Sistema Sentinela
Manual do Administrador

Setembro – 2005

Sumário de Informações do Documento

Tipo do Documento: Manual		
Título do Documento: Manual do Administrador do Sistema Sentinela		
Estado do Documento: EB (Elaboração)		
Responsáveis: Pedro Rodolfo Kalva		
Palavras-Chaves: Sentinela, Segurança		
Resumo: Esse documento contém procedimentos sobre operações realizadas por administradores do sistema Sentinela		
Número de páginas: 24		
Software utilizados: Open Office		
Versão	**Data**	**Mudanças**
1.0	13/04/05	Primeira versão do documento "Manual do administrador do Sistema Sentinela"
1.1	29/09/05	Evolução do Sentinela versão 1.2

Sumário

INTRODUÇÃO

O sistema Sentinela possui a característica de centralização, sendo assim a autonomia dos sistemas hospedeiros é relativa, pois são necessários intermediadores para executar determinadas funções que são comuns a cada um dos sistemas hospedeiros.

O administrador do sistema hospedeiro deve ter acesso a todas as funções que referem-se ao sistema administrado por ele e não deve ter acesso a itens que possam prejudicar sistemas alheios. Funções que necessitam de permissões especiais não podem ser concedidas a estes administradores, sendo este o papel do administrador do sistema Sentinela, que juntamente com outros profissionais irão realizar tarefas que necessitam deste tipo de acesso privilegiado.

ATENÇÃO: Se você não conhece em detalhes o sistema Sentinela é necessário que seja lido primeiro os manuais de Acoplagem e Usuário.

2 ATIVIDADES DO ADMINISTRADOR DO SENTINELA

O administrador do sistema Sentinela possui uma chave especial que possibilita ver e configurar qualquer informação relativa aos sistemas hospedeiros, esta situação é necessária para efetuar as tarefas atribuídas ao administrador. Entre as atribuições do administrador do Sentinela estão:

1. Cadastramento inicial do Sistema Hospedeiro.
2. Verificação de problemas.
3. Migração de usuários
4. Parametros do Sentinela

O primeiro item refere-se a instruções para atender a requisição dos clientes quando for solicitada a criação das configurações para acoplagem de um sistema hospedeiro.

O segundo item refere-se a verificação de uma funcionalidade que pode estar agindo de forma estranha, e os clientes podem não conseguir visualizar dados importantes devido a sua restrição do grupo.

A migração de usuários deve ser feita mediante solicitação da equipe que está desenvolvendo o sistema cliente. Se algum sistema exigir uma base de usuários já formada por outro sistema, pode-se utilizar a ferramenta de migração de usuários do Sentinela. Esta ferramenta efetua o cadastramento automático por meio de um arquivo texto formatado. Maiores informações estão descritas no Capítulo 3 deste manual.

A parametrização do Sentinela afeta todos os sistemas que estão integrados. Devido a sua característica centralizada, a politica de senhas será igual para todos os sistemas. O administrador deve efetuar mudanças nos parâmetros apenas em casos onde existem mudanças no ambientes ou acordo comum em alguma política de gerenciamento de usuários. Este recurso será abordado no Capítulo 4.

3 ADIÇÃO DE UM NOVO SISTEMA HOSPEDEIRO

A equipe do sistema hospedeiro deve entrar em contato com o administrador do Sentinela mediante uma solicitação formal para a inclusão do novo sistema. O administrador deve repassar os arquivos do Sentinela para a equipe de desenvolvimento, repassar o endereço dos manuais e realizar o cadastramento inicial. Para o cadastramento inicial de um sistema hospedeiro, devem ser seguidos os passos:

1. Cadastramento do sistema hospedeiro através da administração do Sentinela;

2. Criação de um grupo administrador para o sistema hospedeiro. Pode ser usado o novo recurso de cópia;

3. Atribuição do grupo para acessar o sistema Sentinela e o sistema hospedeiro. Em caso de cópia de grupo, é necessário apenas ligar ao sistema recém-cadastrado;

4. Definição dos direitos de acesso do grupo para o Sentinela. Se for usado a cópia de grupo este passo não é necessário;

5. Atribuição do(s) usuário(s) ao grupo administrador.

3.1 Cadastramento do Sistema Hospedeiro

De posse de uma chave com permissões de administração, deve-se entrar no sistema Sentinela de DESENVOLVIMENTO, entrar na tela de cadastramento de sistemas e inserir um novo sistema, de acordo com as informações enviadas durante a solicitação de criação de um novo sistema.

Os passos necessários para criar um novo sistema e as informações a serem cadastradas estão descritas em detalhes no manual do usuário do Sentinela.

3.2. Criação de um grupo administrador para o sistema hospedeiro

Deve ser criado um grupo para administrar o sistema hospedeiro. Este grupo é diferente dos grupos que serão criados para os clientes, porque deve acessar o sistema hospedeiro e o sistema Sentinela para cadastramento de funções, atribuições de direitos, etc.

Use o manual do usuário para saber como cadastrar um novo grupo. Lembre-se que o grupo que está sendo criado neste momento será para administrar o sistema cliente, portanto deve ter acesso de administrador. Marque as caixas de "Informações privilegiadas" e "É um grupo administrador" no cadastro de grupo.

O nome do grupo deve conter a sigla do sistema que foi colocado no cadastro do sistema e também deve usar as letras ADM para que fique bem clara a intenção deste grupo. Exemplo:

```
SIS – ADM do sistema Hospedeiro
```

3.3 Atribuição do grupo para acessar o sistema Sentinela e o sistema hospedeiro

Com o grupo administrador do sistema hospedeiro criado, deve-se atribuir que usuários colocados neste grupo irão acessar o sistema hospedeiro e o sistema Sentinela, isto para que seja possível a criação de funções, grupos e outras atribuições. Para efetuar esta operação clique na seguinte opção do menu: Permissões > Direitos > Grupos x Sistema.

Ao abrir a tela, selecione o sistema hospedeiro e inclua o grupo recém-criado. Em seguida adicione **o sistema Sentinela**, conforme a figura 2.1 e 2.2.

