MANUAL DO USUÁRIO

Fevereiro - 2008

Sumário de Informações do Documento		
Tipo do Documento: Manual		
Título do Documento: Sentinela – Manual do Usuário		
Versão do Sistema: 1.4.6		
Estado do Documento: Elaborado		
Responsáveis: Marlon da Cruz Volz, Paulo Eduardo Lobo **Revisado por**: Elisabeth Hoffmann , Cíntia Evangelista		
Palavras-Chaves: Sentinela – Segurança – Usuário – Manual – Interface Administrativa		
Resumo: Procedimentos de uso do proto-agente Sentinela		
Número de páginas: 54		
Software utilizados: brOffice		
Versão	**Data**	**Mudanças**
1.0		Elaboração do Manual
1.1	26/09/05	Evolução do Sentinela versão 1.2
1.2	31/10/07	Manual do Usuário do proto-agente Sentinela v.1.4.5 Atualizado por Marlon da Cruz Volz Histórico de modificações: – Explicação das novas funcionalidades do Sentinela (desde a versão 1.2.5 até a versão 1.4.5). Principalmente o item 'Parâmetros', contendo explicações a respeito da nova funcionalidade do Sentinela Administrativo: Definição de Parâmetros Identificadores das Funções. – As imagens foram atualizadas conforme a versão atual. – Foi revisado todo o texto, que referenciava a versão 1.2, tornando-o mais genérico. Anteriormente era feita muita comparação entre as versões 1.0 e 1.2. Com o texto mais genérico será mais eficiente atualizar o documento para as próximas versões do Sentinela. – Foram removidos itens e/ou informações defasadas que não mais refletem a realidade da Interface Administrativa do Sentinela. – Foi retirada a versão do Sentinela no rodapé deste documento. Evitando equívocos em futuras versões deste manual.
1.3	07/02/2008	Manual do Usuário de proto-agente Sentinela versão 1.4.6 Atualizado por Paulo Eduardo Lobo – Adição de referências no documento: número de páginas no índice, campos do rodapé indicando a versão do sistema, auto-numeração nos tópicos, referências às figuras no texto, referência à data presente na capa do documento; – Adição de texto sobre as telas de “Direitos de Usuários a Grupo” e Apoio ao Usuário com hierarquia; – Revisão do conteúdo técnico;

SUMÁRIO

1 INTRODUÇÃO....4

2 O SISTEMA SENTINELA....5

2.1 Partes do Sentinela....5
2.2 Interface da Administração do Sistema Sentinela....6
2.3 O que deve ser cadastrado? 8
2.4 Como saber quando utilizar cada tipo de função (pública, restrita, exceção, etc.)....10
2.5 Relacionamento entre usuários, grupos, sistemas e funções....12

3 FUNCIONALIDADES DA ADMINISTRAÇÃO DO SENTINELA....13

3.1 Informações sobre o Sistema Hospedeiro....13
3.2 Exceções....15
3.3 Funções....17
3.4 Parâmetros Identificadores das Funções....20
3.5 Funções Auxiliares....22
3.6 Funções Genéricas....24
3.7 Cadastro de Grupos....24
3.8 Cadastro de Usuários....27
3.9 Vinculando Grupos a um Usuário....29
3.10 Vinculação de Usuários a um Grupo....31
3.11 Vinculação de Grupos a Sistema....32
3.12 Direitos de Acesso às Funções....33

4 FUNCIONALIDADES AVANÇADAS NO SENTINELA....35

4.1 Operações....35
4.2 Bloqueio de Grupos....38
4.3 Bloqueio de Funções....39
4.4 Bloqueio de Usuários para um Sistema....40
4.5 Auxílio a Central de Atendimento – Usuários....41
4.6 Restrição por Horário....44
4.7 Sistema de Mensagens....47
4.8 Barra de ícones....49
4.9 Cópia de Grupos....51
4.10 Sistema de Auditoria....52
4.11 Outras funcionalidades....54

1 INTRODUÇÃO

Praticamente todos os sistemas informatizados necessitam de um controle sobre os direitos de acesso dos seus usuários. Normalmente as tarefas envolvidas na segurança da aplicação são desenvolvidas a cada novo sistema, sem um padrão definido. Em muitos casos não são dispensados tempo e recursos necessários, o que torna a segurança um aspecto frágil.

O Sentinela padroniza a segurança das aplicações focado em controle das requisições com informações centralizadas. É genérico e pode atuar em qualquer sistema que usa a tecnologia java/web, interceptando, restringindo requisições e passando informações com características genéricas. Não atua em filtragem de dados, porém fornece uma interface de comunicação para que este recurso possa ser implementado pelo sistema cliente.

O Sentinela permite que as aplicações tenham uma segurança padrão, centralizada e com ganho de produtividade, para que os profissionais responsáveis pelo seus sistemas não tenham que se preocupar com questões da implementação de segurança, proporcionando uma maior concentração no seu negócio.

2 O SISTEMA SENTINELA

O Sentinela atua interceptando as requisições *HTTP* de forma padronizada, conhecida também como *Interception Filter*. Neste padrão, são definidos como os filtros atuam, podendo interferir durante a chamada e também no retorno. Este recurso é gerenciado pelo *container*, assim cada requisição que chega ao servidor é repassada e o Sentinela efetua a análise da requisição.

Internamente o Sentinela trabalha com uma coleção de filtros, que fazem diversas verificações. O Sentinela foi projetado para interceptar TODAS as requisições, sendo otimizado para itens que devem ser prontamente liberados, como as imagens, *scrips js*, folhas de estilo, etc.

2.1 Partes do Sentinela

O Sistema Sentinela possui duas partes denominadas: Sentinela Administração e Sentinela Cliente. A Primeira parte refere-se ao sistema WEB onde os cadastros e permissões são efetuados. A segunda parte é o pacote Java (.jar) usado pela equipe de desenvolvimento que efetivamente aplica as permissões estabelecidas. O Sentinela Cliente é abordado no Manual de Acoplamento do Sistema Sentinela.

A Administração do Sentinela, assunto deste manual, é o recurso que os analistas, desenvolvedores e operadores utilizam para efetuar tarefas de cadastro de usuários, atribuição de direitos de acesso a um usuário, definição de grupos entre outras tarefas. Por tratar-se de informações centralizadas, pode ser que alguns recursos demonstrados neste manual não estejam acessíveis. O processo de cadastro é definido de acordo com a empresa e pode variar de acordo com as responsabilidades de cada área.

2.2 Interface da Administração do Sistema Sentinela

Primeiramente o usuário deve logar-se ao sistema Sentinela. A tela de login possui um recurso de troca de senha (antes de entrar no sistema) e um recurso para recuperação de senha, em que uma nova senha será gerada e remetida ao e-mail do usuário, bastando informar alguns dados pessoais. Caso haja algum erro neste processo a informação do erro será exibida na própria tela de login. A Figura 1 apresenta a tela de login do Sentinela Administração. Observe os *hyperlinks* para as funcionalidades de recuperação e troca de senha.

Figura 1: Tela de Login da Administração do Sistema Sentinela

Outra característica importante da Interface Administrativa do Sentinela é o recurso de mensagens. Uma caixa de mensagens está presente na página principal (*home*) e pode conter mensagens pré-programadas para serem visualizadas por sistema ou por grupos específicos. Esta caixa pode ser colocada em sistemas hospedeiros, possibilitando um recurso de mensagens centralizadas.

Outro recurso é a barra de ícones, em que são exibidos ícones para as funções principais. Ao lugar de encontrar a função no menu, pode-se clicar no ícone correspondente e

acessar diretamente a função. Nem todas as funções possuem ícones nesta barra, somente as funções escolhidas pelo administrador do sistema. É necessário ter permissão de acesso à função para que apareça o ícone na barra.

Nesta barra é possível efetuar chamadas para funções genéricas, possibilitando ter opções para acessar telas de ajuda e funções Java Script e ações como a impressão da tela, por exemplo.

Uma barra de navegação baseada na hierarquia dos menus é utilizada para situar o usuário sobre a última função selecionada. Esta barra também é disponibilizada para os sistemas cliente e indicam o caminho utilizado pelo usuário para selecionar a função atual seguindo a estrutura do menu. Observe que mesmo sendo selecionado pela barra de ícones o caminho indicado será o do menu. Ao acessar funções auxiliares será mostrado o caminho da função principal (função pai).

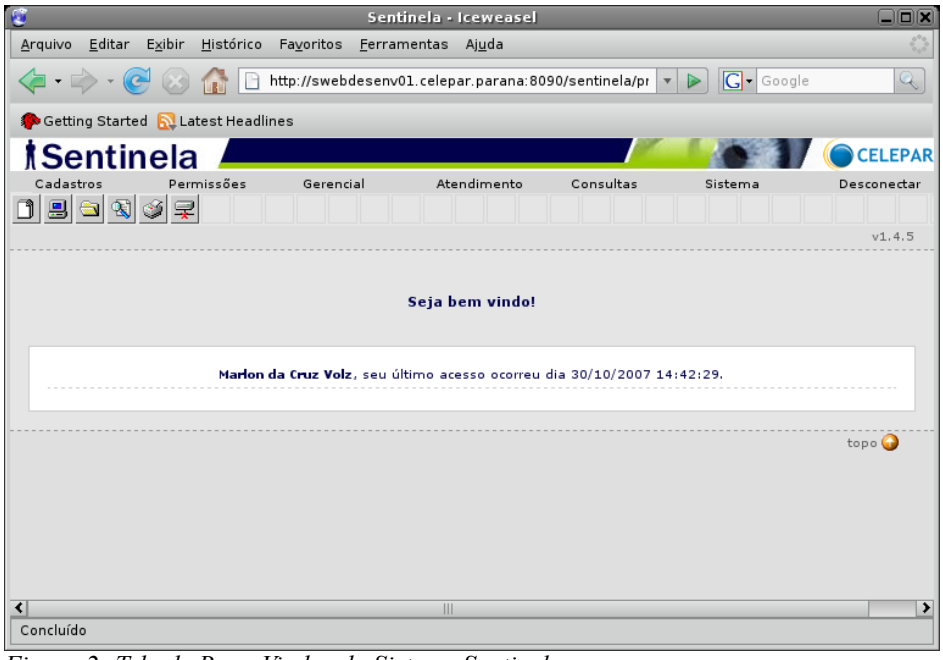

Figura 2: Tela de Boas-Vindas do Sistema Sentinela

O Sentinela também permite que uma determinada função seja colocada no menu público. Este menu não tem hierarquia e pode ser acessado sem que o usuário esteja autenticado. As funções públicas são muito semelhantes às exceções, porém as exceções são apenas validações de requisições liberadas. No caso das funções públicas o desenvolvedor conta com uma *taglibrary* para exibir as opções do menu público e colocá-las nas páginas públicas, sem precisar criar um menu específico para sua aplicação. As funções públicas podem também ficar situadas no menu privado (menu montado após a autenticação), e neste caso é considerada a hierarquia. Para isto basta indicar a função "junção de menus" da tela de inclusão/alteração de funções.

2.3 O que deve ser cadastrado?

Para usar a segurança do Sistema Sentinela primeiramente o Sistema Hospedeiro deve ser acoplado. Instruções de acoplamento são encontradas no "Manual de Acoplamento do Sentinela" no site da Plataforma de Desenvolvimento Pinhão Paraná (www.frameworkpinhao.pr.gov.br).

O segundo passo é efetuar os cadastros, iniciando com a inclusão de dados sobre o Sistema Hospedeiro. Informações básicas sobre o sistema e as URLs que o sistema está autorizado a responder. O cadastro do sistema e de outras funções abordadas neste tópico são detalhadas no Capítulo .

Em seguida devem ser cadastradas as funções que integram o sistema cliente. Existem alguns tipos de funções, a saber:

- Funções Públicas: todos os usuários acessam as funções públicas, independente de estarem autenticados ou não. Há a opção de utilizar a *taglibrary* para a montagem de menu público no Sistema Hospedeiro. É possível também associar funções públicas ao menu restrito, que é exibido apenas após a autenticação do usuário.

- Exceções: são recursos do sistema como imagens, funções Java Script, folhas de estilo, etc. Esses recursos precisam estar cadastrados para serem liberados ao sistema. O acesso às exceções também não depende da autenticação do usuário.
- Funções Genéricas: todos os usuários podem acessar as funções genéricas, desde que estejam autenticados.
- Funções Restritas: o usuário acessará somente as funções permitidas aos grupos que ele pertence. Essas funções serão exibidas no menu de acordo com as permissões de cada usuário.
- Funções Auxiliares: são funções chamadas internamente. Cada função restrita (explicada acima) pode conter várias funções auxiliares associadas. As funções auxiliares são consideradas filhas de uma função restrita. Para critério de permissão, são liberadas ao usuário todas as funções auxiliares cuja função restrita associada (função pai) esteja permitida aos grupos que o usuário pertence.

Os tipos de funções descritos acima serão mais detalhados no item 2.4.

As funções restritas são dispostas de forma hierárquica e disponibilizadas no menu. As chamadas vinculadas a funções devem ser cadastradas como funções auxiliares, que não tem chamada diretamente no menu do sistema e somente serão permitidas caso a função de origem também tenha permissão. Chamadas simples para telas de ajuda, tela de home e outras que podem ser chamadas após o login, podem ser cadastradas como funções genéricas. Figuras, scripts, folhas de estilo, páginas públicas podem ser cadastradas como exceção, que neste caso serão liberadas para o acesso do usuário.

Todo este conjunto de informações refere-se à informações do sistema e pode ser transportado entre ambientes de desenvolvimento, homologação e produção. Estas informações também estão ligadas a codificação do Sistema Hospedeiro, sendo cadastradas de acordo com novas inclusões de funções ou outros recursos.

Com o sistema devidamente configurado, é necessário cadastrar usuários e grupos. Os usuários podem ter vários grupos e os sistemas podem ser acessados por vários grupos. O vínculo de grupo com sistema necessita da atribuição de permissões de acesso que podem ser desde o possível bloqueio da requisição, como a liberação com restrições, recurso usado com apoio de implementações do código da aplicação hospedeira e o uso de "operações" do Sentinela.

Os grupos e usuários não podem ser transportados entre ambientes, pois são sensíveis a ele. Usuários no ambiente de desenvolvimento são praticamente os desenvolvedores, já em produção são os usuários que trabalham oficialmente no Sistema Hospedeiro com as permissões já concedidas. É comum ter apenas um grupo administrador com todos os desenvolvedores do sistema cliente em desenvolvimento. Já em produção existem diversos grupos com diversos usuários, sendo que os desenvolvedores raramente têm acesso em produção.

Com o sistema configurado e os grupos/usuários cadastrados, o sistema já estará funcionando e deverá passar para a fase de gerenciamento, em que permissões poderão ser concedidas e revogadas a qualquer hora, além de poderem sofrer bloqueios e/ou outras formas de tratamento de segurança.

2.4 Como saber quando utilizar cada tipo de função (pública, restrita, exceção, etc.)

Todas as requisições devem ser cadastradas e é comum surgirem dúvidas de onde cadastrar cada uma das requisições. Para saber onde cada requisição deve ser cadastrada deve-se observar os seguintes aspectos:

a) Exceções: Devem ser cadastradas como exceção: as imagens, scripts js, css, html que todos podem acessar, etc. Tudo que pode ser liberado mesmo que o usuário não faça login deve ser cadastrado como exceção.

