesses reais, mais apenas diferentes necessidades para o usuário desempenhar suas funções, daí a concessão do acesso.

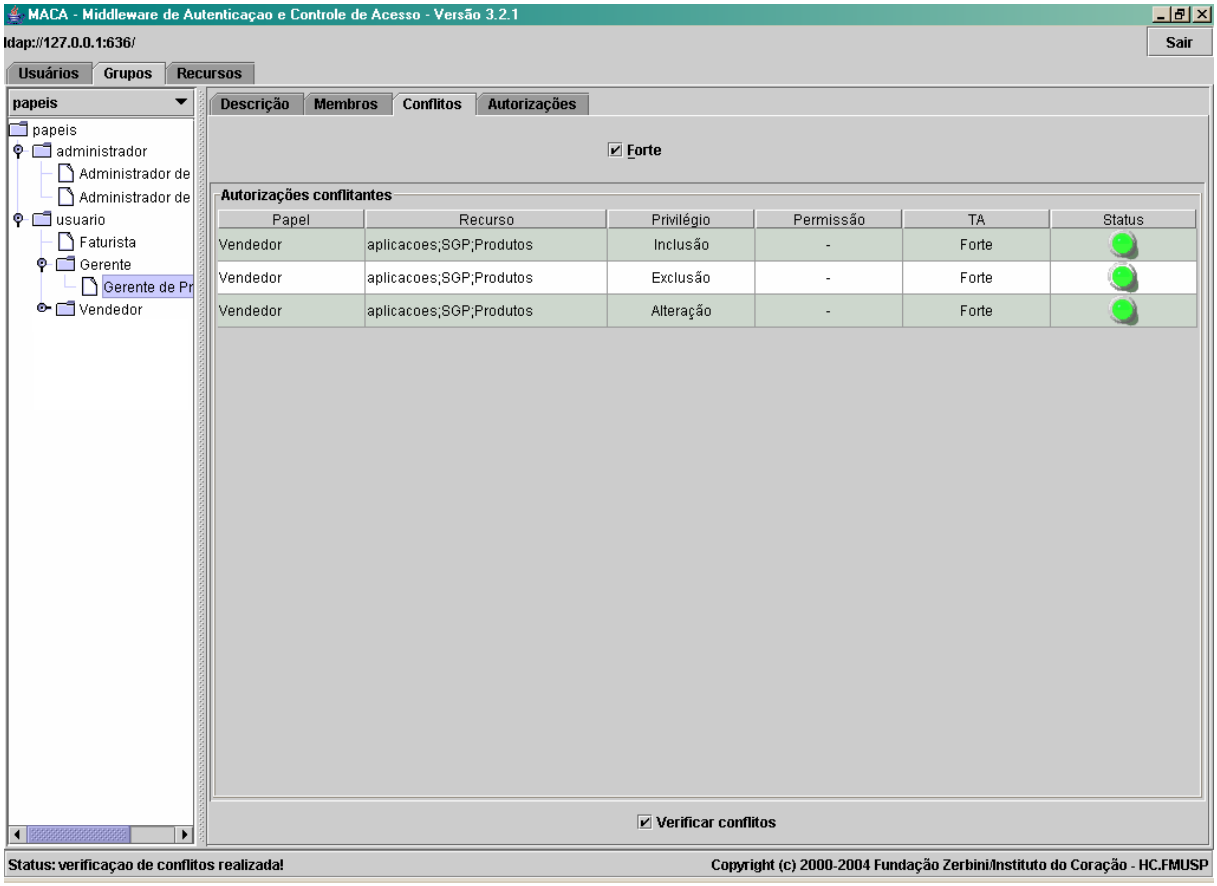
Logo, precisa-se definir a separação de responsabilidades dinâmica para os papeis "Gerente de Produto" e "Vendedor" através de conflitos fortes sobre o acesso ao recurso "Aplicacoes;SGP;Produtos". Para tanto, é preciso definir autorizações positivas fortes com privilégios de alteração, exclusão e inclusão para este recurso no papel "Gerente de Produto" e autorizações negativas fortes para o mesmo recurso com os mesmos privilégios no papel "Vendedor". Feito isto, se um mesmo usuário detiver ambos os papéis, não poderá modificar a tabela de produtos, mas apenas consultá-la. Siga as seguintes instruções para configurá-las:

1. Na janela principal do MACA AD, selecione pasta intitulada "Grupos", selecione grupo "Papeis" e no painel do lado esquerdo, faça um clique duplo no papel "Usuário", depois faça um clique duplo no papel "Gerente" e depois selecione o papel **Gerente de Produto**;
2. No painel do lado direito, selecione a pasta "Autorizações". No *comboBox* "Filtros", utilize as setas ↑ ↓ do teclado para selecionar o recurso **Aplicacoes;SGP** e pressione a tecla ↵ "Enter";
3. No canto inferior direito da janela, marque a opção "Filtro Ativado";
4. Com o papel "Gerente de Produto" selecionado, selecione a linha correspondente a autorização "Aplicacoes;SGP;Pedidos" com privilégio "Alteração" e pressione o botão "Alterar" para modificá-la. Na janela aberta, faça o seguinte:
   - No *comboBox* "Tipo Autorização", selecione o item **Forte**;
   - Pressione o botão "Gravar" e em seguida o botão "Fechar";
5. Selecione agora o papel "Vendedor", selecione a linha correspondente a autorização "Aplicacoes;SGP;Produtos" e pressione o botão "Novo" para criar a autorização que proibirá fortemente a alteração de produtos. Na janela "NOVA Autorização", faça o seguinte:
   - No *comboBox* "Privilégio", selecione o item **Alteração**;
   - No *comboBox* "Tipo Privilégio", selecione o item **–**;
   - No *comboBox* "Tipo Autorização", selecione o item **Forte**;

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

- Pressione o botão “Gravar” e em seguida o botão “Fechar”;

Repita estas operações para os privilégios “exlusão” e “inclusão”. Após estas configurações, selecione o papel “Gerente de Produto” e em seguida, mude para a pasta “Conflitos” e marque a opção “Verificar conflitos com canto inferior do painel”. A janela deverá indicar as autorizações conflitantes, conforme a figura abaixo:



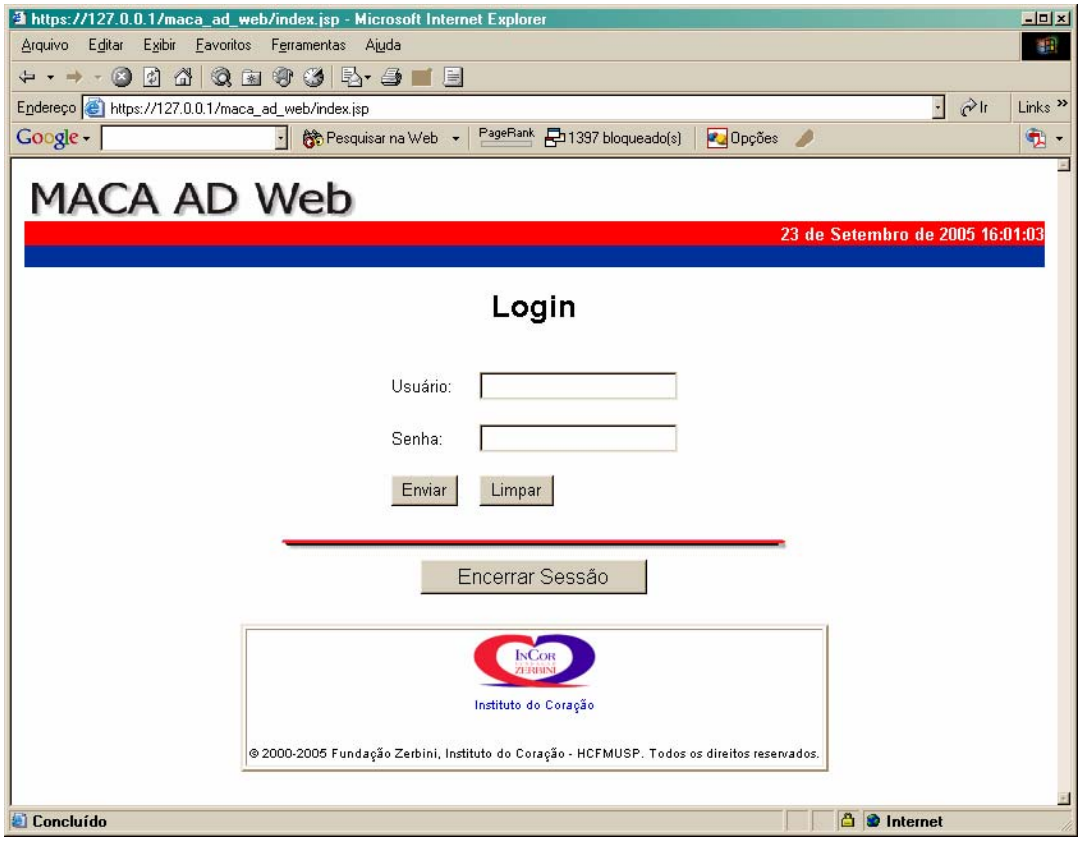
3.5 Cadastrando Contas de Usuários

O cadastramento de contas de usuários é realizada no MACA AD Web e é bastante simples. Para criar uma nova conta, faça o seguinte:

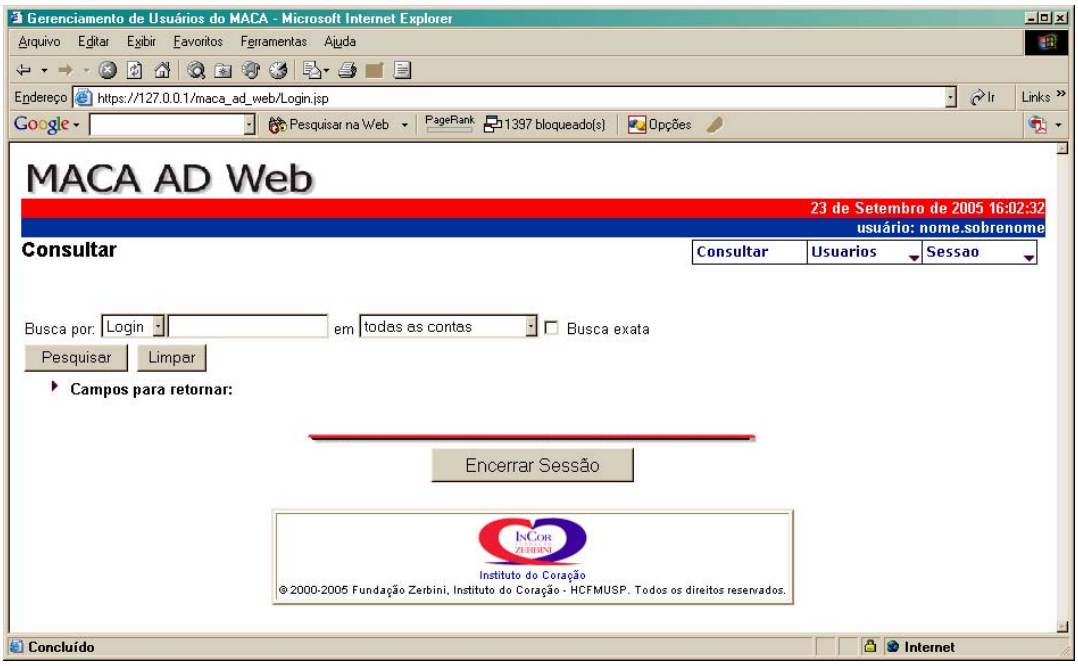
1. Acesse o MACA AD Web entrando com a URL a seguir no seu *browser*:

   https://<dns do servidor do maca ad web>/maca_ad_web/

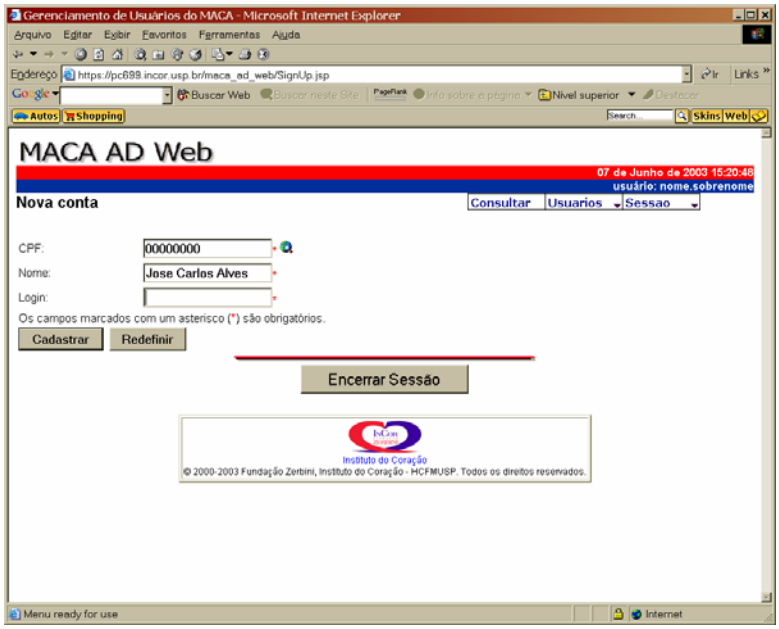
2. Quando a página a seguir aparecer, entre com o seu login, a senha e pressione o botão “Enviar”;