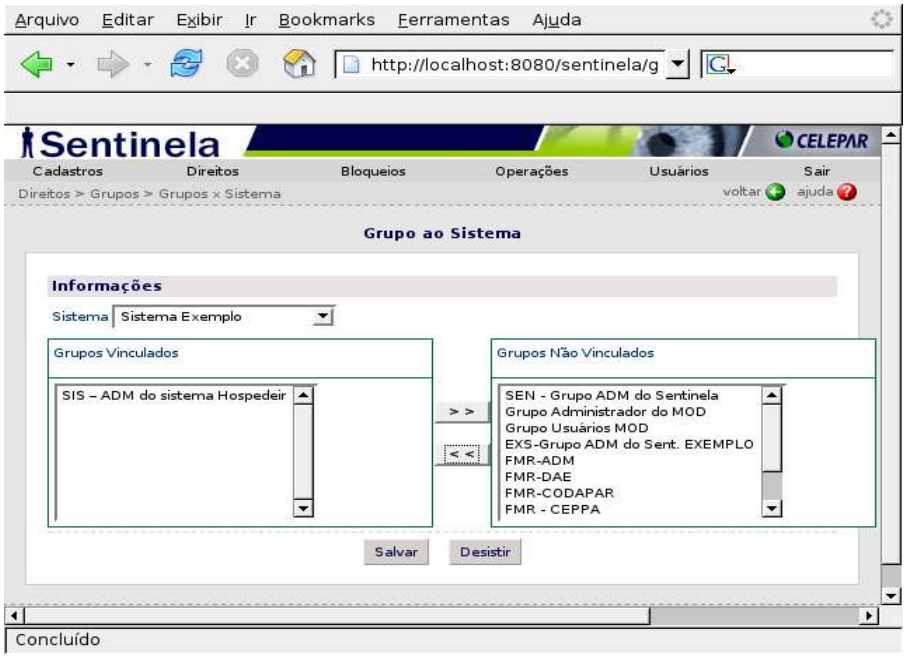

Figura 2.1 – Atribuição do grupo para acessar o sistema hospedeiro e o Sentinela

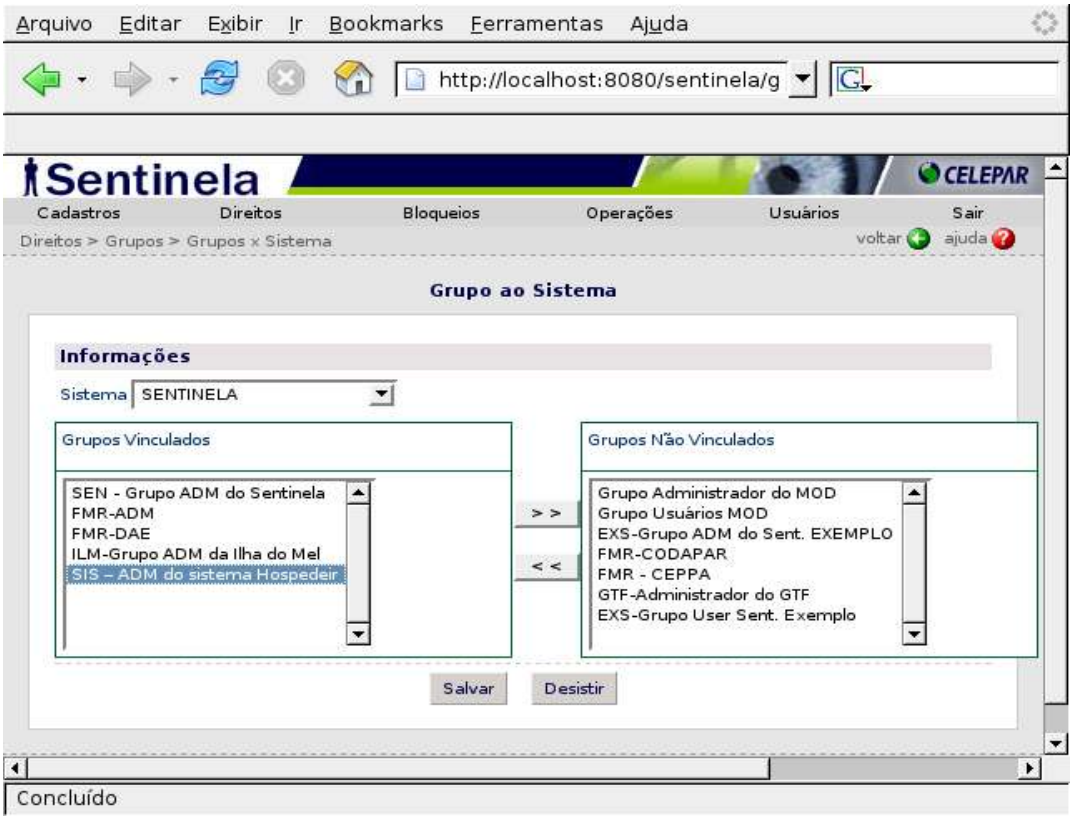

Figura 2.2 – Atribuição do grupo para acessar o sistema hospedeiro e o Sentinela

Com estas definições, todo sistema hospedeiro tem pelo menos um grupo

administrador que pode fazer login no sistema Sentinela. Este grupo será o responsável pela manutenção e atribuição de direitos para seu sistema.

3.4. Definição dos direitos de acesso do grupo para o Sentinela

Neste ponto, o grupo pode apenas efetuar logon no sistema Sentinela. Para atribuir os direitos de acesso deve-se entrar no seguinte item de menu: Direitos > Grupos > Grupos x Função.

ATENÇÃO: Neste formulário deve ser selecionado o sistema Sentinela, e não o sistema hospedeiro, pois trata-se de liberar funções de manutenção que fazem parte do sistema Sentinela.

No anexo estão as opções e acessos que deve ser colocado para o grupo recém criado. Estas opções podem mudar com o tempo de acordo com alguma mudança estratégica ou política, definido pelos administradores do sistema Sentinela.

3.5. Atribuição de Usuários para o Grupo Administrador

Finalmente basta cadastrar/vincular os usuários responsáveis pela administração do sistema hospedeiro no grupo criado. Para fazer isto deve-se cadastrar o novo usuário (se já não estiver cadastrado) através opção de menu: Cadastros > Básicos > Usuário. Consulte o manual do usuário do sistema Sentinela para saber como efetuar esta operação.

Após o cadastramento, deve-se colocar o usuário no grupo criado. Para isto use o seguinte item de menu: Permissões > Direitos x Usuário > Usuário a Grupo.

Pesquise o usuário desejado. Será exibida uma lista de grupos criados e de grupos associados ao usuário. Coloque-o também no grupo recém-criado.