ATENÇÃO: A tela de login não deve ser cadastrada.

b) Funções: os itens a serem exibidos no menu devem ser cadastrados como funções. Ao cadastrar uma função deve-se informar a posição no menu, a requisição e outros detalhes descritos posteriormente.

c) Funções públicas e junção de menus: se a função cadastrada pode ser vista no menu público (para usuários que não estiverem autenticados), então deve ser cadastrada como função e ligada a opção de função pública. Desse modo, este item será exibido no menu público. Caso a opção "junção de menus" seja ativada, esta função será visível no menu público (sem a necessidade de autenticação) e também do menu interno (após a autenticação do usuário).

ATENÇÃO: Ao marcar uma função como "função pública", os usuários poderão acessar mesmo sem se autenticar, similar à exceção.

d) Funções auxiliares: existem requisições que dependem de outras para serem validadas, como um cadastro de várias etapas. Primeiramente uma função é cadastrada e aparece no menu, após a chamada desta função existe a possibilidade de uma chamada para outra requisição, que seria outra parte do mesmo cadastro da função originalmente chamada. As funções auxiliares verificam requisições com base numa função principal, caso o usuário tenha acesso a essa função principal então também terá acesso à função auxiliar.

e) As funções auxiliares herdam as permissões de uma função apontada no momento do cadastro. A função apontada como pai obrigatoriamente deve ser uma função principal (função restrita, que será exibida no menu). As funções auxiliares não aparecem no menu.

f) Funções Genéricas: A última variação de funções atua de forma semelhante às exceções, porém exige que o usuário esteja autenticado. Páginas de ajuda são um bom

exemplo. Não é possível atribuir direitos para as funções genéricas, o único requisito para a chamada é a autenticação.

2.5 Relacionamento entre usuários, grupos, sistemas e funções

Usuários e grupos no proto-agente Sentinela são globais para todo o domínio, assim cada novo sistema deve incluir os usuários que não existem ainda na base de dados ou vincular os usuários já existentes aos grupos deste sistema. Entre ambientes (desenvolvimento, homologação ou produção) os usuários e grupos não se misturam e não podem ser passados por processos de transferência de dados. O cadastro de usuários também é controlado, não sendo permitida a exclusão dos mesmos, pois podem constar no histórico. Usuários podem ser apenas desabilitados após confirmação.

3 FUNCIONALIDADES DA ADMINISTRAÇÃO DO SENTINELA

Para usar o Sentinela é necessário cadastrar dados sobre o Sistema Hospedeiro. Este capítulo irá esclarecer como executar esta tarefa. Todos os cadastros estão na administração do Sentinela, porém pode ser que a chave não tenha permissões de acesso para alguns itens que serão mostrados.

3.1 Informações sobre o Sistema Hospedeiro

Nesta tela ficam registradas as informações sobre o Sistema Hospedeiro. Para acessá-la clicar na seguinte opção de menu: Cadastros > Básicos > Sistemas. Abrirá uma tela como apresentado na Figura 3.

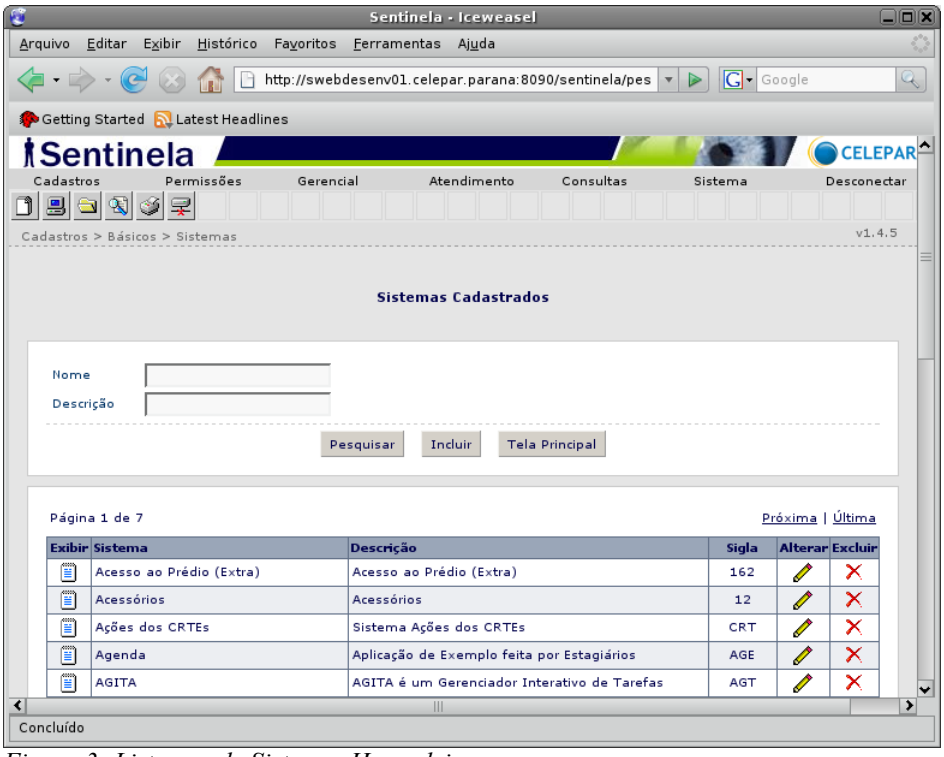

Figura 3: Listagem de Sistemas Hospedeiros

Nesta tela são exibidos os sistemas que seus grupos têm acesso. Se quiser incluir um novo sistema basta clicar no botão incluir.

Não há possibilidade de excluir sistemas, somente torná-los inativos. Para isso é necessário verificar se o sistema não possui dependências, deve-se primeiramente apagar todas as outras informações que utilizam este sistema (funções, exceções, grupos, etc).

Para alterar alguma definição clique no desenho de lápis a esquerda do nome do sistema. Clique em um dos sistemas para visualizar a tela de atualização, conforme a Figura 4.

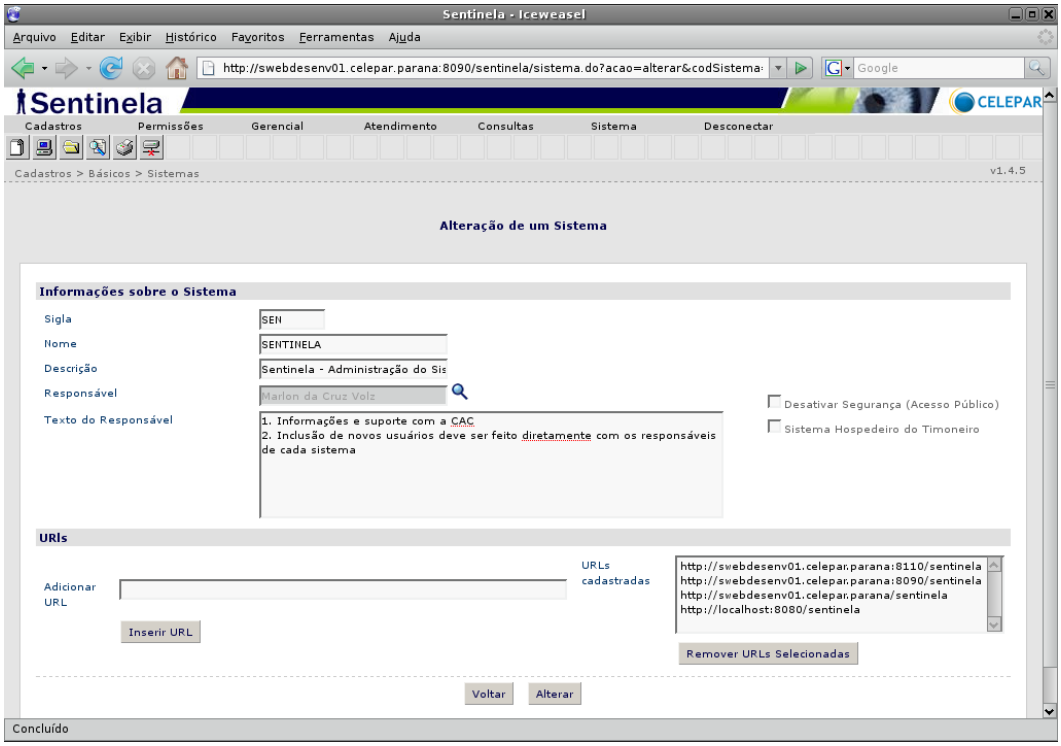

Figura 4: Alteração de Sistema Hospedeiro

O sistema deve obrigatoriamente ter uma sigla (com letras maiúsculas). Preencher também o nome e a descrição do sistema. Em seguida preencher o campo “URL do servidor”, que encontra-se na parte inferior da tela de cadastro. Este endereço deve ser EXATAMENTE da forma como será digitado no Browser. Pode ser informada também a porta do servidor, caso seja necessário, e o nome do contexto (diretório). Não deve ser utilizado o caractere '/' (barra) no final do endereço.

Cada sistema pode fazer referência a vários endereços (URL), pois o mesmo pode ser

acessado a partir de diferentes servidores de aplicações, porém apontando para a mesma base de dados. Lembre-se que a URL é verificada apenas durante a inicialização (quando a primeira tela do sistema é acessada), em que o cache do sistema é preenchido. É necessário ter permissão de atualização em cadastro de sistemas para incluir ou excluir URL's. O campo "nome do responsável" e "texto do responsável" deve ser preenchido para que a Central de Atendimento possa identificar a pessoa de contato do sistema. O texto do responsável deve conter informações úteis para a central de atendimento, como o exemplo abaixo:

"Em caso de problemas com permissões de acesso deve-se entrar em contato com a GTI".

O campo "Desativar Segurança (Acesso público)" refere-se ao tipo de acesso do sistema hospedeiro. Se a caixa de seleção estiver marcada, o sistema não exigirá nenhum tipo de autenticação, liberando todas as requisições, porém o sistema não irá montar menu. Esta opção somente deve ser usada para procedimentos de teste.

O campo "Sistema Hospedeiro do Timoneiro" deve ser marcado, caso o Sistema Hospedeiro do Sentinela também hospede o proto-agente Timoneiro (para sistemas Workflow). Mais detalhes sobre a necessidade de marcar este campo podem ser encontrados nos manuais do Timoneiro (www.frameworkpinhao.pr.gov.br).

Normalmente o cadastro do Sistema Hospedeiro é feito pelos administradores do Sentinela, e os administradores do Sistema Hospedeiro apenas atualizam estas informações.

3.2 Exceções

Com o sistema cadastrado, é necessário cadastrar itens que serão liberados automaticamente pelo Sentinela. Estes itens são imagens, scripts *js*, folhas de estilo e até mesmo páginas estáticas ou dinâmicas que não precisam de segurança, são chamados de exceções, pois não são verificados nos procedimentos de filtragem do proto-agente Sentinela e

nem precisam passar pelo login.

ATENÇÃO: O Sentinela implementa um dispositivo de segurança para a tela de login. Ao chamar a requisição de login (definida pelo arquivo WEB-INF/sentinela.xml) o sentinela efetua um logoff, portanto a requisição para a tela de login não deve ser cadastrada como exceção.

Para cadastrar itens considerados exceções, deve-se entrar no seguinte item de menu: Cadastros > Complementares > Exceções. É apresentado uma tela conforme Figura 5.

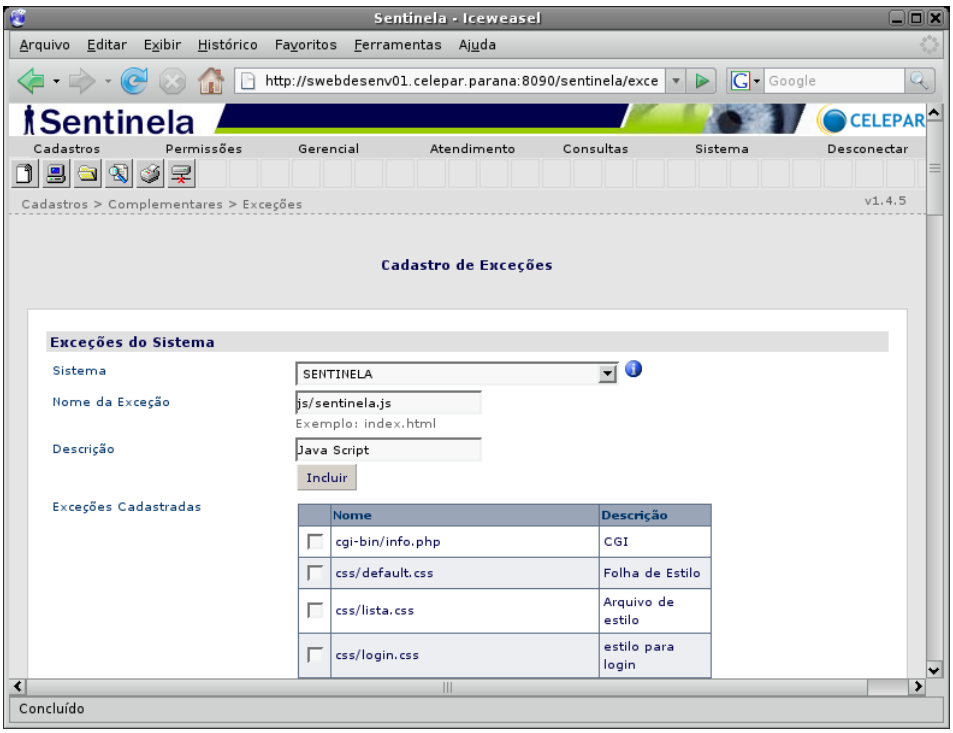

Figura 5: Tela de Cadastro de Exceções

Selecionar o primeiro combo com o nome do sistema com o qual se deseja consultar/inserir/excluir as exceções. Em seguida será apresentada uma lista com as exceções cadastradas para este sistema. No campo "Nome da Exceção" digitar o caminho (requisição) da exceção. Deve-se seguir o exemplo da própria tela de cadastramento, **não colocar barra no início** e digitar o caminho completo a partir do contexto. Segue um exemplo logo abaixo:

Imagem que se quer cadastrar como exceção:

http://10.15.60.97:8080/cpq/imagens/especiais/logotipo.png

No cadastro de sistemas, no campo “URL do Servidor” cadastrou-se:

http://10.15.60.97:8080/cpq

Para a exceção, digitar no campo “Nome da Exceção”:

imagens/especiais/logotipo.png

ATENÇÃO: Não colocar a barra no início.

No campo 'Descrição' informar a exceção. Normalmente são usados termos como: “script”, “folha de estilo”, “imagem”, etc. Para excluir um item, basta clicar na caixa de seleção e, em seguida, no botão “Excluir Selecionados”. Nesta tela não existe operação de atualização, sendo necessário apagar a exceção antiga e cadastrar uma nova exceção a seguir.

Com o sistema e com as exceções cadastradas, o sistema estará funcionando para as telas colocadas como exceção e as configuradas no sentinela.xml (*login*, *pós-login* e *erro*). Estas três chamadas não precisam de cadastro, pois são controladas diretamente pelo Sentinela. Se tiver dúvidas com relação às configurações do Sentinela consulte o *Manual de Acoplamento ao Sistema Hospedeiro*.