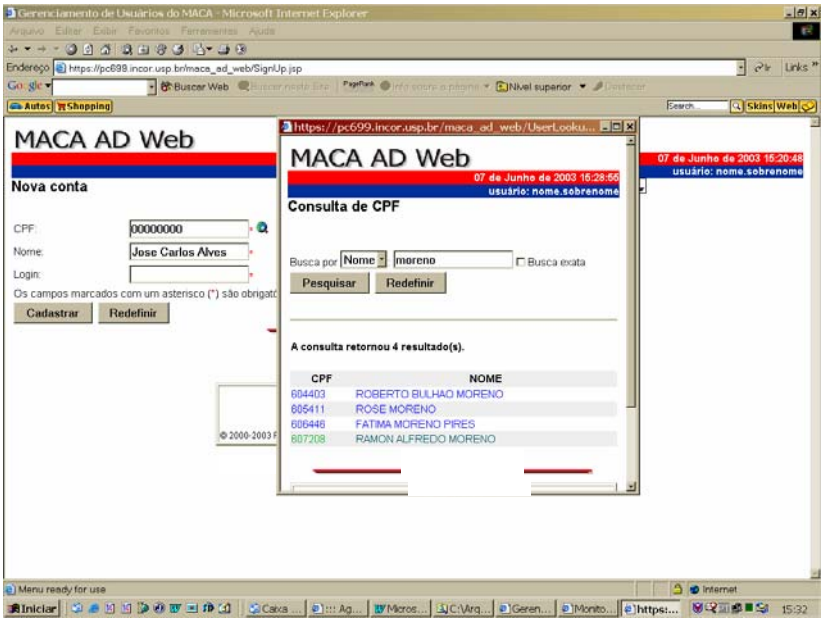
3. A página para consultas de contas de usuários do MACA AD Web (abaixo) aparecerá;



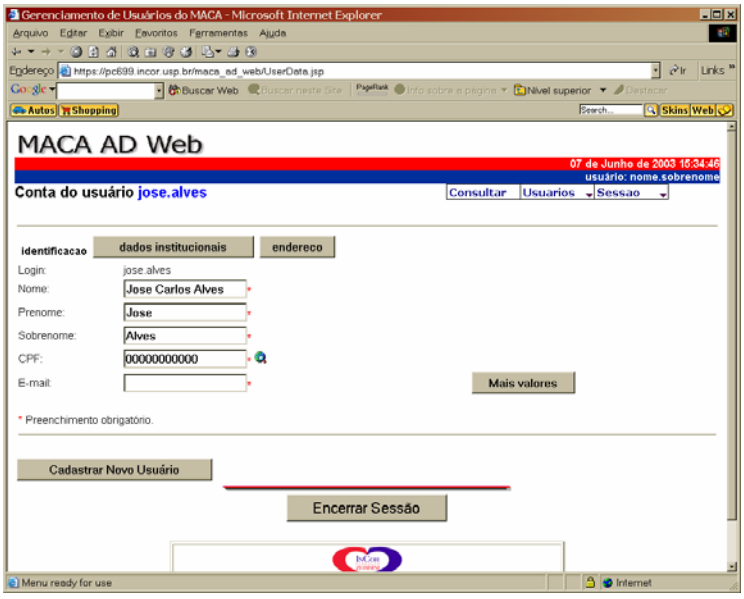
4. Selecione a opção “Usuarios | Nova Conta”, no menu do canto superior direito, para criar uma nova conta, entre com o CPF, o nome completo e *login* do usuário (opcional, pois o MACA AD Web usado o nome e o sobrenome fornecidos no campo anterior para formar o login, caso este campo fique em branco), conforme ilustrado na janela a seguir e pressione o botão “Cadastrar”;



5. Caso haja o ícone  ao lado de um campo, é porque há um *lookup* configurando para o campo. Clique nele para abrir a janela a seguir. Faça a consulta e selecione o usuário desejado clicando sobre ele. Os valores serão transportados para os respectivos campos;