ATENÇÃO: Não altere os outros grupos cadastrados, pois este usuário pode fazer parte de outros sistemas. COLOQUE APENAS O GRUPO RECÉM-CRIADO.

A tela com um exemplo de atribuição de grupos está na figura 2.3.

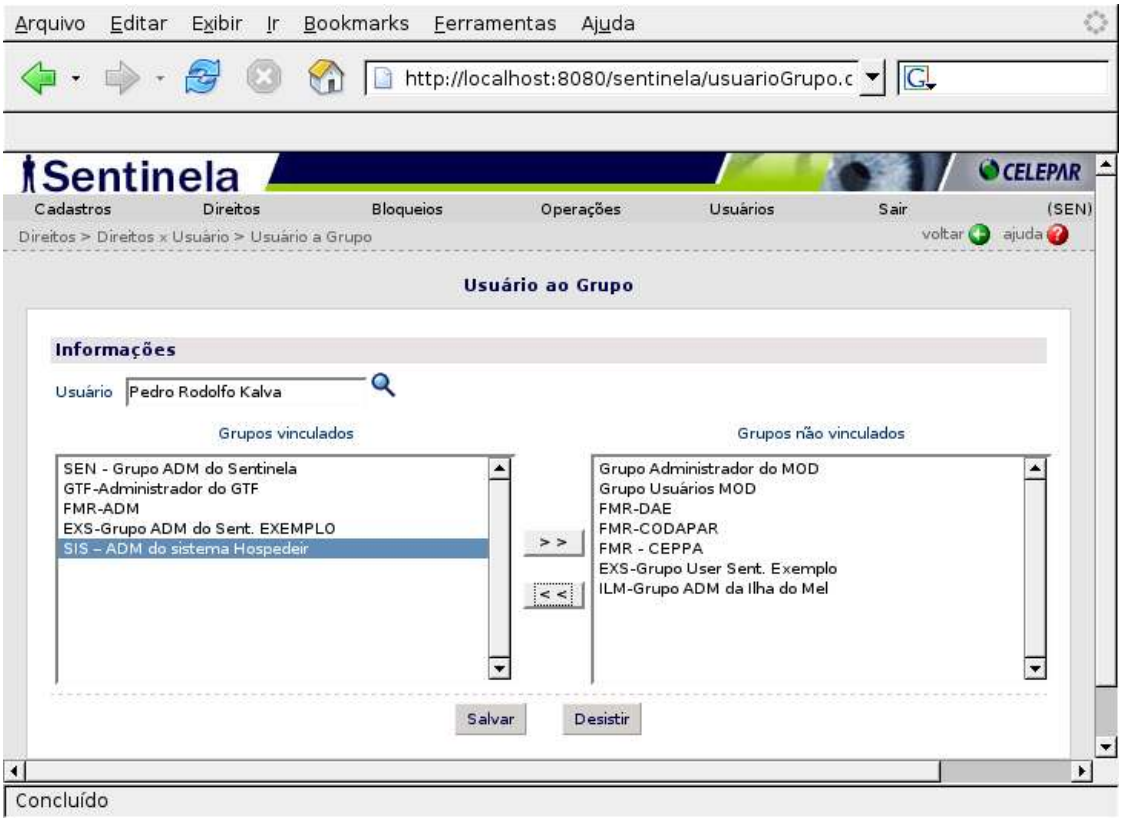

Figura 2.3 – Tela de atribuição de Grupos à Usuários

Após todos estes passos, os usuários vinculados ao grupo recém-criado já podem efetuar login no sistema Sentinela para ajustes e cadastramentos necessários.

3.6. Cópia de grupo

A fim de facilitar todo o trabalho do visto neste capítulo, o Sentinela versão 1.2 contém um novo recurso denominado de “cópia de grupo”. Neste recurso deve ser previamente cadastrado um grupo com a caixa de seleção “*Modelo*” marcada (consulte o manual do usuário para saber como fazer esta operação).

O grupo de modelo deve ter suas permissões ajustadas como o acesso ao sistema Sentinela e as opções que constam no anexo marcadas. Deve também receber as marcas de “grupo administrador” e “informações privilegiadas”. De um nome e descrição que identifique a funcionalidade deste grupo.

Com o grupo de modelo cadastrado e pronto, quando houver um procedimento de criação de novo sistema, as tarefas são reduzidas. Basta criar o novo sistema (tópico 2.1), criar o grupo através da cópia do grupo modelo, atribuir a permissão para acessar o sistema recém criado e colocar o usuário solicitante como integrante deste grupo copiado. Note que a atividade que demanda maior tempo no processo, sem o uso da cópia, é justamente ter que atribuir permissões em funções do Sentinela para o grupo recém criado.

4 MIGRAÇÃO DE USUÁRIOS

A cada dia novos sistemas são publicados. Muitos destes são atualizações que substituem um sistema antigo e a base de usuários necessita ser preservada. Para facilitar este processo, o Sentinela possui uma ferramenta para migrar usuários de outras bases de dados por meio de arquivos textos. Basta formatar um arquivo texto do padrão exigido pelo Sentinela e este será analisado e então migrado para a base de usuários do Sentinela.

O Sentinela efetua uma análise dos dados do arquivo, buscando usuários com similaridades, para que não haja duplicatas. Com as similaridades resolvidas, pode-se importar os usuários e, opcionalmente, já incluí-los em algum grupo. O Sentinela irá gerar informações para retorno, que podem ser usadas em outras etapas da migração por parte do sistema cliente.

Para acessar a tela de migração, clique na opção de menu: Atendimento > Migrar Usuários. Será exibida uma tela como a apresentada na figura 3.1.

Na parte superior desta tela está impresso um resumo do formato aceito pelo Sentinela. Use sempre o sinal de ponto-e-virgula (;) para separar os campos e uma quebra de linha (chr10+chr13) para separar cada registro.

ATENÇÃO: Verifique se o último registro tem a quebra de linha, caso contrário esse registro não será migrado.

DICA: Caso não tenha alguma informação, simplesmente ignore o campo, inserindo o próximo sinal de ponto-e-virgula (;).

Para realizar a migração basta copiar e colar os registros na caixa de texto. Lembre-se de verificar a quebrar de linha do último registro. O Sentinela possui um campo intitulado “Não gravar”, sempre utilize este campo para testar os registros que foram colados na caixa de texto. Caso o teste seja bem sucedido, então desmarque a caixa para efetuar a gravação.
Quando houver a migração, com ou sem a marca na caixa “Não gravar”, será verificado a similaridade entre os dados a serem inseridos e os dados presentes na base de dados. Confira e corrija as informações. Caso deseje ignorar a similaridade, marque a caixa correspondente.