3.3 Funções

São chamadas funções ou requisições, os itens passíveis de atribuições de direitos de acessos e bloqueios. Cada função disponível para o usuário é colocada de forma visual no menu, que tem uma estrutura em forma de árvore onde aparecem nós e folhas. Os nós são apenas para organização do menu e as chamadas são feitas das folhas. Cada clique em uma

folha gera uma nova requisição. Os direitos e restrições somente podem ser aplicados nas folhas, e o Sentinela oculta os nós que não tiverem folhas para fins de organização.

Para cadastrar uma nova função usar a seguinte opção de menu: Cadastros > Básicos > Função. Aparecerá uma listagem de funções, para operações de edição e exclusão das funções já cadastradas. Para inserir uma nova função clicar em "Incluir".

A Figura 6 ilustra a inclusão/alteração de uma função. Selecionar no primeiro combo o sistema para o qual quer atribuir a função. O combo "Menu pai" contêm as funções já cadastradas, e deve ser selecionada a opção que servirá para formar a hierarquia do menu. Se deixar na primeira opção, a função será exibida na raiz, ou seja, diretamente na barra de menu.

A opção "ordem" deve conter um número indicando qual item deve aparecer primeiro em um mesmo nível. Sugere-se que seja cadastrado com intervalos de 5 em 5 ou 10 em 10 para que facilite uma futura troca de posições. A opção "Acesso público", fará com que a função cadastrada não precise ter o direito atribuído, tornando-se uma função pública. Se um grupo tiver a permissão de acesso ao sistema, então a terá também para acesso a função pública. As funções públicas podem ser desenhadas pelo menu público e também no menu privado, bastando selecionar a opção "Realizar junção de menus". Para o menu público a hierarquia não é levada em consideração.

A opção "Ativar log de acesso" permite ao administrador do Sistema Hospedeiro escolher se deseja ou não que a função em questão seja logada. Esta funcionalidade foi criada para evitar logs desnecessários, melhorando a performance durante o processo de segurança.

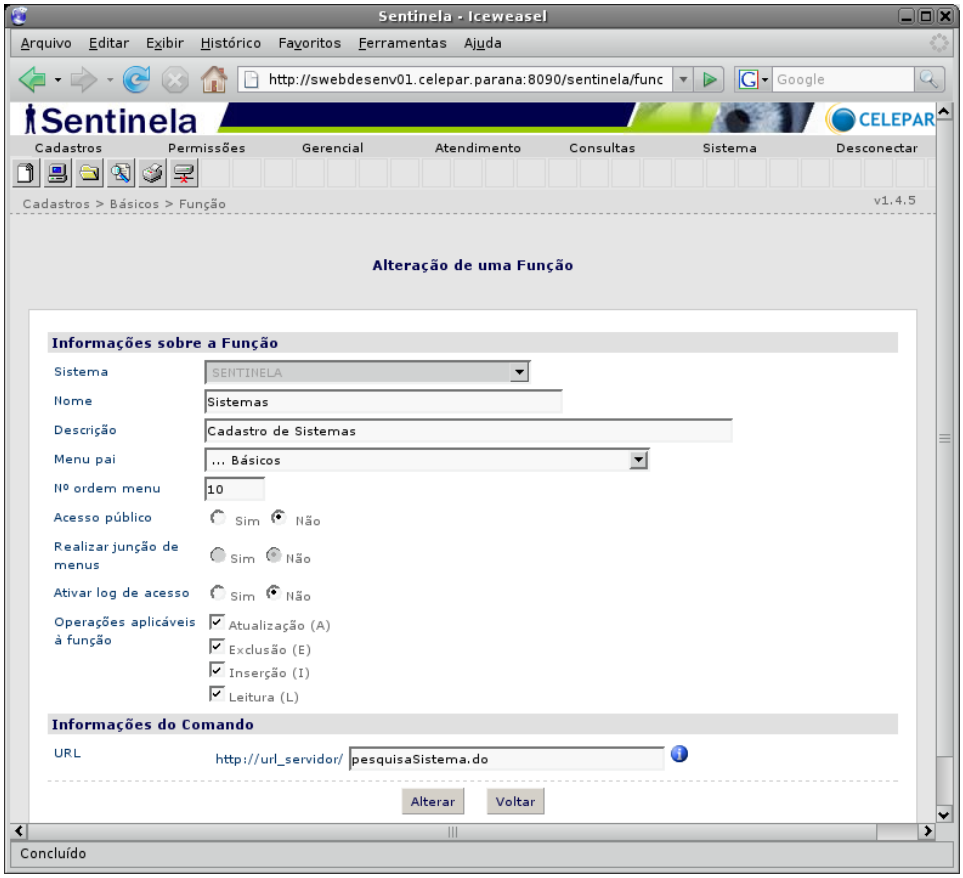

Figura 6: Tela de Cadastro de Função

O campo de operações aplicáveis será detalhado no capítulo correspondente a operações, e indica quais operações podem ser aplicadas a esta função.

O último campo é semelhante ao visto no cadastro de exceções, que deve ser preenchido com a URL chamada, quando o menu for pressionado. Consultar o item 3.2 para maiores informações a respeito do preenchimento deste campo. É possível adicionar parâmetros ao endereço URL (ex.: cadastrar uma função com requisição 'pesquisaSistemas.do?tipo=1' e outra com requisição 'pesquisaSistemas.do?tipo=2'). No caso do exemplo as funções ainda serão consideradas como uma única função para o Filtro de Segurança (verifique o Manual de Acoplamento). Para que o Sentinela reconheça cada função separadamente, é necessário realizar a definição dos parâmetros identificadores. São os parâmetros que irão identificar uma função. Os parâmetros descritos neste campo DEVEM SER EXATAMENTE OS MESMOS cadastrados na tela de definição de parâmetros identificadores, para garantir o correto funcionamento do Filtro de Segurança do proto-agente

Sentinela.

Nas versões anteriores a função era identificada desconsiderando parâmetros na requisição. Detalhes sobre como definir os parâmetros identificadores são explicados no tópico .

ATENÇÃO: Não colocar a barra no início do campo URL.

Ao término do preenchimento basta clicar em “Salvar”. Esta função ainda não será visível até que seja dado o direito de acesso para os grupos.

3.4 Parâmetros Identificadores das Funções

No Sentinela as requisições (URL's) podem conter parâmetros ou não para invocar determinada função. Porém em versões anteriores o Sentinela desconsiderava os parâmetros das requisições, tratando funções com o mesmo prefixo (mas com parâmetros diferentes) da mesma maneira. Para o Filtro de Segurança tais funções eram confundidas. Se uma função estava permitida a determinado grupo a outra função com mesmo prefixo também era permitida. Por isso, as versões anteriores dos manuais do Sentinela avisavam que, cadastrar funções da maneira exemplificada acima, implicava no funcionamento inadequado no tocante à liberação de acesso de funções com o mesmo prefixo de URL.

A versão atual do Sentinela distingue funções que possuam o mesmo prefixo (ex.: '**testeParametros.jsp**?teste=1' e '**testeParametros.jsp**?teste=2'), porém com parâmetros diferentes (?*teste=1* e ?*teste=2*). Para que isso ocorra no momento de concessão de acesso, não basta adicionar à URL os parâmetros, é necessário também definir os parâmetros como identificadores das funções. A Figura 7 ilustra um exemplo de definição de parâmetros identificadores.

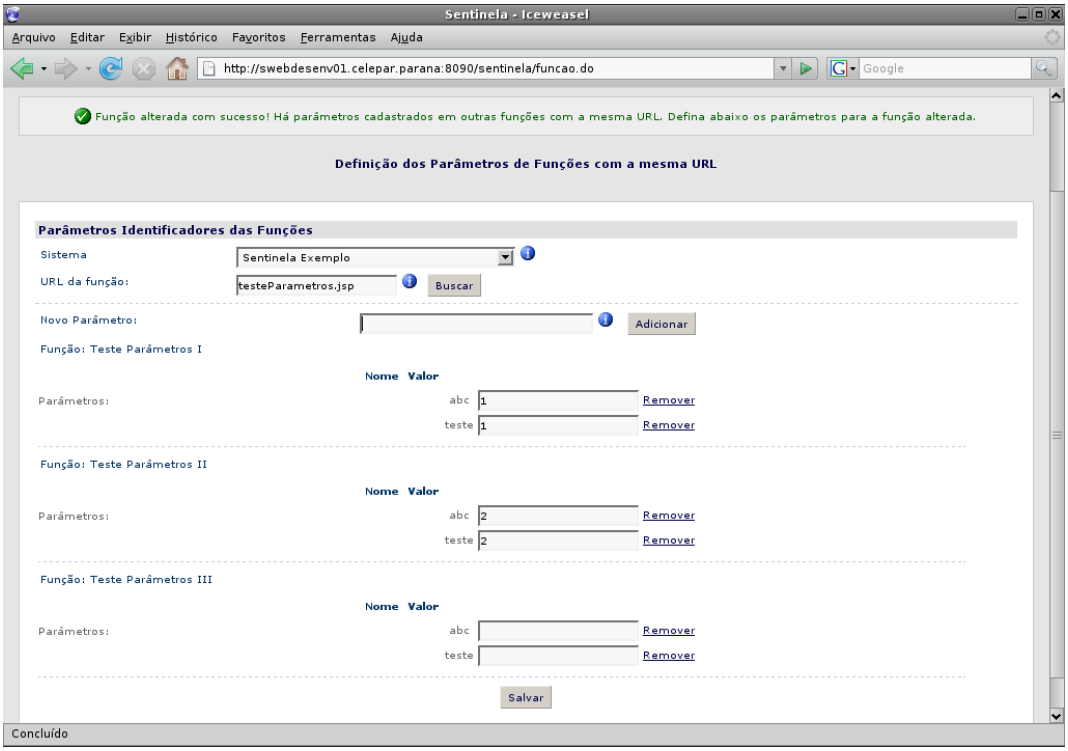

Figura 7: Definição de Parâmetros Identificadores de Funções

Para definir os parâmetros identificadores é necessário acessar o item de menu: Cadastros -> Básicos -> Funções -> Parâmetros.

Primeiramente o campo sistema deve ser selecionado. A seguir, deve-se informar qual a URL (sem parâmetros) desejada. Pressionando o botão 'Buscar' serão listadas todas as funções para o sistema e URLs informados, desde que mais de uma função possua o mesmo prefixo de URL. Ou seja, uma função cuja URL não coincida com qualquer outra não é considerada para definir parâmetros, pois não há essa necessidade. Caso as funções listadas já possuam parâmetros identificadores cadastrados, os mesmos também aparecerão na tela juntamente de seus respectivos valores.

A tela de definição de parâmetros identificadores oferece as opções de adicionar parâmetros, remover parâmetros e definir o valor de cada parâmetro para cada função listada.

Assim que os parâmetros e seus respectivos parâmetros forem definidos, basta clicar sobre o botão 'Salvar'.

Há ainda um comportamento que deve ser observado. Ao incluir uma nova função ou

alterar a URL de alguma função já existente, o Sentinela verifica a existência de outras funções com mesmo prefixo de URL. Se houver alguma ocorrência dessa verificação o Sentinela redireciona o usuário, automaticamente, à tela de definição de parâmetros identificadores para a função recém incluída/alterada. A Figura 7 demonstra este comportamento evidenciado na mensagem exibida na parte superior da tela ("*Função alterada com sucesso! Há parâmetros cadastrados em outras funções com a mesma URL. Defina abaixo os parâmetros para a função alterada*").

> **ATENÇÃO: Os parâmetros e valores informados no campo URL na tela de Cadastro de Funções devem ser exatamente os mesmos parâmetros e valores definidos na tela de Definição de Parâmetros Identificadores. Qualquer disparidade com relação aos parâmetros comprometerá o adequado funcionamento do Filtro de Segurança do proto-agente Sentinela. A observação deste aspecto é de responsabilidade do administrador de cada Sistema Hospedeiro.**

Mais detalhes a respeito dos parâmetros identificadores das funções, principalmente com relação a atuação do Filtro de Segurança na análise de requisições, podem ser verificadas no Manual de Acoplamento do Sentinela (www.frameworkpinhao.pr.gov.br -> Sentinela).

3.5 Funções Auxiliares

O Cadastro de funções é responsável pelas requisições feitas pelo sistema. Além de montar o menu, serve também para validar as requisições do usuário no controle de acesso. Caso a chamada do usuário não conste na lista de funções que ele tem acesso e nem conste em outras listas, como exceções, o acesso será barrado. A requisição pode ter vindo de um preenchimento diretamente na linha de *URL* do navegador do cliente ou de um menu montado com as informações expiradas.

Como o Sentinela controla todas as requisições, precisa de um local para cadastro de outras requisições que não ficam no menu, mas são vinculadas e outras funções, como funções que tem diversas telas, como um *wizard* ou até mesmo cadastros complexos, chamadas para pop-up de pesquisas e outros. Caso o usuário não tenha permissão para acessar determinada função, estas chamadas vinculadas também não podem ser permitidas.

Estas chamadas vinculadas a funções são denominadas "Funções Auxiliares" para o Sentinela. Todos os direitos e restrições aplicados às funções são replicados automaticamente para as funções auxiliares. Caso não sejam cadastradas estas funções, o Sentinela irá bloquear estas chamadas.

Para cadastrar uma função auxiliar, clicar no seguinte item de menu: Cadastros > Complementares > Funções Auxiliares. É apresentado uma tela conforme Figura 8.

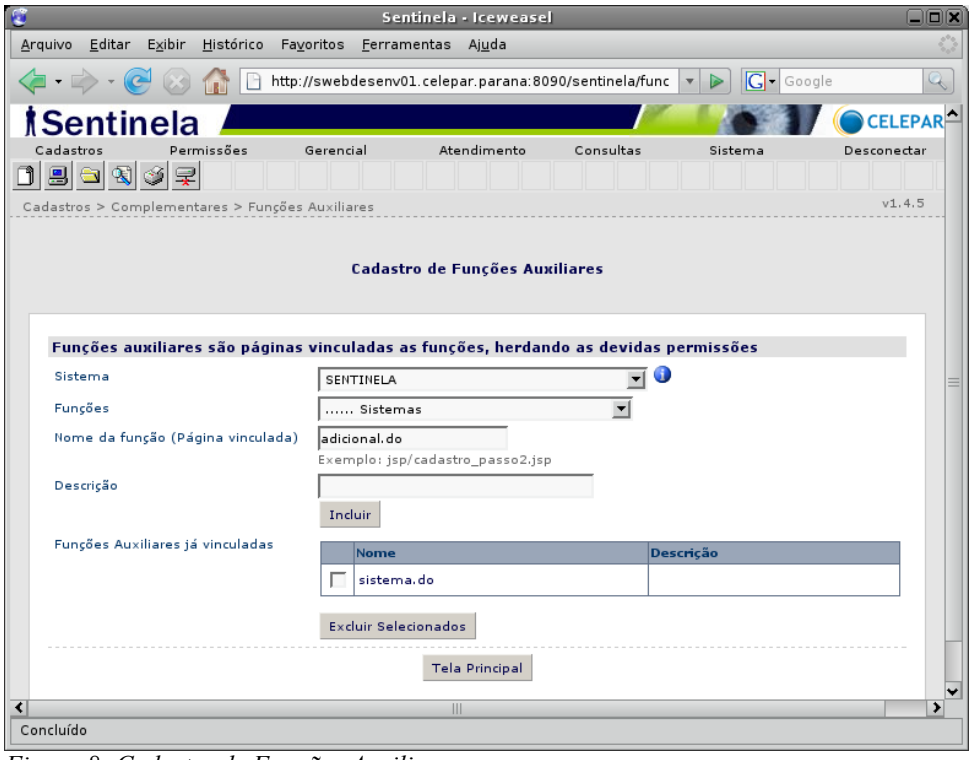

Figura 8: Cadastro de Funções Auxiliares

Selecionar o sistema desejado no primeiro combo, em seguida o segundo combo denominado "Funções" será preenchido. Este deve ser selecionado com a função que se quer

vincular a função auxiliar previamente cadastrada,

Preencher o campo ”Nome da função” da mesma forma como foi feito com o cadastro de exceções e com o cadastro de menus (consultar os tópicos anteriores se houver dúvidas sobre como proceder). A forma de cadastramento é semelhante a tela de cadastro de exceções, onde deve-se preencher os campos “Nome da Função” e “Descrição” e clicar em “Incluir”. O item deverá ir para a lista de funções auxiliares já cadastradas. Para excluir basta selecionar o item na lista e clicar em “Excluir Selecionadas”.