6. Após pressionar o botão “Cadastrar”, complemente as informações de acordo com a página de cadastro abaixo, pressione o botão “Cadastrar Novo Usuário”. Os botões **dados institucionais** e **endereço** exibem grupos de campos do cadastros. Ainda, o campo “E-mail” permite a adição de múltiplos valores pressionando-se o botão “Mais Valores”;

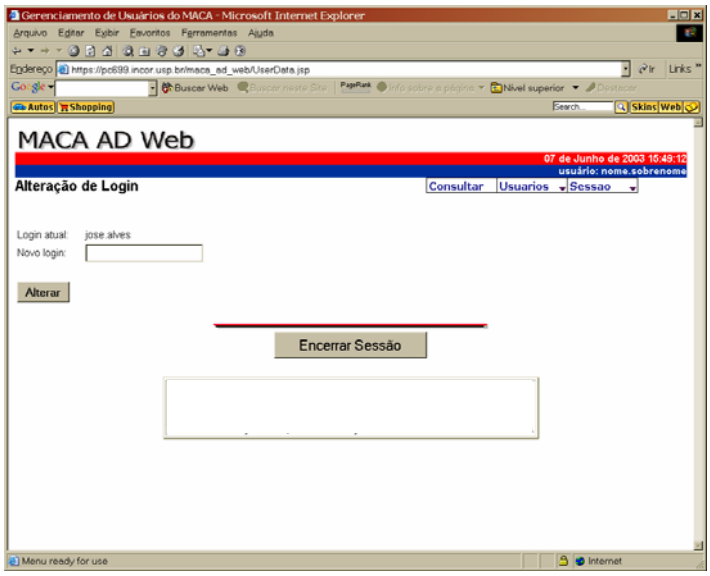


7. Após a gravação, clique na opção “Consultar” do menu. Para consultar um usuário, basta selecionar o campo no *comboBox* **Buscar Por**, selecionar o campo pelo qual se pretende pesquisar (**Nome**, por exemplo), entrar com o critério de pesquisa no campo

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP

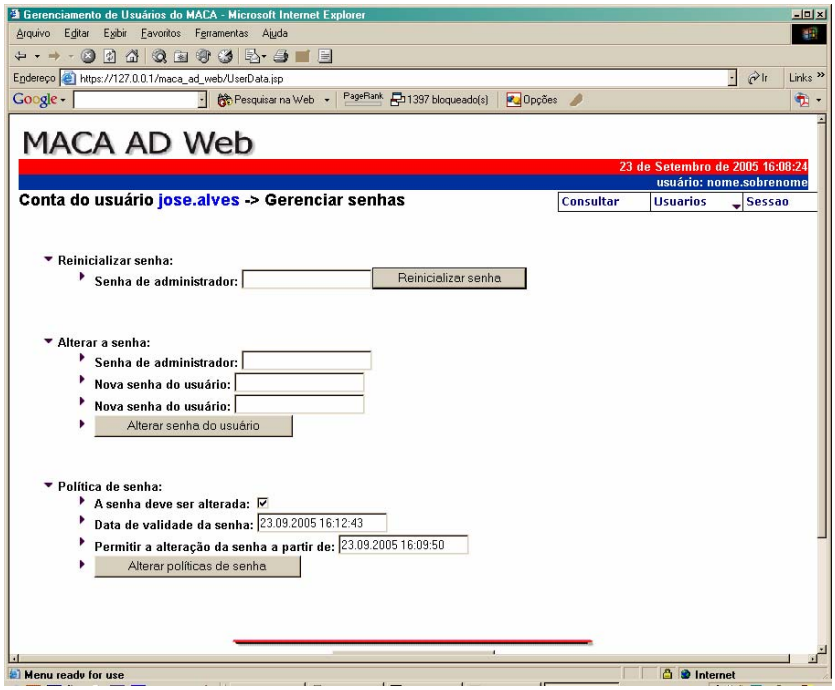
(**Jos*Alves**, por exemplo) e pressionar o botão "Pesquisar". A lista de resultados aparecerá abaixo;

8. Pressionado o link **Campos para Retornar** abaixo do *comboBox*, você poderá escolher as colunas retornardas nas consultas realizadas.
9. Um clicando sobre o nome da coluna ordenará os seus valores em ordem ascendente;
10. Para alterar um usuário, clique no link de uma linha retornada na consulta. Na página aberta, altere os campos necessários e pressione o botão "Gravar";
11. Para alterar o *login* do usuário, pressione o botão "Alterar Login", entre como novo nome e pressione o botão "Alterar";