Ao final da gravação será exibido um relatório de gravação de cada um dos registros com o número de identificação (*id*) de cada usuário. Sugerimos que seja copiado para eventuais conferências e vinculação dos usuário no sistema cliente.

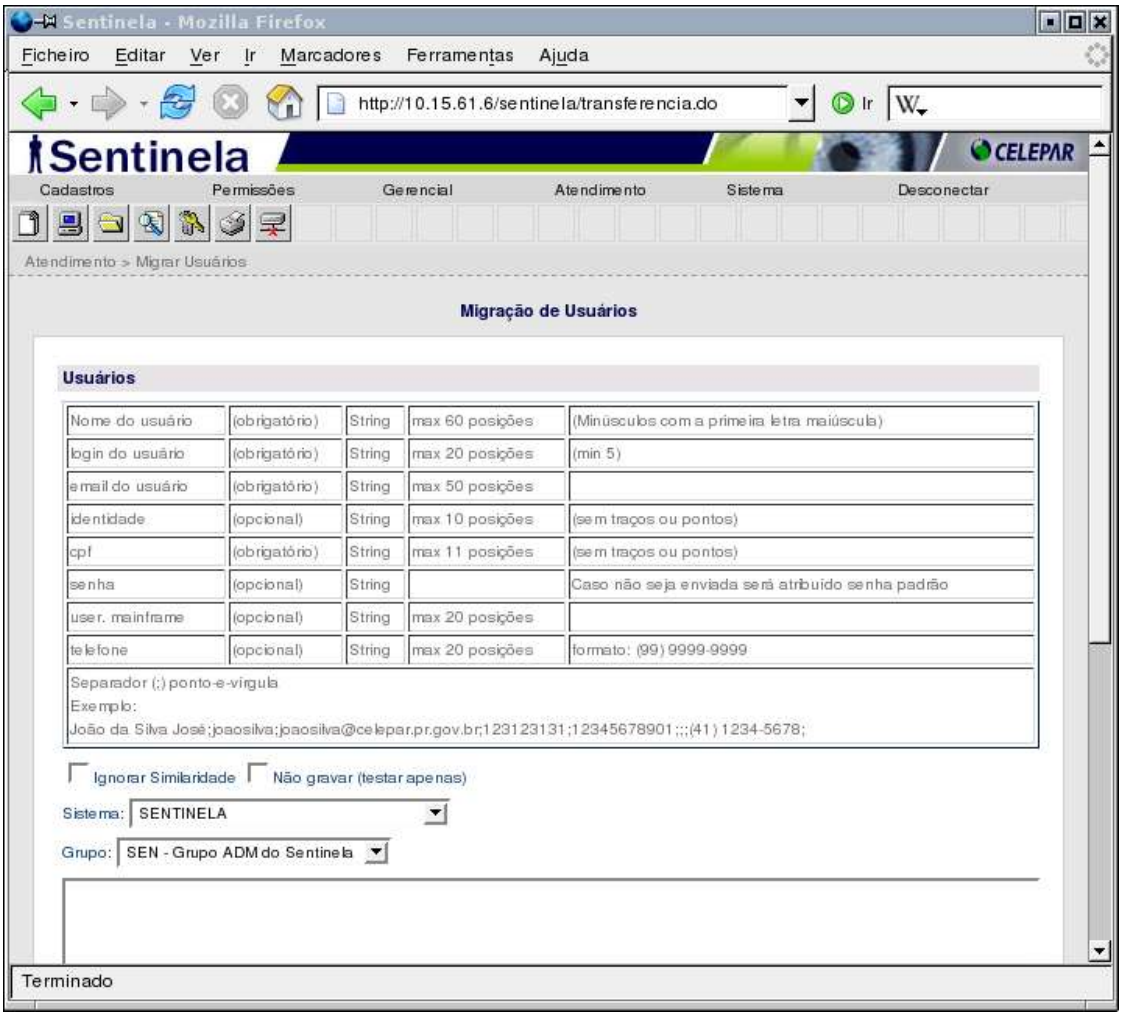

Figura 3.1 – Migração de usuários

Também é possível migrar os usuário e automaticamente atribuí-los a um grupo (somente um). Para isso basta escolher o sistema e o grupo e realizar a importação. Se não quiser colocar os usuários num grupo, é só deixar em branco.

5 PARAMETRIZAÇÃO

Muitas características do sistema Sentinela são definidas de forma global e devem receber configurações de acordo com a política da empresa gestora. Ao se tratar de uma base centralizada, todos os sistemas devem funcionar da forma acordada.

Com relação ao ambiente, a primeira configuração é a própria base de dados e os containers web que detém um endereço e devem ser referenciados pelas equipes de desenvolvimento. Está configuração é externa ao Sentinela e sua mudança deve ser feita de acordo com o tramite da empresa entre as áreas envolvidas.

Outros parâmetros relacionados ao ambiente podem ser configurados pelo Sentinela através da administração do sistema. Somente o grupo administrador do Sentinela deve ter acesso a esta tela, devido a importância dela. Uma configuração errada pode fazer o sistema deixar de funcionar. Para acessar a tela de configuração use a seguinte opção de menu: Atendimento > Parâmetros. Será exibido uma tela como apresentado na figura 4.1.