Uma vez preenchido, o vínculo está formado, e toda as chamadas cadastradas obedecerão os direitos e restrições aplicadas às funções que foram vinculadas.

3.6 Funções Genéricas

Esta modalidade especial de funções operam de forma similar às exceções, mas exigem que o usuário esteja autenticado para acessá-las. Desta forma o usuário adquire o direito de acessar TODAS as funções genéricas assim que efetua o login, independente do tipo do seu acesso. Devem ser cadastradas como funções genéricas: requisições de ajuda, tela de boas-vindas, etc.

Para acessar o cadastro de funções genéricas usar o seguinte caminho nos menus do Sentinela: Cadastros > Complementares > Funções Genéricas. A forma de cadastramento é similar às exceções.

3.7 Cadastro de Grupos

Com o sistema hospedeiro, funções e derivados já cadastrados, deve-se determinar a

quem dará os direitos de acesso cadastrados. Todos os direitos são atribuídos a grupos e nunca a usuários diretamente. Caso houver a necessidade de dar permissão a um único usuário, deve-se criar um grupo para isto e colocar apenas este usuário. Lembrando que em uma empresa, nunca algo está associado a uma pessoa e sim a um cargo ou função e as pessoas assumem estes cargos ou funções. Futuramente outra pessoa pode estar no cargo, necessitando a troca da pessoa neste grupo unitário. É aconselhável fazer um planejamento para os grupos, criando-os de acordo com a necessidade, para evitar manutenção desnecessária.

Clicar na opção de menu: Cadastros > Básicos > Grupos para acessar o cadastramento de grupos. Aparecerá uma tela como ilustrada na Figura 9.

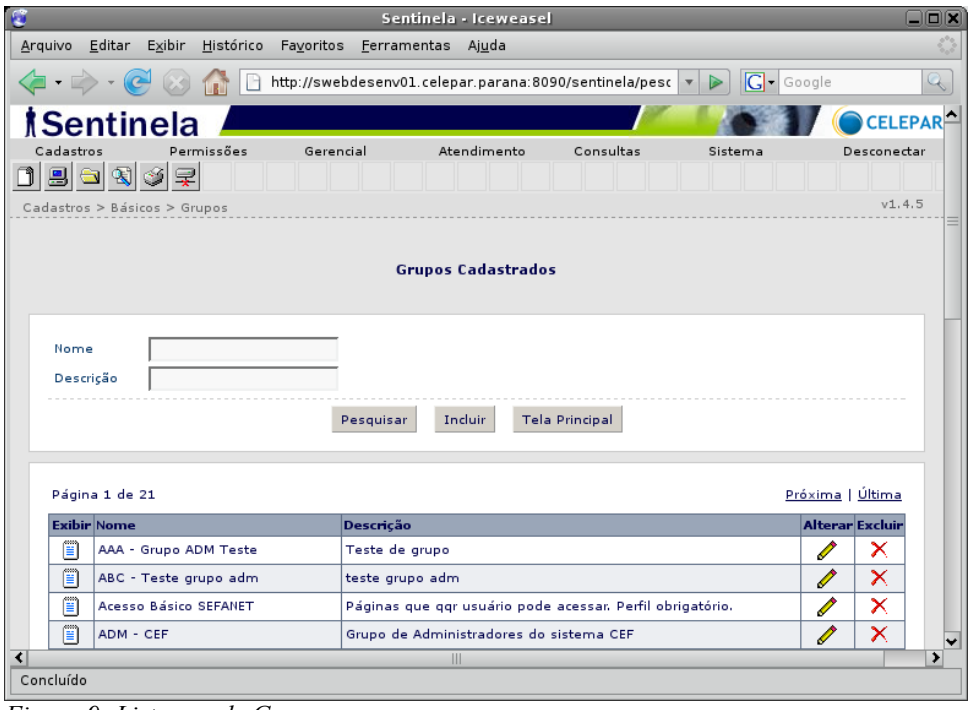

Figura 9: Listagem de Grupo

Nesta tela estão os grupos cadastrados aos quais o usuário logado tem acesso para manutenção. Para editar ou excluir um grupo clicar na opção correspondente. Para incluir um

novo grupo, clicar em “Incluir” na parte inferior desta tela. Aparecerá uma tela como a ilustrada na Figura 10.

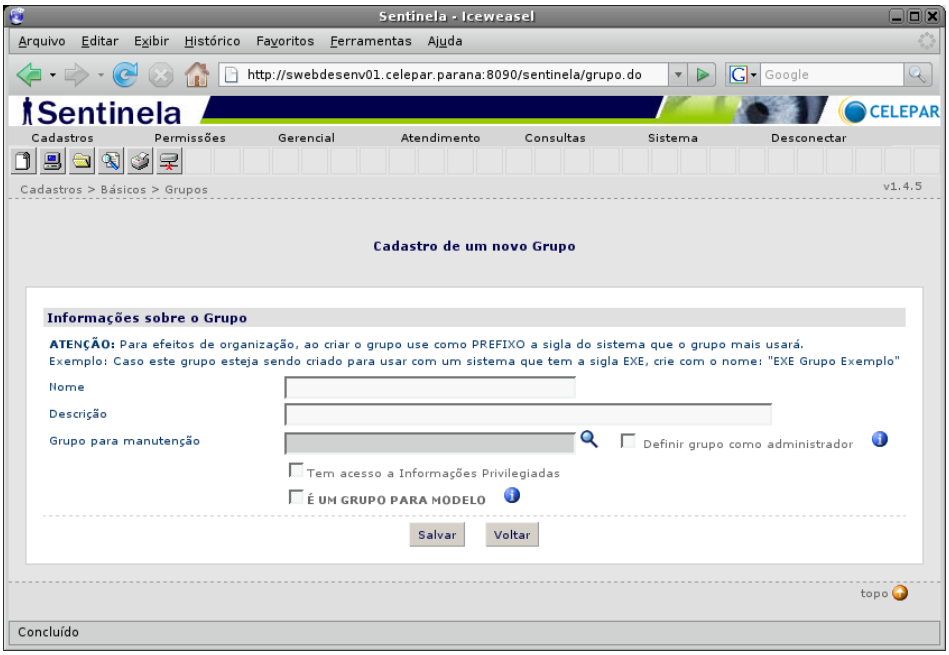

Figura 10: Inclusão de Novo Grupo

Preencher o nome e descrição do grupo, lembrando-se de utilizar o prefixo do sistema no grupo, pois facilita a manutenção. Procurar colocar nomes coerentes com o tema. No campo “Grupo para manutenção” deve ser colocado o grupo que poderá dar as permissões e restrições para o grupo em questão. Normalmente há um grupo administrador com acessos privilegiados para o Sistema Hospedeiro. Para criar grupos com acesso a informações privilegiadas, basta marcar a opção correspondente. Neste caso os usuários colocados neste grupo poderão alterar dados do próprio grupo.

O SentinelaInterface – Interface de Comunicação com o Sistema Hospedeiro (maiores informações no Manual de Acoplamento) – fornece métodos que retornam informações privilegiadas, como 'todos os usuários cadastrados'. Esta informação não deve ser acessível para qualquer usuário e sim para usuários que executam processos específicos que necessitam desta informação. Ao marcar a opção “Tem acesso a Informações Privilegiadas”, o Sentinela estará liberando para o grupo informações que o usuário comum não deveria ver. Os

administradores de cada sistema devem verificar quais os grupos que devem ter este acesso.

Há também os chamados Grupos Administradores. Essa característica é válida somente no Sentinela Administrativo, pois a partir da versão 1.4.3 do Sentinela os grupos comportam-se de maneira hierárquica para fins de administração. Somente Grupos Administradores poderão manter (administrar) outros grupos no Sentinela Administrativo.

O grupo para modelo facilita a criação de novos grupos. Ao criar um novo grupo pelo método convencional, será necessário ainda definir os sistemas que serão acessíveis e as permissões em cada uma das funções. Dependendo do número de funções da sua aplicação, este procedimento pode ser bastante trabalhoso e demorado. O grupo para modelo é usado apenas para facilitar o cadastro, não sendo usado para questões de permissão. Criar um grupo de modelo e introduzir os sistemas acessíveis e suas permissões, quando precisar de um grupo semelhante não criá-lo por esta tela de cadastramento, deve-se acessar a opção: Cadastros > Complementares > Cópia de Grupo e apenas criar um novo grupo a partir de um modelo. As permissões de acesso serão copiadas de acordo com o modelo. ATENÇÃO: Não existe sincronia entre os grupos modelo e os grupos copiados, este processo somente copia sem manter qualquer tipo de vínculo. No Capítulo 4 será abordado o processo de cópia.

3.8 Cadastro de Usuários

Os usuários no Sentinela são centralizados, ou seja, quando um usuário troca de senha ou é desativado vale para todos os sistemas que utilizam o Sentinela. Por este motivo deve-se ter cuidado no momento do cadastro, verificando se o usuário já não existe na base de dados. O ideal é tentar cadastrar o máximo possível de informações, mesmo as que não são obrigatórias, pois em algum sistema isto pode ser necessário.

Para facilitar o cadastramento, o Sentinela normalmente permite que novos usuários sejam inseridos. Isto permite simplicidade no processo de cadastramento, pois mesmo

podendo cadastrar novos usuários não será possível colocá-los em qualquer grupo, mas somente nos quais o usuário possui acesso para manutenção. Mais uma vez isto ressalta a importância do cadastramento correto dos grupos.

É aconselhável que processos de alteração e desativação de usuários sejam feitos por um setor definido na empresa, normalmente feitos pela Central de Atendimento. A desativação de um usuário ocorre somente através do Atendimento ao Usuário (ver Capítulo 4.5) quando o usuário for desligado da empresa, ou por outro motivo. A desativação do usuário também ocorrerá se o mesmo não utilizar o sistema de Segurança Sentinela (direta ou indiretamente) pelo período determinado na definição do Parâmetros Gerais do Sentinela (ex.: 6 meses).

Para acessar o cadastro de usuários, clicar na seguinte opção de menu: Cadastros > Básicos > Usuário. Será exibida uma tela contendo a listagem dos usuários, para incluir um novo usuário clicar em “Incluir”, abrirá uma tela conforme a Figura 11.

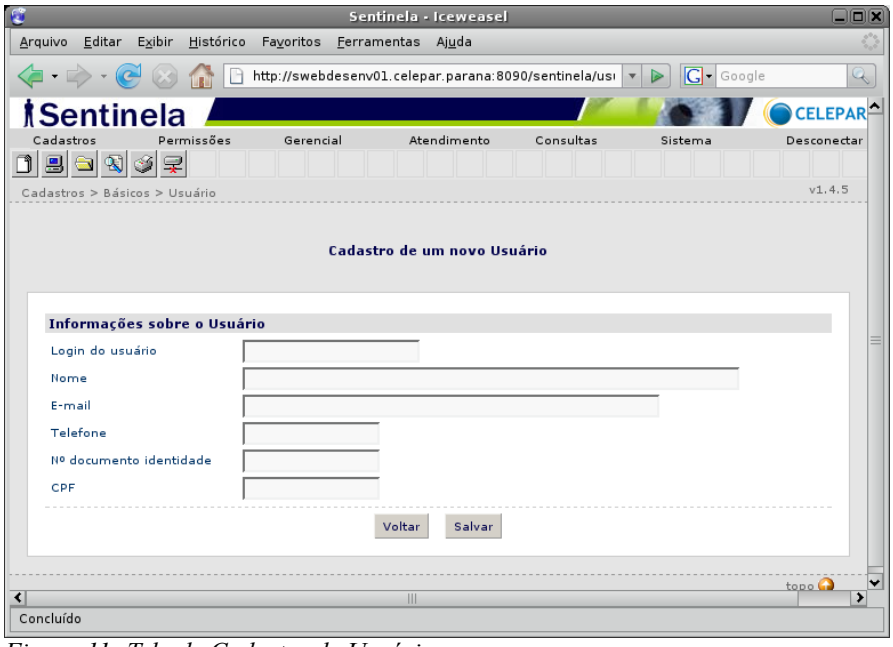

Figura 11: Tela de Cadastro de Usuários

Agora é só preencher os campos com as informações do usuário e clicar em “Salvar”.

A senha inicial está configurada na tela de parâmetros, acessível somente para administradores. Se precisar desativar o usuário, basta clicar no ícone de alteração ao lado do nome do usuário na tela de listagem de usuários (tela anterior).

3.9 Vinculando Grupos a um Usuário

Um usuário pode ser incluído em vários grupos. As permissões dos grupos se somam quando tem permissões para o mesmo sistema. Para acessar a tela correspondente, ir em: Permissões > Direitos > Usuário à Grupos. A tela de vinculação do usuário a grupos será aberta e deve-se localizar o usuário que quer vincular no grupo. Clicar no ícone de pesquisa de usuários para localizá-lo. Ao final desta operação serão exibidos os grupos para os quais este usuário tem acesso. Para remover ou incluir novos grupos basta selecionar na caixa adequada e usar os botões com setas para passar os grupos de lado. Ao final da operação clicar no botão "Salvar". Os grupos que aparecem são somente os que o usuário logado tem acesso de manutenção, assim pode ser que o usuário a ser pesquisado tenha mais grupos vinculados além dos que o usuário logado está vendo. Na Figura 12 é exibido um exemplo da vinculação dos grupos ao usuário.

