Implementação de um Módulo de Autenticação e de Gestão de Perfis de Utilizador

Guilherme Araújo

Dissertação realizada no âmbito do

Mestrado Integrado em Engenharia Electrotécnica e de Computadores

sob orientação de

Engenheiro José Augusto Cardoso Pinto e de

Professor Doutor José Ruela

O Presidente do Júri, Professor Doutor Manuel Ricardo

Faculdade de Engenharia da Universidade do Porto

Departamento de Engenharia Electrotécnica e de Computadores

Rua Roberto Frias, s/n, 4200-465 Porto, Portugal

Março de 2008

Resumo

O Sistema de Arquivo e Acesso Intranet (SAA), desenvolvido e utilizado na PT Comunicações, tem como objectivo complementar o sistema RETA (Recolha e Tratamento de Alarmes) e está inserido na arquitectura de gestão de alarmes. Este sistema, tal como todos do género, necessita de melhorias contínuas, sendo certo que a perfeição nunca será atingida. Mesmo assim, a vontade de melhorar foi determinante para avançar com este projecto ambicioso, que teve como objectivos a *Implementação de um Módulo de Autenticação e de Gestão de Perfis de Utilizador*.

Apesar de os objectivos serem claros, o meio para os atingir era à partida desconhecido, já que não estávamos familiarizados com este sistema. Assim, iniciámos um estudo pormenorizado do Sistema de Arquivo e Acesso Intranet, bem como de vários métodos de Autenticação Automática (do inglês *Single Sign On*).

Foi configurado e implementado um módulo de Autenticação Automática baseado em *Kerberos*, que permite aos utilizadores serem autenticados de uma maneira totalmente transparente e com maior segurança. Esta autenticação, que tira proveito da obrigatoriedade do utilizador ter de introduzir as suas credenciais de cada vez que faz o *login* na sua estação de trabalho, consiste numa troca de *tickets* entre a estação de trabalho do utilizador e um servidor *Kerberos* funcionando como *Key Distribution Center* (KDC). A primeira vantagem inerente a este método de autenticação é a diminuição do número de credenciais diferentes que cada utilizador tem de memorizar, visto que com este método o utilizador apenas tem de introduzir as suas credenciais uma única vez (quando faz *login* na sua estação de trabalho). Em segundo lugar, o aumento da segurança na autenticação, visto que nenhuma *password* é enviada para o servidor Web (em substituição é enviado um *ticket*).

Na continuidade do módulo de Autenticação Automática implementado, foi desenvolvido um método semi-automático de registo, onde praticamente todas as informações necessárias ao registo são obtidas através do servidor LDAP da PT Comunicações e automaticamente preenchidas no formulário de registo. O utilizador apenas tem de seleccionar o Domínio de Gestão onde deseja ser inserido e uma *password* de reserva, apenas utilizada caso o servidor *Kerberos* sofra alguma anomalia.

Um outro resultado obtido com este projecto foi o desenvolvimento e implementação de um módulo de Gestão de Perfis de Utilizador. Com este novo método de gestão, o perfil de cada utilizador é influenciado não só pelo seu perfil individual, mas também pelo perfil do Grupo de Gestão onde está inserido. Assim, a tarefa do Administrador é facilitada, visto que esta nova organização permite definir pormenorizadamente as funcionalidades a que cada colaborador tem acesso, bem como a camada da rede que terá de gerir.

Referimos ainda o facto que todas as funcionalidades mencionadas nesta dissertação passaram a fase de testes, e inclusive, encontram-se todas em ambiente de produção.

Abstract

The Archives and Intranet Access System (AAS) (from the Portuguese *Sistema de Arquivo e Acesso Intranet*) was created by and is used in PT Comunicações and aims at being a complement to the CAA system (Collection and Analysis of Alarms) (from the Portuguese *Recolha e Tratamento de Alarmes*) and is part of the architecture of the alarms management. Although perfection will never be obtained, this system, like all of the kind, needs continuous improvements. Therefore, the will to improve was fundamental to develop this ambitious project with the goal *Implementation of a Single Sign on and Users' Profiles Management Module*.

Although the aims were clear, the means to achieve them were unknown, given that there was no familiarity with this system. Consequently, a thorough study was conducted about the Archives and Intranet Access System, as well as about the several existing methods of Single Sign On.

A module of Single Sign On based on Kerberos was configured and implemented, allowing users to be signed on in a transparent and safe way. This authentication, which takes advantage of the fact that the user must insert their credentials each time they logon to their workstation, consists of an exchange of tickets between the user's workstation and a Kerberos server acting as a Key Distribution Center (KDC). The first advantage of this signing on method is the smaller number of different credentials that each user must memorize, given that with this method the user must insert their credentials only once (when they logon to their workstation). Secondly, the signing on is safer, given that no password is sent to the Web server (instead of it a ticket is sent).

Within the context of the implemented Single Sign On module, it was created a semi-automatic register method, where almost all the information needed to the register is obtained through the LDAP server of PT Comunicações and it is automatically filled in in the register form. The user must only select the Management Domain in which they want to join and a backup password, only to be used if the Kerberos server suffers any anomaly.

Another result obtained with this project was the development and implementation of a Users' Profile Management module. With this new management method, the profile of each user is influenced not only by their own individual profile, but also by the profile of Management Group to which they belong. Therefore, the administrator's task is made easier given that this new organization allows a detailed definition of the functions to which each user may have access, as well as the network layer that they will have to manage.

Let us still add that all the functionalities mentioned in this report passed all the tests and are currently in a production environment.

Prefácio

O Sistema de Arquivo e Acesso Intranet (SAA), desenvolvido e utilizado na PT Comunicações, visa complementar o sistema RETA (Recolha e Tratamento de Alarmes) e está inserido na arquitectura de gestão de alarmes. Este sistema apresenta algumas lacunas, que os colaboradores da empresa pretendem ver colmatadas, no sentido de rentabilizar o sistema em causa. Referimo-nos especificamente à necessidade de introduzir as credenciais todas as vezes que um utilizador entra no Portal.

Ora, quando um utilizador inicia a sua sessão é obrigado a introduzir as suas credenciais na sua estação de trabalho, o que identifica inequivocamente o utilizador. Assim, quando esse mesmo utilizador entra no Portal, já não há previamente qualquer dúvida da autenticidade da sua identidade.

Tendo em conta o exposto e com a intenção de tornar mais eficiente o trabalho dos colaboradores da PT Comunicações, debatemo-nos com uma hipótese: Já que o utilizador está inequivocamente identificado, visto que previamente realizou o *login* na sua estação de trabalho, será mesmo necessário voltar a introduzir as credenciais ao entrar no Portal? Ora, foi exactamente com esta questão em mente que este projecto ambicioso avançou, um projecto com objectivos e resultados esperados bem concretos.

Ao longo desta dissertação haverá sempre o cuidado de dentro do possível utilizar um discurso simples e acessível a um leitor não especializado na área, de modo a que os resultados desta dissertação estejam disponíveis a toda a comunidade.

Não posso deixar de agradecer à PT Comunicações pelos equipamentos fornecidos, bem como pela ajuda e disponibilidade de todos os que aqui trabalham. Agradeço ainda a importante orientação do Engenheiro Cardoso Pinto e do Professor Doutor José Ruela para a consecução deste projecto.

Índice

Índice de Figuras

Índice de Tabelas

Glossário

Com este glossário pretendemos reunir, de forma breve e objectiva, o significado dos mais variados termos, expressões e palavras usadas ao longo desta dissertação. Assim se o leitor se deparar com algum termo desconhecido, este é o lugar ideal para descobrir o seu significado.

carregabd - Carregamento de Registos de Alarme e Notificações em Base de Dados.

geradg - *script* para actualização dos Domínios de Gestão

JA (Janela de Alarmes) - interface em JAVA lançado via *browser*. Comunica por *sockets* com o Servidor de Alarmes (*serval*).

LDAP (*Lightweight Directory Access Protocol)* - protocolo para aceder a dados de configuração de serviço a partir de uma Base de Dados hierárquica central.

RETA - Recolha e Tratamento de Alarmes.

rsync - utilitário para sincronização de ficheiros e directórios (envia apenas os pacotes do ficheiro original que foram alterados).

SAA - Sistema de Arquivo e Acesso Intranet.

serval - módulo distribuidor de alarmes. Lança um servidor de *sockets*, que aceita ligações numa porta TCP (ex. 2345), conforme a configuração. Só transmite a cada cliente ligado os alarmes referentes ao seu Domínio de Gestão e as actualizações respectivas.

SGA - Sistema de Gestão de Alarmes.

SINTRA - Sistema de Tratamento de Avarias.

transpa - processo que monitora a data e hora de actualização dos ficheiros de registo de alarme e envia para o SAA esse ficheiro sempre que é detectada uma alteração na data/hora.

Capítulo 1

1. Introdução

1.1. Enquadramento do Trabalho

O trabalho descrito nesta dissertação insere-se no âmbito da disciplina de Dissertação do Mestrado Integrado em Engenharia Electrotécnica e de Computadores (MIEEC), Ramo Sistemas Telecomunicações, Electrónica e Computadores (TEC). O projecto decorreu nas instalações da PT Comunicações (Praça da Batalha, Porto), sob proposta do Engenheiro Cardoso Pinto da PT Comunicações e sob supervisão do Professor Doutor José Ruela da Faculdade de Engenharia da Universidade do Porto (FEUP).

O Sistema de Arquivo e Acesso Intranet (SAA) é acedível através de um *browser* pelos colaboradores da PT Comunicações. Este sistema tem como principal função a gestão de alarmes. Esta gestão é de extrema importância, uma vez que a qualidade do serviço que a empresa fornece está directamente relacionada com esta gestão, ou seja, quanto melhor forem geridos os alarmes, melhor serviço vai prestar a empresa aos seus clientes.

Neste sentido, a principal função do Portal[1] SAA é fornecer os meios para melhor gerir os alarmes. É portanto óbvia a necessidade de manter este Portal organizado e em segurança, já que graves problemas podem derivar de uma má organização, onde os utilizadores não encontram as funcionalidades que estão à procura ou, ainda pior, se os utilizadores utilizarem funcionalidades a que não deveriam ter acesso.

Torna-se portanto óbvia a necessidade de gerir os utilizadores, para estes, por sua vez, poderem gerir da melhor maneira os alarmes.

1.2. Objectivos do Trabalho

O trabalho de desenvolvimento aqui apresentado, sob o tema de *Implementação de um Módulo de Autenticação e de Gestão de Perfis de Utilizador*, foi levado a cabo com o

[1] Interface Web destinado a uso interno (pelos funcionários da empresa)

principal objectivo de reformular o controlo de acessos do Sistema de Arquivo e Acesso Intranet (SAA).

Esta reformulação consiste no desenvolvimento e implementação de um método para gerir os perfis dos utilizadores.

Com este novo método pretende-se que seja possível organizar os utilizadores em grupos, onde cada grupo terá um perfil próprio. Assim, o perfil do utilizador é não só baseado no seu perfil individual, mas também no perfil do grupo em que está inserido. Deste modo pretende-se controlar melhor o nível de acesso de cada utilizador, aumentando desta forma a segurança do sistema e dos próprios utilizadores.

A reformulação anunciada consiste ainda na implementação de um método de autenticação automática, onde os utilizadores não tenham que introduzir as suas credenciais de cada vez que acedam ao Portal. Porém, é imperativo garantir que não exista um decréscimo de segurança na autenticação.

1.3. Resultados

Este trabalho centrou-se na reformulação do controlo de acessos do Sistema de Arquivo e Acesso Intranet (SAA), tendo sido este objectivo cumprido.

É importante salientar que sistemas como o SAA apresentam grande complexidade. No caso específico do SAA, este suporta mais de seiscentos utilizadores, exigindo concomitantemente uma fiabilidade na ordem dos cem por cento. Tendo em conta o exposto, não é possível afirmarmos categoricamente que a reformulação desenvolvida colocou o sistema num nível de perfeição. Estamos portanto conscientes de que novas e constantes reformulações serão sempre úteis para um aperfeiçoamento contínuo e infindável do sistema em causa.

Contudo, não podemos deixar de sublinhar que no âmbito deste projecto cumprimos integralmente a especificação dada. Porém, conscientes de que mais funcionalidades constituiriam uma mais-valia para o sistema em causa, não deixámos de desenvolver algumas funcionalidades que não constavam da especificação e que passaremos a explanar.

Assim, de acordo com a especificação dada, foi configurado e implementado um módulo de Autenticação Automática baseado em *Kerberos*, que permite aos utilizadores serem autenticados de uma maneira totalmente transparente e com maior segurança. Esta autenticação, que tira proveito da obrigatoriedade do utilizador ter de introduzir as suas credenciais de cada vez que faz o *login* na sua estação de trabalho, consiste numa troca de *tickets* entre a estação de trabalho do utilizador e um servidor *Kerberos* funcionando como *Key Distribution Center* (KDC).

Na continuidade do módulo de Autenticação Automática implementado, foi desenvolvido um método semi-automático de registo, onde praticamente todas as informações necessá-

rias ao registo são obtidas através do servidor LDAP da PT Comunicações e automaticamente preenchidas no formulário de registo. O utilizador apenas tem de seleccionar o Domínio de Gestão onde deseja ser inserido e uma *password* de reserva, apenas utilizada caso o servidor *Kerberos* sofra alguma anomalia.

Um outro resultado obtido com este projecto, foi o desenvolvimento e implementação de um módulo de Gestão de Perfis de Utilizador. Com este novo método de gestão, o perfil de cada utilizador é influenciado não só pelo seu perfil individual, mas também pelo perfil do Grupo de Gestão onde está inserido. Assim, a tarefa do Administrador é facilitada, visto que esta nova organização permite definir pormenorizadamente as funcionalidades a que cada colaborador tem acesso, bem como a camada da rede que terá de gerir.

1.4. Estrutura da Dissertação

Este trabalho encontra-se estruturado em quatro capítulos e uma secção de anexos, sendo que ao primeiro capítulo corresponde a presente introdução ao trabalho.

No segundo capítulo são apresentadas as noções básicas para fornecer ao leitor todos os fundamentos teóricos necessários para uma compreensão total da presente dissertação.

O terceiro capítulo apresenta o trabalho desenvolvido, bem como fundamenta todas as opções tomadas ao longo do mesmo.

O quarto e último capítulo apresenta as conclusões gerais deste trabalho, analisando os seus principais resultados e efectuando uma comparação entre a proposta inicial e os resultados obtidos.

Os anexos são maioritariamente constituídos por código PHP e JavaScript.

Capítulo 2

2. Estado da Arte

2.1. Introdução

Serve esta secção para fornecer ao leitor todos os fundamentos teóricos necessários para uma compreensão total da presente dissertação. Pretendemos que a leitura se torne agradável e de fácil compreensão, permitindo assim que mesmo os leitores sem formação específica nos assuntos em análise possam compreender e tirar o máximo proveito deste trabalho.

2.2. SAA – Sistema de Arquivo e Acesso Intranet

2.2.1. Introdução

Visto este trabalho ter por base um Portal, começamos por fazer uma apresentação detalhada do referido Portal, bem como de todo o sistema que o envolve.

2.2.2. Objectivo

O Sistema de Arquivo e Acesso Intranet (SAA) tem como objectivo complementar o sistema RETA (Recolha e Tratamento de Alarmes), implementando uma camada de acesso através da *intranet* e um arquivo de notificações e registos de alarme em Base de Dados. Desta forma garante-se o acesso à informação histórica por um intervalo de tempo alargado e de uma forma amigável.

A plataforma disponibiliza condições de processamento e de comunicação adequadas à implementação de diversos módulos de tratamento da informação, sem afectar o funcionamento em tempo real, que é um dos requisitos do RETA.

2.2.3. Módulos Principais

O sistema (SAA) pode ser decomposto em três partes:

- Interface com o RETA;
- Base de Dados;
- Interface Web (Portal).

Nas secções seguintes vamos apresentar com pormenor cada uma destas três partes do SAA.

2.2.4. Interfaces

Tal como é possível observar na figura 1, existe uma interface entre o RETA e o SAA, responsável pela transferência dos seguintes tipos de informação:

- Notificações de alarme;
- Registos de alarme activos;
- Registos de alarme arquivados;
- Comandos de operação manual sobre os registos de alarme activos.

As restantes interfaces existentes destinam-se a obter informação de cadastro de locais, criar e consultar registos de avaria (SINTRA) e a obter informação de cadastro de circuitos alugados (GECA).

Na figura da página seguinte é possível ver a integração do Sistema de Arquivo e Acesso Intranet (SAA) na arquitectura do Sistema de Gestão de Alarmes (SGA).

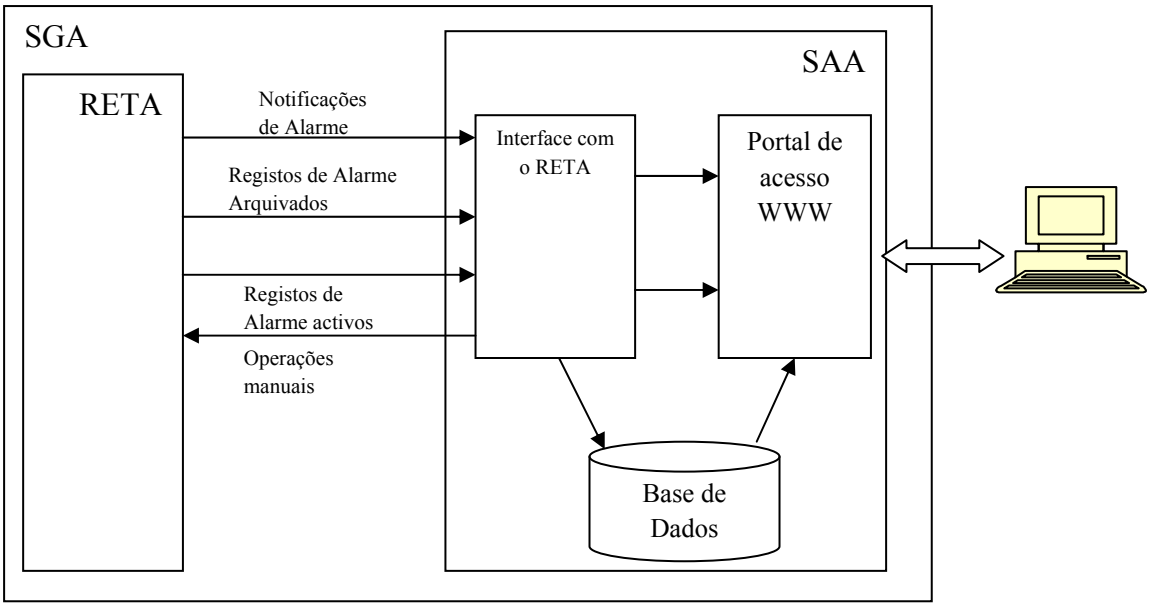

Figura 1 - Integração do Sistema SAA

2.2.5. Plataforma

A plataforma utilizada é baseada no Sistema Operativo *Linux*, que começou por ser instalado numa configuração típica de *hardware Pentium III* a 500 MHz, com 18GB de disco e 768MB de RAM. Esta plataforma permite utilizar diversos produtos *Open Source*, seguindo uma orientação crescente no domínio do *software*.

2.2.6. Arquitectura

Na figura 2 está representada a arquitectura do Sistema, incluindo os componentes principais.

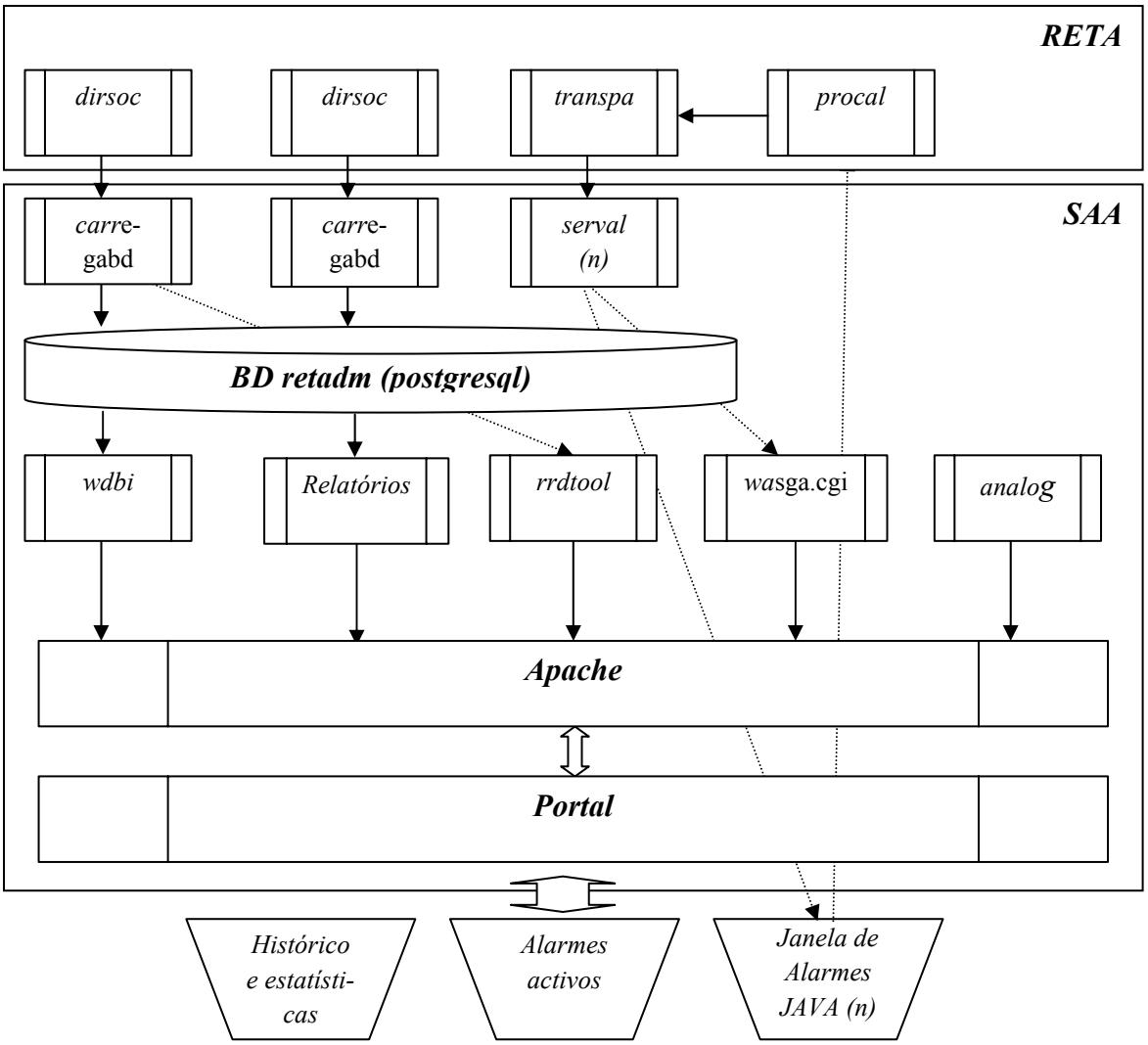

Figura 2 - Arquitectura do Sistema

Os componentes principais são o Sistema de Gestão de Base de Dados *postgresql*, o Servidor Web *Apache* e o Portal SAC (Sistema de Automatização de Conteúdos).

As linguagens utilizadas são predominantemente o PERL e o PHP.

São utilizados os módulos de interface DBI, DBD e PG do PERL.

Para o acesso à Base de Dados através da Web, foi utilizado inicialmente o *WDBI*[2], baseado em PERL, que facilita a construção de interfaces. Actualmente está a ser feita a migração de todos os módulos de interface com o utilizador para PHP, sobretudo por permitir maior flexibilidade.

Os módulos *dirsoc* e *transpa* são usados para transferir do RETA respectivamente as notificações e registos arquivados de alarme e os registos de alarmes activos. O *transpa* utiliza ainda o comando *rsync*. Os registos de alarme transferidos, que ficam nos ficheiros

[2] Web DataBase Interface Installation

alm_arq, são usados pela Janela de Alarmes em JAVA e pelo acesso HTML aos alarmes activos.

Para carregamento das *notificações* e *registos de alarme arquivados* na Base de Dados em tempo real existe o módulo *carregabd*. As notificações e registos de alarme são transferidas através da rede pelo módulo *dirsoc* do RETA, são lidas pelo *carregabd*, tratadas e carregadas na Base de Dados.

2.2.6.1. Estrutura de processos

Na máquina onde corre o SAA está também instalado o RETA, para gerir os processos e monitorar o funcionamento. Os alarmes gerados por esta instância do RETA devem ser transferidos para o RETA. Esses processos não estão representados no esquema, dado que saem foram do âmbito deste trabalho (fazem parte de uma instalação RETA normal).

A estrutura dos processos pode ser seguida na Figura 2:

- Processos Permanentes:
  - No SAA: *carregabd* (2), *serval* (2);
  - No RETA: *transpa*; *dirsoc* (2).
  - É necessário que estejam a correr os *daemons postmaster* e *httpd*, respectivamente para o gestor de Base de Dados *Postgresql* e para o servidor *Apache*.

- Processos Temporários:
  - *postgres* - um por acesso, durante a sessão http;
  - *httpd* - número de processos limitado por configuração, oito lançados inicialmente;
  - *wasga.cgi* e *wdbi.cgi*: um por sessão, conforme o tipo de serviço, para consulta html aos registos de alarme activos ou para consulta à Base de Dados.

O lançamento e paragem de processos permanentes é feito através do menu de administração do RETA para os processos do RETA e do SAA e dos respectivos *scripts* de controlo. Tal como no caso anterior, no lado do RETA os processos permanentes também são mantidos pelo módulo de administração do RETA.

2.2.6.2. Bases de Dados

Existem duas Bases de Dados:

- *retadm* para a informação de Alarme, Domínios de Gestão e uso geral.

- *yerba* para o Portal e controlo de acessos. Inclui também a tabela principal de utilizadores, que é sincronizada com a correspondente na Base de Dados *retadm*. A gestão de utilizadores é feita nesta Base de Dados, e o módulo do Portal que efectua esta função providencia a alteração na tabela da Base de Dados *retadm*, que contém apenas a informação necessária para os Domínios de Gestão do SAA e do RETA.