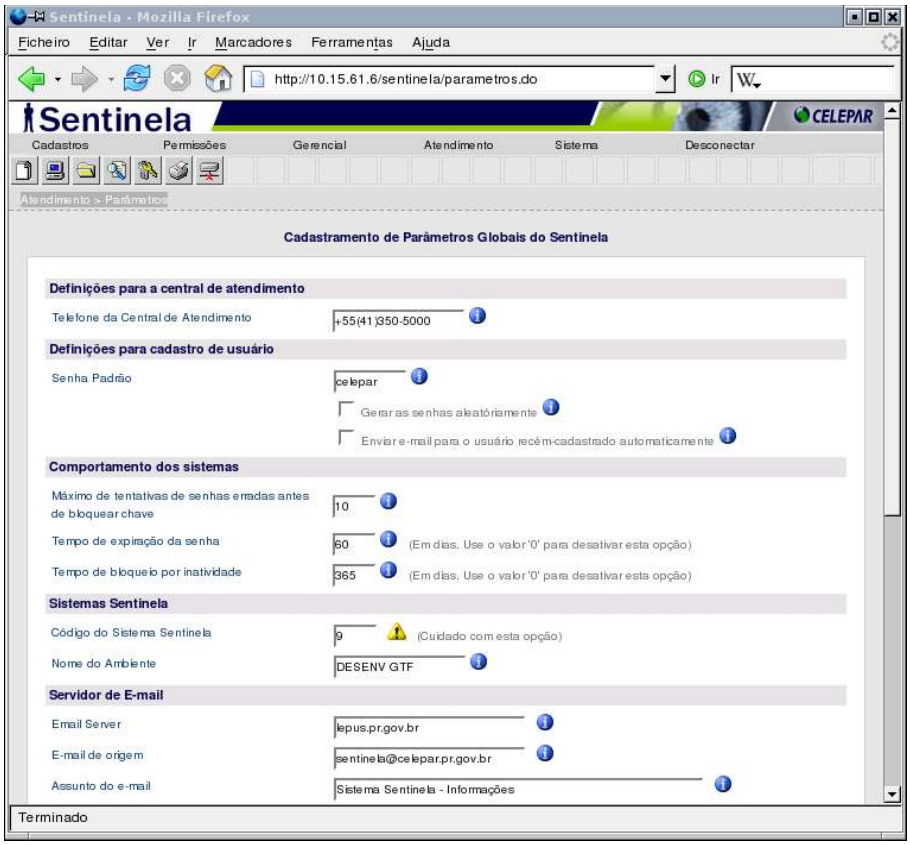

Figura 4.1 – Tela de parâmetros

Nesta tela pode-se modificar o comportamento de algumas partes do Sentinela. Inicialmente tem-se um campo onde deve-se atribuir o telefone da central de atendimento. Este telefone será exibido em situações de erro em que o usuário deverá solicitar ajuda externa. Também é exibido na tela de login.

A segunda seção define o comportamento relacionado às senhas de usuários. Ao cadastrar um novo usuário pode ser escolhido entre cadastrar com uma senha padrão, e neste caso fornecida pelo campo apropriado, ou a geração de uma senha aleatória e desconhecida. Em seguida tem um campo onde ao ser marcado, está sendo autorizado o envio de um e-mail automático para o usuário recém cadastrado com os dados de login. Use estas opções de forma correta para não criar situações errôneas. Caso seja escolhido a geração de senhas aleatórias, é interessante que o e-mail seja enviado, pois senão o usuário não tem como ingressar ao sistema, a menos que seja definido pela política da empresa que o usuário deve contactar-se com a central de atendimento antes.

DICA: A senha padrão cadastrada nesta tela não precisa respeitar as diretrizes de criação de uma nova senha.

ATENÇÃO: Independente do conjunto de opções escolhidos, o usuário já terá a senha expirada, a menos que seja desabilitado o recurso de expiração de senhas.

Na seção "*Comportamento dos sistemas*" é definido parâmetros como: número de tentativas inválidas, tempo de expiração de senha e tempo de bloqueio por inatividade. Estes itens podem ser desativados, se assim for definido pela política da empresa. Segue o conceito de cada um destes itens:

- Número de tentativas inválidas: É a quantidade de senhas erradas que o usuário irá tentar antes da chave bloquear. Para isso é necessário que o nome de login esteja correto. O desbloqueio da chave somente pode ser feito pela central de atendimento.

- Tempo de expiração de senha: É o tempo (em dias) que os usuários devem mudar a senha. Quando este tempo expirar, durante o procedimento de login será exibido uma mensagem solicitando a troca de senha. O usuário será obrigado a trocar de senha antes de poder ingressar ao sistema. A senha digitada deve seguir as regras de senhas.

- Inatividade: Refere-se ao tempo em que o usuário não efetua login em nenhum dos sistemas que utilizam o Sentinela. Normalmente este tempo é alto (6 meses ou um ano) e formaliza a questão de que se não acessou durante todo este tempo é porque provavelmente não está mais na ativa. A chave é desativada (mesmo procedimento de desligamento) e pode ser reativada somente pela central de atendimento.

Na seção logo abaixo tem-se um código e nome do ambiente. O código identifica o sistema Sentinela propriamente dito, que somente pode ser acessado por usuários *root*. Este campo somente deve ser alterado caso haja algum tipo de reinstalação do sistema, onde o Sentinela mude de código. Para evitar qualquer tipo de problema é recomendado que os dados do Sentinela sejam copiados da forma como se encontram, através do procedimento de migração. Em ambientes já instalados não é necessário efetuar qualquer tipo de alteração neste valor.

O campo nome do ambiente identifica o ambiente que o sistema está operando, como: desenvolvimento, homologação ou produção.

As configurações de e-mail servem para o envio automático de mensagens. Os campos iniciais referem-se ao servidor de e-mail, que será colocado como remetente e a mensagens atribuídas como assunto.

Os campos “Mensagem de cadastro” e “Mensagem de troca de senha” são mensagens que os usuários receberão nas situações de cadastro e troca de senha. Siga as orientações colocadas junto ao campo para configurar a mensagem. Use as strings “%1” (e “%2” e/ou “%3” para troca de senha) para indicar a posição onde será colocado informações dinâmicas.

Finalmente as configurações do “Selo Sentinela” referem-se a mensagem exibida quando o usuário posicionar o cursor do mouse sobre o ícone do Sentinela e a url que será exibida (numa nova página) quando o usuário clicar no ícone. O Selo tem a função de identificar que o sistema cliente utiliza a segurança do sistema Sentinela e pode obter maiores informações a respeito do Sentinela através da mensagem do selo e da página oficial.

6 PASSAGEM DE INFORMAÇÕES PARA A PRODUÇÃO

Esta funcionalidade gerou muita discussão sobre como seria o correto funcionamento, pois ao trabalhar em múltiplos ambientes podemos ter problemas de sincronismo entre as informações destes ambientes. O problema ocorre quando um sistema ou função é cadastrada em desenvolvimento e uma outra função é cadastrada em produção. Estas funções podem adquirir o mesmo identificador, uma vez que estão em ambientes diferentes. Uma solução seria impedir cadastramentos em um dos ambientes, porém está restrição poderia ocasionar problemas, uma vez que a passagem destas informações entre ambientes é um processo que necessita de verificação e tem que ser feito por uma determinada área.