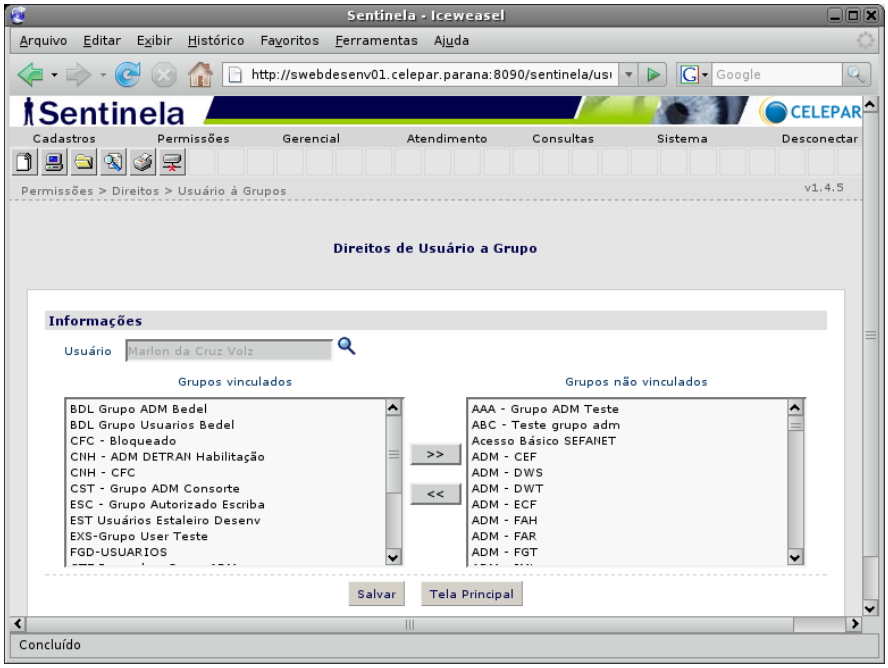

Figura 12: Tela de Vinculação de Usuários a Grupos

3.10 Vinculação de Usuários a um Grupo

Para facilitar a inclusão de vários usuários a um grupo apenas, a função Vincular Usuários a um Grupo foi disponibilizada. Nela, deve-se primeiro escolher o sistema do qual o grupo faz parte. Após escolhido o sistema, deve-se escolher o grupo ao qual deseja-se adicionar os usuários. Selecionando o grupo aparecerá uma lista povoada com os usuários que estão vinculados atualmente a esse grupo. Para adicionar um usuário, basta clicar no botão "+", e uma tela de busca de usuário aparecerá, permitindo a busca do usuário desejado na base de dados. Para se excluir usuários, basta que o usuário seja selecionado na caixa e o ícone "–" seja clicado. Após todas as alterações terem sido feitas, o clique no botão Salvar grava os vínculos desses usuários com esses grupos. A tela de Vinculação de Usuários a um Grupo pode ser vista na Figura 13.

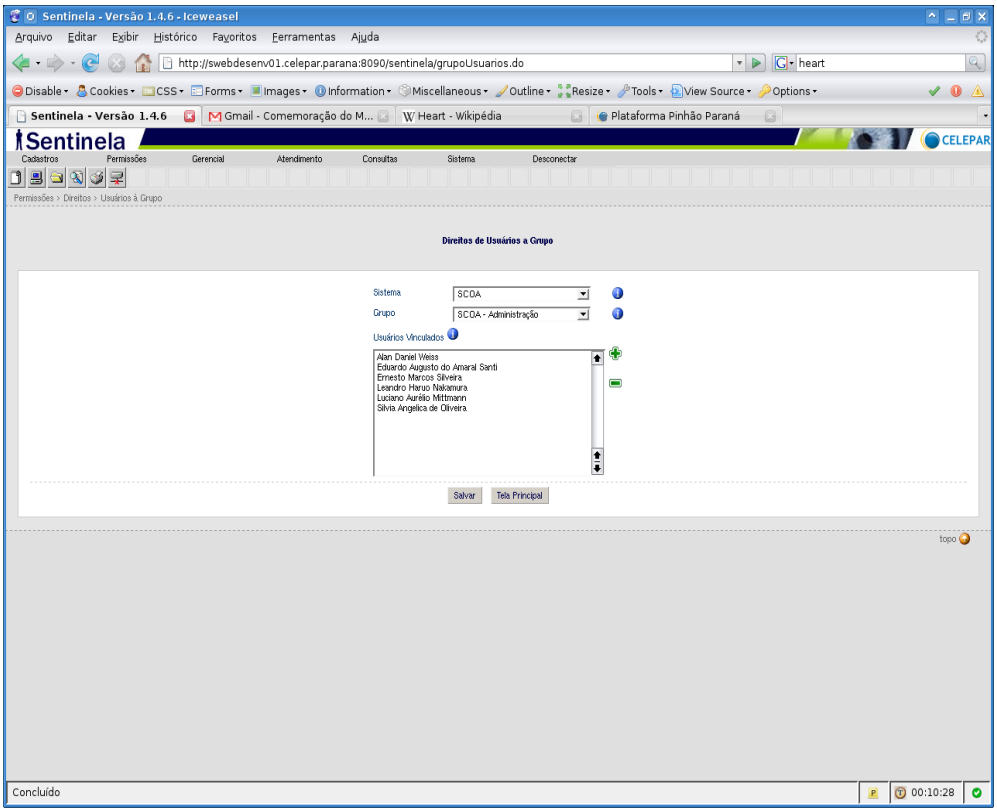

Figura 13: Vinculando Usuários a um Grupo

3.11 Vinculação de Grupos a Sistema

Com os grupos criados e os usuários vinculados a eles, falta definir o que cada grupo acessa, e para isso é necessário primeiramente vincular grupos a sistemas. Clicar na opção: Permissões > Direitos > Grupos à Sistema. Será exibida uma tela conforme Figura 14.

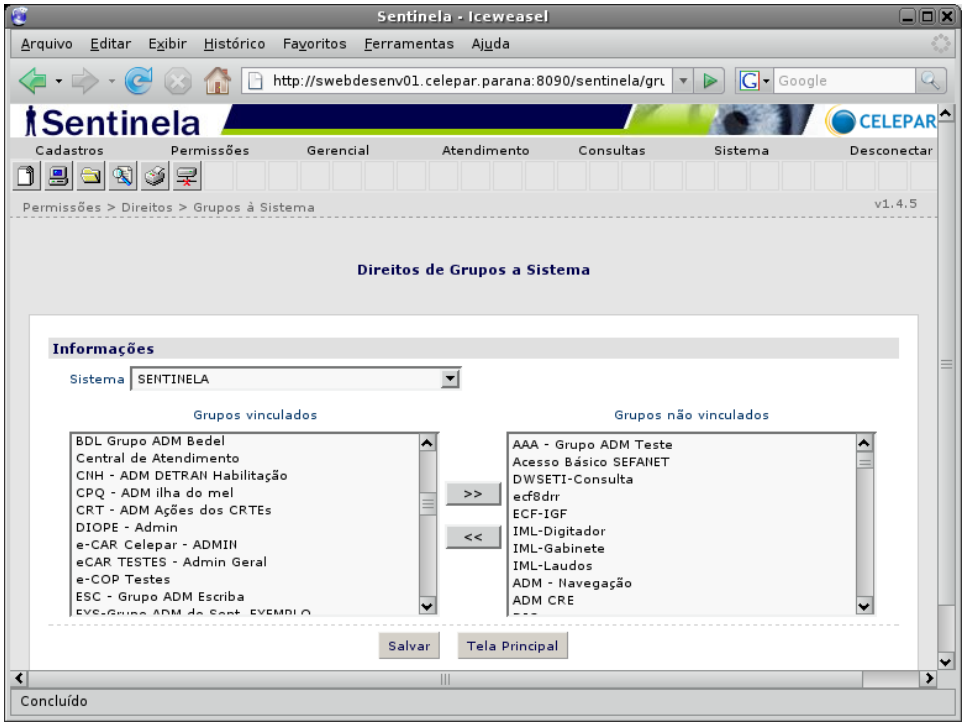

Figura 14: Vinculação de Grupos a Sistema

Primeiramente selecionar o sistema desejado, as caixas com os grupos vinculados e os grupos não vinculados serão preenchidas. Para vincular ou desvincular, basta mover os grupos de um lado para outro e clicar no botão “Salvar”. Nesta tela o usuário logado verá todos os grupos, pois como administrador do sistema pode escolher quais grupos terão acesso.

Após esta vinculação, os usuários dos grupos colocados na caixa “Grupos Vinculados” já conseguem se logar no seu sistema, porém não conseguirão ver nenhuma função ainda. Este vínculo será mostrado no tópico abaixo.

3.12 Direitos de Acesso às Funções

Esta é a última das operações básicas necessárias para a manutenção de segurança para os sistemas acoplados ao Sentinela.

Até o momento foram criados todos os itens necessários e atribuída permissão para os grupos acessarem os sistemas. Neste ponto serão definidas as permissões que cada grupo irá acessar. O grupo destinado a tirar relatórios terá apenas as funções de relatório habilitadas, o grupo que pode cadastrar determinados itens, somente poderá acessar estas telas de cadastros e assim por diante. Para acessar a tela que possibilita este controle clicar em: Permissões > Direitos > Funções a grupos. Será exibida uma tela conforme Figura 15.

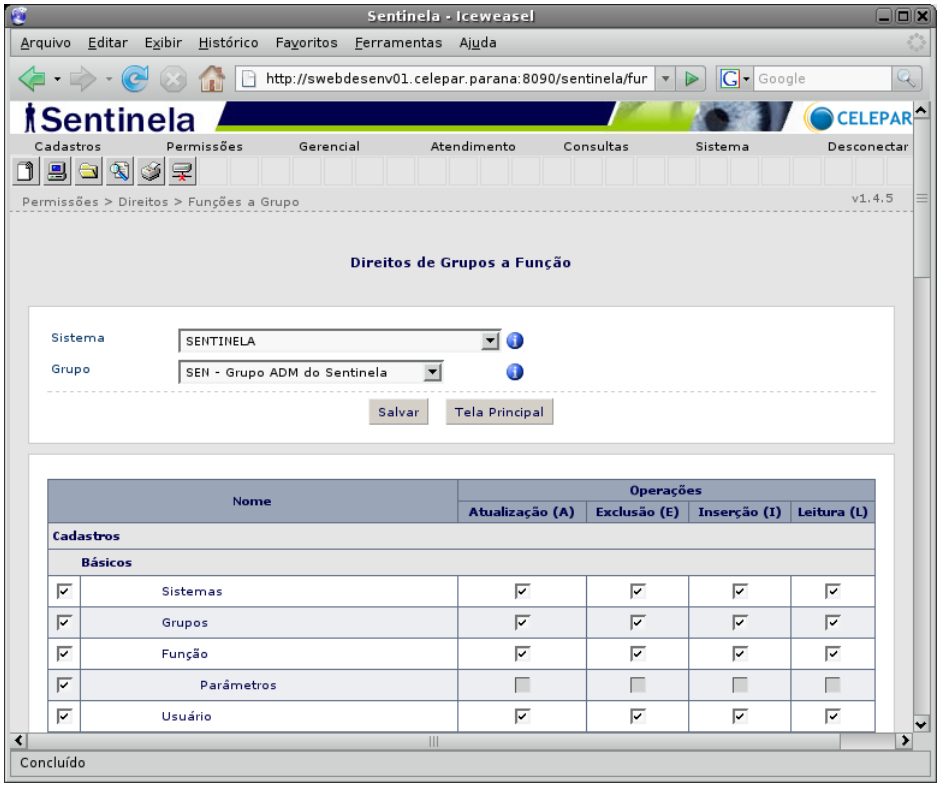

Figura 15: Tela de Atribuição de Direitos de Acesso às Funções

Ao abrir esta tela, selecionar o primeiro combo com o sistema para o qual se quer atribuir os direitos. Em seguida selecionar o grupo. Os grupos que aparecem neste combo são os vinculados ao sistema, assunto abordado no tópico anterior. Uma listagem de funções será

gerada com a estrutura de funções que foi cadastrada para o sistema. Somente as funções aparecerão. Exceções, funções auxiliares e genéricas não são passíveis de direitos, sendo que funções auxiliares herdam os direitos atribuídos às funções vinculadas e as exceções são consideradas públicas. Qualquer dúvida em relação a exceções e funções auxiliares consultar o tópico correspondente.

Marcar as funções as quais deseja-se que o grupo acesse, basta clicar na caixa correspondente. É necessário efetuar esta operação para todos os grupos vinculados a este sistema. Ao final clicar no botão "Salvar". Logo após realizada esta operação, o usuário poderá visualizar as funções acessíveis pelo seu menu. Existe um tempo de cache que deve ser considerado se o usuário já estiver logado ao sistema.

Observar que a esquerda da tela existem colunas com caixas de seleção. Estas colunas referem-se às "operações" que serão abordadas no próximo capítulo.

4 FUNCIONALIDADES AVANÇADAS NO SENTINELA

O Capítulo 3 abordou as funcionalidades básicas que praticamente todos os sistemas utilizam. Neste capítulo serão abordados outros recursos do Sentinela, como o uso das operações nas funções, bloqueios temporários de grupos, bloqueios temporários de funções, desativação de usuários e procedimento de ajuda ao usuário pela central de atendimento.

4.1 Operações

As operações são recursos do Sentinela que permitem filtrar determinadas ações que podem ser feitas em uma determinada função. Um exemplo para isto seria uma função do tipo cadastro, onde em uma única tela é possível consultar, gravar, atualizar e excluir. Existem grupos que poderão somente consultar, outros inserir e outros podem fazer todas as operações.

Como o Sentinela efetua a interceptação da requisição, não há como prover um bloqueio nesta situação, pois faz parte da lógica do sistema hospedeiro. Para contornar este problema o Sentinela usa um cadastro de operações que indica o que cada grupo pode fazer à nível de operações (consulta, inserção, atualização e exclusão, por exemplo). O Sentinela libera a requisição e informa ao sistema hospedeiro por meio de uma *taglib* e de sua interface quais operações desta função podem ser acessadas. Fica sob a responsabilidade do sistema hospedeiro efetuar as ações necessárias, para que não seja possível efetuar as operações indevidas. Consultar o manual de acoplamento para obter informações sobre como usar a interface do Sentinela e a *taglib* de operações.

As operações são definidas por Sistema, sendo assim o usuário logado deve cadastrar a forma como seu sistema irá interpretar as operações. Alguns sistemas utilizam a mesma tela (mesma requisição) para leitura e escrita, neste caso terão duas operações (leitura e escrita). Em outros sistemas tem-se quatro operações por requisição, como: leitura, inserção, atualização e remoção. Outros sistemas têm apenas uma opção como “privilegiado” ou

“acesso especial”. Seja qual for a denominação escolhida, o Sentinela suporta até 20 operações distintas. É importante saber que ao escolher operações elas poderão ser usadas em todo o sistema.

Com as operações fica muito fácil esconder controles como botões ou links para outras páginas, bastando usar a taglib de operações. A qualquer momento também é possível testar um acesso, bastando informar a operação desejada ou requerida em determinado momento do processamento. É importante ficar claro que o Sentinela não irá barrar nenhuma requisição devido à operações e apenas fornece um conjunto de ferramentas que permite testar e até mesmo barrar o acesso, porém o teste tem que ser feito a partir do sistema hospedeiro.

Para usar o recurso das operações, deve-se configurar os tipos de operação para o sistema, clicando em: Cadastros > Complementares > Operação. É apresentada uma tela conforme Figura 16.