2.2.6.2.1. Estrutura da Base de Dados retadm

A estrutura da BD *retadm* é visível no diagrama apresentado em seguida:

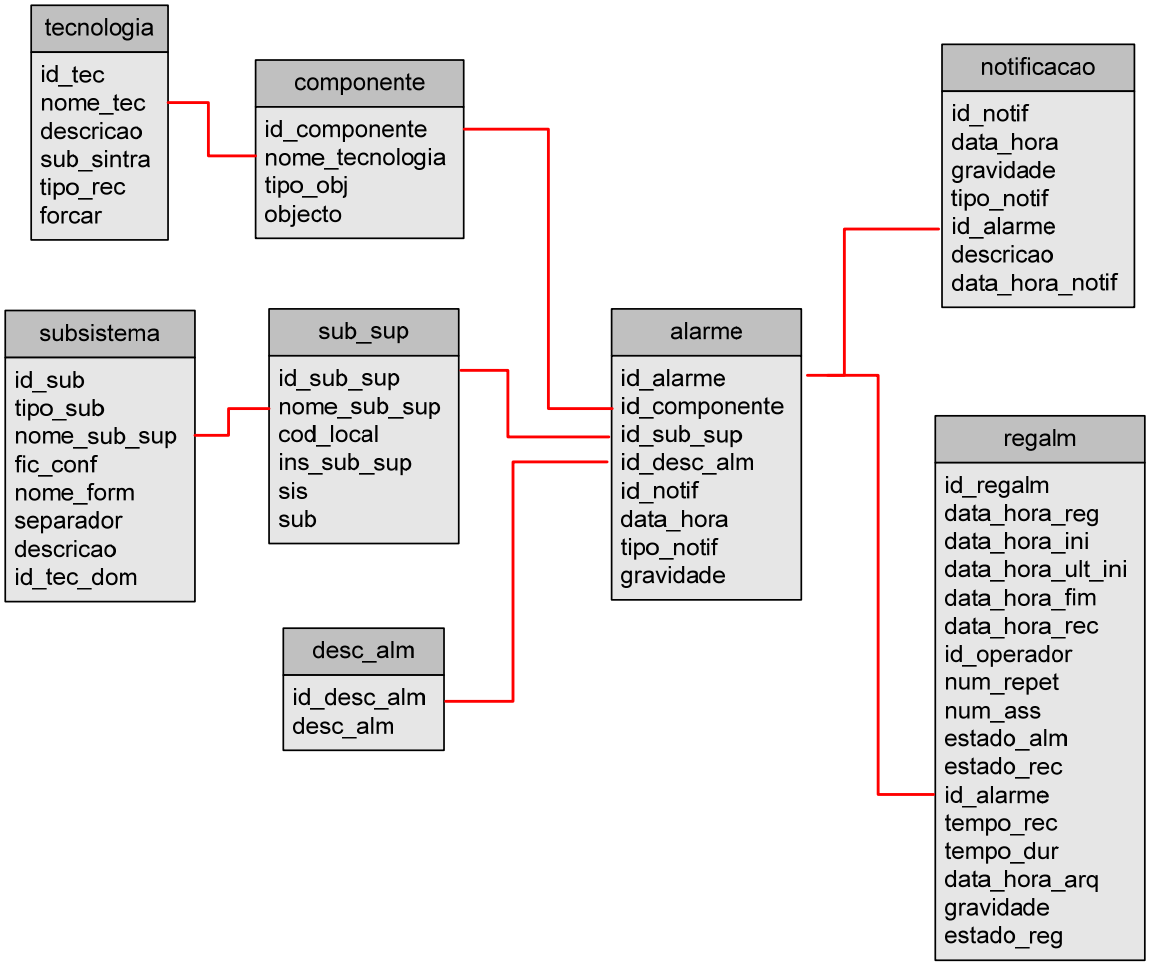

Figura 3 - Esquema da Base de Dados retadm (alarmes)

As tabelas *notificação*, *alarme*, *componente* e *regalm* desdobram-se em dois conjuntos, respectivamente para alarmes de subsistemas de circuitos alugados (sufixo _c) e para alarmes de rede (sufixo _r). Esta aproximação tem por objectivo desdobrar a informação por afinidade tecnológica, por questões de desempenho da Base de Dados.

Em resumo, as tabelas desdobradas são as seguintes:

- *notificação*: *notificacao_c*, *notificacao_r*, *notificacao_ch* e *notificaçao_rh*
- *alarme: alarme_c* e *alarme_r*
- *componente: componente_c* e *componente_r*
- *regalm: regalm _c* e *regalm _r*

Há uma relação hierárquica entre as tabelas, exemplificada na Figura 4 para as tabelas notificação, que tira partido das características do SGBD *postgresql*. Se executarmos um comando *SQL select* sobre a tabela *notificacao* obtemos os registos de todas as tabelas filhas e netas. Se executarmos o mesmo comando sobre a tabela *notificacao*_r, serão obtidos registos das tabelas *notificacao_r* e *notificacao_rh*.

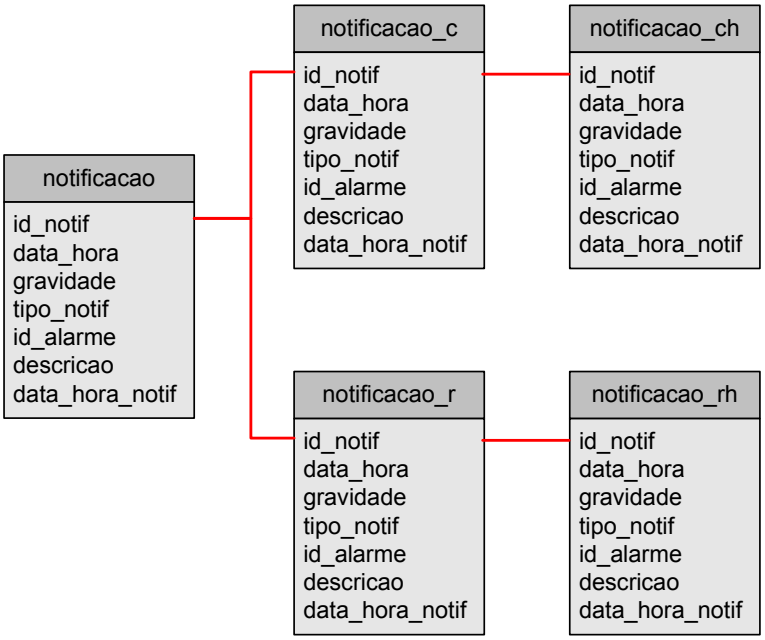

Figura 4 - Hierarquia das tabelas notificação

Nas tabelas *notificação*, *alarme* e *componente* não é carregada qualquer informação.

Nas tabelas *notificacao_c* e *notificacao_r* são carregadas em tempo real as notificações de alarme de Circuitos Alugados e de Rede. Esta função é executada pelo módulo *carregabd*.

Para as tabelas *notificacao_ch e notificacao_rh* são transferidos diariamente respectivamente os alarmes de Circuitos Alugados e de Rede com mais de um dia. Esta função é executada pelo módulo *acth.*

As tabelas *notificacao_ch* e *notificacao_rh* são filhas, respectivamente, das tabelas *notificacao_c* e *notificacao_r* que por sua vez são filhas da tabela *notificação*.

As tabelas *alarme_c* e *alarme_r* são filhas da tabela *alarme*.

As tabelas *componente_c* e *componente_r* são filhas da tabela *componente*.

Por cada nova notificação carregada na Base de Dados são actualizados na tabela *alarme* correspondente os seguintes campos: *id_notif*, *data* / *hora actual*, *gravidade* e *tipo de notificação* (Início / Fim). Assim, é possível obter o último estado de um dado alarme consultando apenas as tabelas *alarme* e evitando as tabelas *notificacao* que têm muito mais informação. Esta função é executada pelo módulo *carregabd*.

Se não existir a combinação *componente* / *sub_sup* / *desc_alm* que forma o Ponto de Alarme na tabela alarme, são criados os registos necessários.

2.2.6.2.2. Estrutura da Base de Dados do Portal

Das diversas tabelas existentes na Base de Dados *yerba* (mais precisamente 45 tabelas), salientam-se pela sua importância a tabela *yerba_usuarios*. Esta é sincronizada com a tabela *operador* da Base de Dados *retadm*, permitindo assim a manutenção dos operadores através do Portal. Esta sincronização é feita através do *script usuarios.php*, que actualiza as duas Bases de Dados e pelo módulo *geradg* que corre diariamente.

Devido à pouca importância que esta BD tem no âmbito deste trabalho, não será apresentada a sua estrutura.

2.2.7. Módulos funcionais

Para simplificar a descrição, o Sistema SAA foi dividido em módulos funcionais:

- Interface com o RETA
- Interface com outros OS[3]
- Domínios de Gestão
- Portal
- Servidor de Alarmes
- Acesso ao histórico de Notificações
- Acesso ao histórico de Registo de Alarme
- Acesso HTML aos registos de alarme activos
- Janela de Alarmes
- Monitor de Pontos de Alarme
- *Backup*
- Gráficos
- Limpeza

[3] Operation System

- Relatórios
- Estatísticas Web

Explicamos agora com mais detalhe os módulos mais importantes.

2.2.7.1. Interface com o RETA

A interface com o RETA é assegurada pelos seguintes módulos:

- *carregabd*;
- *transpa*;
- *ja_procal*.

2.2.7.1.1. carregabd - Carregamento de Registos de Alarme e Notificações

Tanto os *Registos de Alarme* arquivados como as *Notificações de Alarme* dos diversos sub-sistemas são enviadas em tempo real pelo módulo *dirsoc* do RETA e recebidas pelo *script carregabd* do SAA. A comunicação é feita através de um canal *socket*, que é estabelecido entre os dois processos, funcionando o *carregabd* como servidor. Em caso de falha de comunicação entre os dois processos, a ligação é interrompida e o *dirsoc* passa a tentar ligar-se de novo de 30 em 30 segundos. Nesse caso, o *carregabd* coloca-se de novo à escuta. O *carregabd* actualiza ainda a Base de Dados *rrdtool*, de 5 em 5 minutos. Esta informação é usada para representar graficamente no Portal a evolução das Notificações de Alarme.

2.2.7.1.2. transpa

Este processo monitora a data e hora de actualização dos ficheiros de registo de alarme e envia para o SAA esses ficheiros sempre que é detectada uma alteração na data/hora. Utiliza o módulo *rsync*. O comando *rsync* racionaliza a transferência, enviando apenas os pacotes do ficheiro original que foram alterados.

2.2.7.1.3.ja_procal - Comandos de Reconhecimento e Fim Manual

As operações manuais sobre os alarmes, emitidas a partir da *Janela de Alarmes JAVA*, são processadas no SAA por um *script* (*CGI*), que comunica por *remsh* ou *ssh* com o RETA.

O mecanismo utilizado obedece à especificação de interface do RETA, que se baseia num *pipe* (*fifo_pa*) que é lido regularmente pelo comando *procal*. No *pipe* é escrito um comando, que identifica a operação, o operador e o ficheiro com as chaves dos alarmes.

2.2.7.2. Interface com outros OS

As interfaces existentes actualmente destinam-se a obter informação de cadastro de locais, criar e consultar registos de avaria (SINTRA) e a obter informação de cadastro de circuitos alugados (GECA).

2.2.7.3. Controlo de Acessos, Domínios de Gestão e Domínios Organizacionais

Os *Domínios de Gestão* (também referidos como *grupo* ou ainda com a abreviatura *DG*) são baseados numa estrutura de informação em Base de Dados (bd *retadm*), com uma interface *Web* criada inicialmente em *WDBI*.

A Figura 5 representa a parte da estrutura da Base de Dados que diz respeito aos *Domínios de Gestão*. Esta estrutura permite gerar combinações de locais e tecnologias abrangidos por cada *operador*.

Dada a complexidade da construção dos *Domínios de Gestão*, foi necessário desenvolver um *script* para fazer a actualização – *geradg*. A tabela final de DG é a *dg_pr*, onde existem todas as combinações de *local / tecnologia*, para todos os grupos.

Existem as entidades *grupo* e *operador*. Um *grupo* é formado pela combinação de um esquema de *Domínios Geográficos (esq_loc)* e de um esquema de *famílias tecnológicas (grp_tec)*.

Cada *operador* pertence a um único *grupo*, que por sua vez pode ter vários *operadores*.

O módulo contempla um mecanismo de comunicação já citado com a Base de Dados de referência de *Pontos de Instalação* (SINTRA), para que os *Domínios de Gestão* sejam adaptados automaticamente, de acordo com a evolução da Rede no que respeita a novos códigos de local.

Adicionalmente, existe a possibilidade de criar excepções, isto é, locais cuja informação não está contemplada no Repositório de *Pontos de Instalação*.

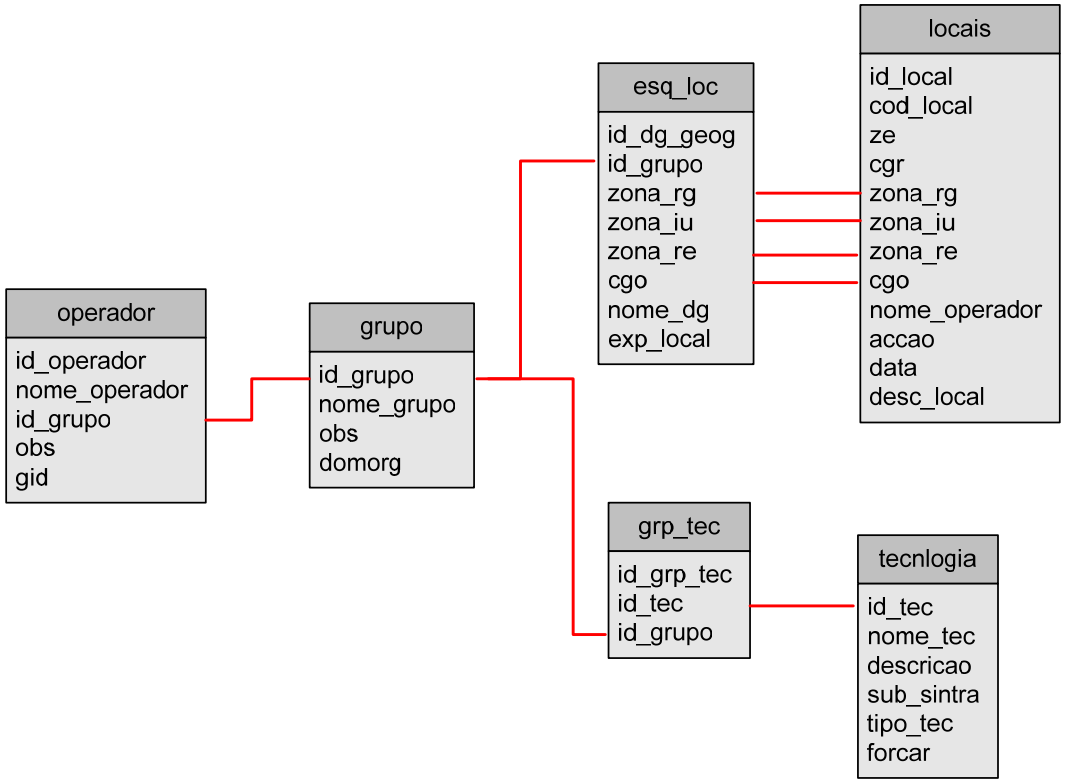

Figura 5 - Esquema da parte da Base de Dados relativa aos Domínios de Gestão

As combinações de locais e tecnologias são confrontadas com o histórico de alarmes ocorridos, e apenas são considerados nos domínios de gestão pares local / tecnologia onde já tenha ocorrido pelo menos um alarme, sendo enviados para um ficheiro de *log* os códigos que tiveram alarme mas que não existem nas tabelas de locais.

O subsistema de administração de *Domínios de Gestão* substitui também o subsistema existente no RETA, tornando este mais flexível e fácil de gerir, e garantindo ainda a coerência entre RETA e SAA. É gerado um arquivo dos Domínios de Gestão pelo *geradg* que pode ser transportado para as outras máquinas RETA onde são necessários os Domínios de Gestão. Esta actualização é feita diariamente de uma forma automática, por *remote shell* ou *ssh*.

A associação de *operadores* a *grupos*, assim como a criação de *operadores*, é feita no Portal. Os novos utilizadores criados no Portal escolhem o *grupo* e são registados automaticamente na Base de Dados *retadm* onde residem as estruturas de informação dos *Domínios de Gestão*.

Resumo das operações relacionadas com Domínios de Gestão:

Operação	Local onde é realizada
Criação de novos Domínios de Gestão (Grupos)	No Portal, *Form* Domínios de Gestão
Configuração de tecnologias ou locais vistos por um DG	No Portal, *Form* Domínios de Gestão
Criação de utilizadores SAA	No Portal [Novo Utilizador]
Criação de utilizadores RETA	No Sistema Operativo (devem existir no Portal)
Alteração do DG de um utilizador	No Portal
Eliminação de um utilizador SAA	Directamente na Base de Dados
Eliminação de um utilizador RETA	No Sistema Operativo
Alteração do privilégio de acesso	Directamente na Base de Dados
Activação das alterações aos DG no SAA	Executar geradg
Activação das alterações aos DG no RETA	Executar geradg

Tabela 1 - Operações relacionadas com Domínios de Gestão

2.2.7.3.1. Manutenção dos Domínios de Gestão

O acesso à Base de Dados para manutenção dos Domínios de Gestão é baseado no *WDBI.*

O acesso ao menu de administração de Domínios é feito através do Portal e é restrito ao utilizador de administração (*root*).

Diariamente é executado o script *geradg* para actualizar os Domínios de Gestão de acordo com as alterações introduzidas durante o dia. Este *script* é configurado no *crontab* mas também pode ser executado manualmente, se necessário. Antes de terminar, envia um sinal aos processos *serval* para carregarem a nova tabela de Domínios de Gestão.

Este *script* carrega e actualiza a tabela *dg_pr* da Base de Dados, a partir da qual são gerados os Domínios de Gestão para os sistemas RETA e SAA.

A tabela *yerba_usuarios* da Base de Dados *yerba* guarda toda a informação dos utilizadores que se registam no Portal e o script *geradg* vai actualizar a tabela *operador* da Base de Dados *retadm* com essa informação.

2.2.7.3.2. Interface entre o Portal e o Sistema de Administração dos Domínios de Gestão

Esta interface é necessária para completar o processo de registo de utilizadores e garantir a coerência entre os utilizadores RETA da própria máquina e SAA.

Um novo utilizador pode registar-se no Portal, escolhendo *user*, *password* e *grupo*. O procedimento insere o novo utilizador também na Base de Dados *retadm*, com o *grupo* escolhido, ficando a partir daí activo o novo perfil para todas as sessões do utilizador.

Será ainda gerado automaticamente o *link* para o Domínio de Gestão (grupo) respectivo no RETA. Se o utilizador RETA não existir, será necessária a criação do *user* UNIX, que terá que ser feita manualmente, se tal se justificar. Se o utilizador RETA já existir e houver alteração do *grupo*, o *link* anterior será mudado para o novo grupo.

Inicialmente, as contas RETA ficam bloqueadas no Portal, para impedir que um novo utilizador assuma a identidade de outro já existente no RETA e lhe altere o Domínio de Gestão. Os utilizadores RETA terão que contactar o Administrador do Portal para lhe desbloquear a conta.

2.2.7.3.3. Privilégios de acesso

Para controlar os privilégios de acesso pelos utilizadores aos diferentes módulos, é utilizado o campo *gid* da tabela *yerba_usuarios* da Base de Dados *yerba*. Cada tipo de privilégio tem um *bit* associado:

bit	peso	Tipo	Privilégio
0	1	Administração do Portal	root, configuração do Portal
1	2	Operação	Janela de Alarmes
2	4	Operação	Janela de alarmes com mapas
3	8	Operação	Alterar o estado do alarme e do componente (Reconhecimento, Fim manual e Inibição de alarmes)
4	16	Operação	Acesso a módulos adicionais de consulta
5	32	Operação	Ver monitoria, tabelas de configuração e Domínios
6	64	Operação	Utilizador normal

7	128	Administração	Administrar monitoria, tabelas de configuração e Domínios (Tecnologias, Subsistemas, Domínios de Gestão, Perfis e Domínios Organizacionais)

Tabela 2 – Privilégios de Acesso

Não existindo nenhum formulário no Portal que permita alterar os perfis, qualquer alteração terá de ser configurada directamente na Base de Dados (*yerba*) na tabela *yerba_usuarios*, alterando o campo *gid*.

2.2.7.4. Portal

Um dos grandes objectivos do Portal consiste em apoiar a comunicação entre as equipas de *Administração da Aplicação* ou de *Desenvolvimento* e os utilizadores.

Assim, sempre que haja informações sobre o sistema, novas funcionalidades, anomalias, recomendações, etc., deve ser colocada informação no Portal utilizando o módulo *noticias*, desenhado para o efeito.

Para garantir a manutenção de uma imagem de qualidade junto dos utilizadores, as *Noticias* devem ser sempre validadas pelo responsável da *Exploração* ou do *Desenvolvimento*.

2.2.7.4.1. Menu

Apresentamos na imagem seguinte uma figura do menu do Portal. De notar que o menu apresentado está na realidade todo numa coluna vertical, mas, para melhor enquadrar na página, foi aqui divido em três colunas verticais.

Figura 6 - Menu do Portal

Os *items* mais relevantes no contexto desta dissertação são explicados com detalhe em seguida.

2.2.7.4.1.1. Alarmes Activos

Tal como é possível ver na figura da secção anterior, os Alarmes Activos são divididos em quatro grandes pontos, sendo eles:

- Geral
- Megabit
- Dados
- Anomalias

Os três primeiros pontos desta lista estão relacionados com os Domínios Organizacionais da empresa, sendo que o "Geral" remete para a rede básica, "Megabit" para a rede de circuitos e "Dados" para as redes de dados. Facilmente se percebe que os alarmes que vamos encontrar dentro de cada uma destas divisórias vão estar relacionados com o nome da mesma, ou seja, se um utilizador está a consultar os alarmes dentro do "Megabit", apenas vai ter acesso aos alarmes relacionados com a rede de circuitos.

Quanto ao último item da lista, "Anomalias", faz a interface com o *Sintra* permitindo visualizar a lista de anomalias (com *ticket* no *Sintra*) activas e as resolvidas.

2.2.7.4.1.1.1. Consulta

Tal como o próprio nome indica, permite aos utilizadores consultar / pesquisar alarmes activos, sendo possível seleccionar filtros para realizar pesquisas mais eficientes e concretas. É também possível consultar históricos de alarmes para um dado componente. Não existe refrescamento automático, sendo que os resultados apresentados na página são os da altura do carregamento da mesma.

2.2.7.4.1.1.2. Janela de Alarmes

Tal como a Consulta, permite visualizar alarmes activos, sendo alimentada pela mesma fonte da Consulta. Tal como na Consulta, também a Janela de Alarmes permite seleccionar filtros, permitindo assim aos seus utilizadores apenas verem os alarmes que pretendem. Tem no entanto duas diferenças fundamentais, ao contrário da Consulta, na Janela de Alarmes é possível reconhecer e terminar alarmes activos, sendo ainda possível abrir e consultar registos de avaria. A outra diferença é relativa ao refrescamento, sendo que a Janela de Alarmes está permanentemente actualizada, visto que vai ler o *socket* de 5 em 5s (apenas lê as diferenças entretanto ocorridas).

2.2.7.4.1.1.3. Janela de Alarmes Dupla

Tal como é previsível, são duas Janelas de Alarmes, cada uma com todas as funcionalidades enumeradas anteriormente, permitindo assim ter diferentes filtros configurados ao mesmo tempo, tudo no mesmo ecrã (existe uma separação vertical entre as duas Janelas de Alarmes).

2.2.7.4.1.1.4. Mensagens da JA

Permite a consulta dos IPs dos utilizadores que estão com sessões activas na Janela de Alarmes, bem como permite consultar uma lista de operações manuais e acessos (à Janela de Alarmes).

2.2.7.4.1.2. Arquivo

O Arquivo, devido à sua complexidade e grandeza, será explicado com detalhe na secção *2.2.7.5 – Acesso ao Arquivo de Alarmes*.

2.2.7.4.1.3. Servidor de Alarmes

A necessidade de disponibilização de alarmes em tempo real via *Intranet* determinou o desenvolvimento de uma *Janela de Alarmes* em JAVA, que se liga através de um *socket* a um servidor de alarmes na máquina do SAA.

Assim, desenvolveu-se um módulo que lê os *registos de alarme* do RETA e transmite-os aos clientes a si ligados (via *socket*) de acordo com o seu perfil de Domínio de Gestão.

2.2.7.5. Acesso ao arquivo de alarmes

2.2.7.5.1. Introdução

Este módulo é constituído por um conjunto de componentes, configurados para implementar as diversas interfaces necessárias. É baseado no *WDBI*, um programa desenvolvido na ESA em *perl,* que traduz os ficheiros de especificação de interface (*.fdf*) em comandos para o SGBD *postgresql* e gera páginas *HTML*.

2.2.7.5.2. Estrutura do módulo e integração

A figura 7 representa o esquema de integração:

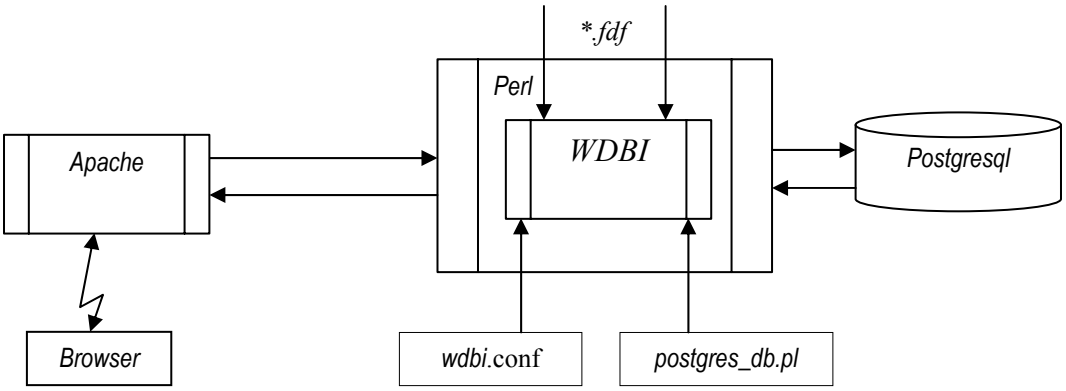

Figura 7 - Interface com o utilizador

Para consultar a informação existente na Base de Dados, existe um conjunto de FDFs (*Form Definition Files*) que abrangem as diversas áreas.