Esta é apenas uma pequena parcela dos problemas que tem este tipo de operação, sendo assim foi definido um processo seguro, porém podendo dificultar um pouco o trabalho do desenvolvedor. As definições são as seguintes:

a) Os sistemas somente podem ser inseridos em desenvolvimento;

b) A única passagem possível é de desenvolvimento para a produção;

c) Quando houver homologação, a passagem segue a seguinte ordem: desenvolvimento -> Homologação -> Produção;

a) A passagem somente pode ser executada UMA ÚNICA VEZ;

b) A partir da passagem, as alterações devem ser cadastradas nos dois ambientes;

c) Não pode-se passar informações de grupos, usuários e permissões;

d) As informações que podem ser passadas são: sistema, funções, funções auxiliares, funções genéricas, exceções e ícones;

A passagem deve ser formalizada por uma solicitação vinda da equipe que desenvolve o sistema cliente. O Sentinela apenas gera o *script* padrão SQL que deve ser executado em produção (ou em outro ambiente alvo). Estes *scripts* também podem ser usados para

acompanhar o Sistema Sentinela em novas instalações.

Para acessar a tela de geração de scripts acesse a opção: Atendimento > Geração de Script. Será aberta uma tela como a apresentada pela figura 5.1.

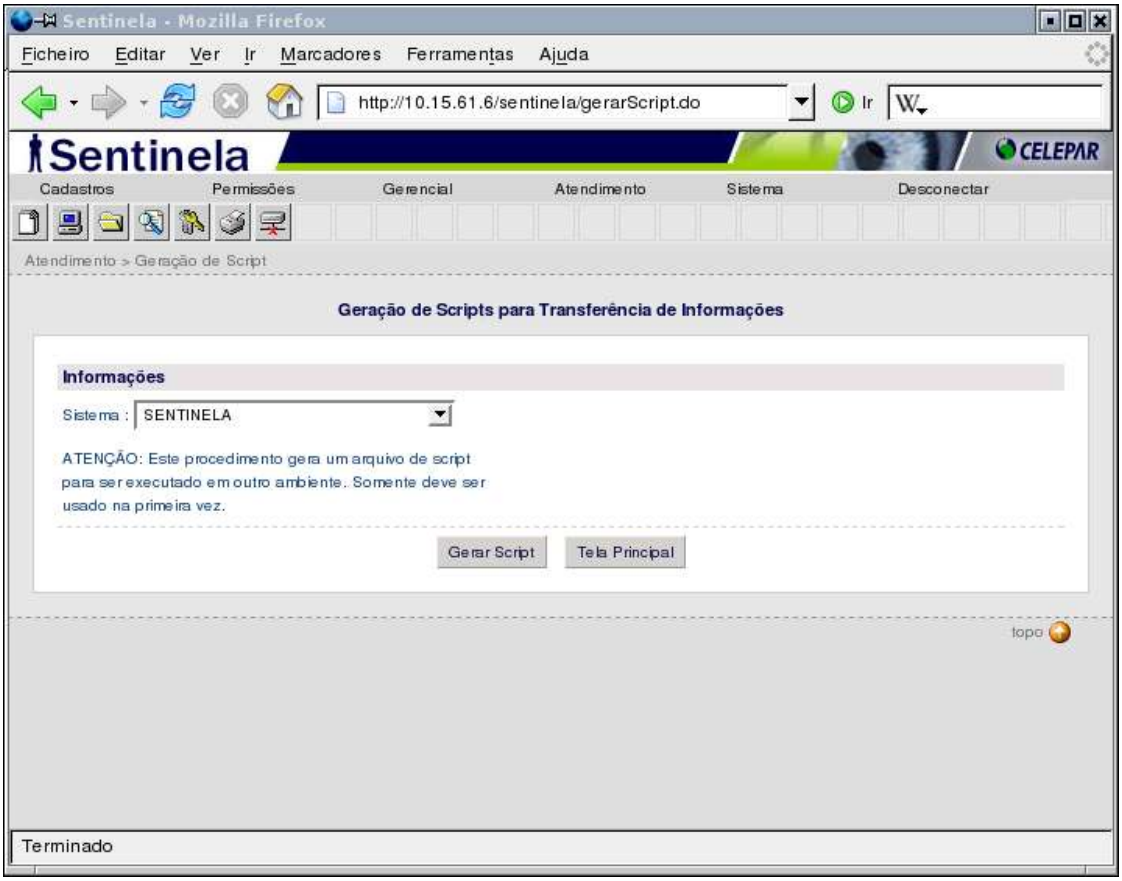

Figura 5.1 – Tela de geração de script

A manipulação desta função é bastante simples, basta escolher o sistema a ser transferido e clicar no botão "*Gerar Script*".

ATENÇÃO: O Sentinela não controla a quantidade de vezes que foi gerado o script. Pode ocorrer problemas se o script for executado mais de uma vez no ambiente alvo.

7 RESOLUÇÃO DE PROBLEMAS

Neste capítulo seguem os principais registros de problemas que houveram com o Sentinela desde a versão 1.0, seguida dos procedimentos para correção. Das solicitações feitas, aproximadamente 90% eram problemas com componentes externos ao Sentinela, portanto as primeiras providências para tentar encontrar um problema são:

- Verifique a versão do sentinela (pacote jar);
- Verifique se a base de dados está operando normalmente;
- Verifique o arquivo *-ds.xml no jboss ou o context.xml no tomcat;
- Verifique no cadastro de sistemas, se o sistema cliente está cadastrado e se o endereço digitado no browser é o mesmo cadastrado;
- Lembre-se que endereços como "*localhost*" são trocados de acordo com as configurações do arquivo sentinela.xml
- Verifique os logs do sistema cliente para verificar se o problema não se dá pela falta de alguma biblioteca (jar);
- Verifique o arquivo WEB.xml da aplicação e veja se o conteúdo referente ao Sentinela está correto;
- Lembre-se que o sentinela trabalha com *caches*. Na dúvida reinicie o serviço;
- Procure trabalhar com o ambiente especificado: LINUX, FIREFOX, JAVA TIGER (1.5), JBOSS (4.0.2 ou mais recente), PostgreSQL 8.0;
- Leia sempre os LOGS;

DICA: Persistindo o problema, o Sentinela pode ser facilmente desativado comentando o código referente ao filtro no arquivo WEB.xml. Ao comentar este código o Sentinela nem sequer inicializa e a aplicação tem que funcionar normalmente.