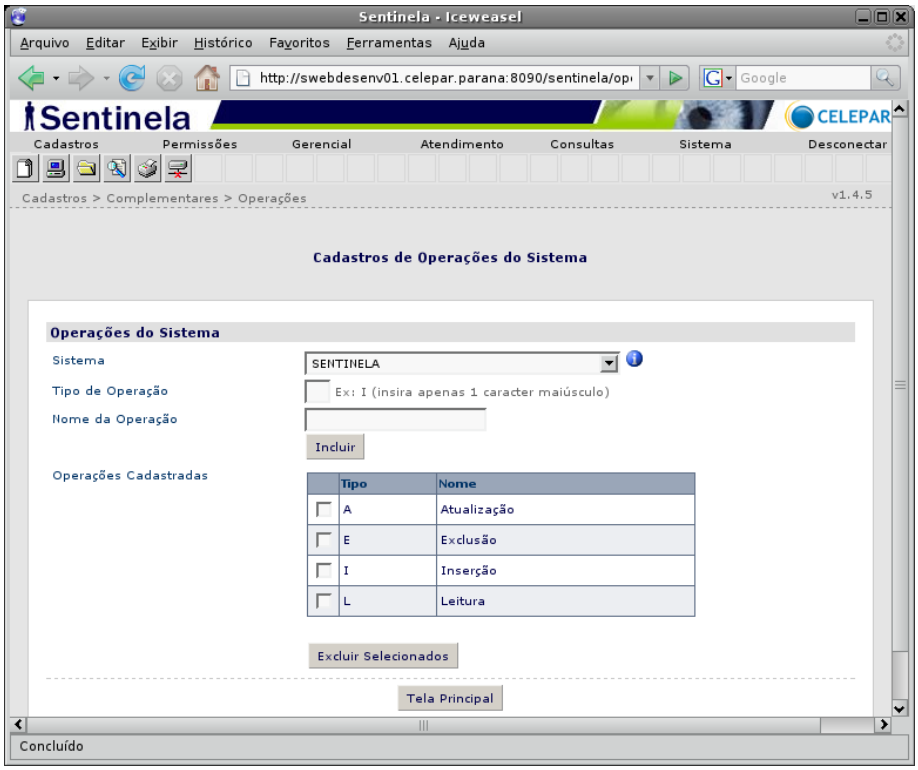

Figura 16: Configuração de Operações

Selecionar o sistema para o qual se deseja configurar as operações. Cada sistema pode ter até 20 operações diferentes e cada uma delas deverá ser representada por uma letra maiúscula. No momento do uso da *taglib* para listar as operações permitidas, serão disponibilizadas estas letras de acordo com as permissões do grupo. Preencher a letra no campo "Tipo de Operação". Descrever a operação no campo "Nome da Operação" e clicar em "Inserir". Para remover um registro incorreto basta selecionar o item desejado na listagem e clicar em "Excluir Selecionados".

As operações são cadastradas por sistemas porém pode ser que determinadas funções não usem as operações ou usem apenas algumas delas. A partir do momento em que sejam cadastradas as operações, devem ser definidas quais as funções que as utilizarão. Por padrão todas as funções anteriormente cadastradas não ficarão habilitadas a usar as operações, sendo possível atribuir estes direitos. Para efetuar esta operação entrar no cadastro de funções e clicar no ícone de atualização da função. A tela de atualização se abrirá e aparecerá a lista de operações. Marcar as caixas das operações que se aplicam à função. Ao cadastrar uma nova função, as caixas das operações já aparecerão para serem marcadas.

ATENÇÃO: As caixas de operações no cadastro de função são recursos que facilitam o cadastramento e a atribuição de direitos, porém não influenciam no funcionamento do Sentinela.

Após cadastradas as operações e atribuídas às funções, a tela de atribuição de direitos ficará como mostrada na Figura 17.

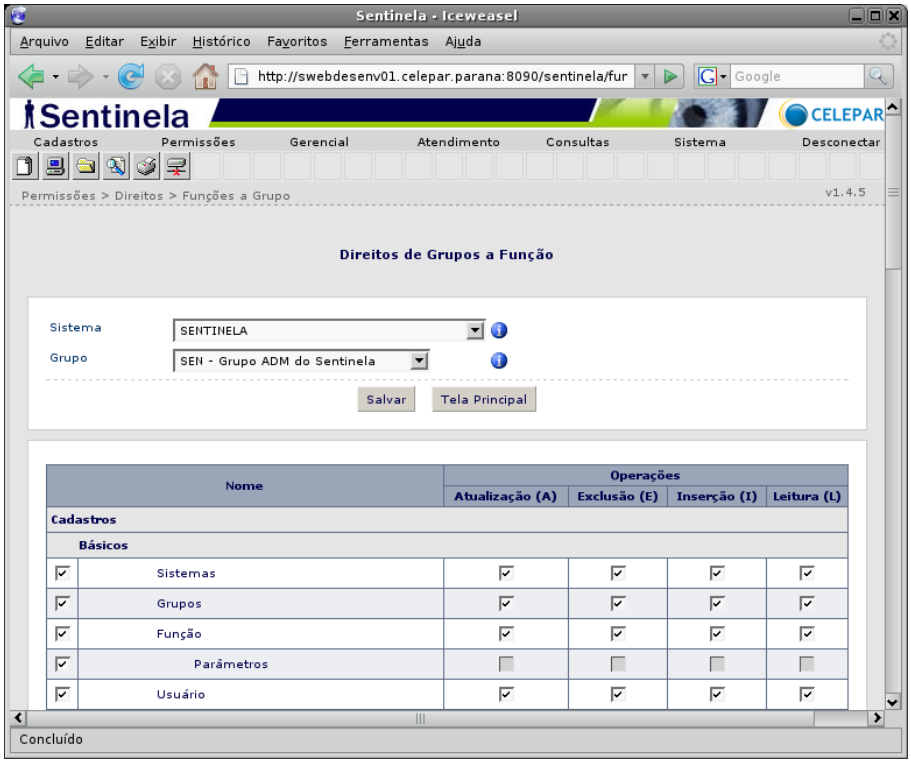

Figura 17: Operações na Atribuição de Direitos

Cada operação cadastrada para um sistema terá uma nova coluna, que além de marcar se o grupo tem acesso à função (bloqueio da requisição) através da caixa localizada a esquerda, deve marcar também a(s) coluna(s) que representa(m) as operações permitidas para o grupo. Observar que desta forma os acessos podem ter múltiplas formas. Uma requisição pode ter acesso simples ou acessos com vários níveis de privilégios. Observar também que algumas colunas aparecem desabilitadas, indicando que a operação não se aplica à função. A definição do que fica habilitado é marcado na tela de cadastro de funções.

4.2 Bloqueio de Grupos

Em alguns momentos pode ser necessário bloquear algum grupo por questões administrativas. Sem um recurso próprio para esta finalidade seria necessário modificar a definição do grupo entrando na tela de direitos, ocasionando perda das funções que são acessíveis. Estas informações teriam que ser anotadas e depois recadastradas.

Com o recurso de bloqueio de grupos, qualquer administrador de sistemas hospedeiros pode bloquear seus grupos, bastando alguns cliques. Acessar a seguinte opção de menu: Permissões > Bloqueios > Grupos. Deverá abrir uma tela conforme Figura 18.

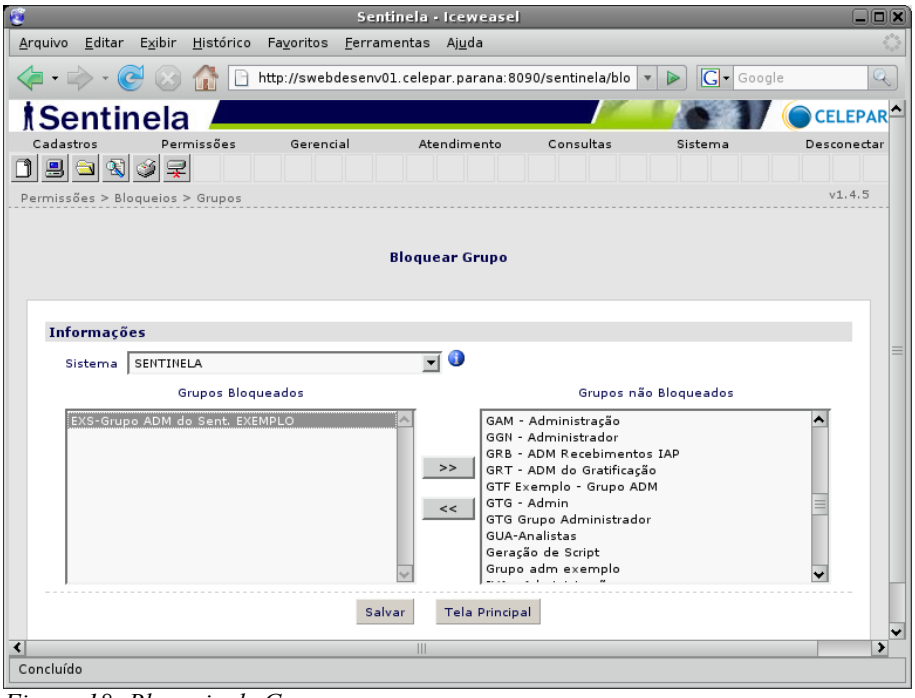

Figura 18: Bloqueio de Grupos

Selecionar no combo o sistema que possui os grupos que deseja bloquear ou desbloquear. Os grupos que acessam o sistema serão mostrados e poderão ser movidos entre as caixas de bloqueados ou não bloqueados e ao final clicar em “Salvar”.

4.3 Bloqueio de Funções

Da mesma forma que o bloqueio de grupos, o bloqueio de funções facilita a tarefa de tornar temporariamente indisponível algum recurso do Sistema Hospedeiro. Neste caso o recurso é uma função. Ao bloquear uma função, o usuário não mais visualizará no seu menu. Caso o menu já tenha sido desenhado e nenhuma atualização de página foi feita pelo seu navegador, ao clicar na opção, a requisição será barrada, sendo apresentado a tela de erro.

Para bloquear funções, clicar no seguinte item de menu: Bloqueios > Função. É apresentada uma tela conforme Figura 19.

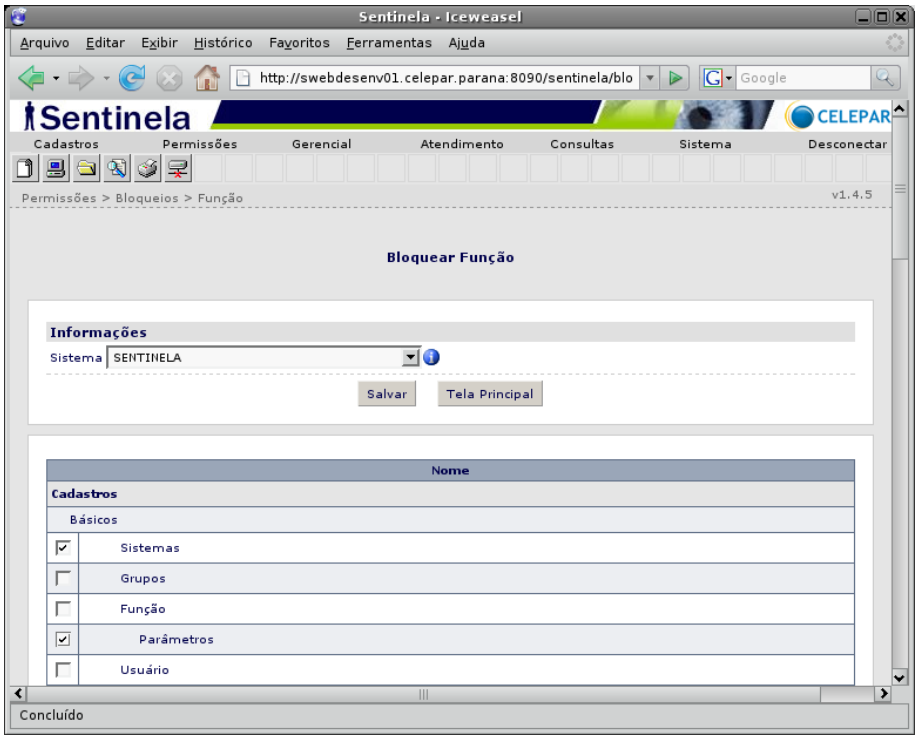

Figura 19: Bloqueio de Funções

A operação de bloqueio e desbloqueio é muito simples, basta selecionar o sistema desejado e serão exibidas as funções cadastradas. Marcar as opções que se quer bloquear e clicar em "Salvar".

4.4 Bloqueio de Usuários para um Sistema

Por questões administrativas pode ser necessário bloquear um usuário para um determinado sistema. Devido a natureza do usuário poder pertencer a diversos grupos e os grupos poderem acessar diversos sistemas, pode ficar complicado simular este bloqueio tentando-se retirar o usuário do grupo. Sendo assim o Sentinela possibilita bloquear o acesso de um usuário para um determinado sistema.

Para efetuar o bloqueio basta selecionar a opção: Permissão > Bloqueios > Usuários. Será aberta uma tela como apresentado na Figura 20.

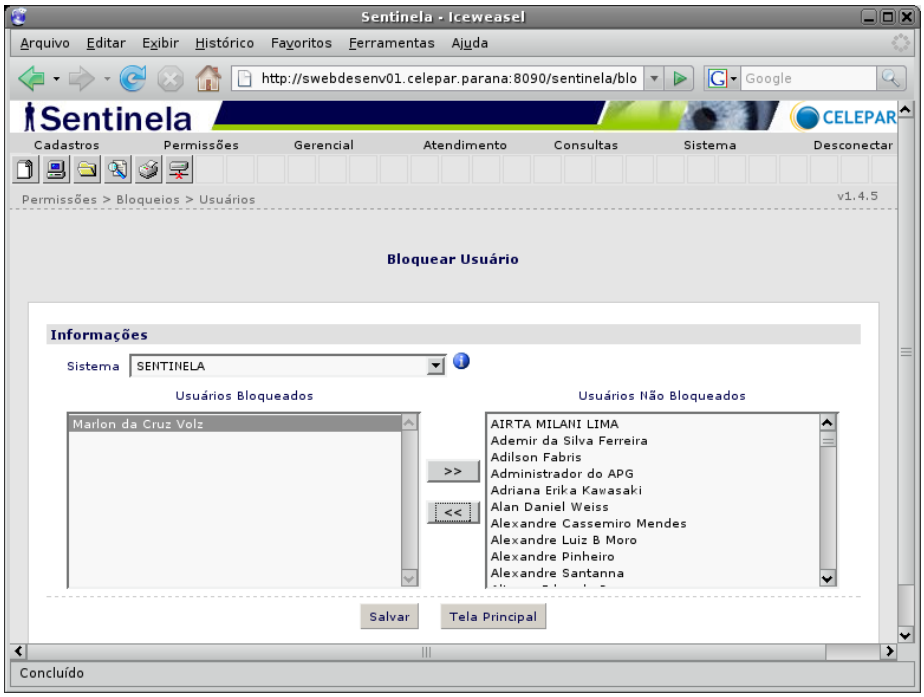

Figura 20: Bloqueio de Usuários para um Sistema

A partir desta tela basta escolher um sistema e colocar os usuários a serem bloqueados na caixa da esquerda. Após a gravação, os usuários escolhidos não poderão mais acessar o sistema.

4.5 Auxílio a Central de Atendimento – Usuários

Muitas vezes um usuário deve ser colocado como indisponível, por motivos diversos como: férias, dispensa, etc. Com sistemas descentralizados é necessário entrar em cada um e bloquear o usuário, com o risco de esquecer o bloqueio em algum sistema. Como o Sentinela trabalha com a base centralizada, basta bloquear uma única vez e em um único local para que este usuário fique indisponível em todos os sistemas que o implementam. Este recurso também está disponível na tela de Atendimento ao Usuário.

Em função do trabalho por base centralizada de usuários, existem atividades, como cadastro de usuários e atendimentos, que cabem à Central de Atendimento. Uma das tarefas de atendimento ocorre quando a senha é perdida e o usuário entra em contato para que sua senha seja alterada. O Sentinela dispõe de uma tela para esta atividade, que por questões de segurança, normalmente é acompanhada da confirmação de alguns dados para a correta identificação do usuário.