Os três *forms* mais importantes, que são por omissão configurados no Portal, são os seguintes:

- Pontos de alarme
- Registos Arquivados do Processamento de Alarmes
- Notificações

2.2.7.5.3. Pontos de Alarme

Consulta aos Pontos de Alarme, com o estado actual e *links* para acesso ao último registo de alarme arquivado, alarmes activos no processamento de alarmes no local / tecnologia, lista de notificações recebidas no próprio dia e no dia anterior (esta lista dá por sua vez acesso a todo o histórico), informação adicional de registos, pontos de alarme e avarias.

A figura 8 representa a árvore de navegação do *form Ponto de Alarme*. O *form Arquivados* tem associada uma estrutura semelhante.

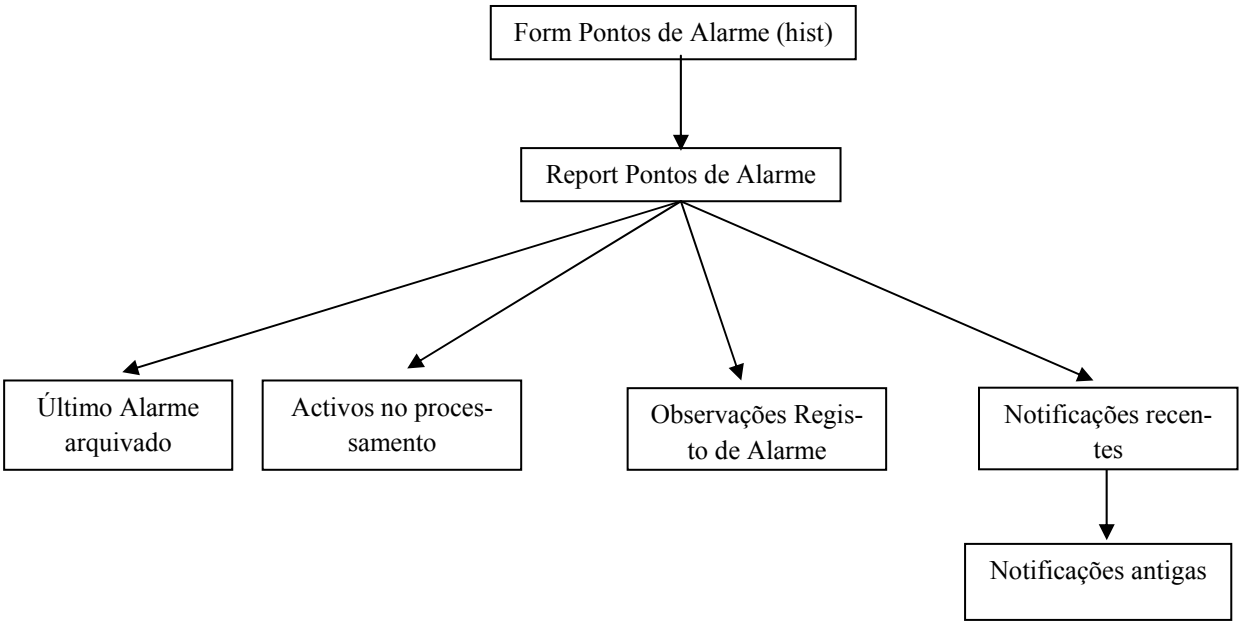

Figura 8 - Hierarquia de navegação do form Pontos de Alarme

2.2.7.5.4. Registos do Processamento de Alarme Arquivados

Consulta aos *Pontos de Alarme*, consulta aos *Registos Arquivados* e *links* para acesso ao último registo de alarme arquivado, alarmes activos no processamento de alarmes no local / tecnologia, lista de notificações recebidas no próprio dia e no dia anterior (esta lista dá por sua vez acesso a todo o histórico), informação adicional de registos, pontos de alarme e avarias.

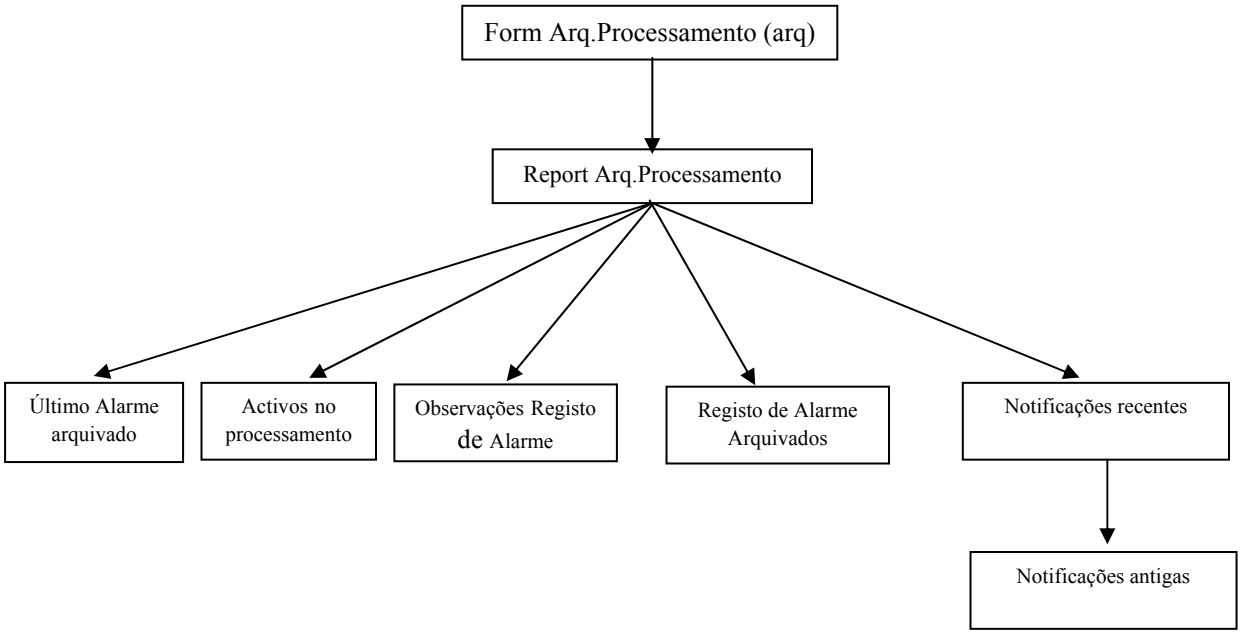

Figura 9 - Hierarquia de navegação do form Arquivados do Processamento

A figura 10 mostra a parte do esquema da Base de Dados que permite compreender a relação entre a tabela de *Registos Arquivados* do *Processamento de Alarmes* e as tabelas que definem os *Pontos de Alarme*. A estrutura que permite aceder às *Notificações* na secção anterior e seguinte usa a tabela *notificacao*.

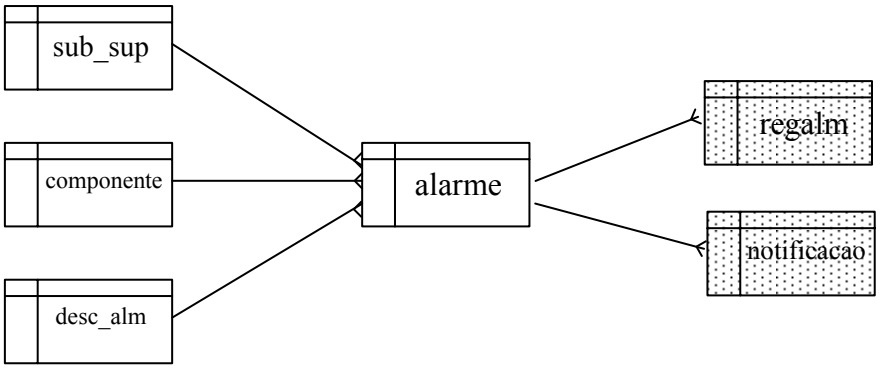

Figura 10 - Estrutura de join para acesso ao Registo de Alarme e à Notificacao

2.2.7.5.5. Notificações de Alarme

Consulta ao histórico, para notificações de alarme ocorridas desde a data configurada (por omissão 6 meses). O *join* pode ser visto na figura 10.

2.2.7.6. Acesso HTML aos registos de alarme activos (wasga)

Este módulo tem por objectivo disponibilizar um método alternativo à *Janela de Alarmes*, mais leve, para consulta aos *Registos de Alarme Activos*. Não tem os mesmos requisitos de refrescamento, e permite maior flexibilidade. É a ferramenta adequada para utilizadores que não tenham funções de Supervisão.

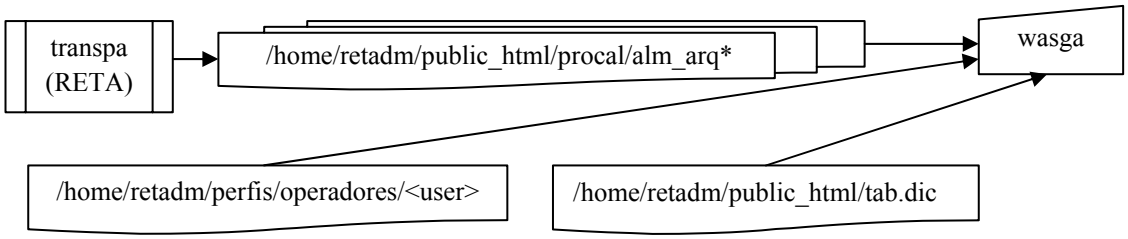

Figura 11 - Integração do wasga

2.2.7.7. Monitor de Pontos de Alarme

O *Monitor de Pontos de Alarme* tem por objectivo permitir aos técnicos controlarem se um determinado alarme não aparece há mais tempo do que é razoável.

É feita diariamente uma verificação do tempo que passou desde a última ocorrência de cada um de um conjunto de alarmes configurados.

Os *Pontos de alarme* que ultrapassaram o tempo configurado são incluídos numa lista que é enviada por *e-mail* para o responsável, com cópia para outro endereço.

Os resultados obtidos com este módulo são utilizados em conjugação com rotinas de teste dos alarmes mais relevantes, efectuadas periodicamente no terreno.

Se for feita uma rotina periódica, provocando esses alarmes, todos os alarmes cujo teste tenha falhado aparecem nos relatórios.

2.2.7.8. Gráficos

2.2.7.8.1. Introdução

É utilizada uma ferramenta poderosa - *rrdtool* - para guardar e manter dados estatísticos. Actualmente só está a ser tratado o número de notificações por segundo e por subsistema de recolha de alarmes.

2.2.7.8.2. Estrutura do módulo e integração

O período de amostragem é de 5 minutos.

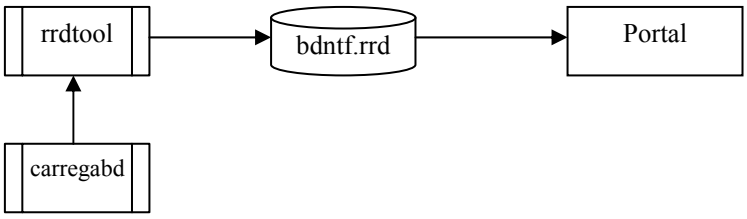

Figura 12 - Tratamento da taxa de notificações por segundo

No Portal está disponível por omissão o gráfico da evolução das notificações na última hora. Existe um *link* para aceder aos valores acumulados.

2.2.7.9. Limpeza e Arquivo

2.2.7.9.1. Passagem de alarmes para arquivo

A maior parte das consultas tem como alvo os alarmes do próprio dia ou do dia anterior. Para evitar que na utilização mais frequente seja pesquisado todo o arquivo, e ainda para que a informação não tenha que ser carregada directamente nessas tabelas, as notificações são carregadas e permanecem apenas o tempo mínimo nas tabelas *notificacao_c* e *notificacao_r*. Daí serão transferidas posteriormente para as tabelas de arquivo *notificacao_ch* e *notificacao_rh.* De salientar que os registos transferidos das tabelas *notificacao_c* e *notificacao_r* para as tabelas *notificacao_ch* e *notificação_rh* mantêm a mesma chave.

2.2.7.9.2. Limpeza da Base de Dados

Para evitar que a Base de Dados cresça sem limites e mantenha o bom desempenho, existe o *script acth* que é executado diariamente (*crontab*). Este *script* elimina os registos das tabelas *notificacao_xh* com mais de 180 dias e passa as notificações anteriores às 0 horas do dia anterior de *notificacao_x* para *notificacao_xh.*

2.2.7.9.3. Vacuum

É executado de 10000 em 10000 registos inseridos o comando *vacuum analyze* sobre as tabelas notificação e alarme, para manter o desempenho da Base de Dados, dado que estas tabelas estão constantemente a ser alteradas. Esta operação é efectuada pelo módulo de carregamento *carregabd*. Operação idêntica é feita para as tabelas *regalm_x*.

2.3. Single Sign On

2.3.1. Introdução

Com o crescimento das empresas os seus funcionários são confrontados com a necessidade de realizarem várias autenticações nas diversas aplicações internas, de maneira a poderem realizar o seu trabalho. A cada uma destas autenticações equivale uma "caixa" para introduzirem *username* + *password*, que pode equivaler a um conjunto de credenciais diferentes para cada aplicação. Estes processos diminuem a produtividade, visto que frequentemente os utilizadores trocam ou esquecem-se das *passwords,* o que obriga a interromper a acção em curso para pensar no conjunto de credenciais a introduzir naquela aplicação em concreto.

No entanto, estes contratempos dizem apenas respeito aos utilizadores. Debrucemo-nos agora sobre os administradores, que têm de manter vários servidores de autenticação (uma para cada aplicação) para manter a integridade da empresa.

Naturalmente esta necessidade não só implica um grande esforço, como é ainda dispendiosa. Isto acontece devido ao facto de cada aplicação necessitar de um administrador que tenha conhecimento de segurança informática, de maneira a poder desenvolver o seu servidor de autenticação.

A situação que foi descrita pode ser visualizada na figura seguinte:

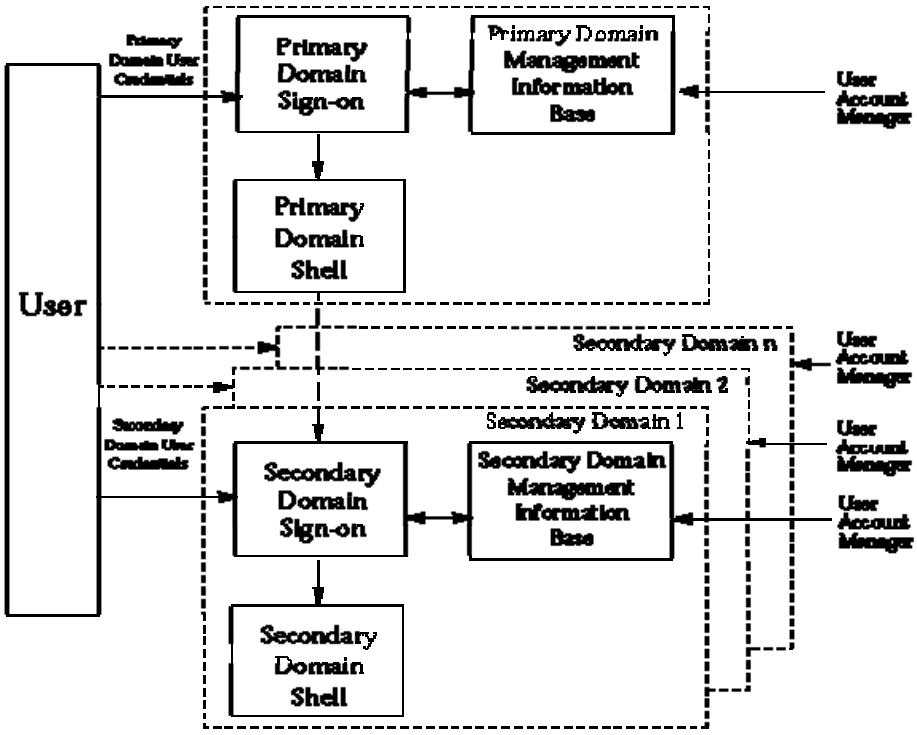

Figura 13 - Empresa sem Single Sign On

Assim, tornou-se essencial um sistema que solucionasse estes problemas. Com esta ideia em mente surgiu o Single Sign On. Através deste método de autenticação, todas as aplicações que necessitem de autenticação recorrerão ao servidor de autenticação principal, donde obterão todas as informações que necessitem do utilizador que querem autenticar. Logicamente tem de existir uma "confiança" entre as aplicações e o servidor de autenticação, visto que vai ser este que vai validar a identidade dos utilizadores.

Na figura seguinte é perceptível este método de autenticação:

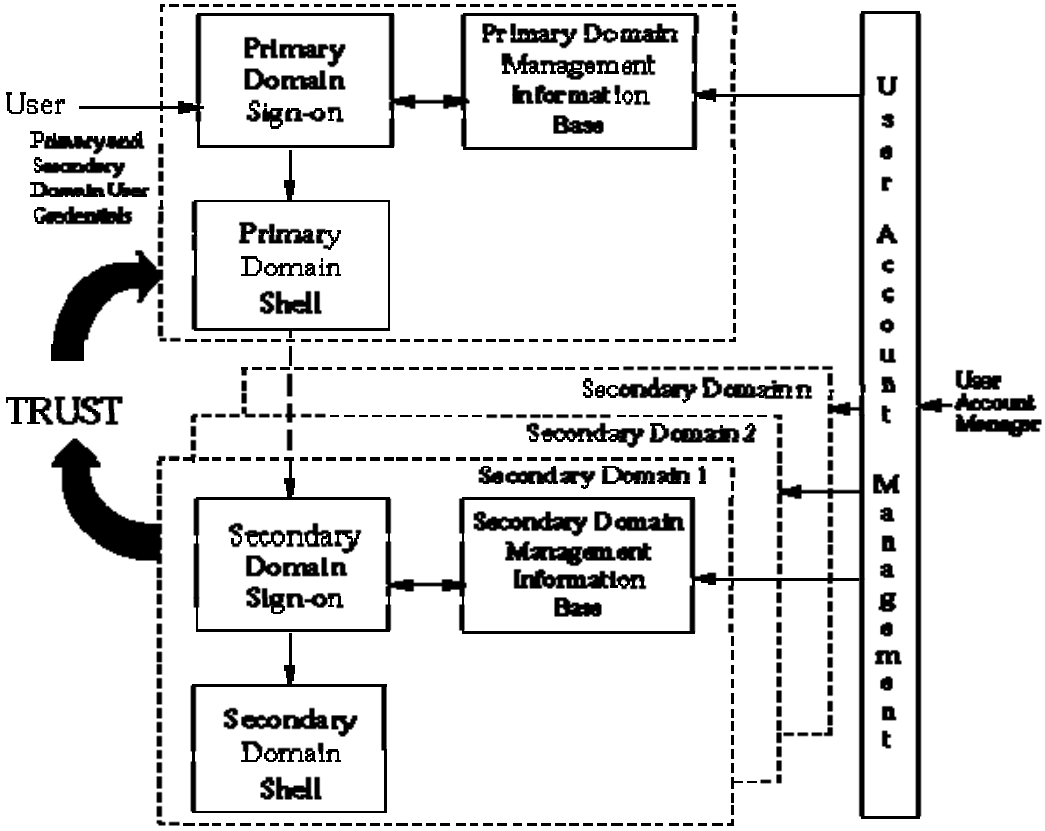

Figura 14 - Single Sign On

2.3.2. Definição

Single Sign On (SSO), também conhecido como *Entreprise Single Sign On* (ESSO), é a capacidade dada aos utilizadores para usarem o mesmo *username* e *password* em múltiplas aplicações dentro da rede da empresa.

Existem dois tipos de SSO:

- A forma mais conhecida de SSO ocorre quando os utilizadores apenas têm um conjunto de credenciais (*username* + *password*) para todas as aplicações dentro da

rede da empresa (mas têm de a introduzir sempre que pretendem aceder a uma aplicação interna);

- A outra forma, também denominada como "*Integrated Windows Authentication*", é menos utilizada devido à complexidade da sua implementação, mas os resultados conseguidos com a mesma são mais interessantes. Nesta forma de SSO, o utilizador apenas tem de introduzir as suas credenciais (*username* + *password*) ao entrar no sistema (tipicamente ao realizar o *logon* na sua estação de trabalho), sendo que a autenticação nas aplicações internas que o necessitem é feita de uma forma transparente para o utilizador.

2.3.3. Vantagens

O uso de SSO traz benefícios não só para os utilizadores, como para os administradores e para a própria empresa.

Comecemos então por ver as vantagens de que os utilizadores usufruem:

- Credenciais únicas (*username* + *password*) para memorizar (diminuindo a probabilidade de esquecimento da *password* e da necessidade de a escrever num papel);
- No caso do *Integrated Windows Authentication*, evita-se que os utilizadores tenham que introduzir as suas credenciais várias vezes no mesmo dia (só têm que introduzir de cada vez que entram no sistema);

Para os administradores:

- Apenas têm de manter um servidor de autenticação (possivelmente replicado);
- Todas as modificações ao perfil do utilizador são realizadas no mesmo sítio (evita a necessidade de ter de alterar o perfil em vários servidores se, por exemplo, o utilizador mudar de funções);

Para a empresa:

- Capacidade de utilizar a mesma política de autenticação em toda a empresa;
- Serviço de autenticação centralizado;
- Medidas de segurança relacionadas com a autenticação deixam de ser um requisito para os programadores aplicacionais;

- Aumento da segurança do Portal da empresa, visto que apenas são necessárias *cookies* com datas de expiração definidas para o final da sessão, evitando assim as *cookies* com validade para vários dias que poderiam pôr em causa a segurança da empresa;
- Diminuição de tráfego (que se traduz em poupanças) no *helpdesk* (direccionado para as *passwords*), visto que acabam os problemas de esquecimento de *passwords*;

2.3.4. Desvantagens

Tal como todos os sistemas, o SSO também tem desvantagens e perigos, destacando-se a dificuldade de implementação. No entanto, esta desvantagem não acarreta perigos, apenas impossibilita a implementação por um grande número de programadores.

As desvantagens que podem ser verdadeiramente perigosas para o sistema surgem apenas se este não for bem projectado e configurado. Nestes casos, se o sistema de autenticação sofrer algum problema que cause indisponibilidade do serviço (mas as aplicações não sofram o mesmo problema), os utilizadores poderão não conseguir autenticar-se perante as aplicações, o que reduz drasticamente a produtividade. Assim, torna-se essencial desenvolver sistemas de reserva, que permitam a autenticação dos utilizadores, garantindo sempre a segurança de todos (sistema, aplicações e utilizadores).

2.4. Kerberos

2.4.1. Introdução

O *Kerberos* é um protocolo de autenticação que exige a prova de identidade do utilizador para cada serviço de rede invocado, exigindo também que os servidores provem a sua identidade em relação aos clientes. Este protocolo constitui hoje um modelo *standard* para a autenticação, em particular para ambientes de rede heterogéneos e de grande dimensão. O *Kerberos* tem estado em produção num dos ambientes abertos mais desafiadores que existem, o *Project Athena* no *Massachusetts Institute of Technology* (MIT). No âmbito do *Project Athena*, o *Kerberos* protege um ambiente com mais de 10 000 utilizadores que acedem a milhares de estações de trabalho e a centenas de servidores, com milhares de sessões e dezenas de milhares de mensagens de correio electrónico diárias. Todo este ambiente assegura que o *Kerberos* é um dos mais bem testados protocolos de autenticação em utilização hoje em dia.

2.4.2. Características

Uma das principais características do *Kerberos* é o sistema de autenticação centralizado, em que um único servidor de autenticação pode ser utilizado por um número virtualmente ilimitado de computadores. Complementarmente, o sistema *Kerberos* garante que todas as autenticações realizadas através da *Internet* são feitas por sistemas robustos de cifra, evitando a transmissão de *passwords* em claro e a possibilidade de terceiros capturarem a *password* por simples escuta do canal de comunicação.

A ideia básica na origem do *Kerberos* é que uma terceira parte confiável possa disponibilizar os meios para que os participantes de uma rede possam confiar mutuamente uns nos outros. Esta terceira parte é o servidor de segurança *Kerberos*. Os participantes podem ser qualquer *hardware* ou *software* que comunique através da rede. Adicionalmente à autenticação, o *Kerberos* oferece também, em simultâneo, privacidade e integridade para mensagens na rede.

O sistema *Kerberos* assume uma arquitectura distribuída cliente / servidor e pode utilizar um ou mais servidores *Kerberos* para fornecer o serviço de autenticação.

Enumeraremos agora algumas das características deste protocolo de autenticação:

- É seguro, ou seja, é garantido que ninguém, mesmo autorizado, conseguirá obter informação necessária para personificar outro utilizador autorizado;
- É confiável, na medida em que a sua arquitectura distribuída assegura que a falta de disponibilidade do serviço *Kerberos* significa a falta de disponibilidade do serviço suportado (em todos os serviços que confiam no *Kerberos* para controlo de acesso);

- É transparente, o utilizador não tem percepção dos processos de autenticação em curso;
- A escalabilidade do sistema é capaz de suportar um largo número de clientes e servidores, seguindo uma arquitectura modular e distribuída.

O *Kerberos* oferece ainda uma série de serviços que importa salientar:

- canais seguros – consistem numa via de comunicação que assegura integridade e confidencialidade aos intervenientes no processo;
- integridade – possibilidade de os intervenientes num processo de comunicação poderem certificar-se de que as mensagens trocadas não foram modificadas de forma não autorizada durante a transmissão;
- confidencialidade – concebido com o intuito de contrariar situações de intercepção passiva de mensagens;
- autenticação – permite que um interveniente num processo de comunicação determine que a identidade de outro participante é genuína, e vice-versa;
- controlo de acesso – protege informação de eliminação ou modificação não autorizada, através do controlo das entidades a quem são disponibilizados acessos;
- não repúdio – garante a possibilidade de prova para o emissor de que a informação foi entregue e, simultaneamente, prova para o destinatário relativamente à origem da informação.

A melhor forma de encarar o *Kerberos* é como sendo uma família de serviços de segurança e autenticação.

Actualmente, existem clientes *Kerberos* para a maioria dos sistemas operativos. Deste modo, um sistema central de autenticação baseado em *Kerberos* pode suportar uma rede de clientes heterogéneos e com necessidades distintas.

2.4.3. Funcionamento

Este sistema (*Kerberos*) é tipicamente usado quando um utilizador dentro da rede da empresa tenta usar um determinado serviço da rede e o serviço pretende garantir a autenticidade do utilizador. Para isto, o utilizador apresenta um *ticket* ao serviço, que o examina para verificar a identidade do utilizador. Se tudo estiver correcto, o utilizador é aceite. Para isto, o *ticket* tem de conter informação que garanta a identidade do utilizador (demonstrando que o portador sabe algo que somente o verdadeiro utilizador saberia, como, por exemplo, uma senha).