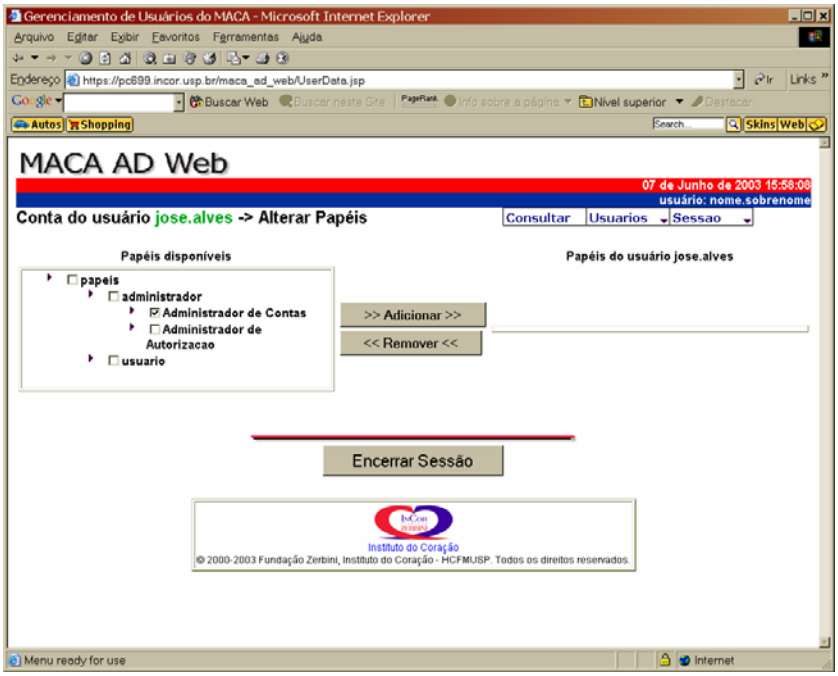


12. Para definir a senha de um usuário, clique no botão "Gerenciar Senhas" do cadastro do usuário que terá a aparência da janela a seguir. O *link* "Reinicializar Senha" permite que o administrador gere automaticamente uma senha para o usuário. O *link* "Alterar Senha" permite que o administrador defina uma nova senha para o usuário. Por fim, o *link* "Política de Senha" disponibiliza uma série de políticas de senha, dependendo das configurações específicas habilitadas nas configurações do MACA AD Web. Neste exemplo, esta habilitada a opção que obriga o usuário a trocar a senha no próximo login;

www.incor.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP



13. Para alterar os papéis de um usuário, pressione o botão “Alterar Papéis” no cadastro do usuário e a seguinte página aparecerá. Para atribuir, selecione alguns dos papéis disponíveis e pressione o botão “Adicionar”. Para remover, selecione alguns dos papéis do usuário e pressione o botão “Remover”;



14. Ao sair do MACA AD Web, **jamais esqueça de ENCERRAR a sessão**;

4 Definições e Acrônimos

- **API**: *Application Programming Interface*;
- **BIGS**: Base de Informações de Gerenciamento de Segurança;
- **CABP**: Controle de Acesso Baseado em Papéis;
- **CORBA**: *Common Object Request Broker Architecture*;
- **CSS**: *CORBA Security Service*;
- **HC.FMUSP**: Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo;
- **InCor**: Instituto do Coração;
- **LDAP**: *Lightweight Directory Access Protocol*;
- **MACA**: *Middleware* de Autenticação e Controle de Acesso;
- **MACA CS**: servidor CORBA do MACA para autenticação de usuários e controle e acesso;
- **MACA AD**: módulo para administração das políticas de autorização e controle de acesso e gerência de contas de usuários;
- ***Middleware***: serviço propósito geral que se situa entre plataformas e aplicações;
- **NIST**: *National Institute of Standards and Technology*;
- **OMG**: *Object Management Group*;
- **RAD – *Facility***.*Resource Access Decision Facility*;
- **SGBD**: Sistema Gerenciador de Bancos de Dados;
- **TLS:** *Transport Layer Security*;
- **SASL**: *Simple Authentication and Security Layer*;

www.**incor**.usp.br
Av. Dr. Enéas de Carvalho Aguiar, 44 – 05403-000 São Paulo – SP