Problemas encontrados:

1- Login e pós login tem que ser requisições diferentes. O Sentinela efetua o processo de LOGOFF ao encontrar uma chamada para a requisição de login. Lembre-se que o Sentinela analisa a requisição sem levar em conta os parâmetros passados.

2- Sentinela aparenta não funcionar. As chamadas são feitas para a aplicação e todas são liberadas.

2.1 - Verificar o arquivo web.xml e verificar se o filtro está devidamente configurado e sem comentários.

2.2 - Verificar se a opção "Desativar Segurança - Sistema público" está desmarcada. Esta opção desabilita a segurança. Esta opção é encontrada em cadastro de sistemas na administração do Sentinela.

3- Quando apresentado: "Sistema não pode ser resolvido". O procedimento que causa este erro é o momento em que a url digitada pelo usuário no navegador é analisada e comparada com os registros de sistema da base de dados. Quando o sistema não puder ir à base de dados ou não encontrar o registro apropriado, ocorre este erro.

3.1 - Verifique se o banco de dados está acessível no servidor em que está sendo executado a aplicação. O JBOSS necessita de um arquivo terminado em DS para criar o pool de conexões. Deve ter um registro com o nome do DS de SentinelaClientDS.

3.2 - Verifique se o drive do Postgre está no projeto. Normalmente neste caso o log apresentado emite um erro de driver incorreto ou não encontrado.

3.3 - Verifique se o banco está rodando. Use um terminal SQL para verificar se a base de dados do sentinela pode ser acessado do local onde se está executando o sistema cliente.

3.4 - Verifique se o registro se encontra na base de dados. No log do JBOSS aparece a url em busca, que é o endereço digitado no browser ou um endereço configurado no sentinela.xml. Assegure-se que este endereço esteja cadastrado na base de dados.

8 ANEXOS

8.1 Regras para composição de senha

Itens de funcionamento interno do Sentinela:

- A periodicidade para troca de senha é feita de forma centralizada e parametrizada.
- Limite de tentativas inválidas é cadastrada de forma centralizada e parametrizada.
- Bloqueio da chave em caso de inatividade, sendo cadastrada de forma centralizada e parametrizada. Inatividade é quando um usuário não efetua login em um determinado período de tempo.
- Troca de senha feita por confirmação do CPF e login sendo enviado para o e-mail uma nova senha cadastrada.

As seguintes regras deverão ser seguidas durante a troca de senha:

- O tamanho mínimo da senha é de 5 (cinco) caracteres;
- O Sentinela não aceitará senhas nas seguintes condições:
- Quando quatro caracteres coincidirem com quatro caracteres de informações cadastradas para o usuário. (RG, CPF, email, login e nome)
  Ex. para a usuária MARIANA GODOY, não serão aceitas senhas do tipo MARIxxxx ou xxxGODOxxxx.
- Se houver coincidência com a chave de acesso do usuário.
  Ex. Para o usuário prkalva, não será aceita a senha prkalva e nenhuma variante como: prkalva1 ou 1prkalva.
- Se houver similaridade com a última senha utilizada anteriormente nos seguintes casos:
  Ex. se a senha anterior era "REGISTRO", não serão aceitas senhas do tipo:
  REGxxxxx (Três primeiros caracteres idênticos).
  xEGIxxxx (Três caracteres idênticos a partir do segundo).
  xxxxxTRO (Três últimos caracteres idênticos).

- Se houver mais de duas repetições de caracteres iguais e adjacentes.

  Ex. não serão aceitas senhas do tipo CCARRMT

- Se houver coincidência com uma das seguintes palavra/prefixos restritos:

ABCDxxxx	CURITIBx	NOVxxxxx
ABRxxxxx	DETRANxx	OUTxxxxx
AGOxxxxx	DEZxxxxx	PARANAxx
ASDFGxxx	FEVxxxxx	PASSxxxx
ATLETICx	JANxxxxx	POSITIVx
BRASILxx	JESUSxxx	SENHAxxx
CELEPARx	JUNxxxxx	SETxxxxx
CIRETRAx	MAIxxxxx	TESTxxxx
CORITIBx	MARxxxxx	1234xxxx

8.2. Arquitetura do Sentinela

A figura A2.1 representa a forma de atuação do Sentinela *client*. A requisição é interceptada através do *design pattern Intercepting Filter*.

Figura A2.1 – Interceptação das requisições

O Sentinela divide-se em duas partes, o pacote cliente e a administração do Sentinela. As duas partes funcionam de forma autônoma, sendo que as informações cadastradas podem servir para gerenciar outros sistemas, como um integrador de aplicações.

Poderiam ser desenvolvidos diferentes clientes, até mesmo para outras tecnologias. A versão atual suporta apenas aplicações Java.

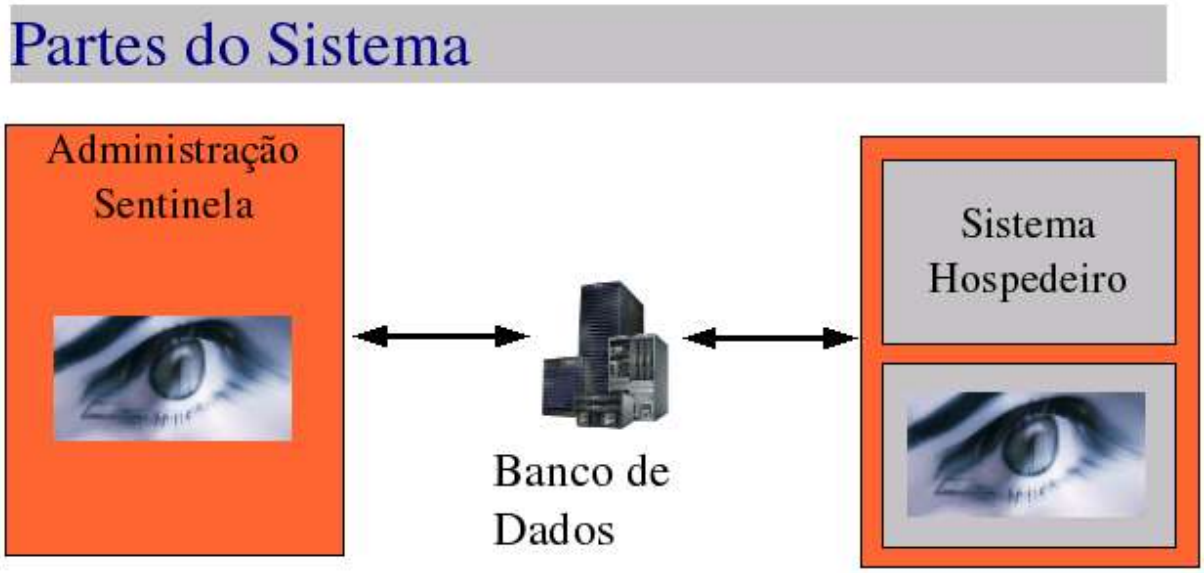

Figura A2.2 – Partes do sistema Sentinela

O Sentinela preferencialmente usa o JBOSS como container web. O pacote *client* fica junto com outras bibliotecas do sistema cliente e é definido e gerenciado como filtro a partir de informações contidas no arquivo WEB-INF/web.xml da aplicação cliente.