Vejamos então como o *Kerberos* trabalha:

Quando um utilizador pretende utilizar um serviço, após ter-se autenticado na sua estação de trabalho, tem de começar por recorrer ao serviço de autenticação do *Kerberos*, de forma a serem-lhe concedidas credenciais que são depositadas em *cache* e que lhe permitirão, posteriormente, dirigir-se ao sistema *Kerberos*. Isto acontece para solicitar o acesso a serviços que estão protegidos desta forma. O elemento que fornece as credenciais iniciais é o servidor de autenticação (AS – *Authentication Server*) e a credencial toma o nome *de Ticket Granting Tick*et (TGT) e inclui o *UserID*, o endereço de rede do cliente, a validade da credencial e a *Chave de Sessão Cliente/TGS*. Quando um utilizador pretende aceder a um determinado serviço, tem de apresentar as suas credenciais a um outro elemento, o servidor de fornecimento de *tickets* (TGS – *Ticket Granting Server*). Este verifica as credenciais que lhe são apresentadas e determina a validade das mesmas. O TGS disponibilizar-lhe-á, ou não, as credenciais para acesso ao serviço pretendido. Se o acesso for permitido, é fornecido um *ticket* para acesso ao serviço, denominado *Application Service Ticket* (AST) que inclui o U*serID*, o endereço de rede do cliente, o período válido e uma C*have de Sessão Cliente/Servidor*. Na posse deste, o cliente pode dirigir-se ao servidor que presta o serviço pretendido e autenticar-se perante o mesmo utilizando esse AST. Opcionalmente, pode ainda ser exigido a este servidor que se autentique perante o cliente.

Na figura seguinte vemos o processo descrito:

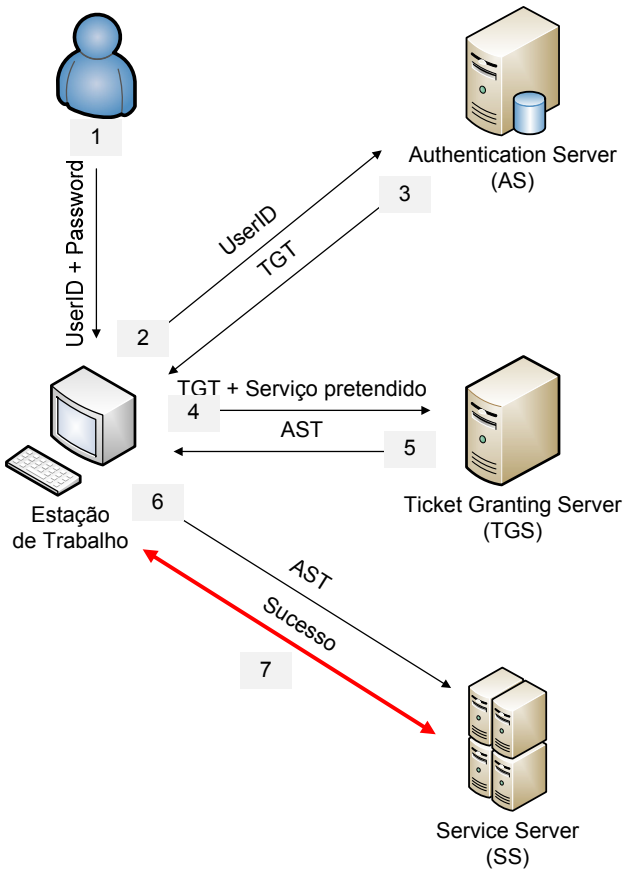

Figura 15 - Funcionamento do Kerberos

De notar que o pedido de um TGT ocorre uma vez por utilizador e por sessão enquanto o pedido de AST ocorre uma vez por tipo de serviço, dentro da sessão. Já o pedido de serviço a um servidor ocorre uma vez por sessão de serviço.

É também possível efectuar o pedido para acesso a serviços em servidores que estão localizados em sistemas remotos, também eles protegidos por um sistema *Kerberos*. Para tal, torna-se necessário que os sistemas *Kerberos* se autentiquem mutuamente, de forma a permitir que utilizadores com credenciais de um possam ser reconhecidos pelo outro. Desta forma, se um utilizador pretender utilizar um serviço de um sistema remoto tem de começar por efectuar o pedido de um *ticket* adequado ao seu TGS, para poder colocar, por sua vez, o pedido de acesso ao serviço no TGS remoto. Será este que lhe poderá entregar um AST para a utilização do serviço pretendido. Assim, a autenticação do utilizador ocorre localmente, mas são-lhe concedidos serviços que estão em outros domínios, tal como é possível ver na figura seguinte:

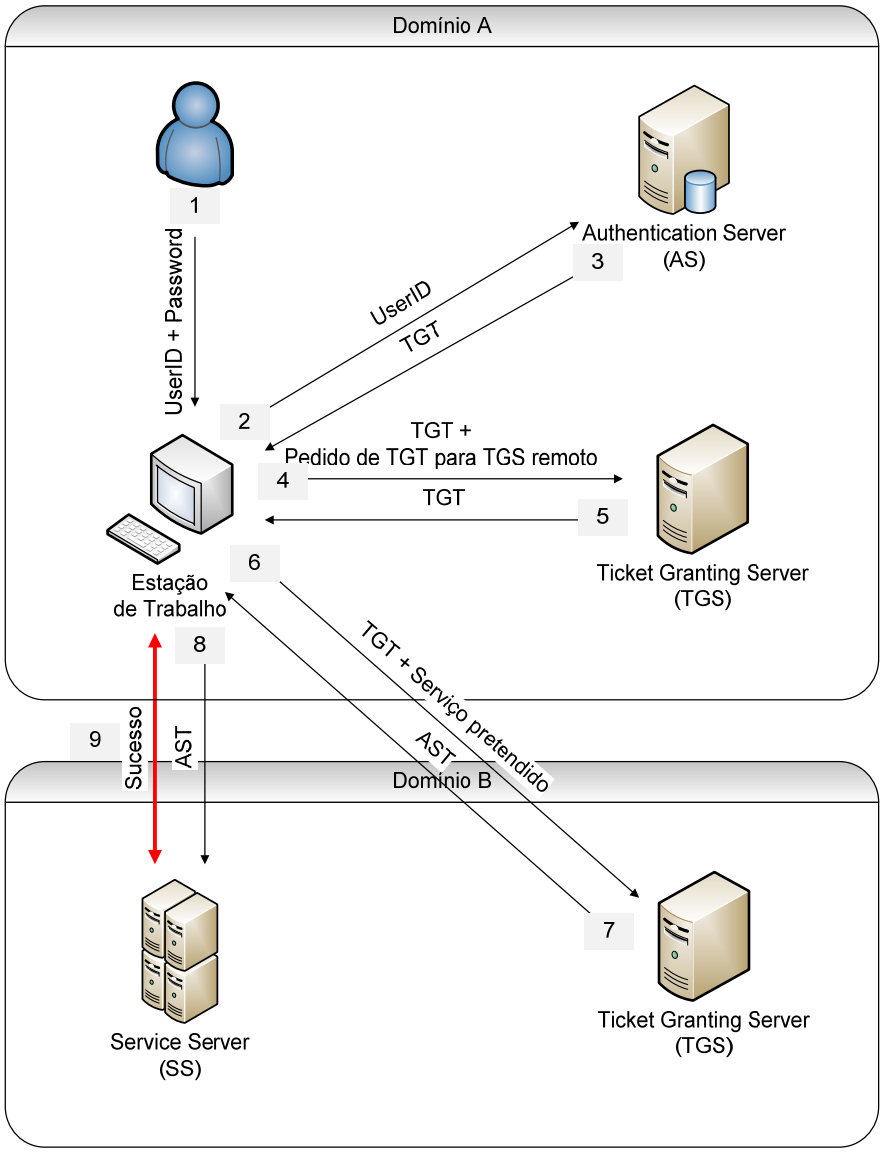

Figura 16 - Autenticação Kerberos em múltiplos domínios

2.4.4. Limitações do Kerberos

Tal como todos os sistemas, o *Kerberos* também tem limitações.

A maior limitação é a obrigatoriedade de ter um servidor *Kerberos* que, se indisponível, pode fazer com que ninguém consiga autenticar-se na rede (isto pode ser resolvido utilizando diversos servidores *Kerberos*). Outra das limitações está relacionada com o facto de este sistema ser apenas adequado para aplicações cliente/servidor. Também estão relatados problemas com *multi-homed hosts* (utilizam mais de um endereço IP).

Debrucemo-nos ainda sobre mais uma lacuna que está relacionada com a necessidade de manter os relógios de todas as partes envolvidas sincronizados (em geral a diferença não pode ultrapassar dez minutos) evitando assim problemas com os *timestamps,* visto que os *tickets* têm um tempo de vida e se o relógio do cliente não estiver sincronizado com o do servidor, a autenticação irá falhar.

Capítulo 3

3. Trabalho Desenvolvido

3.1. Introdução

Nesta secção apresentamos todo o trabalho desenvolvido, os resultados alcançados, bem como a justificação de todas as opções tomadas, permitindo assim uma total integração do leitor com o trabalho apresentado.

3.2. Módulo de Gestão de Perfis de Utilizador

3.2.1. Introdução

Da leitura da secção 2 facilmente se conclui que o Portal SAA permite que os seus utilizadores realizem um vasto número de operações. Essas operações vão desde simples Pesquisas de Alarme até Operações Administrativas. Para tornar o Portal mais seguro e mais intuitivo para os utilizadores foi desenvolvido um módulo de Gestão de Perfis de Utilizador.

Foi com isto em mente que este módulo foi desenhado, testado e implementado, com o objectivo de reduzir o número de opções dadas a cada utilizador. Cada utilizador apenas utiliza um número reduzido de operações dependendo da sua função na empresa, não havendo por isso necessidade de lhe dar liberdade total, o que poderia causar graves problemas tendo em conta que, por exemplo, o reconhecimento errado de um alarme pode causar sérios danos.

3.2.2. Implementação

3.2.2.1. Alteração de Perfil de Utilizador

As alterações efectuadas permitem ao Administrador do Sistema (visto ser o único que tem acesso a este módulo) mudar o perfil de um operador, recorrendo a um ambiente gráfico disponível no Portal. Assim, as alterações são feitas de uma maneira mais óbvia e simples, em oposição ao método anteriormente utilizador que obrigava a fazer as mudanças directamente na Base da Dados (*yerba*).

Para controlar os privilégios de acesso pelos utilizadores aos diferentes módulos, é utilizado o campo *gid* da tabela *yerba_usuarios* da Base de Dados *yerba*. Cada tipo de privilégio tem um *bit* associado:

Bit	Peso	Tipo	Privilégio
0	1	Administração do Portal	root, configuração do Portal
1	2	Operação	Janela de Alarmes
2	4	Operação	Janela de alarmes com Mapas
3	8	Operação	Alterar o estado do alarme e do componente (Reconhecimento, Fim manual e Inibição de alarmes)
4	16	Operação	Acesso a módulos adicionais de consulta
5	32	Operação	Ver monitoria, tabelas de configuração e Domínios
6	64	Operação	Utilizador normal – perfil por omissão
7	128	Administração	Administrar monitoria, tabelas de configuração e Domínios (Tecnologias, Subsistemas, Domínios de Gestão, Perfis e Domínios Organizacionais)

Tabela 3 - Privilégios de Acesso

Tendo isto em conta, foram criados dois ambientes gráficos para alterar perfis:

1. Permite visualizar simultaneamente uma lista com vários operadores, sendo possível aplicar filtros para uma pesquisa mais exacta e alterar vários perfis em simultâneo;

2. Pode ser acedido através do primeiro ou directamente através das opções do Administrador e dá acesso a uma vista personalizada de um dado utilizador.

Passamos agora a descrever os dois com mais pormenor.

3.2.2.1.1. Formulário que permite mudar vários perfis ao mesmo tempo

O objectivo deste formulário foi permitir ao Administrador comparar vários utilizadores ao mesmo tempo, permitindo assim gerir melhor os perfis. De notar que neste formulário também é dada a possibilidade ao Administrador de alterar o Grupo de Gestão dos utilizadores, visto que o Grupo de Gestão também é um factor que influencia as opções de cada utilizador (este assunto será abordado com mais detalhe nas secções seguintes).

Na figura seguinte é visível o ambiente gráfico criado:

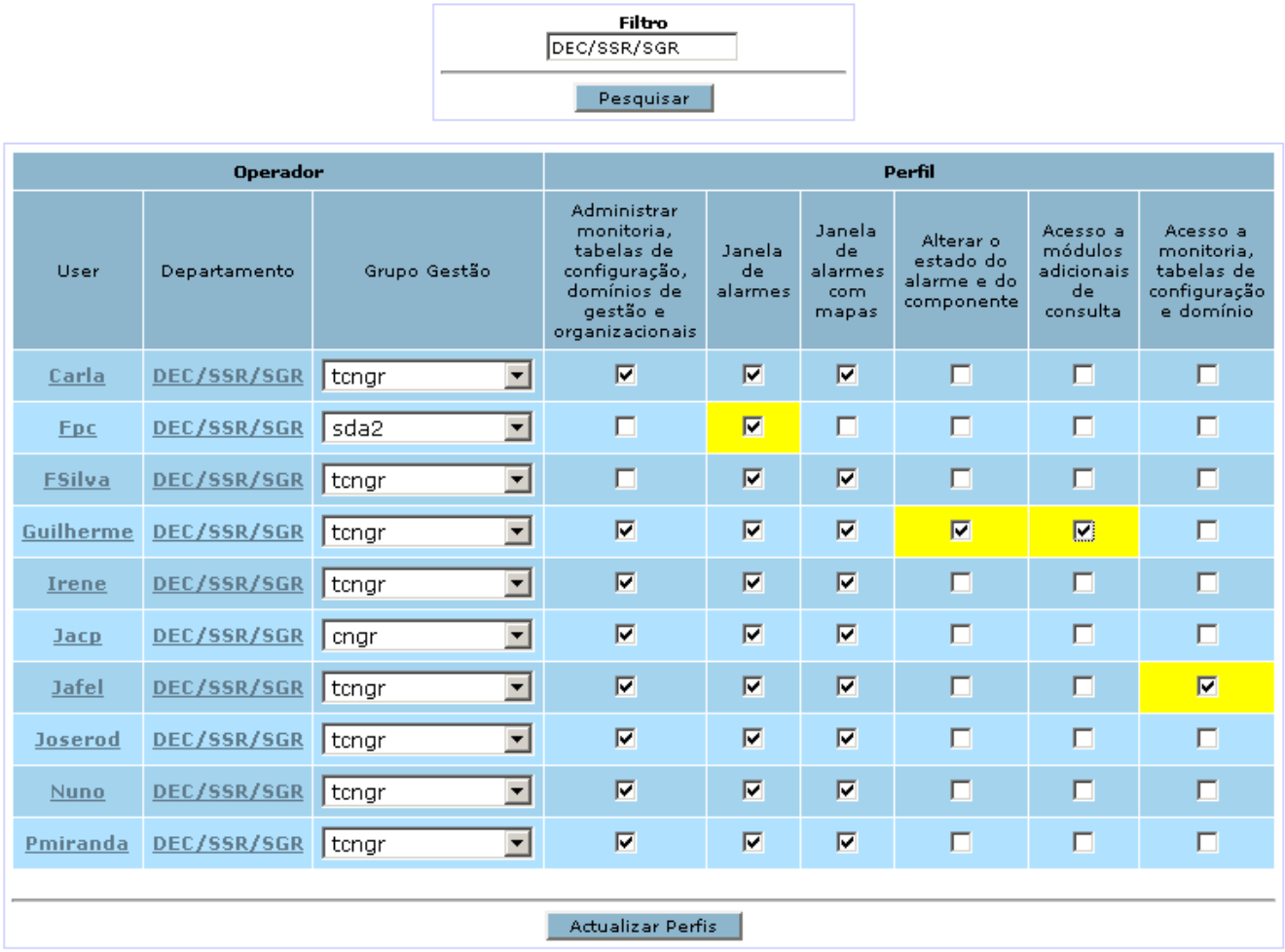

Figura 17 - Formulário para editar perfis de utilizador

Através desta figura é facilmente perceptível a facilidade com que os perfis são alterados, bastando para isso "clicar" nas *checkboxes* para activar ou desactivar uma funcionalidade. É possível listar vários utilizadores ao mesmo tempo e realizar várias alterações em diversos utilizadores em simultâneo (tal como é visível na imagem anterior), o que nos levou a optar por assinalar a amarelo as mudanças efectuadas. Assim, quando o Administrador

alterar algum perfil essa mudança fica a amarelo até o botão "Actualizar Perfis" ser submetido.

No momento em que a página é carregada não são apresentados utilizadores no ecrã, visto que não fazia sentido carregar os cerca de 600 utilizadores para depois editar o perfil de uma minoria (possivelmente até só de um). Por esse motivo, quando a página é carregada apenas aparece o filtro que o Administrador tem de escolher antes de os utilizadores serem listados. Existe naturalmente a possibilidade de não ser escolhido nenhum filtro, o que faz com que todos os operadores sejam listados.

O filtro permite pesquisar pelo *alias* do operador, pelo nome (apesar de esta informação não aparecer visível na página), pelo departamento e/ou pelo Grupo de Gestão. Com estas funcionalidades torna-se possível comparar utilizadores de uma forma rápida e simples, bem como fazer várias alterações de uma só vez (por exemplo, mudar o perfil de todos os utilizadores de um dado departamento).

Este formulário, quando submetido, vai actualizar o campo *gid* da tabela *yerba_usuarios* (bd *yerba*), sendo depois este campo (e o Domínio de Gestão) usado para gerar os menus visíveis a cada utilizador.

3.2.2.1.2. Formulário individual para mudar o perfil de um operador

Na figura seguinte é visível o ambiente gráfico criado:

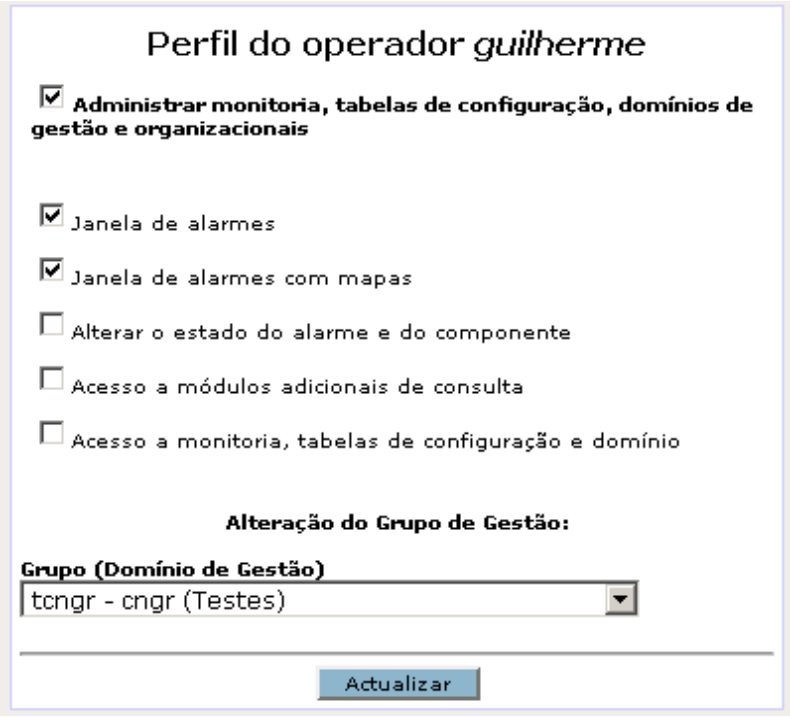

Figura 18 - Formulário individual para mudar perfil de utilizador

Com esta interface o Administrador tem uma visão mais pormenorizada do perfil do operador, continuando a dispor da possibilidade de o alterar através das *checkboxes*. Este formulário, tal como o anterior, permite modificar o Domínio de Gestão do operador (que, tal como já foi referido, também é usado para gerar os menus visíveis a cada utilizador).

3.2.2.1.3. Base de Dados

Todas as alterações referidas nesta secção terão impacto na Base de Dados *yerba*, tabela *yerba_usuarios*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
Uid	*integer*	Número identificador
Gid	*integer*	Perfil
Nombre	*character varying (35)*	Nome
Alias	*character varying (20)*	*Username*
Clave	*character varying (32)*	*Password*
Correo	*character varying (50)*	E-Mail
Icq	*character varying (35)*	Departamento
Edad	*character (2)*	(não é usado)
Web	*character varying (80)*	Telefone
Sexo	*character (1)*	(não é usado)
Pais	*character varying (35)*	Grupo de Gestão
Idioma	*character varying (40)*	Idioma
Estilo	*character varying (50)*	Estilo de Apresentação
Detalle	*text*	Descrição
Publico	*character (1)*	Visibilidade (pública ou privada)

Tabela 4 - Base de Dados yerba - Tabela yerba_usuarios

Tal como é possível constatar na tabela apresentada anteriormente, o nome das colunas está em espanhol. Este facto advém da estrutura da Base de Dados (*yerba*) ter sido rea-

proveitada de um Portal proveniente da Argentina. É também por este facto que alguns campos têm finalidades bastantes diferentes do que o seu nome poderia sugerir (por exemplo, a coluna *pais* poderia sugerir que fosse destinada a albergar a nacionalidade do utilizador, mas na verdade é destinada ao Grupo de Gestão do mesmo).

3.2.2.2. Grupos de Acesso

Os Grupos de Acesso estão relacionados com a organização estrutural da empresa (PT Comunicações), sendo que derivam da história da mesma, quando eram diferentes empresas (dentro do mesmo grupo) que analisavam diferentes áreas. Hoje em dia, apesar de estar tudo concentrado na mesma empresa, as divisões mantêm-se visto que são diferentes departamentos que supervisionam as diferentes áreas.

Assim, existem actualmente quatro grupos de acesso, estando eles visíveis na imagem seguinte:

Figura 19 - Grupos de Acesso

Apesar de estes grupos não serem alterados com frequência, todo o módulo de Gestão de Perfis foi baseado nestes grupos, uma vez que é através deles que a separação dos menus é feita. Assim, tudo foi feito de uma maneira genérica, sendo apenas necessário alterar os Grupos de Acesso neste formulário para alterar os mesmos nos menus.

3.2.2.2.1. Base de Dados

Todas as alterações referidas nesta secção terão impacto na Base de Dados *retadm*, tabela *acessos*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
nome	*character(10)*	Sigla identificadora do sub-sistema
descricao	*character(70)*	Sigla identificadora da tecnologia
peso	*integer*	Domínio físico (r ou c)

Tabela 5 - Base de dados retadm - Tabela acessos

3.2.2.3. Tecnologias

Este formulário, tal como o próprio nome permite concluir, refere-se a tudo o que está relacionado com as Tecnologias. Assim, é aqui possível adicional uma nova tecnologia, editar uma já existente ou até mesmo removê-la. Para tal, são usados (Base de Dados *retadm*) os seguintes dados:

- **Tecnologia**: sigla que caracteriza a tecnologia;
- **Descrição**: pequena descrição que geralmente apenas contém o nome da Tecnologia por extenso (visto que no campo Tecnologia apenas contém a sigla);
- **Sub-Sintra**: campo numérico que tem por objectivo fazer a interligação com o *sintra*[4], ou seja, atribui uma equipa do *sintra* à Tecnologia em questão;
- **Forçar**: *checkbox* que, quando seleccionada, faz com que esta Tecnologia, independentemente de ter alarmes no histórico ou não, vai ser usada no *geradg* para gerar pares local / tecnologia (sem a *checkbox* seleccionada, apenas os pares local / tecnologia com alarmes no histórico vão ser criados);
- **Domínio Organizacional**: o Domínio Organizacional é usado no módulo *notif* com o objectivo de apenas apresentar as Tecnologias associadas ao Domínio Organizacional do operador (que no fundo está associado ao Domínio de Gestão). Devido à complexidade da explicação que foi dada, apresentamos um pequeno exemplo: se um operador pertence ao Domínio de Gestão (grupo) *sda2* vai ter o Domínio Organizacional associado aos "Dados", logo no módulo *notif* só vai ter acesso às tecnologias que tenham o mesmo Domínio Organizacional ("Dados").

[4] Sistema de Tratamento de Avarias

Apresentamos então uma imagem do formulário que permite adicionar uma nova tecnologia:

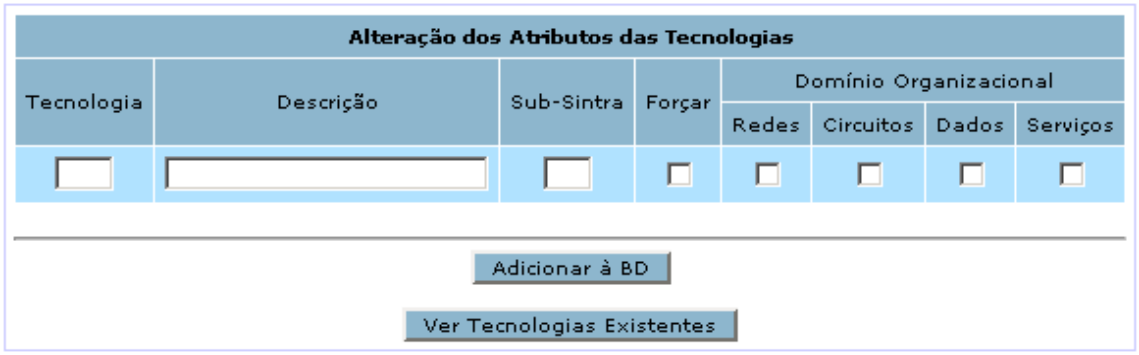

Figura 20 - Formulário para adicionar nova Tecnologia

E uma imagem da edição de uma tecnologia já existente:

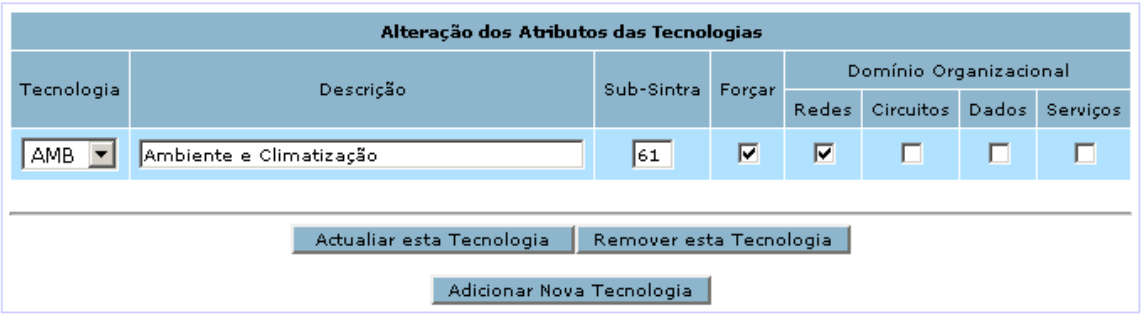

Figura 21 - Formulário para editar uma Tecnologias já existente

Tal como é possível constatar pela análise de qualquer uma das imagens apresentadas em cima, é necessário seleccionar o Domínio Organizacional referente à tecnologia em causa. Esse Domínio Organizacional vai permitir enquadrar a Tecnologia na sua área de impacto.