Para acessar a tela de atendimento ao usuário usar a seguinte opção de menu: Atendimento > Apoio ao Usuário. Aparecerá a tela mostrada na Figura 21.

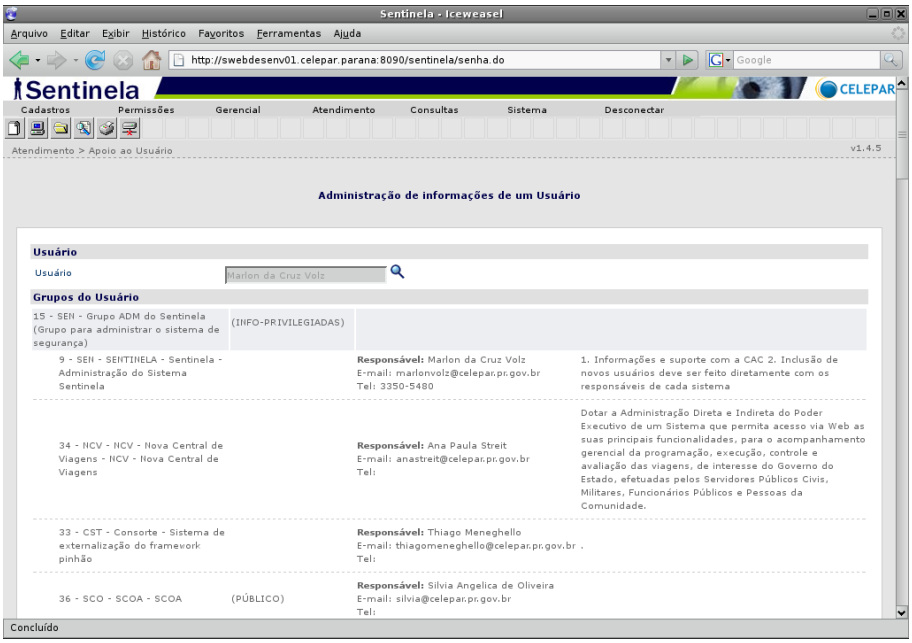

Figura 21: Tela de Atendimento ao Usuário

Selecionar o usuário desejado utilizando a pesquisa acessível por meio do ícone com o desenho de uma lupa. As informações que aparecem logo abaixo são relativas aos acessos que o usuário possui. Estas informações exibem na linha azul o grupo seguido dos sistemas acessíveis por meio do grupo. Notar que características do grupo, como "Informações privilegiadas" serão exibidas. Nas linhas que indicam os sistemas ficam disponíveis informações sobre o contato com o responsável pelo sistema. Em caso de dúvidas a respeito

de um sistema, a central de atendimento poderá utilizar esta informação.

Pode ser que o mesmo sistema se repita em outras linhas. Isto ocorre em situações onde o usuário tem mais de um grupo e mais de um grupo acesse o mesmo sistema. Apesar de acessar o mesmo sistema, podem ocorrer diferenças nas permissões. Neste caso valem os maiores privilégios.

Após a tabela indicativa dos grupos e sistemas acessíveis, estão as informações sobre o usuário e algumas opções, conforme é apresentado na Figura 22.

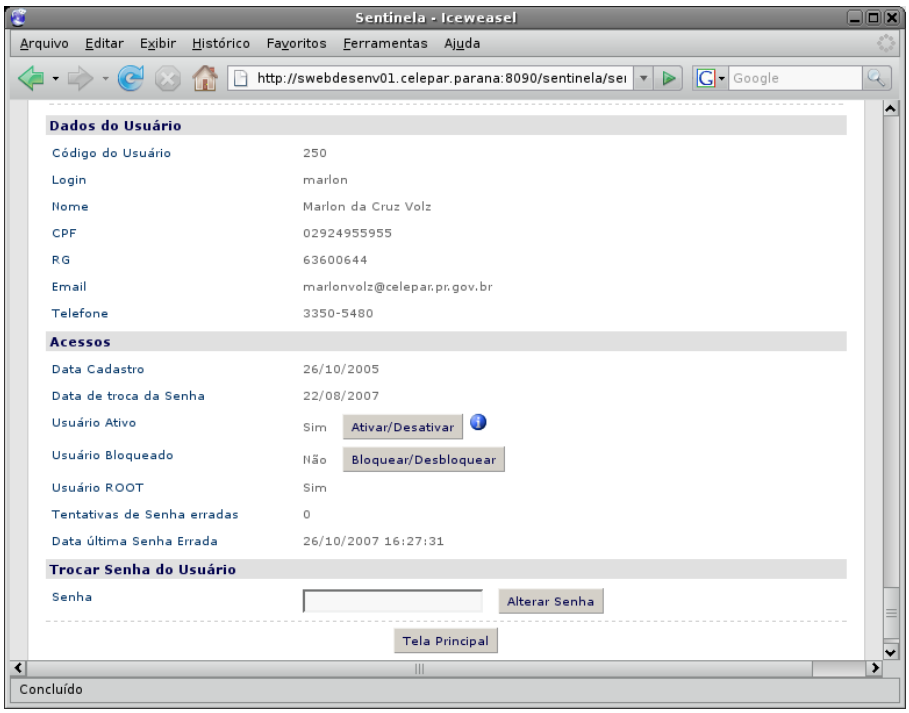

Figura 22: Tela de Troca de Senha, Desbloqueio e Reativação de Usuários

Nesta tela existem informações que podem ser confirmadas com o usuário. Logo abaixo contêm informações a respeito de acessos. As opções de ativação/desativação (em caso de desligamento) e bloqueio/desbloqueio (do usuário) podem ser feitas ao clicar no botão correspondente.

Uma melhoria que foi incorporada ao sistema na versão 1.4.6, foi a criação de uma tela de atendimento ao usuário com restrição de hierarquia de grupos. Essa tela permite que os

administradores possam gerenciar acessos e bloqueios/desbloqueios de usuários que pertençam ao mesmo grupo do administrador ou à grupos-filhos do grupo do administrador.

ATENÇÃO: Por definição o usuário é bloqueado após uma determinada quantidade de tentativas de acesso com a senha incorreta (padrão: 10 tentativas).

ATENÇÃO: O usuário é automaticamente desativado se não usar sua chave por um determinado tempo (padrão: 6 meses).

ATENÇÃO: As definições padrão podem ser alteradas. Consultar o cadastro de parâmetros gerais no manual do administrador para obter detalhes.

4.6 Restrição por Horário

As restrições por horário permitem que seja atribuído horário de início e fim para acesso a determinados recursos. Ao cadastrar uma restrição por horário, o Sentinela passará a monitorar as requisições levando em conta a hora e o recurso que recebeu a atribuição. Os recursos que podem ser bloqueados por horário são: sistema, função e grupo. Para acessar estas opções, ir no item de menu: Permissões > Restrições por Horário > **Recurso**. Será vista uma listagem das restrições para o recurso escolhido. Para inserir uma nova restrição clicar na opção inserir. Abrirá uma tela como a apresentada na Figura 23.

Figura 23: Tela de Restrição de Horário para Função

Escolher o sistema que contém a função, indicar uma data inicial para a vigência da restrição e uma data final. Pode-se deixar em branco para indicar "indefinido". Clicar em "Salvar e Continuar". Será então exibida a segunda parte do cadastramento, que é similar a tela de alteração das restrições. O usuário pode cadastrar as funções que deseja restringir escolhendo o horário de início e fim e dia da semana. Pode inserir quantos registros quiser, conforme apresentado na Figura 24.

ATENÇÃO: O Sentinela não opera com feriados. Caso seja necessário um horário especial para um determinado dia, deve ser cadastrada uma nova restrição de horário com data início e data fim para o dia específico.

ATENÇÃO: O exemplo aborda a restrição de funções. Caso necessite restringir o sistema inteiro, usar a opção de restrição de sistema.

ATENÇÃO: Se forem cadastradas diversas restrições com horários comuns, será considerado o somatório delas, ficando o mais restrito possível. Cuidado para não criar situações inesperadas ao cadastrar muitas restrições por horário.

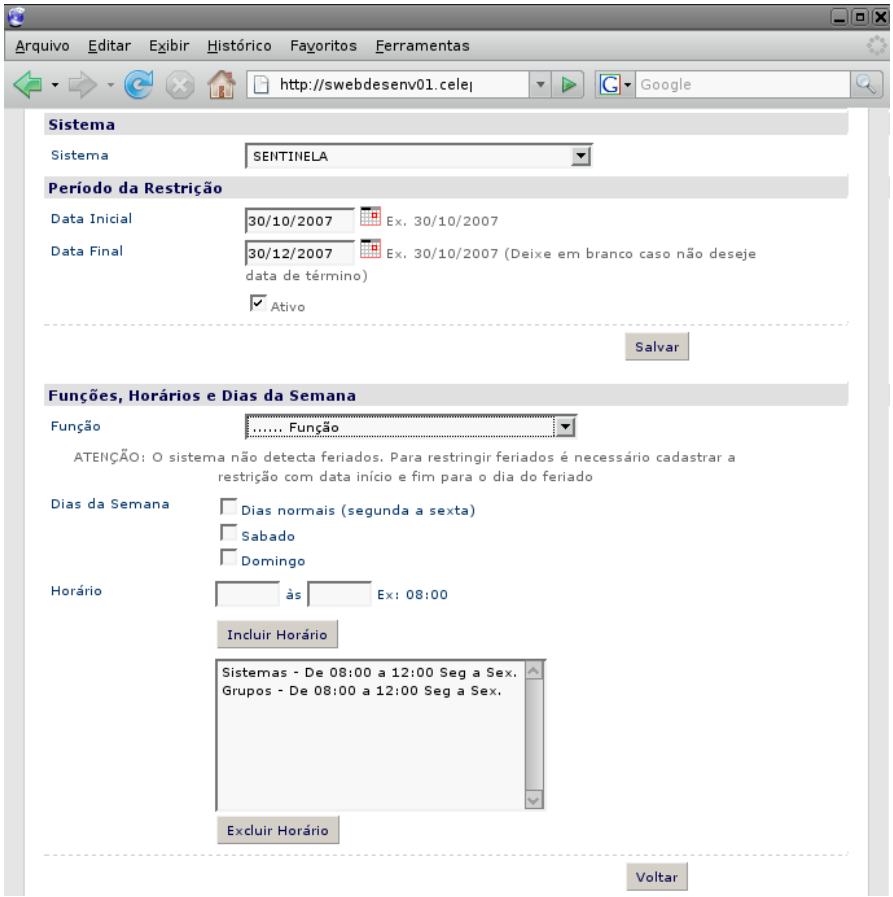

Figura 24: Restrição por Horário - continuação

O usuário pode a qualquer momento desativar a restrição e ativar posteriormente, bastando retirar a marca da caixa de seleção correspondente. Observar que o Sentinela mudará o comportamento quando forem cadastradas requisições deste tipo. Ao encontrar alguma restrição, ela somente será liberada se encontrar um registro que corresponda ao horário no momento do processamento da requisição. Ao cadastrar uma restrição por horário e não inserir nenhum item, a requisição será barrada por não encontrar um registro liberando o horário atual.

O cadastro de restrição de sistema e grupo são similares às restrições de função, porém abordam diferentes recursos. Observar que ao restringir um grupo, pode ser que determinado usuário possua outro grupo sem a restrição de acesso e este usuário notará uma mudança no seu menu a partir de determinado horário.

ATENÇÃO: O horário levado em consideração é o horário do servidor.

ATENÇÃO: Recomenda-se que sejam feitos testes com este recurso a fim de evitar surpresas. Deve-se assegurar que houve bom entendimento a respeito do funcionamento deste recurso, antes de disponibilizá-lo para os usuários.

4.7 Sistema de Mensagens

Este recurso pode ser usado pelos sistemas cliente para a exibição de mensagens e/ou avisos diversos. É necessário que o sistema implemente a *taglib* de mensagens na tela de boas vindas. Detalhes sobre a *taglib* consultar o Manual de Acoplamento.

As mensagens podem ser cadastradas por qualquer usuário administrador que tenha permissão neste cadastro. O escopo de visibilidade da mensagem é de acordo com suas permissões. O usuário cadastrante pode registrar uma mensagem e definir os sistemas e grupos que podem ler. Para acessar o cadastro de mensagens deve-se ir até a seguinte opção de menu: Gerencial > Mensagens. Será exibida uma lista de mensagens cadastradas. Para incluir uma nova mensagem clicar no botão "Inserir". Será aberta uma tela de acordo com a apresentada na Figura 25.

Preencher: o campo "Nome para a Mensagem" com um nome curto, o campo "Mensagem" com o texto correspondente, os campos "Data Inicial" e "Data Final" com a respectivas datas de vigência. Podem ser incluídos *tags html*, porém deve-se tomar o cuidado para não colocar *tags* que deterioram a tela de boas vindas. Lembrar-se que cada sistema tem um *layout* que deve ser respeitado. Também não usar links diretamente. O correto é direcionar um *link* para uma nova janela a fim de não prejudicar o uso do sistema. Cuidar para não colocar mensagens longas e lembrar-se que diversas mensagens poderão aparecer além daquela que se está cadastrando.

O campo “Grupo para Manutenção” indica a permissão de quem pode alterar ou excluir esta mensagem. Por motivos de segurança, o cadastrante tem seu nome e a data/hora gravados para posterior conferência.

Os sistemas que o usuário cadastrante tem acesso aparecem em forma de caixas de seleção, bem como os grupos. O usuário deve marcar os sistemas para os quais ele deseja que suas mensagens sejam exibidas.

ATENÇÃO: Não existem formas de garantir que as mensagens serão lidas pelos usuários, uma vez que o uso da *taglib* de mensagens é opcional.

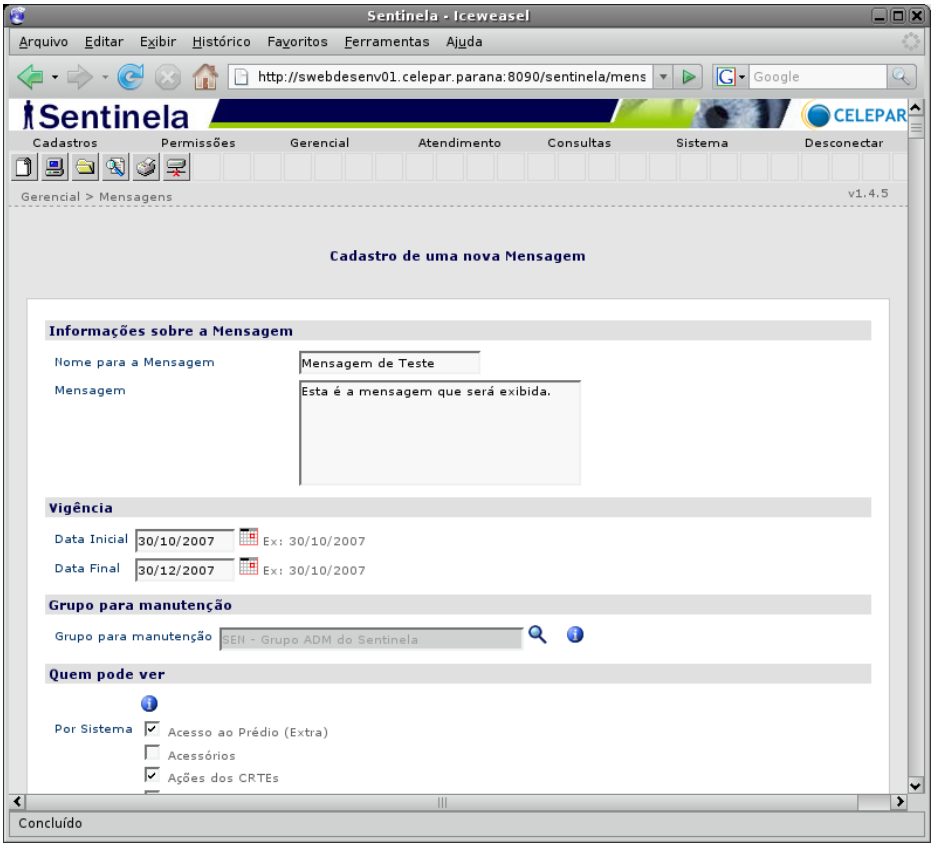

Figura 25: Tela de Cadastramento de Mensagens

4.8 Barra de ícones

A fim de prover maior praticidade para seus usuários, o Sentinela incluiu uma barra de ferramentas que simula clique no menu. Este recurso é muito conhecido em sistemas *stand-alone* onde um ícone representa um atalho para uma opção do menu. Para usar este recurso, primeiramente é necessário usar a *taglib,* correspondente nas páginas do sistema hospedeiro. Informações sobre a *taglib* está no Manual de Acoplamento.