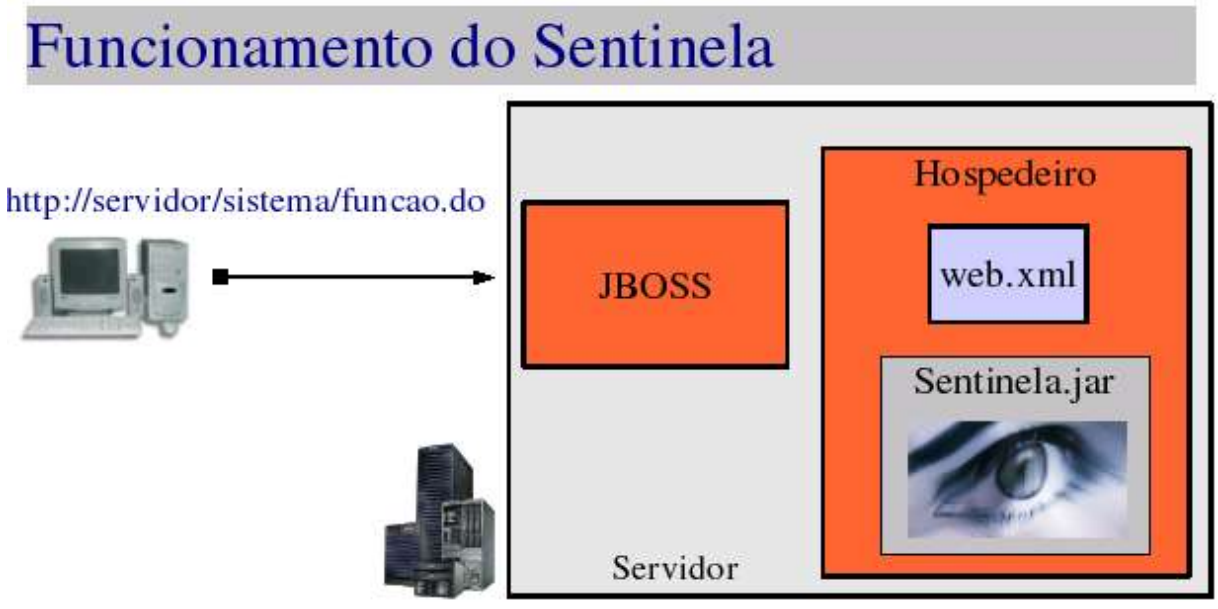

Figura A2.3 – Funcionamento do Sentinela

Internamente o Sentinela possui um sistema de cache dividido em duas partes. A primeira é

relacionado à informações comuns sobre o sistema (as exceções ficam aqui). O segundo é relacionado às permissões do usuário (o menu fica aqui). Os filtros são expansíveis, porém necessitam recompilação.

Figura A2.4 – Funcionamento do Sentinela Cliente

O Sentinela possui internamente diversos módulos que controlam a autenticação, autorização, restrições e muitos outros módulos. A versão 1.0 concentrou-se na estrutura básica enquanto a versão 1.2 trouxe inovações e melhorias nas funcionalidades, além de um amplo conjunto de ferramentas para aproveitar a centralização.

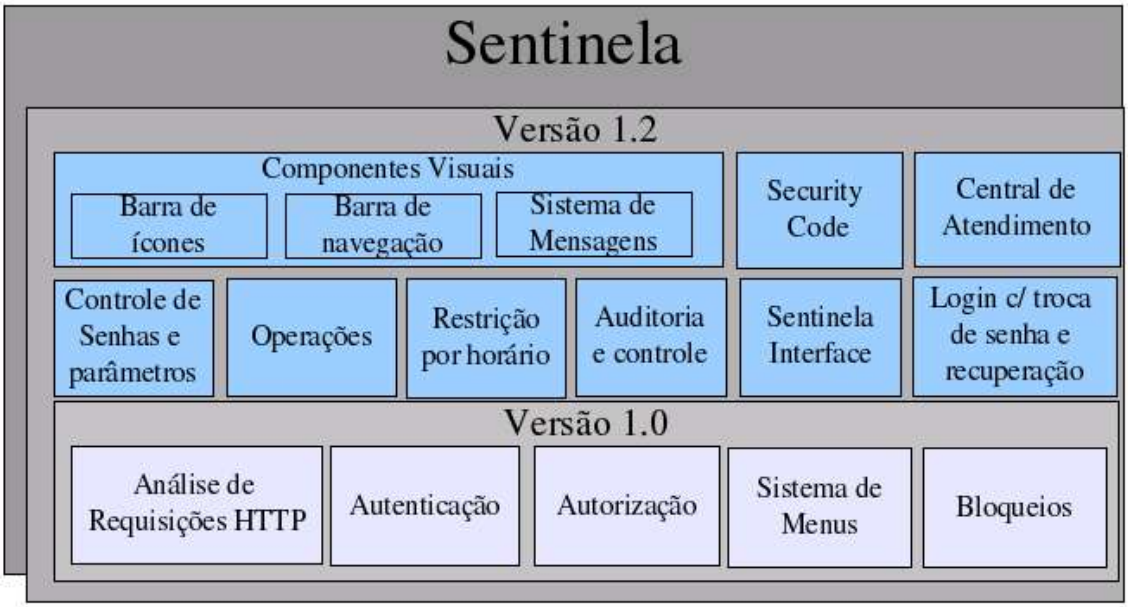

Figura A2.4 – Componentes do Sentinela