3.2.2.3.1. Base de Dados

Todas as alterações referidas nesta secção terão impacto na Base de dados *retadm*, tabela *tecnologia*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_tec	*integer*	Número identificador
nome_tec	*character (3)*	Sigla identificadora da tecnologia

descricao	*character (70)*	Descrição
sub_sintra	*integer*	Equipa do Sintra
tipo_tec	*integer*	Domínio Organizacional
forcar	*character (1)*	Bit para forçar no *geradg*

Tabela 6 - Base de dados retadm - Tabela tecnologia

3.2.2.4. Sub-Sistemas

Tal como no caso das Tecnologias, este formulário refere-se a tudo o que se relaciona com os Sub-Sistemas. Recorrendo à tabela *subsistema* os dados referentes ao Sub-Sistema seleccionado são carregados e apresentados no formulário. Entre os dados carregados da Base de Dados encontramos:

- **Sub-Sistema:** sigla que caracteriza o Sub-Sistema;
- **Descrição:** pequena descrição que geralmente apenas contém o nome do Sub-Sistema por extenso (visto que no campo Sub-Sistema apenas contém a sigla);
- **Tecnologia Dominante:** tecnologia que os alarmes internos ao sistema herdam (com base no sub-sistema);
- **Ficheiro de Configuração:** ficheiro com configurações usado pelo formatador;
- **Formatador:** informação sobre o nome do binário usado para formatar;
- **Separador:** *string* (que pode ser uma expressão regular) que indica onde começa o relatório de alarme deste sub-sistema;
- **Domínio Organizacional:** o Domínio Organizacional é usado no módulo *notif* com o objectivo de apenas apresentar os Sub-Sistemas associadas ao Domínio Organizacional do operador (que no fundo está associado ao Domínio de Gestão). Devido à complexidade da explicação que foi dada, apresentamos um pequeno exemplo: se um operador pertence ao Domínio de Gestão (grupo) *sda1* vai ter o Domínio Organizacional associado às "Redes", logo no módulo *notif* só vai ter acesso aos sub-sistemas que tenham o mesmo Domínio Organizacional ("Redes").

Na imagem seguinte é possível observar o formulário descrito:

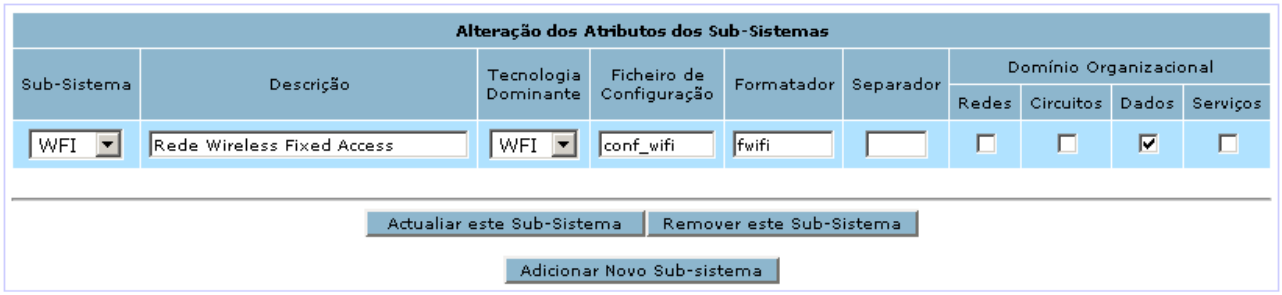

Figura 22 - Formulário para editar um Sub-Sistema já existente

Além da possibilidade de editar um Sub-Sistema existente, o Administrador tem a possibilidade de o remover e de adicionar um novo Sub-Sistema. Na imagem seguinte é possível ver o formulário respectivo a este último caso (adicionar novo Sub-Sistema):

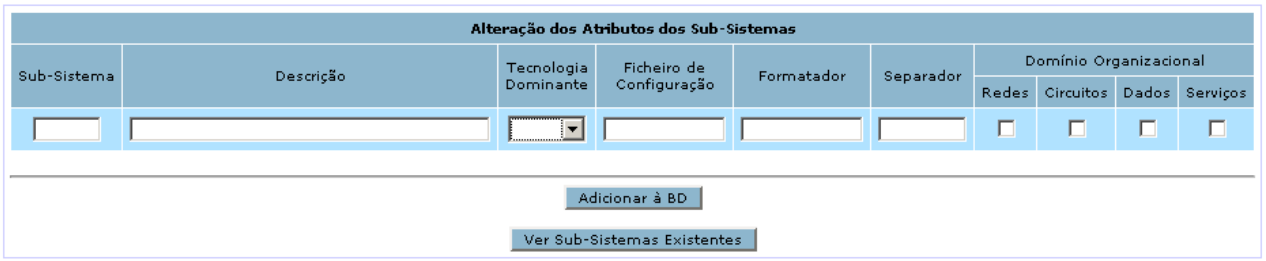

Figura 23 - Formulário para adicionar novo Sub-Sistema

3.2.2.4.1. Base de Dados

Todas as alterações referidas nesta secção terão impacto na Base de dados *retadm*, tabela *subsistema*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_sub	*integer*	Número identificador
tipo_sub	*integer*	Domínio Organizacional
nome_sub_sup	*character (3)*	Sigla identificadora do sub-sistema
fic_conf	*character (15)*	Ficheiro de configuração
nome_form	*character (15)*	Nome do binário usado
separador	*character (15)*	String separadora de relatórios

descricao	*character (70)*	Descrição
id_tec_dom	*integer*	Tecnologia dominante

Tabela 7 - Base de Dados retadm - Tabela subsistema

3.2.2.5. Domínios Organizacionais

Este formulário é extremamente importante no âmbito da reestruturação do RETA, pois é através deste formulário que os alarmes são encaminhados para o processamento correcto.

Assim sendo, cada par Sub-Sistema / Tecnologia tem um Domínio Físico e um Domínio Organizacional, sendo que o Domínio Físico apenas é utilizado para saber em que Base de Dados será guardado o Relatório do Alarme. O papel do Domínio Organizacional é mais evidente aos olhos dos utilizadores, porque cabe a este encaminhar os alarmes para o Processamento de Alarmes correcto.

Apresentamos agora uma imagem elucidativa do formulário criado:

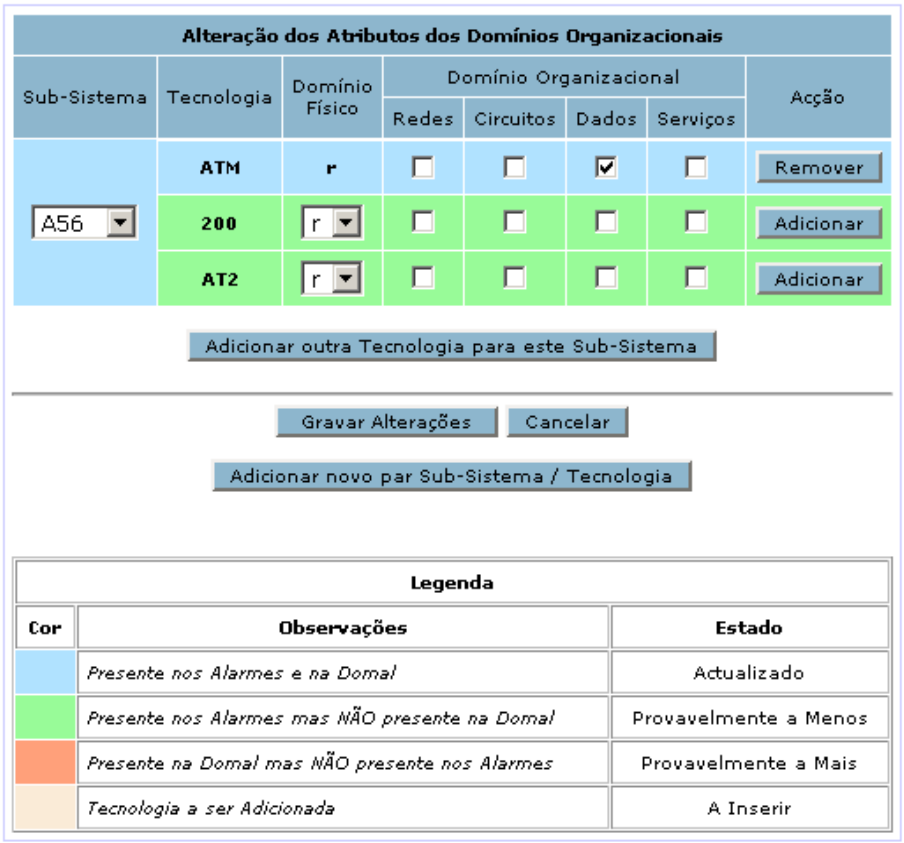

Figura 24 - Domínios Organizacionais

Este formulário permite não só seleccionar um Domínio Físico e um Domínio Organizacional para um par Sub-Sistema / Tecnologia, como dá possibilidade ao Administrador do Sistema (lembrar que apenas o Administrador tem acesso a estes módulos) de adicionar ou remover Tecnologias para o Sub-Sistema seleccionado.

Para facilitar a tarefa do Administrador são disponibilizadas no formulário dicas relativamente às Tecnologias que o Sub-Sistema seleccionado deveria ter. Para isto, é percorrida a tabela *Alarmes* para detectar as Tecnologias dos alarmes presentes na tabela (que tem o histórico dos alarmes dos últimos 6 meses) para o Sub-Sistema em questão. Depois de todas as Tecnologias serem pesquisadas, são comparadas com as que já estão associadas ao Sub-Sistema e, em caso de a Tecnologia já estar associada, é atribuída a cor azul no formulário. No caso de existir uma Tecnologia nos alarmes mas ainda não estar associada ao Sub-Sistema, é atribuída a cor verde (sendo de notar que esta Tecnologia provavelmente estará em falta e deverá ser associada ao Sub-Sistema). Por último, no caso em que a Tecnologia já esteja associada ao Sub-Sistema mas não seja encontrado nenhum alarme para aquele Sub-Sistema com essa Tecnologia, será atribuída a cor laranja (ao contrário do primeiro caso, em que a Tecnologia estará possivelmente a mais na tabela, e poderá ser removida visto não existirem alarmes para a mesma).

É ainda possível ao Administrador adicionar uma Tecnologia manualmente para o Sub-Sistema escolhido, sendo apenas necessário carregar no botão "Adicionar outra Tecnologia para este Sub-Sistema" sendo que o formulário terá o seguinte aspecto:

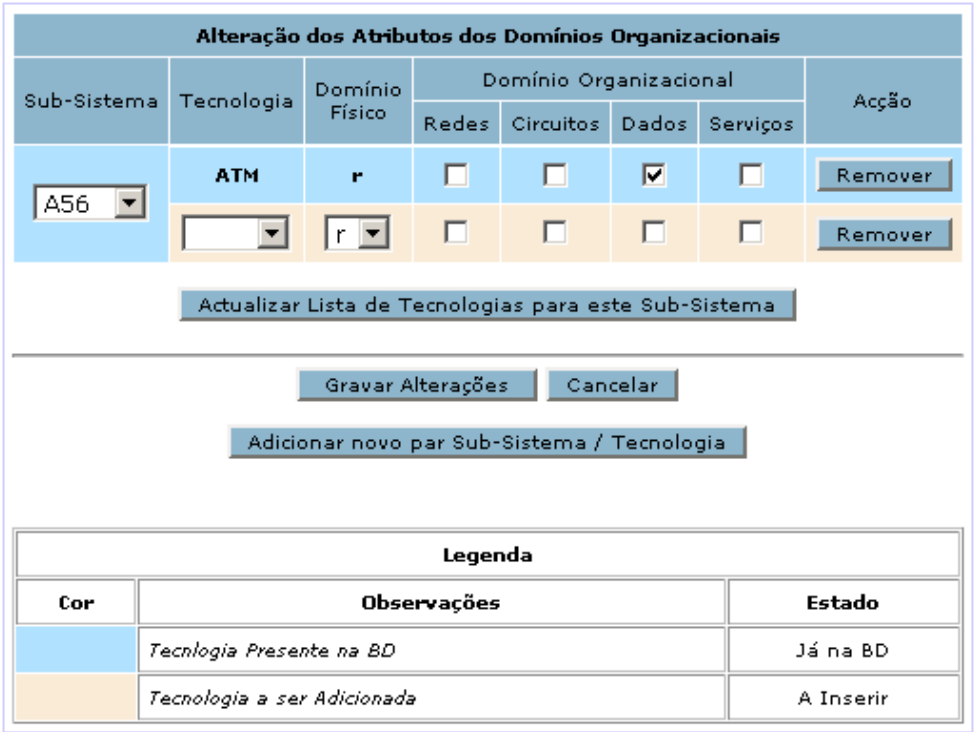

Figura 25 - Formulário para adicionar nova Tecnologia para um dado Sub-Sistema

Neste formulário o Administrador pode seleccionar uma Tecnologia da lista de Tecnologias existentes (de notar que as tecnologias já associadas a este Sub-Sistema – neste caso o ATM – não aparecem na lista) para atribuir ao Sub-Sistema (neste caso o A56). É também conveniente que seja seleccionado o Domínio Físico (que por omissão é o r – rede) e o Domínio Organizacional, já que se o Domínio Organizacional não for seleccionado, os alarmes do par Sub-Sistema / Tecnologia adicionado não vão ser encaminhados para nenhuma área (vão directamente para o Histórico).

É ainda possível adicionar um novo par Sub-Sistema / Tecnologia bastando para isso no botão respectivo. O formulário apresentado será o seguinte:

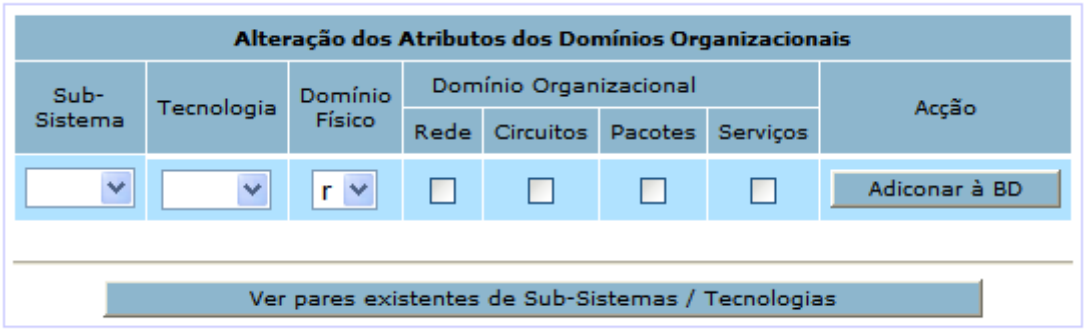

Figura 26 - Formulário para adicionar novo par Sub-Sistema / Tecnologia

De notar que apenas é possível seleccionar Sub-Sistemas existentes. O mesmo se passa com as Tecnologias. Deste modo, se a intenção do Administrador for seleccionar uma Tecnologia que ainda não existe na lista, tem de primeiro criá-la no formulário respectivo (ver secção *3.2.2.3 – Tecnologias*). O mesmo se passa para os Sub-Sistemas (ver secção *3.2.2.4 – Sub-Sistemas*).

3.2.2.5.1. Base de Dados

Todas as alterações referidas nesta secção terão impacto na Base de dados *retadm*, tabela *domal*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
nome_sub_sup	*character(3)*	Sigla identificadora do sub-sistema
nome_tec	*character(3)*	Sigla identificadora da tecnologia
domfil	*character(1)*	Domínio físico (r ou c)
mdomo	*smallint*	Domínio Organizacional

Tabela 8 - Base de Dados retadm - Tabela domal

3.2.2.6. Domínios de Gestão

3.2.2.6.1. Introdução

Este formulário, referente aos Domínios de Gestão, é o mais complexo de todos os apresentados até ao momento, resultado da grande flexibilidade do mesmo e do número de opções que permite realizar.

Tal como será possível observar com maior detalhe nas secções seguintes, o Administrador tem disponíveis as seguintes opções:

- Criar um Domínio de Gestão novo;
- Actualizar um Domínio de Gestão já existente;
- Remover um Domínio de Gestão já existente;
- Consultar / Editar / Adicionar novas / Remover Tecnologias de um dado Domínio de Gestão;
- Consultar / Editar Esquemas de Locais de um dado Domínio de Gestão;
- Consultar / Adicionar Excepções não contempladas pelo resultado do GeraDG;
- Ver Resultados do GeraDG para um dado Domínio de Gestão.

Apresentamos em seguida uma descrição dos itens referidos anteriormente, bem como algumas imagens ilustrativas dos formulários criados.

3.2.2.6.2. Adicionar Domínio de Gestão

Este formulário permite adicionar um novo Domínio de Gestão. Para tal, basta o Administrador preencher os seguintes campos:

- **Domínio:** o nome do Domínio de Gestão a ser adicionado;
- **Observação:** uma pequena descrição para melhor identificar o Domínio a ser criado;
- **Domínio Organizacional:** este campo é de extrema importância visto ser através do Domínio de Gestão que os alarmes são distribuídos. É portanto neste campo que é feita a associação do Grupo de Gestão criado com a sua área de intervenção (no fundo os alarmes a que vão ter acesso).

Na imagem seguinte está ilustrado o formulário criado:

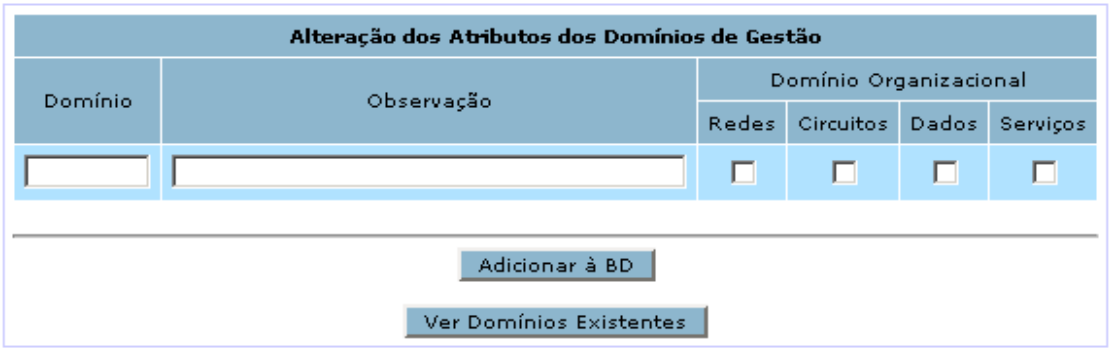

Figura 27 - Formulário para adicionar um novo Domínio de Gestão

3.2.2.6.2.1. Base de Dados

As alterações referidas anteriormente terão impacto na Base de dados *retadm*, tabela *grupo*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_grupo	*integer*	Número identificador
nome_grupo	*character (20)*	Sigla identificadora do grupo
obs	*character(30)*	Observação
domorg	*smallint*	Domínio Organizacional

Tabela 9 - Base de Dados retadm - Tabela grupo

3.2.2.6.3. Actualizar um Domínio de Gestão já existente

Este é o formulário base que permite gerir um Domínio de Gestão, através do qual é possível realizar todas as operações enumeradas em 3.2.2.6.1. De notar, no entanto, que as únicas operações que podem ser executadas directamente neste formulário são a de Editar um Domínio de Gestão (bastando para isso editar directamente os campos pretendidos) e a de Remover um Domínio de Gestão. Para todas as outras existe um *link* (um botão) que remete para o formulário pretendido.

Na imagem da página seguinte é visível o que foi explicado anteriormente.

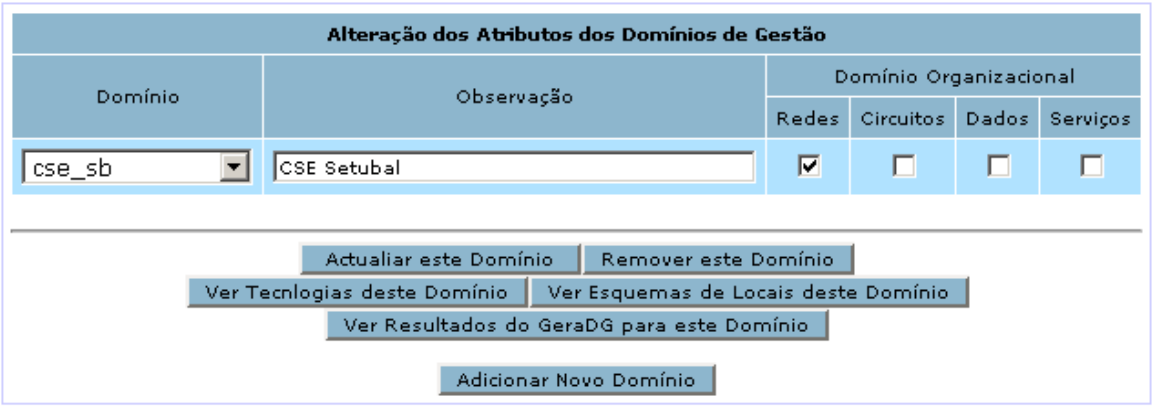

Figura 28 - Formulário que permite editar um Domínio de Gestão

3.2.2.6.3.1. Base de Dados

As alterações referidas anteriormente terão impacto na Base de dados *retadm*, tabela *grupo*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_grupo	*integer*	Número identificador
nome_grupo	*character (20)*	Sigla identificadora do grupo
obs	*character(30)*	Observação
domorg	*smallint*	Domínio Organizacional

Tabela 10 - Base de Dados retadm - Tabela grupo

3.2.2.6.4. Tecnologias

Um Domínio de Gestão correctamente configurado necessita de tecnologias associadas, pois essas tecnologias permitirão ao *geradg* criar pares Local / Tecnologia para posteriormente serem vistos na Janela de Alarmes. Assim, tornou-se essencial criar um formulário para adicionar (e remover) tecnologias de um dado Domínio de Gestão.

Esse formulário é visível na figura da página seguinte.

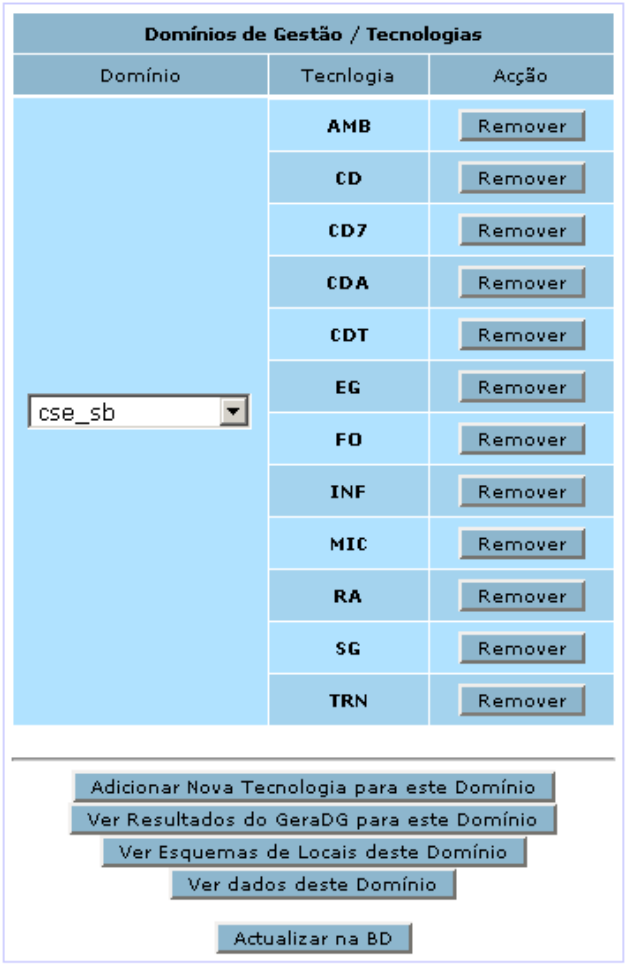

Figura 29 - Formulário que permite adicionar ou remover Tecnologias de um Domínio de Gestão

3.2.2.6.4.1. Base de Dados

As alterações referidas anteriormente terão impacto na Base de dados *retadm*, tabela *grp_tec*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_grp_tec	*integer*	Número identificador
id_tec	*integer*	Identificador da Tecnologia
id_grupo	*integer*	Identificador do Domínio de Gestão

Tabela 11 - Base de Dados retadm - Tabela grp_tec

3.2.2.6.5. Esquema de Locais

Este formulário apresenta alguma complexidade, dada a sua capacidade de gerar expressões regulares de uma maneira rápida e simples. Com este formulário não é necessário conhecer o funcionamento das expressões regulares, sendo suficiente o conhecimento do que se pretende que aquelas abranjam e preencher os campos respectivos.

Para atingir este fim recorreu-se ao *JavaScript*, sendo gerada dinamicamente a expressão regular à medida que o Administrador vai preenchendo os campos. Após o preenchimento de todos os campos, a expressão regular final fica visível no campo a cinzento que tem o título "Expressão Regular Gerada". Cabe em seguida ao Administrador decidir se quer utilizar a expressão gerada ou construir manualmente uma expressão regular de raiz. Para isto já é preciso ter conhecimentos sobre expressões regulares, sendo que a mesma deve ser introduzida no campo correspondente (no campo assinalado como tal). De notar que se o Administrador optar por utilizar a expressão regular gerada dinamicamente através de *JavaScript*, deve carregar no botão "Usar a expressão regular gerada". Ao carregar no botão, a expressão que estava no campo a cinzento vai ser copiada para o campo inferior, destinado a ter a expressão regular final a ser introduzida na Base de Dados.