Com a barra de menus incorporada às páginas do sistema hospedeiro, basta efetuar um cadastramento simples dos ícones que poderão aparecer. Acessar a opção: Cadastros > Complementares > Ícones. Abrirá uma tela como a apresentada na Figura 26.

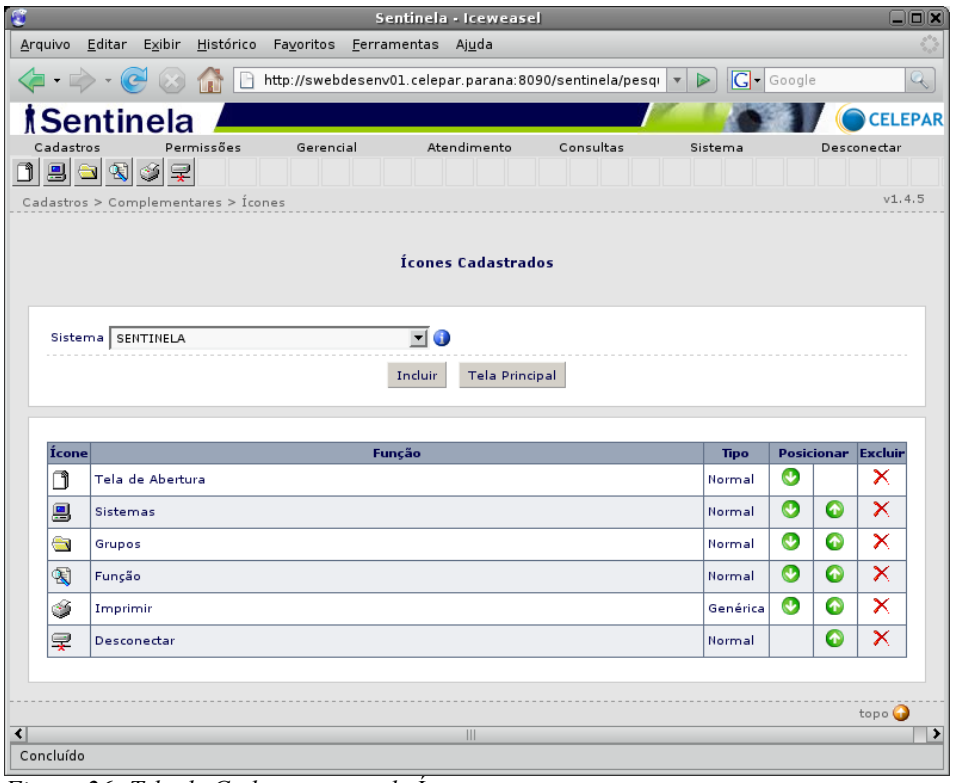

Figura 26: Tela de Cadastramento de Ícones

Cada linha da tabela representa um ícone a ser incluído na barra de ferramentas do sistema hospedeiro. A ordem de exibição pode ser ajustada nesta tela, bastando clicar nas setas para cima ou para baixo. Caso queira incluir um novo ícone basta clicar na opção incluir. Será exibida uma tela como a apresentada na Figura 27.

Escolher uma função no combo e um ícone, em seguida clicar em “Salvar”. O usuário será redirecionado para a tela com a listagem dos ícones cadastrados e poderá ajustar o seu posicionamento. Podem ser cadastrados como ícone e constar na barra de ferramentas as funções e as funções genéricas.

ATENÇÃO: Somente aparecerão os ícones caso o sistema hospedeiro implemente a taglib da barra de ícones nas suas páginas.

Os ícones aparecerão na barra de ferramentas (também conhecido como barra de ícones) se o usuário tiver permissões para acessar as funções. Desta forma a barra poderá apresentar-se diferente para usuários com diferentes permissões.

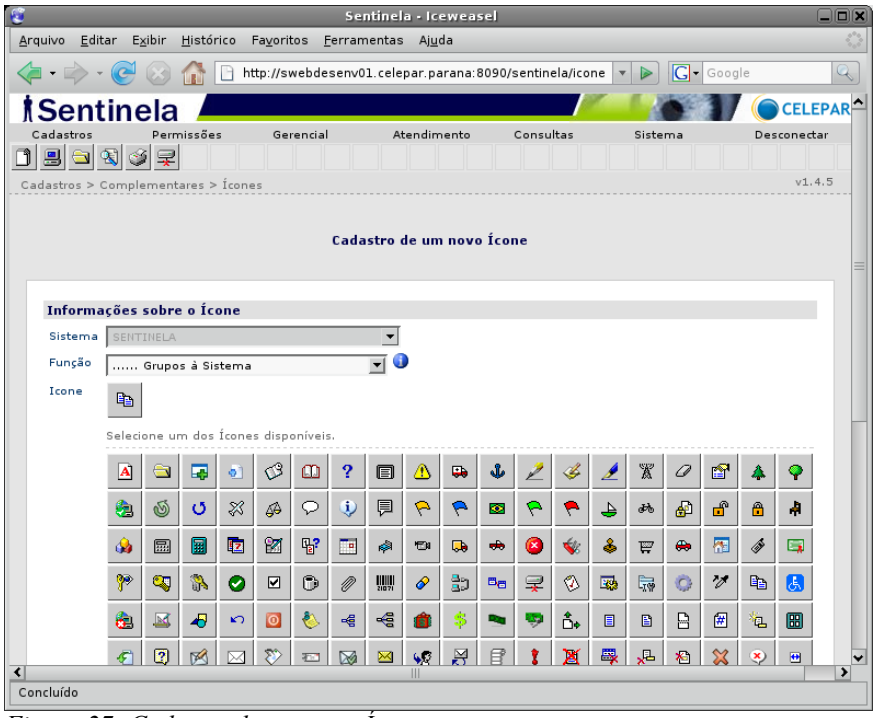

Figura 27: Cadastro de um novo Ícone

PERGUNTA FREQUENTE: DE ONDE VEM OS ÍCONES?

É PRECISO CADASTRÁ-LOS COMO EXCEÇÃO?

O Sentinela trata os ícones de forma diferenciada, não sendo necessário nenhum cadastro adicional e nem qualquer tipo de cópia de arquivos de imagens. O Sentinela usa a

tecnologia "*open and send stream*" onde as imagens já estão compactadas no pacote Sentinela Cliente e envia o *stream* mediante comando. Sendo assim o usuário não poderá adicionar mais imagens.

4.9 Cópia de Grupos

O cadastro de grupos já foi explicado no item 3.7 deste manual. Para acessar a tela de cópia de grupo, o usuário deverá ir até a opção: Cadastros > Básicos > Grupos. Abrirá uma tela como apresentado na Figura 28.

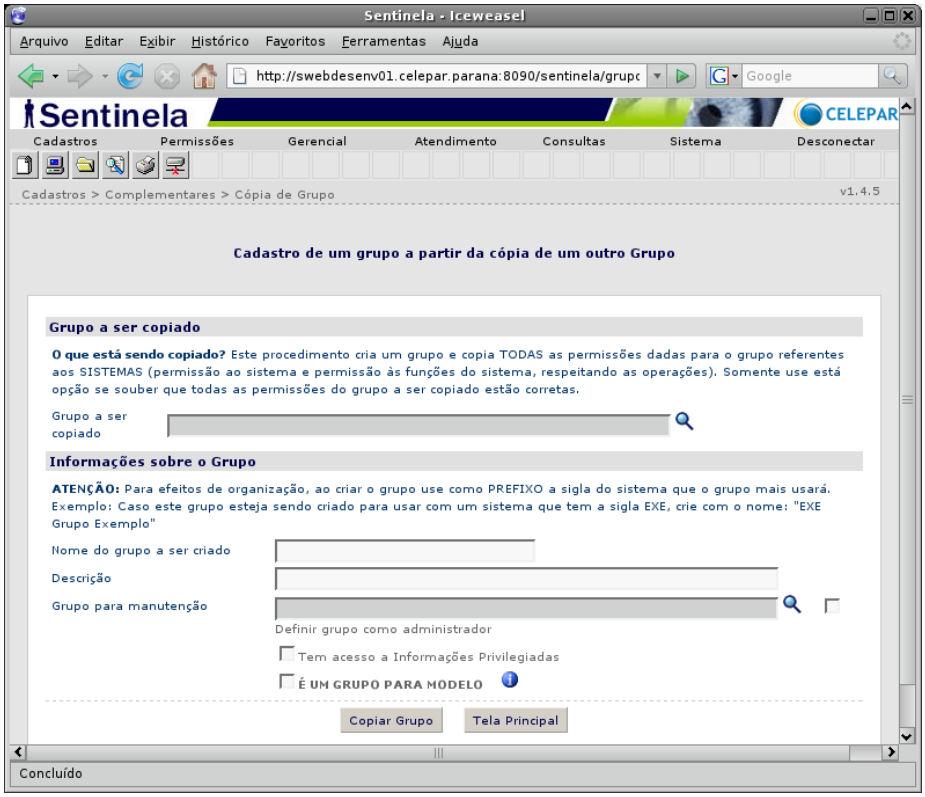

Figura 28: Tela de Cópia de Grupos

O cadastramento é similar à inclusão de um novo grupo, com a vantagem de automaticamente cadastrar todas as permissões a sistemas e funções do grupo copiado. Apenas deve-se indicar o grupo a ser copiado e preencher o restante das informações como se

tivesse criando um novo grupo. Qualquer dúvida sobre grupos consulte o tópico 3.7 .

4.10 Sistema de Auditoria

O Sentinela conta com um esquema de auditoria simples que os sistemas podem utilizar. A auditoria em sistemas clientes pode ser ativada ou desativada e em caso de ativação, pode-se verificar os últimos acessos à requisições.

Para ativar uma auditoria não é necessário implementar nada no código do sistema cliente, salvo no caso de "mensagem de auditoria", que está detalhada no Manual de Acoplamento. Acessar a seguinte opção de menu: Gerencial > Auditoria em Sistemas > Ativação/Desativação. Verificar o sistema que se quer auditar e clicar em "Ativar/desativar auditoria". O usuário será levado a uma tela que pede algumas opções e a confirmação. No campo "Tipo de auditoria" deixar sempre em "Banco de dados", pois o tipo "Arquivo texto" é reservado para usos futuros.

A partir deste ponto o sistema cliente já está sendo auditado, para ver os registros gerados pela auditoria acessar a seguinte opção de menu: Gerencial > Auditoria em Sistemas > Relatório Auditoria. O usuário deve selecionar um sistema e opcionalmente preencher os outros campos para facilitar sua busca. Pode rastrear por data, grupo, usuário, etc. O limite de registros visualizáveis é de 3.000 linhas. A Figura 29 apresenta um exemplo desta tela.

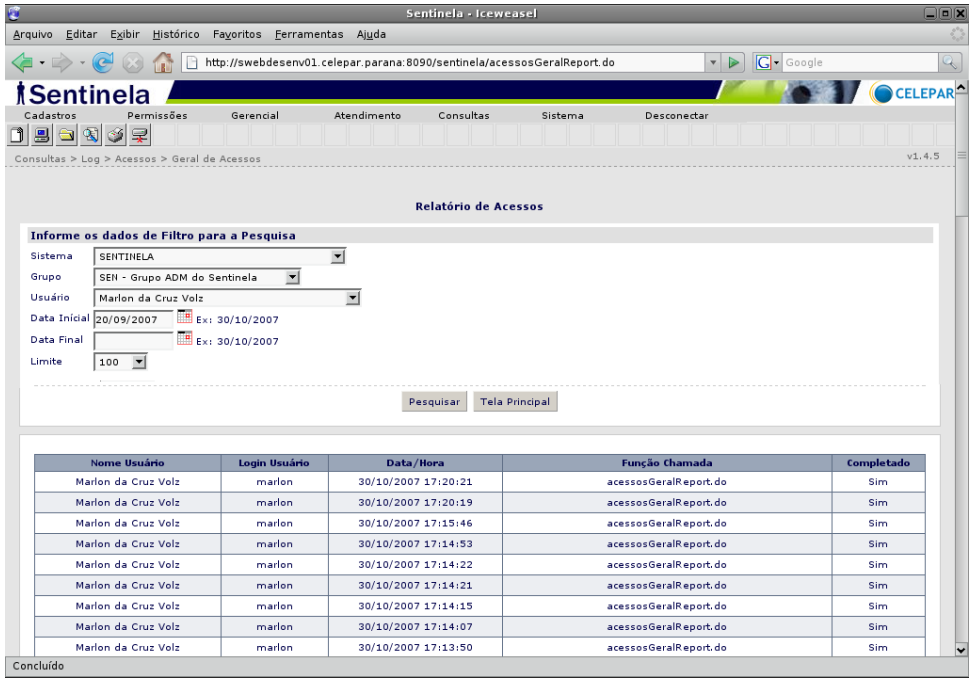

Figura 29: Relatório de Auditoria (Relatório de Acessos)

Nesta tela é apresentado o usuário, data/hora, função chamada, possível mensagem de retorno e o status da requisição. Caso o usuário tenha tentado acessar alguma requisição da qual não tem permissão (via digitação direta na linha de URL do *browser*), ficará registrada a tentativa. O Campo mensagem pode ser preenchido pelo sistema cliente através do SentinelaInterface (detalhes no manual de acoplamento).

Quando um sistema tem sua auditoria ativada ou desativada, o usuário que efetuou a operação é registrado por questões de segurança. Para visualizar operações de ativação/desativação de auditoria, acessar a seguinte opção: Consultas > Log > Ativação Auditoria. Será aberta uma tela conforme apresentado na Figura 30.

Figura 30: Relatório de Ativação/Desativação de Auditoria por Sistema

4.11 Outras funcionalidades

Além das funcionalidades abordadas neste manual, o Sentinela tem recursos como: migração de informações para o ambiente de produção, parametrização do sistema, possibilitando mudanças no comportamento, importação em massa de usuários. Estas funcionalidades são exclusivas dos administradores do Sentinela e algumas dessas funcionalidades são acessíveis ao grupo da Central de Atendimento (CAC). Esses recursos são abordados no Manual do Administrador do Sentinela (www.frameworkpinhao.pr.gov.br -> Sentinela).