Na figura seguinte é visível o ambiente criado:

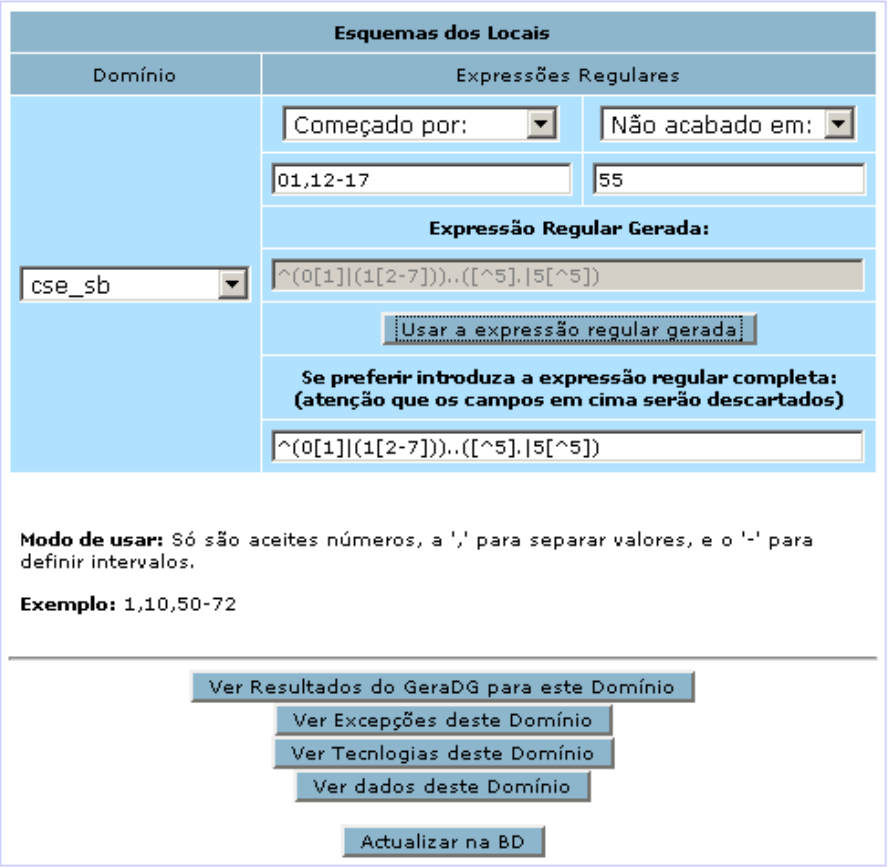

Figura 30 - Formulário que permite criar expressões regulares para associar a um Domínio de Gestão

Tal como é possível visualizar na figura anterior, a expressão regular gerada na imagem vai contemplar todos os códigos de local que comecem por "01" e por todos os valores no intervalo de "12 a 17". De notar que os códigos que acabem em "55" não serão apresentados, visto ter sido essa a configuração escolhida neste exemplo.

No exemplo seguinte os locais pretendidos já não são os mesmos, tendo-se optado por ver todos os códigos de local que não comecem por "02" e que acabem no intervalo de "00 a 49":

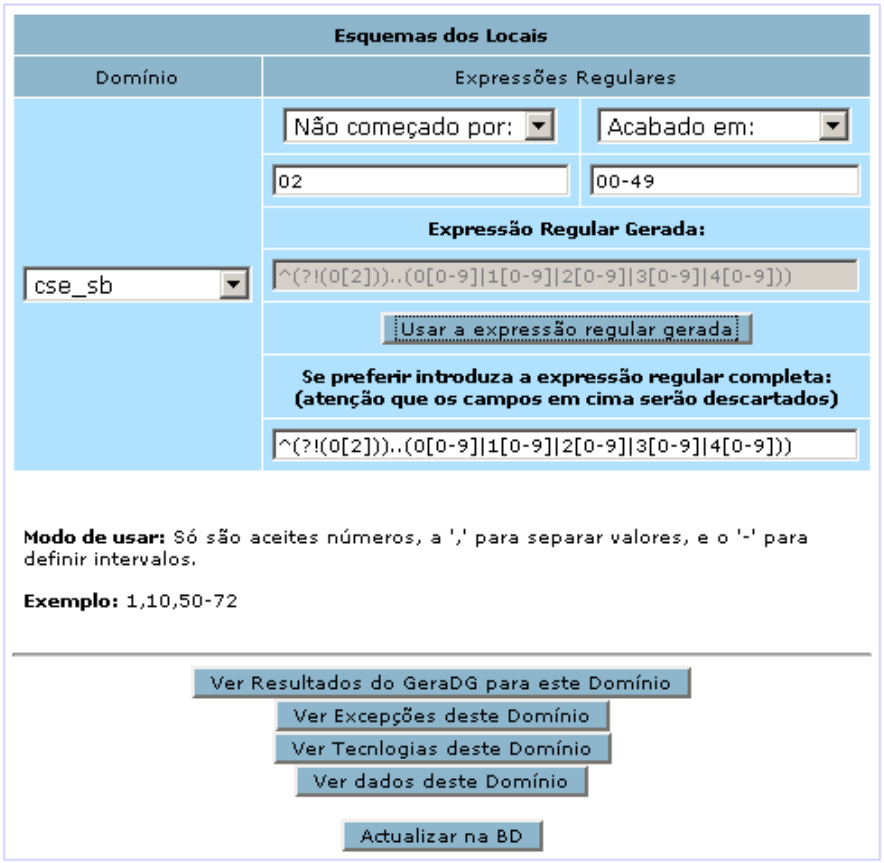

Figura 31 - Formulário que permite criar expressões regulares para associar a um Domínio de Gestão

É no entanto importante salientar que estes exemplos foram escolhidos propositadamente com o intuito de ilustrar o funcionamento da aplicação. Na grande maioria dos casos reais (embora haja excepções) a configuração é mais elementar, sendo por exemplo apenas relevante ver todos os códigos locais começados por "01".

Este último exemplo pode ser visualizado na figura seguinte.

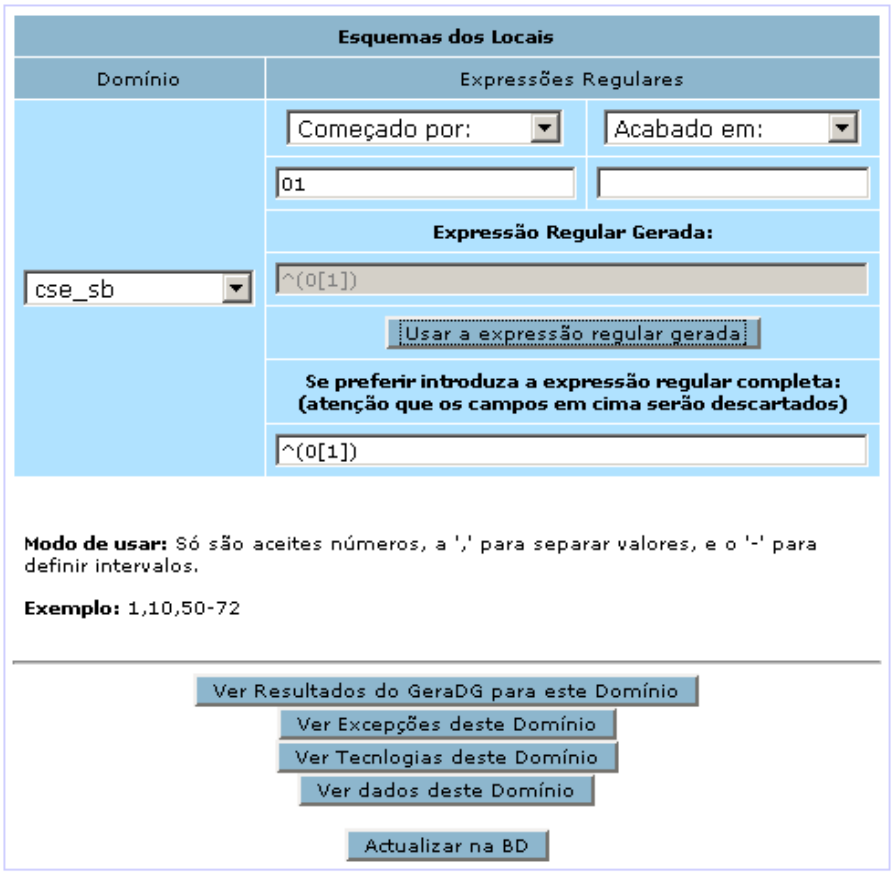

Figura 32 - Formulário que permite criar expressões regulares para associar a um Domínio de Gestão

Devido à sua importância e complexidade, apresentamos no **Anexo A** o código *JavaScript* desenvolvido para o efeito (gerar expressões regulares dinamicamente).

3.2.2.6.5.1. Base de Dados

As alterações referidas anteriormente terão impacto na Base de dados *retadm*, tabela *esq_loc*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_dg_geog	*integer*	Número identificador
id_grupo	*integer*	Identificador do Domínio de Gestão
nome_dg	*character (20)*	Nome
exp_local	*character varying*	Expressão Regular

Tabela 12 - Base de Dados retadm - Tabela esq_loc

3.2.2.6.6. Excepções

Devido à complexidade da rede da PT Comunicações e, apesar dos benefícios trazidos com o uso de expressões regulares para gerar os códigos locais visíveis de cada Domínio de Gestão, foi necessário continuar a dar a possibilidade de introduzir manualmente pares Local / Tecnologia para um dado Domínio de Gestão. Assim, no seguimento do que foi feito, foi criado um formulário para o efeito, evitando assim a introdução manual na Base de Dados (como era feito anteriormente).

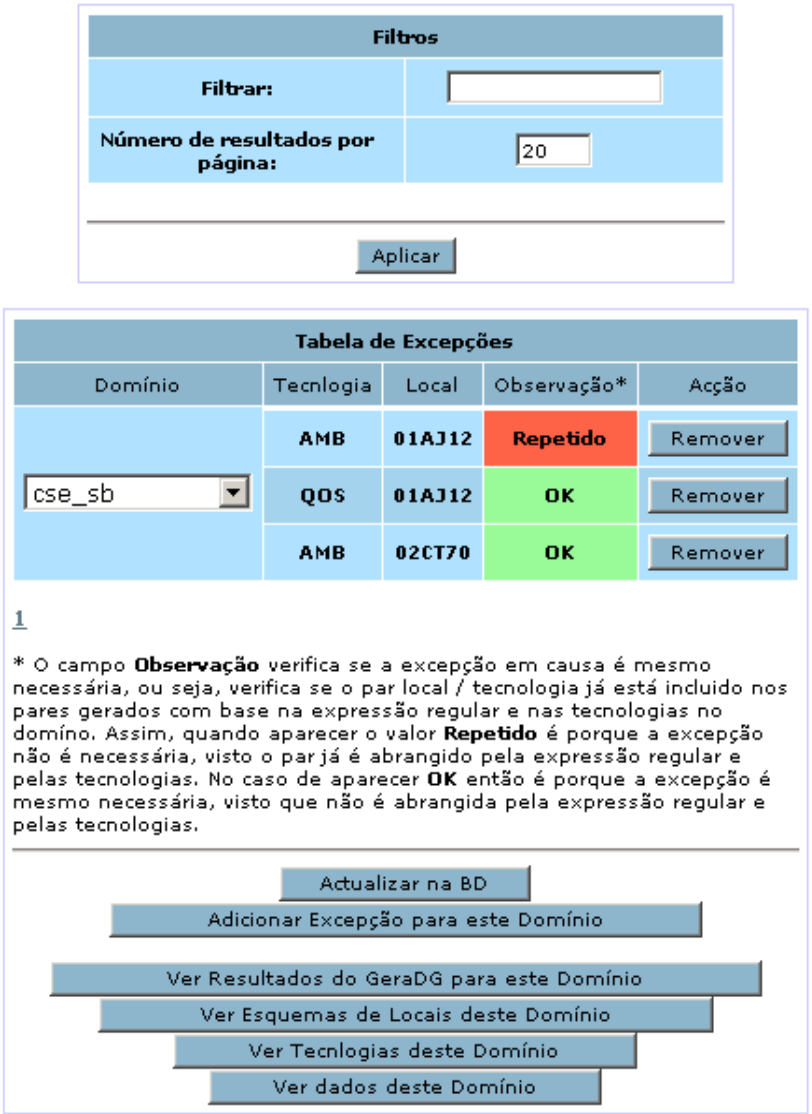

Figura 33 - Tabela de Excepções para um Domínio de Gestão

Tal como é possível observar, é dada ao Administrador a possibilidade de aplicar filtros de maneira a possibilitar a pesquisa por entre as excepções já adicionadas. Assim, além de facilitar a pesquisa de um local ou uma tecnologia em concreto, pode evitar que sejam introduzidas excepções repetidas.

É ainda de salientar o campo "Observação" que, tal como é visível na imagem, *"verifica se a excepção em causa é mesmo necessária, ou seja, verifica se o par local / tecnologia já está incluído nos pares gerados, com base na expressão regular e nas tecnologias no domínio. Assim, quando aparecer o valor Repetido é porque a excepção não é necessária, visto que o par já é abrangido pela expressão regular e pelas tecnologias. No caso de aparecer OK então é porque a excepção é mesmo necessária, visto que não é abrangida pela expressão regular e pelas tecnologias*."

3.2.2.6.6.1. Base de Dados

As alterações referidas anteriormente terão impacto na Base de dados *retadm*, tabela *dg_ex*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_dg	*integer*	Número identificador
id_grupo	*integer*	Identificador do Domínio de Gestão
cod_local	*character (6)*	Código Local
nome_tec	*character (3)*	Nome da Tecnologia

Tabela 13 - Base de Dados retadm - Tabela dg_ex

3.2.2.6.7. GeraDG

Este formulário permite consultar a lista de pares Tecnologia / Local gerados pelo *script geradg*. Para facilitar a leitura destes pares, está disponível um filtro onde é possível escolher um local ou uma tecnologia para limitar os resultados apresentados.

Na página seguinte é visível este formulário.

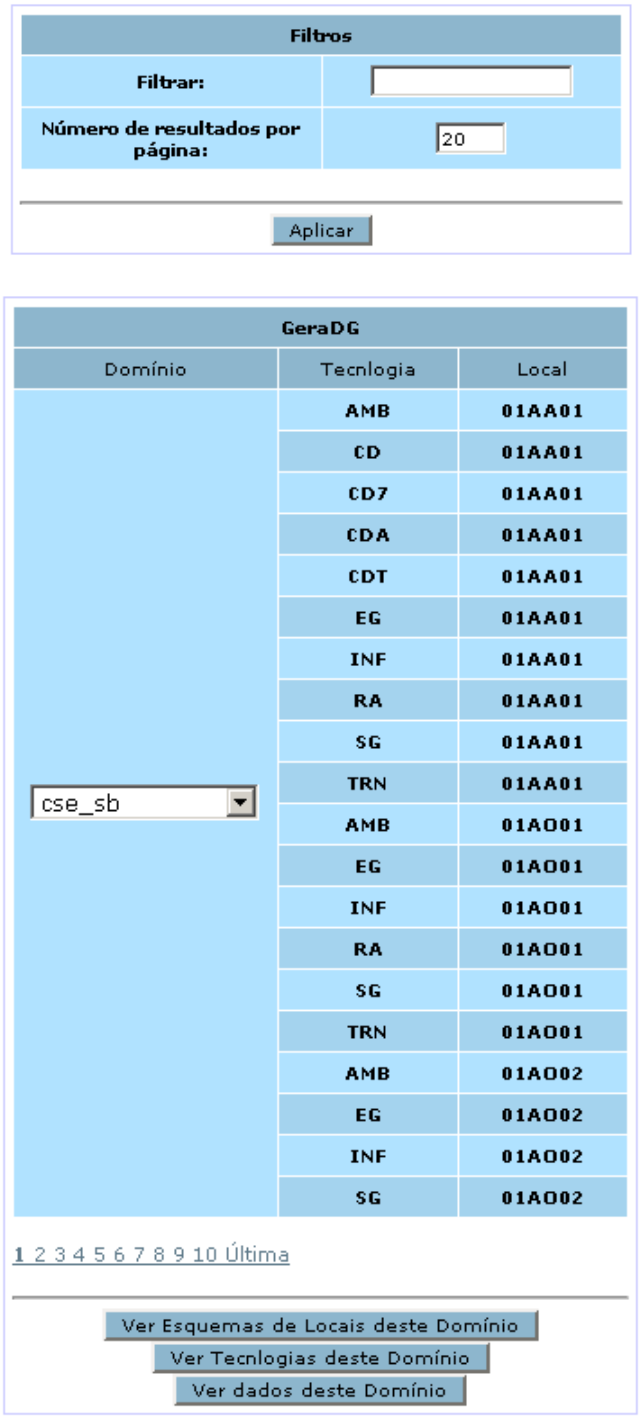

Figura 34 - Resultados do GeraDG para um Domínio de Gestão

3.2.2.6.7.1. Base de Dados

As alterações referidas anteriormente terão impacto na Base de dados *retadm*, tabela *dg_pr*. Esta tabela tem o seguinte formato:

Coluna	Tipo	Finalidade
id_dg	*integer*	Número identificador
id_grupo	*integer*	Identificador do Domínio de Gestão
cod_local	*character (6)*	Código Local
nome_tec	*character (3)*	Nome da Tecnologia

Tabela 14 - Base de Dados retadm - Tabela dg_pr

3.3. Módulo de Autenticação

3.3.1. Introdução

Serve a presente secção para apresentar o módulo de autenticação automática.

Este módulo teve como objectivo proporcionar aos utilizadores a possibilidade de realizarem o *login* automático no Portal sem terem de introduzir o conjunto *username* / *password* de cada vez que desejem aceder ao mesmo. No entanto, esta vantagem não pode ser substituída pelos perigos eminentes que a não inserção de credenciais poderia causar. Assim, este módulo teve como objectivo, além da óbvia possibilidade de realizar a autenticação de uma maneira automática (transparente) para o utilizador, a continuidade da segurança quer do sistema SGA como dos próprios utilizadores.

É ainda importante referir que uma das particularidades que este módulo tinha de cumprir, era a possibilidade de realizar o *login* manual (através da inserção do conjunto *username* / *password*) visto que por questões de continuidade de serviço, não podemos deixar de conseguir autenticar no Portal, devido a algum problema derivado do módulo de autenticação. Outra das razões que obrigaram este módulo a dispor de um sistema de autenticação alternativo ao automático, deveu-se ao facto de os colaboradores da empresa muitas vezes acederem ao Portal das suas próprias residências, através de um túnel seguro. Nestas condições, visto os colaboradores estarem a utilizar computadores pessoais que não têm de passar por nenhuma autenticação fidedigna ao iniciar a sua sessão, torna-se evidente a necessidade de continuar a dispor de uma autenticação manual.

3.3.2. Possibilidades

A implementação deste módulo apresentou diversas dificuldades, desde logo pelo desconhecimento das possibilidades existentes para atingir o fim pretendido (autenticação automática). Assim, vimo-nos obrigados a ensaiar várias tentativas, que contudo nos foram constantemente revelando as suas lacunas. Finalmente, chegámos a uma solução, que iremos posteriormente explanar de forma mais pormenorizada. Debrucemo-nos agora sobre todas as possibilidades pensadas para a implementação da funcionalidade de *login* automático (de notar que algumas nunca chegaram sequer a ser testadas):

- Através das credenciais do *Windows* usando *JavaScript*;
- Através das credenciais do *Windows* usando *ASP.NET*;
- Através de informações armazenadas em *cookies*;
- Através das variáveis de ambiente obtidas por *ActiveX*;
- Através do endereço IP identificador de cada estação de trabalho;

- Através das credenciais necessárias para aceder ao *proxy*;
- Através das credenciais do *Windows* usando *applets Java*;
- Através de uma chave DAS/RSA armazenada na BD e uma cópia localmente na estação de trabalho de cada utilizador;
- Através de um módulo de autenticação do *Apache – mod_auth_kerb*.

3.3.3. Análise Individual

Nesta secção vamos fazer uma análise individual e detalhada de cada possibilidade listada na secção anterior.

3.3.3.1. Através das Credenciais do Windows usando JavaScript

A primeira possibilidade pensada e estudada para realizar a implementação da funcionalidade de *login* automático recorria à obtenção das credenciais *Windows* usando *JavaScript*. No entanto, esta solução foi rapidamente abandonada devido ao facto de o *JavaScript*, apesar de ser executado do lado do cliente, não ser capaz de aceder às variáveis de ambiente do Sistema Operativo, logo não tem capacidade para obter as credenciais da estação de trabalho.

3.3.3.2. Através das credenciais do Windows usando ASP.NET

Tal como no caso anterior, esta possibilidade foi rapidamente abandonada devido ao facto de necessitar de um servidor a correr com Sistema Operativo *Microsoft Windows*. Este requerimento é obrigatório visto que o *ASP.NET* é a plataforma da *Microsoft* para o desenvolvimento de aplicações Web.

3.3.3.3. Através de informações armazenadas em cookies

Quando um utilizador introduz o seu conjunto *username* / *password* no Portal, tal como em todos os sites, uma *cookie* é criada com os dados da sessão. Esta *cookie* tem a função

de manter o utilizador ligado durante um determinado período de tempo (em alguns casos até a página ser fechada, nos restantes, um período de tempo fixo). Quando se pensou nesta solução, o objectivo era aproveitar este *tempo de vida* da *cookie* para manter o utilizador ligado durante um grande período de tempo. Assim, quando a *cookie* de sessão fosse criada, em vez de ter uma data de expiração 24h depois da data de início de sessão, seria atribuída uma data consideravelmente mais elevada (na ordem das semanas), evitando assim a necessidade de o utilizador realizar o *login* diariamente. Esta solução no entanto não resolvia o nosso problema, apenas o contornava, criando a ilusão de que o utilizador não tinha que introduzir as suas credenciais de cada vez que acedia ao Portal.

3.3.3.4. Através das variáveis de ambiente obtidas por ActiveX

Esta solução, apesar de só funcionar no *Microsoft Internet Explorer*, revelou resultados satisfatórios. Recorrendo a *ActiveX* é possível obter variáveis ambientais (para este caso específico só nos interessa o *username* e o domínio do utilizador ligado na estação de trabalho) que podem ser usadas para fazer a autenticação do utilizador. No entanto, mais uma vez, não passava de uma ilusão. Apesar de não ser necessário introduzir o conjunto *username* + *password* para aceder ao Portal, não era realizada nenhuma autenticação. Apenas era mapeado o *username* obtido por *ActiveX* (que corresponde ao *username* do utilizador que se autenticou na estação de trabalho) com o *username* correspondente do Portal.

3.3.3.5. Através do endereço IP identificador de cada estação de trabalho

Esta possibilidade foi equacionada partindo de dois pressupostos errados – que todos os computadores da PT Comunicações tem um endereço IP fixo e que as estações de trabalho não são partilhadas – pelo que mal estes aspectos foram corrigidos (na verdade apesar de algumas estações de trabalho terem endereço IP fixo, a maioria tem endereço IP variável atribuído dinamicamente por DHCP), a possibilidade foi imediatamente descartada, visto não ser possível associar inequivocamente um endereço IP a uma estação de trabalho e consequentemente a um utilizador.

3.3.3.6. Através das credenciais necessárias para aceder ao proxy

Visto que para aceder a qualquer página é necessário fazer previamente a autenticação no *proxy* (no *Microsoft Internet Explorer* essa autenticação é feita de uma forma transparente para o utilizador utilizando as credenciais da estação de trabalho, enquanto que em qualquer outro *browser* é necessário introduzir manualmente as mesmas credenciais), foi pensado em aproveitar de alguma forma essa autenticação para a usar na autenticação do Portal. No entanto esta solução também foi abandonada devido ao facto de não ter sido possível obter nenhuma informação do *proxy* que pudesse ser usada no módulo de autenticação automática.

3.3.3.7. Através das credenciais do Windows usando applets Java

Esta possibilidade foi das últimas a ser testada e, tal como as outras, revelou-se incapaz de solucionar o problema da autenticação automática. Apesar de o *Java* ser capaz de aceder a informações pessoais (como o *username*), as *applets Java* não têm a mesma capacidade visto que são aplicações integradas num *browser*. Devido a esse motivo, apesar de com *applets Java* sermos capazes de retornar várias informações, nenhuma delas identifica inequivocamente o utilizador ou a estação de trabalho.

3.3.3.8. Através de uma chave DAS/RSA armazenada na BD e uma cópia localmente na estação de trabalho de cada utilizador

Esta alternativa, baseada na actualmente usada para efectuar *login* automático nos servidores SSH, requer que uma chave (que pode ser DSA, RSA, etc.) seja criada e armazenada quer do lado do cliente, quer do lado do servidor. Se no momento da autenticação, a chave que o cliente tem localmente for igual a uma previamente guardada no servidor, então o utilizador está autenticado. Esta solução no entanto também não se mostrou satisfatória, visto que não era possível garantir a segurança quer do sistema (SAA), quer dos utilizadores, uma vez que bastava um utilizador apropriar-se da chave de outro utilizador para conseguir entrar no sistema com a identidade do segundo.

3.3.3.9. Através de um módulo de autenticação do Apache – mod_auth_kerb

Este módulo – *mod_auth_kerb* – permite realizar autenticações baseadas em *Kerberos* em servidores *Apache*. Suporta ainda *Basic Authentication* e *Negociate Authentication* sendo que, no primeiro caso, é necessário introduzir as credenciais no *browser* para aceder aos conteúdos, enquanto o segundo método (*Negociate Authentication*) é baseado em troca de *tickets,* evitando desse modo a inserção das credenciais.

Tal como o leitor pode constatar, com este módulo - *mod_auth_kerb* - e particularmente com o último método descrito - *Negociate Authentication* - reunimos as condições necessárias para atingir o objectivo da autenticação automática.

Nas secções seguintes serão explicadas detalhadamente todas as configurações necessárias para o correcto funcionamento deste módulo (*mod_auth_kerb*).

3.3.4. Solução Adoptada

3.3.4.1. Introdução

Tal como é possível constatar pela leitura da secção anterior, de todas as possibilidades estudadas apenas uma revelou não ter impedimentos para atingir o objectivo proposto (implementação de um módulo de autenticação automática).

Avancemos agora para uma explicação detalhada da solução adoptada (autenticação automática recorrendo ao módulo do Apache *mod_auth_kerb*).

3.3.4.2. Enquadramento

Desde o *Windows 2000* que um *Windows Domain Controller* (DC) pode actuar como um servidor Kerberos *Key Distribution Center* (KDC). Este facto permite a aplicações *kerberizadas* (do inglês *kerberized*) autenticarem-se perante um DC através de GSSAPI/Kerberos. Assim, os servidores *Apache* que usem o *mod_auth_kerb* podem utilizar a Base de Dados do DC para realizarem a denominada "Autenticação Básica" (do inglês *Basic Authentication*), bem como a "Autenticação Negociada" (*Negociate Authentication*) através do GSSAPI/Kerberos. Com este último método de autenticação, o *browser* não tem de enviar para o servidor *Apache* o conjunto *username* / *password* mas em substituição envia um *ticket Kerberos*.

As vantagens inerentes do uso da autenticação GSSAPI/Kerberos são:

- O utilizador apenas tem de introduzir as suas credenciais uma única vez (quando faz *login* na sua estação de trabalho);
- Nenhuma *password* é enviada para o servidor Web (em substituição é enviado um *ticket*).

3.3.4.3. Configurações

3.3.4.3.1. Cenário

Antes de apresentarmos os ficheiros de configuração, apresentamos uma figura com o cenário montado:

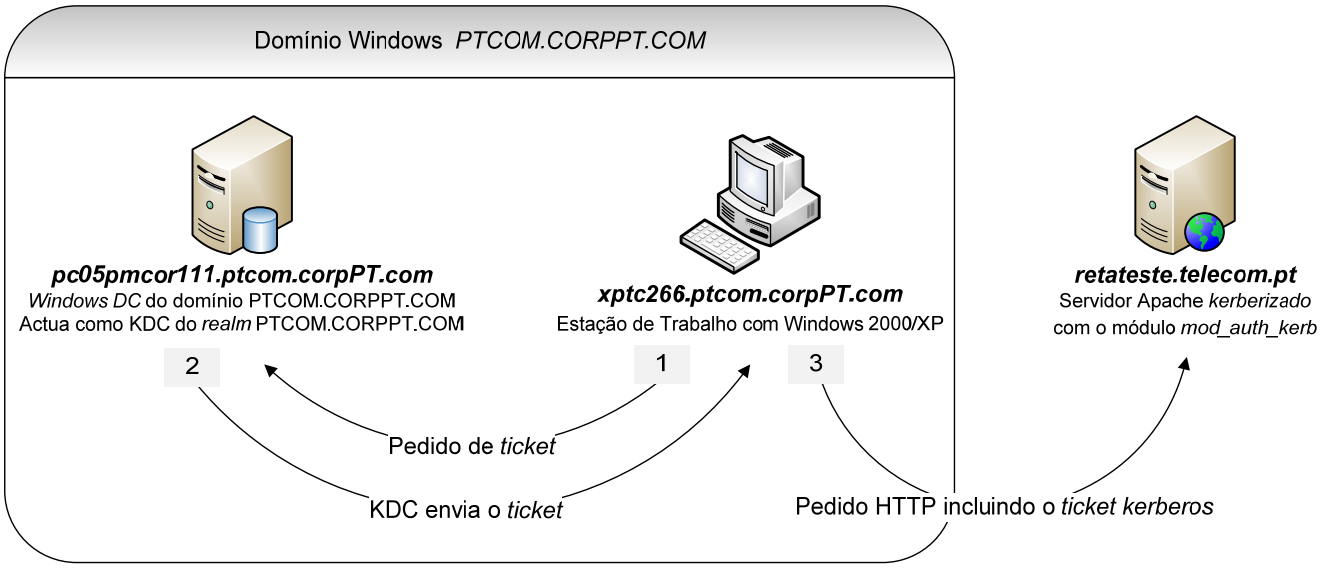

Figura 35 - Cenário Exemplo

No nosso cenário podemos destacar:

- PTCOM.CORPPT.COM é o *Windows Domain* e o *realm Kerberos* que quermos usar para autenticação;
- *pc05pmcor111.ptcom.corpPT.com* é o FQDN (F*ully Qualified Domain Name*) do *Windows DC* do domínio PTCOM.CORPPT.COM. Também actua como KDC para o *realm* PTCOM.CORPPT.COM;
- *retateste.telecom.pt* é o FQDN do servidor Apache *kerberizado* com o módulo *mod_auth_kerb*;
- *xptc266.ptcom.corpPT.com* é o FQDN da Estação de Trabalho com Windows 2000/XP membro do Domínio Windows PTCOM.CORPPT.COM.

É ainda de notar que não existe comunicação directa entre o KDC *ldap.ptcom.corppt.com* e o servidor *Apache retateste.telecom.pt*.

3.3.4.3.2. Configuração do Kerberos no Servidor Web

O servidor Web que aloja o nosso Portal e que queremos *kerberizar* está registado no DNS como *retateste.telecom.pt* É portanto neste servidor que temos que configurar o *Kerberos*. Esta configuração (do *Kerberos*) está localizada no ficheiro */etc/krb5.conf*.

Apresentamos então o referido ficheiro (*/etc/krb5.conf*) configurado para o nosso caso:

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  default_realm = PTCOM.CORPPT.COM

[realms]
  PTCOM.CORPPT.COM = {
        kdc = pc05pmcor111.ptcom.corpPT.com
        admin_server = PTCOM.CORPPT.COM
  }

[domain_realm]
  retateste.telecom.pt = PTCOM.CORPPT.COM
```

Para confirmarmos que as configurações introduzidas funcionam, basta executar o seguinte comando:

```
kinit xptc266
```

Se tudo estiver bem configurado, será pedida a introdução da *password* respectiva ao utilizador *xptc266* e o programa terminará sem nenhum erro. No caso de ocorrer algum erro, a causa do referido erro será apresentada no ecrã.

Na figura seguinte, foi executado o comando anteriormente especificado, sendo que na primeira vez que o comando foi executado foi introduzida a *password* para o utilizador em questão (*xptc266*). Na segunda vez que o comando foi executado, em vez da *password* correcta, foi introduzida uma *password* errada.

```
[retadm@retateste ~]$ kinit xptc266
Password for xptc266@PTCOM.CORPPT.COM:
[retadm@retateste ~]$
[retadm@retateste ~]$
[retadm@retateste ~]$
[retadm@retateste ~]$ kinit xptc266
Password for xptc266@PTCOM.CORPPT.COM:
kinit(v5): Preauthentication failed while getting initial credentials
[retadm@retateste ~]$
```

Figura 36 - kinit

3.3.4.3.3. Criação do Service Principal no KDC

Cada aplicação *kerberizada* necessita de um *Service Principal* no KDC.

Com base no que foi dito é facilmente perceptível que temos de criar um *Service Principal* para o servidor Web *retateste.telecom.pt*.

Para isto é necessário:

1. Criar uma conta de utilizador no Domínio Windows PTCOM.CORPT.COM;
2. Executar o comando *ktpass* para mapear a conta criada com o *Service Principal*.

3.3.4.3.3.1. Criação da conta

À conta criada foi dado o nome *HTTP-retateste* uma vez que se destina ao servidor Web *retateste.telecom.pt*, bem como pelo facto de a conta ser usada com o *Service Principal* HTTP.

As características da conta são então as seguintes:

```
X = checked
_ = not checked


_   User must change password at next logon
_   User cannot change password
X   Password never expires
_   Store password using reversible encryption
_   Account is disabled
_   Smart card is required for interactive logon
_   Account is trusted for delegation
_   Account is sensitive and cannot be delegated
X   Use DES encryption types for this account
_   Do not require Kerberos pre-authentication
```

3.3.4.3.3.2. ktpass

Para mapear a conta criada com o *Service Principal* HTTP foi necessário correr o seguinte comando:

```
ktpass -princ HTTP/retateste.telecom.pt@PTCOM.CORPPT.COM
-mapuser HTTP-retateste -crypto DES-CBC-MD5 +DesOnly -pass **********
-ptype KRB5_NT_PRINCIPAL -out retateste.keytab
```

De notar que o comando executado cria o ficheiro *retateste.keytab*, que será usado na secção seguinte.

O *output* na janela de DOS gerado depois de executar o referido comando foi:

```
Targeting domain controller: pc05pmcor111.ptcom.corpPT.com
Using legacy password setting method
Successfully mapped HTTP/retateste.telecom.pt to HTTP-retateste.
Key created.
Output keytab to retateste.keytab:
Keytab version: 0x502
keysize 69 HTTP/retateste.telecom.pt@PTCOM.CORPPT.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 5 etype 0x3 (DES-CBC-MD5) keylength 8
(0x4c6145d945574f76)
Account HTTP-retateste has been set for DES-only encryption.
```

3.3.4.3.4. Configuração do Apache com o mod_auth_kerb

Depois de instalar o pacote *mod_auth_kerb* no servidor *Apache* que está a ser *kerberizado* (*retateste.telecom.pt*) é necessário configurar o *Apache* para o utilizar correctamente.

Assim, ao ficheiro de configuração do *Apache httpd.conf* foram adicionadas as seguintes linhas:

```
LoadModule auth_kerb_module modules/mod_auth_kerb.so

<Directory /var/www/html/portal>
    AuthType Kerberos
    AuthName "Introduza as suas credenciais da RIN"
    KrbMethodNegotiate On
    KrbMethodK5Passwd On
    KrbAuthRealms PTCOM.CORPPT.COM
    Krb5KeyTab /etc/httpd/conf/httpd.keytab
    require valid-user
    ErrorDocument 401 "<meta http-equiv='refresh' content='0;
  URL=http://retateste.telecom.pt/teste/index.php'>"
</Directory>
```

Sendo que em seguida é suficiente fazer um *restart* ao apache para as configurações surtirem efeito:

```
/etc/init.d/httpd restart
```

3.3.4.4. Integração no Portal

Para a autenticação automática funcionar, as alterações também tiveram que abranger o Portal. Assim, foi necessário alterar a tabela *yerba_usuarios* da Base de Dados *yerba* para adicionar uma coluna com a finalidade de mapear o *username* da RIN[5] com o *username* do Portal (para cada utilizador). A tabela *yerba_usuarios* ficou então com a seguinte estrutura:

Coluna	Tipo	Finalidade
uid	*integer*	Número identificador
gid	*integer*	Perfil
nombre	*character varying (35)*	Nome
alias	*character varying (20)*	*Username*
clave	*character varying (32)*	*Password*
correo	*character varying (50)*	E-Mail
icq	*character varying (35)*	Departamento
edad	*character (2)*	(não é usado)
web	*character varying (80)*	Telefone
sexo	*character (1)*	(não é usado)
pais	*character varying (35)*	Grupo de Gestão
idioma	*character varying (40)*	Idioma
estilo	*character varying (50)*	Estilo de Apresentação
detalle	*text*	Descrição
publico	*character (1)*	Visibilidade (pública ou privada)
alias_alt	*character (50)*	*Username* da RIN

Tabela 15 - Tabela yerba_usuarios modificada para suportar Autenticação Automática

[5] Rede Informática Nacional – rede interna usada pelos colaboradores da PT Comunicações

Apresentamos agora o diagrama do processo de autenticação automática:

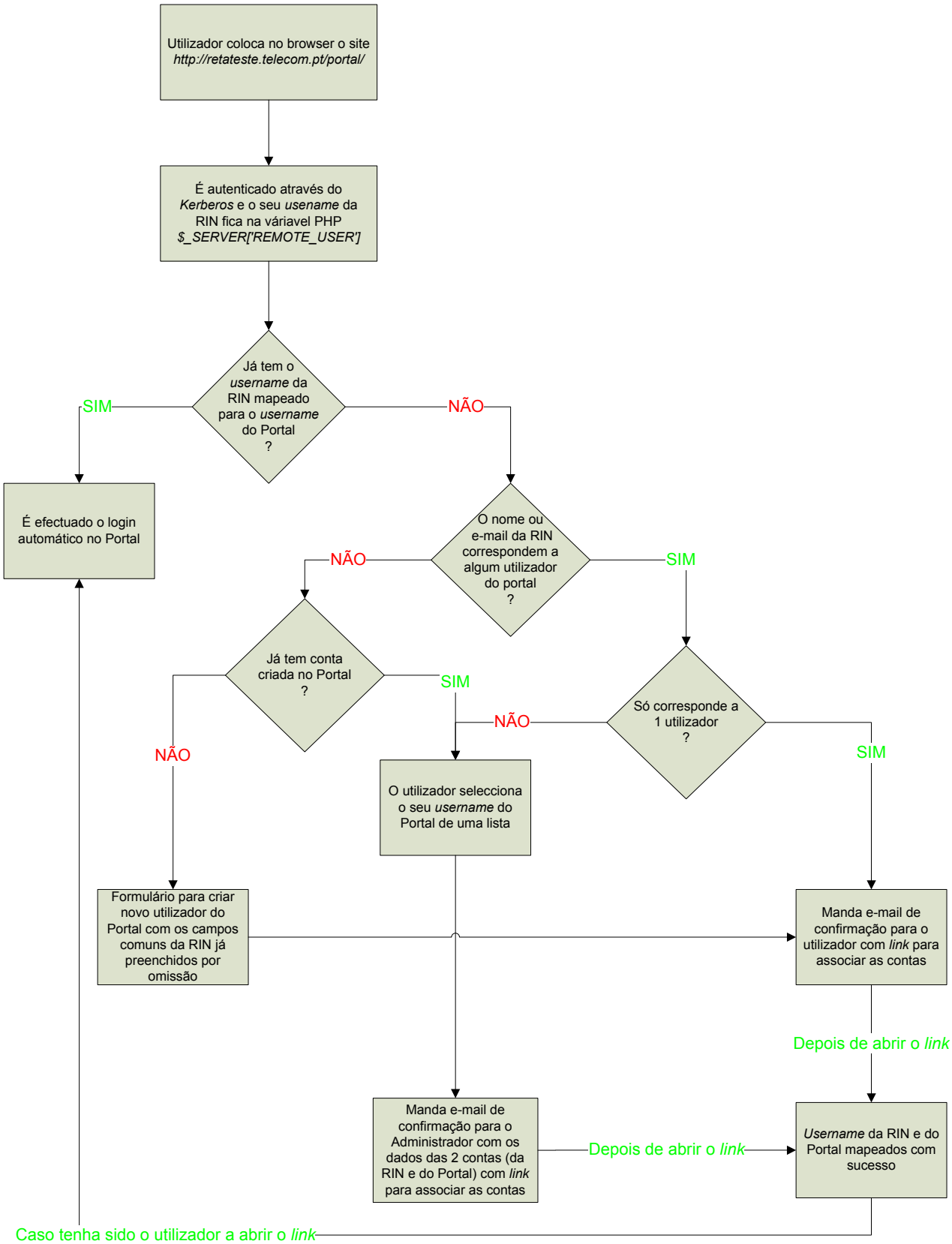

Figura 37 - Diagrama do processo de Autenticação Automática

Devido à complexidade do diagrama da página anterior, apresentamos em seguida uma explicação detalhada dos casos em que o utilizador autenticado na RIN ainda não tem o seu *username* do Portal mapeado com o da RIN.

A parte do diagrama correspondente é apresentada em seguida:

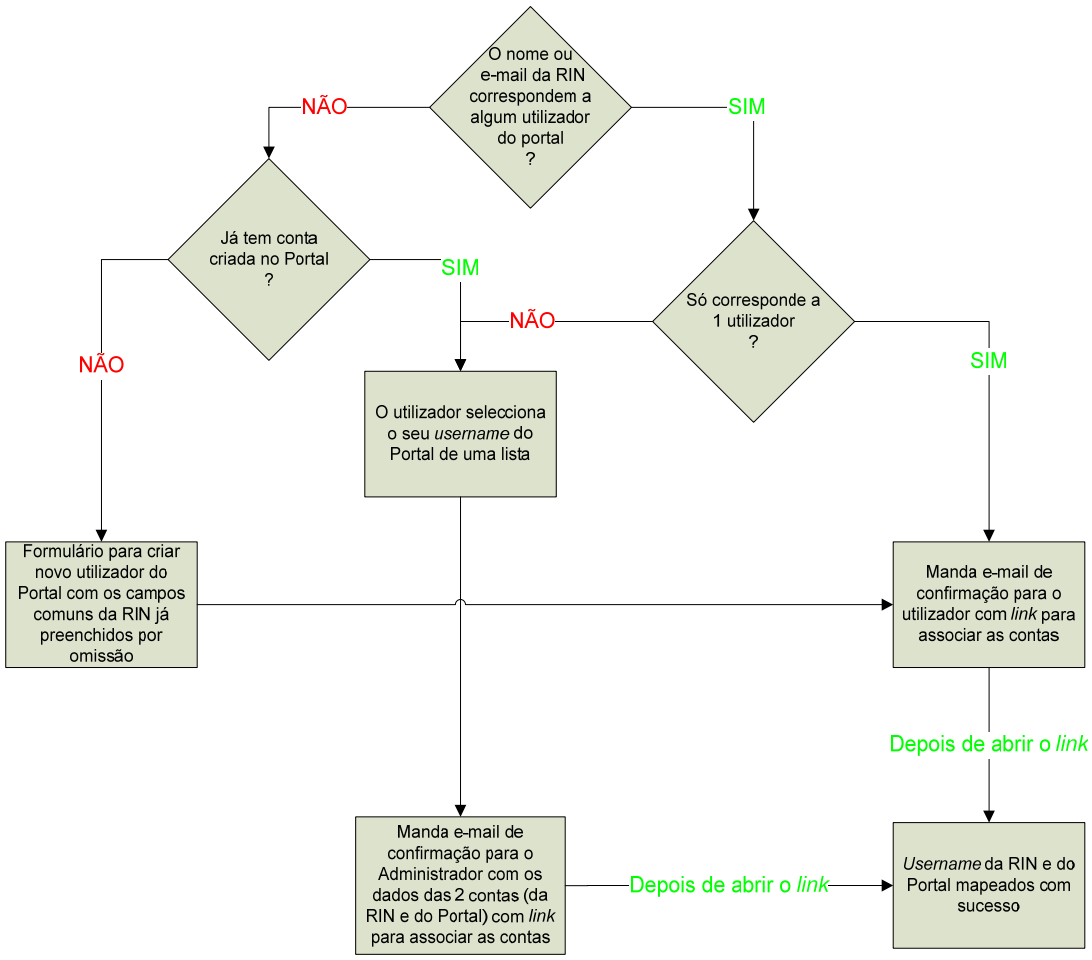

Figura 38 - Diagrama de um caso particular do processo de Autenticação Automática

De notar que o código PHP integrado no Portal para suportar a Autenticação Automática encontra-se disponível no **Anexo B**.

3.3.4.4.1. Conta da RIN não corresponde a nenhum utilizador do Portal

A parte do diagrama correspondente é apresentada em seguida:

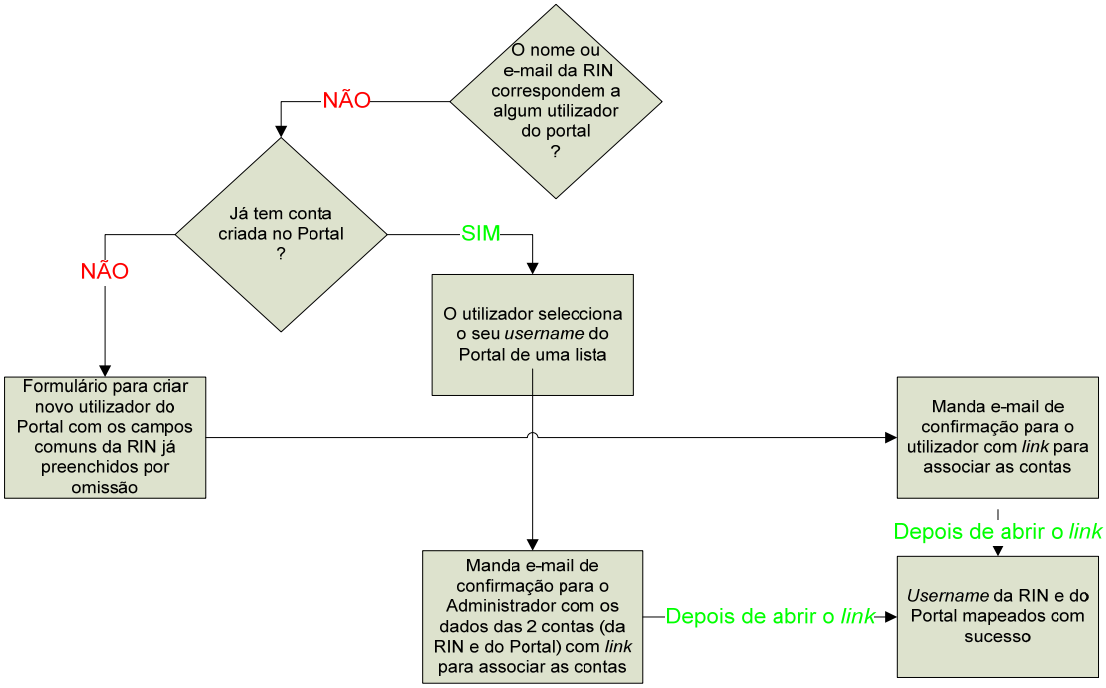

Figura 39 - Diagrama de um caso particular do processo de Autenticação Automática

Nestes casos, quando ao utilizador autenticado na RIN não corresponde nenhum utilizador do Portal, é apresentada a seguinte mensagem no Portal:

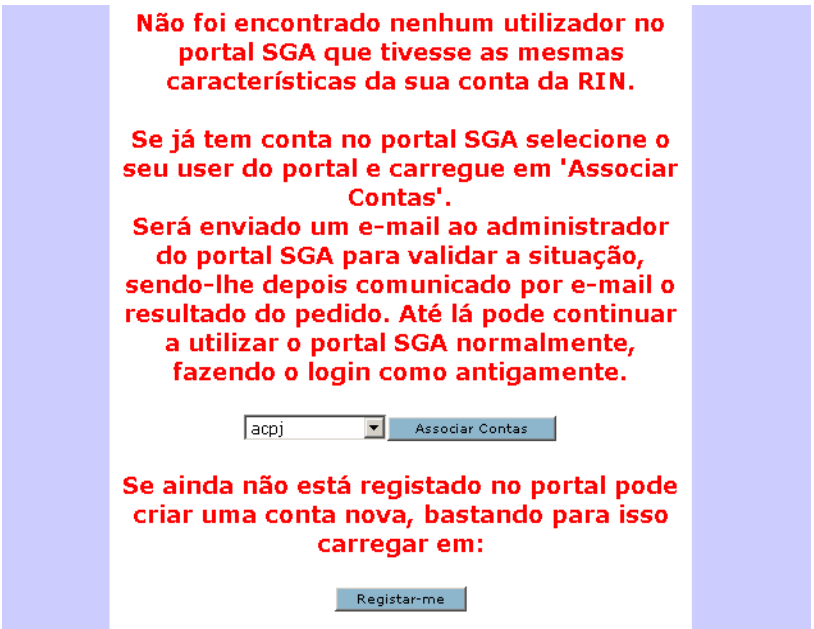

Figura 40 - Nenhum utilizador encontrado

Tal como é possível constatar pela imagem anterior, caso o utilizador já tenha uma conta do Portal, deve seleccioná-la da lista para proceder à associação das duas contas. Se pelo contrário ainda não está registado no Portal, deve carregar no botão *Registar-me*.

No caso de o utilizador optar por registar-se no Portal, esse processo é praticamente automático visto que todas as informações necessárias (com excepção da *password* e do Domínio de Gestão) são importadas da conta da RIN para a conta do Portal.

Este processo – importação dos dados da conta da RIN para a conta do Portal – é feito através da integração de um módulo *open source* denominado adLDAP (disponível no endereço *http://adldap.sourceforge.net*) no módulo de registo. Com este módulo (adLDAP) é possível validar utilizadores num servidor LDAP pré-configurado e obter informações (nome, departamento, telefone, etc.) com base no *username*. Assim, uma vez que o *mod_auth_kerb* autentica o utilizador e retorna o *username* do mesmo, é possível utilizar este *username* para, através do adLDAP, obter as informações necessárias ao registo no Portal. No Anexo B está disponível o código PHP da integração no Portal.

De notar, na figura seguinte, que com a Autenticação Automática a *password* apenas é relevante caso o utilizador faça *logout* no Portal e depois queira voltar a fazer *login* sem ter que reabrir o *browser* (esta funcionalidade tem particular interesse quando se pretende entrar com a conta de Administrador e depois voltar à conta corrente).

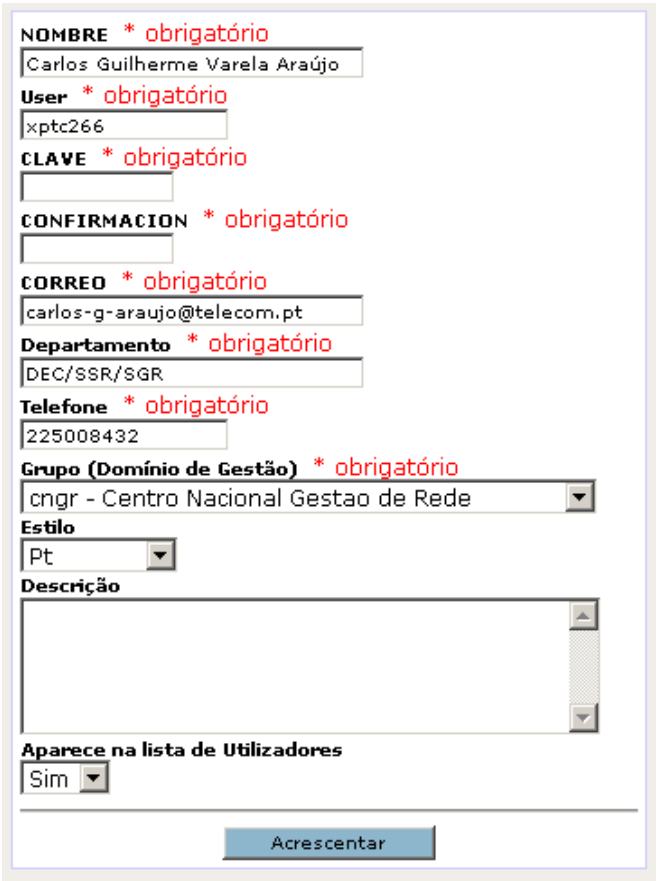

Figura 41 - Registo de novo utilizador

Quando o utilizador pressiona o botão "Acrescentar", o registo da nova conta fica concluído (incluindo a associação da conta da RIN com a criada).

3.3.4.4.2. Conta da RIN corresponde a um único utilizador do Portal

A parte do diagrama correspondente é apresentada em seguida:

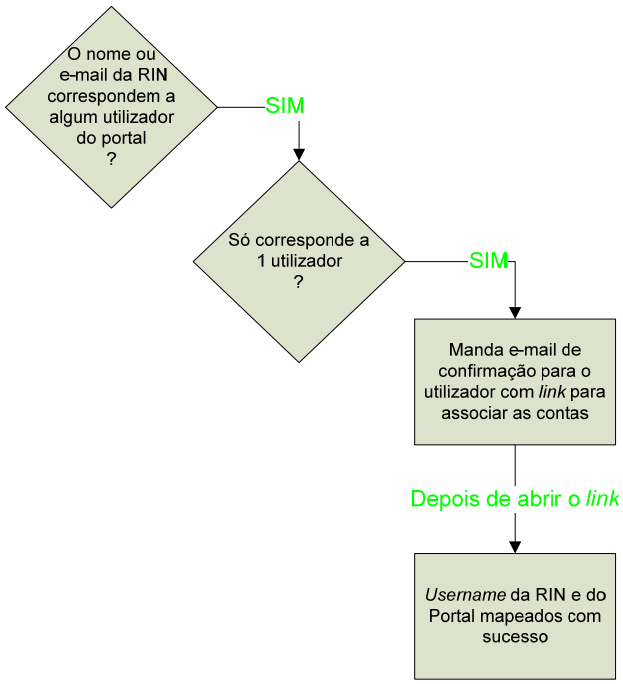

Figura 42 - Diagrama de um caso particular do processo de Autenticação Automática

Se existir na Base de Dados do Portal um único utilizador que tenha algum destes dados em comum com o utilizador em questão (o utilizador que foi autenticado na RIN), é actualizada a informação do referido utilizador, sendo que esta actualização traduz-se na escrita no campo *alias_alt* da tabela *yerba_usuarios* (BD *yerba*) uma *string* constituída por:

- *hash* MD5 do número de segundos desde 1 de Janeiro de 1970 00:00:00 GMT;
- *username* da RIN.

Esta *string* fica então com o seguinte aspecto:

```
217271f0e4ceef4b0e9a6f7348ed3981-xptc266
```

É então enviado um e-mail ao referido utilizador com os dados das contas que este deseja associar (a da RIN e a do Portal) e um *link* para fazer a referida associação. Após o utilizador carregar no *link* mencionado, as contas são associadas e é enviado um e-mail para o Administrador do Portal com os dados das duas contas associadas (apenas para garantir que as contas que foram associadas pertencem ao mesmo utilizador).

3.3.4.4.3. Conta da RIN corresponde a mais do que um utilizador do Portal

A parte do diagrama correspondente é apresentada em seguida:

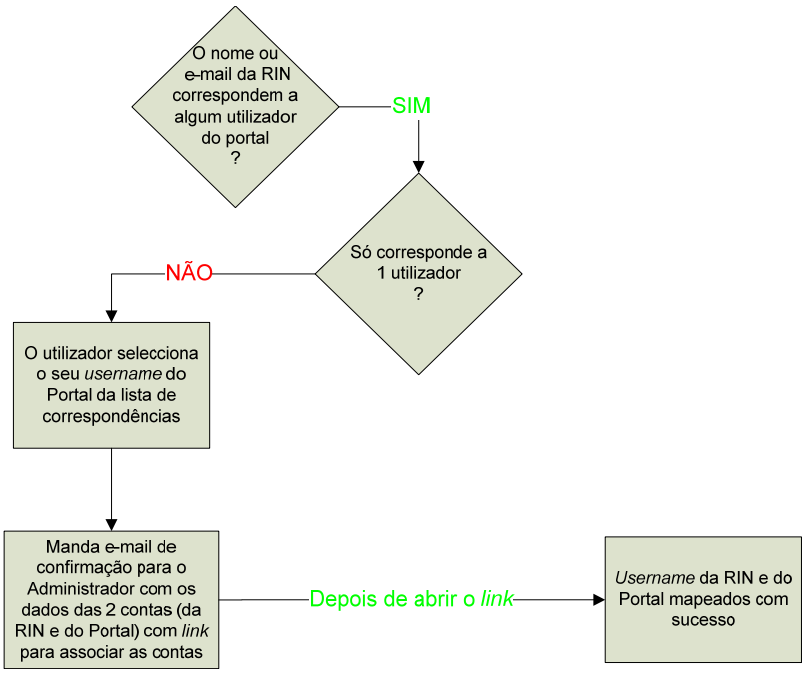

Figura 43 - Diagrama de uma caso particular do processo de Autenticação Automática

Neste último caso que vamos analisar, apesar de o utilizador autenticado pela RIN ainda não ter associado esta conta (da RIN) à sua conta do Portal, existem na BD do Portal mais do que um utilizador com características idênticas à conta do utilizador da RIN. Assim sendo, será apresentada a seguinte mensagem ao utilizador:

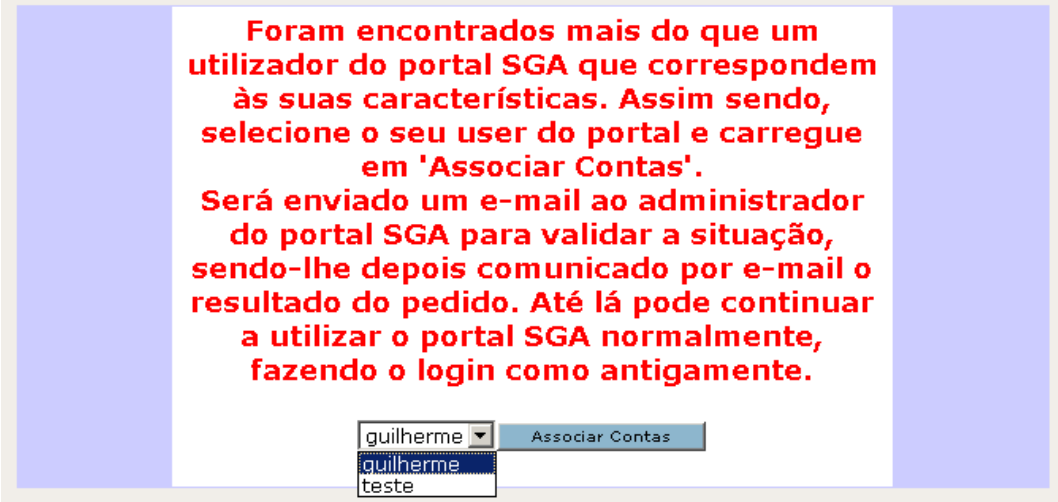

Figura 44 - Mais do que um utilizador encontrado

Tal como é possível observar na figura anterior, é dada a possibilidade ao utilizador de seleccionar o seu utilizador do Portal para associar ao da RIN. Para evitar que sejam associados utilizadores erradamente, nestas situações, em vez de o e-mail de associação de contas ser enviado para o utilizador em questão, será enviado para o Administrador. Este terá a função de comparar os dados das duas contas e caso conclua que ambas pertencem ao mesmo utilizador, procederá à associação das referidas contas, bastando para isso clicar no *link* que é enviado na mensagem de correio electrónico.

Para finalizar apresentamos um e-mail exemplo enviado ao Administrador:

O utilizador da RIN com *login* **xptc266** pediu para associar a sua conta da RIN com a conta do Portal SAA com *login* **guilherme**.

Os dados referentes ao *login* **xptc266** na RIN são:
Nome: *Carlos Guilherme Varela Araújo*
E-Mail: *carlos-g-araujo@telecom.pt*
Departamento: *DEC/SSR/SGR*
Telefone:

Os dados referentes ao *login* **guilherme** no Portal SAA são:
Nome: *Guilherme Araújo*
E-Mail:
Departamento: *DEC/SSR/SGR*
Telefone: *225008432*

Se achar que esta associação é válida carregue no seguinte *link*:
Associar contas

Muito obrigado,
SAA

Capítulo 4

4. Conclusão

Todos os objectivos propostos foram ultrapassados com êxito, tendo inclusive sido desenvolvida uma funcionalidade complementar.

O primeiro objectivo passou por nos inteirarmos do estado do desenvolvimento do Sistema de Arquivo e Acesso Intranet (SAA), visto serem tantas e tão distintas as funcionalidades que o Portal (SAA) suporta.

O segundo objectivo atingido com este projecto passou pelo desenvolvimento e implementação de um módulo de gestão de perfis de utilizador. Através deste método de gestão, o perfil de cada utilizador é influenciado não só pelo seu perfil individual, mas também pelo perfil do Grupo de Gestão onde está inserido. Assim, a tarefa do Administrador é facilitada, visto que esta nova organização permite definir pormenorizadamente as funcionalidades a que cada colaborador tem acesso, bem como a camada da rede que terá de gerir. Este objectivo foi cumprido com êxito.

O último objectivo consistiu na implementação de um módulo de Autenticação Automática baseado em *Kerberos*, que permite aos utilizadores serem autenticados de uma maneira totalmente transparente e com maior segurança. Esta autenticação aproveita o facto de que o utilizador é obrigado a introduzir as suas credenciais sempre que faz o *login* na sua estação de trabalho. Em vez de serem enviadas *passwords* pela rede, este método recorre a uma troca de *tickets* entre a estação de trabalho do utilizador e um servidor *Kerberos* que funciona como *Key Distribution Center* (KDC).

Este método de autenticação apresenta vários benefícios, nomeadamente a diminuição da probabilidade do utilizador se esquecer da *password*, libertando-o ainda do incómodo – e consequente perigo de segurança – de recorrer a infindáveis rascunhos para apontar as inúmeras *passwords*. Esta vantagem decorre do facto de com este método o utilizador apenas ter de introduzir as suas credenciais uma única vez (quando faz *login* na sua estação de trabalho). Além disso, é ainda importante salientar como uma vantagem óbvia o aumento da segurança na autenticação. Na realidade, nenhuma *password* é enviada para o servidor Web, sendo em substituição enviado um *ticket*. Tal como no caso anterior, este objectivo também foi atingido com êxito.

Na continuidade do módulo de Autenticação Automática implementado, foi desenvolvida uma funcionalidade complementar que consistiu num método semi-automático de registo,

onde praticamente todas as informações necessárias ao registo são obtidas através do servidor LDAP da PT Comunicações e automaticamente preenchidas no formulário de registo. O utilizador apenas tem de seleccionar o Domínio de Gestão onde deseja ser inserido e uma *password* de reserva, apenas utilizada caso o servidor *Kerberos* sofra alguma anomalia.

Referimos ainda o facto que todas as funcionalidades mencionadas nesta dissertação passaram a fase de testes, e inclusive, encontram-se todas em ambiente de produção.

Bibliografia

MAMEDE, Henrique São, Segurança Informática nas Organizações, FCA, 2006

SILVA, Pedro Tavares, Segurança dos Sistemas de Informação, Centro Atlântico, 2003

OLIVEIRA, Wilson, Segurança da Informação – Técnicas e Soluções, 2001

Authentication World, Single Sign On, http://www.authenticationworld.com/Single-Sign-On-Authentication/

IBM, Build and Implement a Single Sign On Solution, http://www.ibm.com/developerworks/web/library/wa-singlesign/

The Open Group, Single Sign On, http://www.opengroup.org/security/sso/

MIT, Kerberos: The Network Authentication Protocol, http://web.mit.edu/Kerberos/

SOURCEFORGE.NET, Kerberos Module For Apache, http://modauthkerb.sourceforge.net/index.html

Ken Hornstein, Kerberos FAQ, http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html

Marcos Muniz Filho, Kerberos, http://www.gta.ufrj.br/grad/99_2/marcos/kerberos.htm

Answers.com, Kerberos, http://www.answers.com/kerberos?cat=technology

IST, Serviço de Autenticação Kerberos, https://ciist.ist.utl.pt/servicos/kerberos.php

META CENTRUM, Kerberos for WWW Authentication, http://meta.cesnet.cz/cms/opencms/en/docs/software/devel/negotiate.html

RFC 4120, Kerberos V5, http://www.ietf.org/rfc/rfc4120.txt

RFC 1510, The Kerberos Network Authentication Service (V5), http://www.ietf.org/rfc/rfc1510.txt

RFC 4757, The RC4-HMAC Kerberos Encryption Types Used by Microsoft Windows, http://www3.tools.ietf.org/html/rfc4757

Anexos

Anexo A – *Código Javascript para gerar expressões regulares*

```
<SCRIPT LANGUAGE="JavaScript1.1">
function actualizar() {
  var texto=document.getElementById('exp_ger');
  var exp1=document.getElementById('exp1').value;
  var exp2=document.getElementById('exp2').value;
  var r_exp1=document.getElementById('r_exp1').value;
  var r_exp2=document.getElementById('r_exp2').value;
  var r_exp3=document.getElementById('r_exp3').value;
  var inicio='';
  var fim='';
  var exp_reg='';
  var intervalo,valores;

  var re = new RegExp('[^0-9\-\,]');
  var botao=document.getElementById('botao').getAttribute('disabled');

  if((r_exp1.match(re)!=null)||(r_exp2.match(re)!=null)){
      if(botao!='false'){
            document.getElementById('botao').setAttribute('disabled','');
            texto.value='Erro! Apenas sÃ£o permitos nÃºmeros, a \',\' e o \'-\'';
            return;
      }
  }
  else{
      if(botao!='true')
            document.getElementById('botao').removeAttribute('disabled');
  }

  if(r_exp1!=''){
      //Se o texto estiver associado ao campo 'ComeÃ§ado Por:'
      if(exp1=='comecar'){
            valores=r_exp1.split(',');
            for(i=0;i<valores.length;i++){
                  intervalo=valores[i].split('-');
                  if(intervalo.length==2){
                        if((intervalo[0].length==1)&&(intervalo[1].length==1)){
                              if(inicio=='')
                                    inicio='^(['+intervalo[0]+'-'+intervalo[1]+']';
                              else{
                                    if((inicio[inicio.length-1]==']') ||
  (inicio[inicio.length-1]==')'))
                                          inicio=inicio+'|['+intervalo[0]+'-
  '+intervalo[1]+']';
                                    else if(inicio[inicio.length-1]!=')')
                                          inicio=inicio+']|['+intervalo[0]+'-
  '+intervalo[1]+']';
```

```
                              }
                        }
                        else
if((intervalo[0].length==2)&&(intervalo[1].length==2)){
                              var dif1=intervalo[1].charAt(0)-
intervalo[0].charAt(0);
                              var dif2=intervalo[1].charAt(1)-
intervalo[0].charAt(1);
                              if((dif1<0) ||(dif1==0 && dif2<=0)){
                                    texto.value='Erro! O intervalo tem de ser
crescente!';
                                    if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                    return;
                              }
                              else{
                                    if(dif1==0){
                                          if(inicio=='')

    inicio='^('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+']';
                                          else{
                                                if((inicio[inicio.length-1]==']')
|| (inicio[inicio.length-1]==')'))

    inicio=inicio+'|('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+'])';
                                                else if(inicio[inicio.length-
1]!=')')

    inicio=inicio+']|('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+'])';
                                          }
                                     }
                                     else{

    for(a=intervalo[0].charAt(0);a<=intervalo[1].charAt(0);a++){
                                                if(a==intervalo[0].charAt(0)){
                                                      if(inicio=='')

    inicio='^(('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                      else{

    if((inicio[inicio.length-1]==']') || (inicio[inicio.length-1]==')'))

    inicio=inicio+'|('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                            else
if(inicio[inicio.length-1]!=')')

    inicio=inicio+']|('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                      }
                                                }
                                                else if(a==intervalo[1].charAt(0))

    inicio=inicio+intervalo[1].charAt(0)+'[0-'+intervalo[1].charAt(1)+'])';
                                                else
                                                      inicio=inicio+a+'[0-9]|';
                                          }
                                     }
                              }
```

```
                        }
                        else{
                              texto.value='Erro! O intervalo tem nao pode ser da
forma \'x-xx\'! Tem de ser da forma \'xx-xx\'!';
                              if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                              return;
                        }
                  }
                  else{
                        if(valores[i].length==1){
                              if(inicio=='')
                                    inicio='^(['+valores[i];
                              else{
                                    if((inicio[inicio.length-
1]==']')||inicio[inicio.length-1]==')')
                                          inicio=inicio+'|['+valores[i];
                                     else
                                          inicio=inicio+valores[i];
                              }
                        }
                        else if(valores[i].length==2){
                              if(inicio=='')

    inicio='^('+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                              else{
                                    if((inicio[inicio.length-1]==']') ||
(inicio[inicio.length-1]==')'))

    inicio=inicio+'|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                    else if(inicio[inicio.length-1]!=')')

    inicio=inicio+']|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                    else

    inicio=inicio+'|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                              }
                        }
                        else{
                              texto.value='Erro! SÃ³ valores entre 0 e 99!';
                              if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                              return;
                        }
                  }
            }
    }

    //Se o texto estiver associado ao campo 'NÃ£o ComeÃ§ado Por:'
    if(exp1=='naocomecar'){
          var valores=r_exp1.split(',');
          for(i=0;i<valores.length;i++){
                var intervalo=valores[i].split('-');
                if(intervalo.length==2){
                      if((intervalo[0].length==1)&&(intervalo[1].length==1)){
                            if(inicio=='')
                                  inicio='^(?!(['+intervalo[0]+'-
'+intervalo[1]+']';
                            else{
```

```
                                    if((inicio[inicio.length-1]==']') ||
(inicio[inicio.length-1]==')'))
                                          inicio=inicio+'|['+intervalo[0]+'-
'+intervalo[1]+']';
                                     else if(inicio[inicio.length-1]!=')')
                                          inicio=inicio+']|['+intervalo[0]+'-
'+intervalo[1]+']';
                               }
                         }
                         else
if((intervalo[0].length==2)&&(intervalo[1].length==2)){
                               var dif1=intervalo[1].charAt(0)-
intervalo[0].charAt(0);
                               var dif2=intervalo[1].charAt(1)-
intervalo[0].charAt(1);
                               if((dif1<0) ||(dif1==0 && dif2<=0)){
                                    texto.value='Erro! O intervalo tem de ser
crescente!';
                                    if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                    return;
                               }
                               else{
                                    if(dif1==0){
                                          if(inicio=='')

    inicio='^(?!('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+']';
                                          else{
                                               if((inicio[inicio.length-1]==']')
|| (inicio[inicio.length-1]==')'))

    inicio=inicio+'|('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+'])';
                                               else if(inicio[inicio.length-
1]!=')')

    inicio=inicio+']|('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+'])';
                                          }
                                    }
                                    else{

    for(a=intervalo[0].charAt(0);a<=intervalo[1].charAt(0);a++){
                                               if(a==intervalo[0].charAt(0)){
                                                    if(inicio=='')

    inicio='^(?!(('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                    else{

    if((inicio[inicio.length-1]==']') || (inicio[inicio.length-1]==')'))

    inicio=inicio+'|('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                         else
if(inicio[inicio.length-1]!=')')

    inicio=inicio+']|('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                    }
                                               }
                                                else if(a==intervalo[1].charAt(0))
```

```
    inicio=inicio+intervalo[1].charAt(0)+'[0-'+intervalo[1].charAt(1)+'])';
                                                      else
                                                            inicio=inicio+a+'[0-9]|';
                                                }
                                          }
                                    }
                              }
                              else{
                                    texto.value='Erro! O intervalo tem nao pode ser da
forma \'x-xx\'! Tem de ser da forma \'xx-xx\'!';
                                    if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                    return;
                              }
                        }
                        else{
                              if(valores[i].length==1){
                                    if(inicio=='')
                                          inicio='^(?!(['+valores[i];
                                    else{
                                          if((inicio[inicio.length-1]==']') ||
(inicio[inicio.length-1]==')'))
                                                inicio=inicio+'|['+valores[i];
                                          else
                                                inicio=inicio+valores[i];
                                    }
                              }
                              else if(valores[i].length==2){
                                    if(inicio=='')

    inicio='^(?!('+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                    else{
                                          if((inicio[inicio.length-1]==']') ||
(inicio[inicio.length-1]==')'))

    inicio=inicio+'|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                          else if(inicio[inicio.length-1]!=')')

    inicio=inicio+']|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                          else

    inicio=inicio+'|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                    }
                              }
                              else{
                                    texto.value='Erro! SÃ³ valores entre 0 e 99!';
                                    if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                    return;
                              }
                        }
                  }
            }

if(inicio!=''){
            if((inicio.charAt(inicio.length-1)!=']')&&(inicio.charAt(inicio.length-
1)!=')'))
```

```
                inicio=inicio+'])';
          else
                inicio=inicio+')';
    if(exp1=='naocomecar')
          inicio=inicio+')';
}


if(r_exp2!=''){
    //Se o texto estiver associado ao campo 'Acabado Em:'
    if(exp2=='acabar'){
          var valores=r_exp2.split(',');
          for(i=0;i<valores.length;i++){
                var intervalo=valores[i].split('-');
                if(intervalo.length==2){
                      if((intervalo[0].length==1)&&(intervalo[1].length==1)){
                            if(fim=='')
                                  fim='(['+intervalo[0]+'-'+intervalo[1]+']';
                            else{
                                  if((fim[fim.length-1]==']') || (fim[fim.length-
1]==')'))
                                        fim=fim+'|['+intervalo[0]+'-
'+intervalo[1]+']';
                                  else if(fim[fim.length-1]!=')')
                                        fim=fim+']|['+intervalo[0]+'-
'+intervalo[1]+']';
                            }
                      }
                      else
if((intervalo[0].length==2)&&(intervalo[1].length==2)){
                            var dif1=intervalo[1].charAt(0)-
intervalo[0].charAt(0);
                            var dif2=intervalo[1].charAt(1)-
intervalo[0].charAt(1);
                            if((dif1<0) ||(dif1==0 && dif2<=0)){
                                  texto.value='Erro! O intervalo tem de ser
crescente!';
                                  if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                  return;
                            }
                            else{
                                  if(dif1==0){
                                        if(fim=='')

    fim='('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+']';
                                        else{
                                              if((fim[fim.length-1]==']') ||
(fim[fim.length-1]==')'))

    fim=fim+'|('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+'])';
                                              else if(fim[fim.length-1]!=')')

    fim=fim+']|('+intervalo[0].charAt(0)+'['+intervalo[0].charAt(1)+'-
'+intervalo[1].charAt(1)+'])';
                                        }
                                  }
                                  else{
```

```
    for(a=intervalo[0].charAt(0);a<=intervalo[1].charAt(0);a++){
                                                if(a==intervalo[0].charAt(0)){
                                                      if(fim=='')

    fim='('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                      else{
                                                            if((fim[fim.length-
1]==']') || (fim[fim.length-1]==')'))

    fim=fim+'|('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                            else if(fim[fim.length-
1]!=')')

    fim=fim+']|('+a+'['+intervalo[0].charAt(1)+'-9]|';
                                                      }
                                                }
                                                else if(a==intervalo[1].charAt(0))

    fim=fim+intervalo[1].charAt(0)+'[0-'+intervalo[1].charAt(1)+'])';
                                                else
                                                      fim=fim+a+'[0-9]|';
                                          }
                                    }
                              }
                        }
                        else{
                              texto.value='Erro! O intervalo nao pode ser da forma
\'x-xx\'! Tem de ser da forma \'xx-xx\'!';
                              if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                              return;
                        }
                  }
                  else{
                        if(valores[i].length==1){
                              if(fim=='')
                                    fim='(['+valores[i];
                              else{
                                    if(fim[fim.length-1]==']')
                                          fim=fim+'|['+valores[i];
                                    else
                                          fim=fim+valores[i];
                              }
                        }
                        else if(valores[i].length==2){
                              if(fim=='')

    fim='('+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                              else{
                                    if((fim[fim.length-1]==']') || (fim[fim.length-
1]==')'))

    fim=fim+'|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                    else if(fim[fim.length-1]!=')')

    fim=fim+']|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
                                    else

    fim=fim+'|'+valores[i].charAt(0)+'['+valores[i].charAt(1)+']';
```

```
                              }
                        }
                        else{
                              texto.value='Erro! SÃ³ valores entre 0 e 99!';
                              if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                              return;
                        }
                  }
            }
      }

      //Se o texto estiver associado ao campo 'NÃ£o Acabado Em:'
      if(exp2=='naoacabar'){
            var valores=r_exp2.split(',');
            for(i=0;i<valores.length;i++){
                  var intervalo=valores[i].split('-');
                  if(intervalo.length==2){
                        if((intervalo[0].length==1)&&(intervalo[1].length==1)){
                              if(fim=='')
                                    fim='([^'+intervalo[0]+'-'+intervalo[1];
                              else
                                    fim=fim+intervalo[0]+'-'+intervalo[1];
                         }
                         else
if((intervalo[0].length==2)&&(intervalo[1].length==2)){
                              var dif1=intervalo[1].charAt(0)-
intervalo[0].charAt(0);
                              var dif2=intervalo[1].charAt(1)-
intervalo[0].charAt(1);
                              if((dif1<0) ||(dif1==0 && dif2<=0)){
                                    texto.value='Erro! O intervalo tem de ser
crescente!';
                                    if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                    return;
                              }
                              else{
                                    texto.value='NÃ£o suportado! Introduza a
expressÃ£o manualmente!';
                                          if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                                          return;
                              }
                         }
                         else{
                              texto.value='Erro! O intervalo nao pode ser da forma
\'x-xx\'! Tem de ser da forma \'xx-xx\'!';
                              if(botao!='false')

    document.getElementById('botao').setAttribute('disabled','');
                              return;
                         }
                   }
                   else{
                        if(valores[i].length==1){
                              if(fim=='')
                                    fim='([^'+valores[i];
```

```
                              else
                                    fim=fim+valores[i];
                        }
                        else if(valores[i].length==2){
                              if(valores.length==1)

      fim='([^'+valores[i].charAt(0)+'].|'+valores[i].charAt(0)+'[^'+valores[i].ch
  arAt(1);
                              else{
                                    texto.value='NÃ£o suportado! Introduza a
  expressÃ£o manualmente!';
                                    if(botao!='false')

      document.getElementById('botao').setAttribute('disabled','');
                                          return;
                              }
                        }
                        else{
                              texto.value='Erro! SÃ³ valores entre 0 e 99!';
                              if(botao!='false')

      document.getElementById('botao').setAttribute('disabled','');
                              return;
                        }
                  }
            }
      }
  }

  if(fim!=''){
            if((fim.charAt(fim.length-1)!=']')&&(fim.charAt(fim.length-1)!=')'))
                  fim=fim+'])';
            else
                  fim=fim+')';
  }

  if((inicio!='')&&(fim!=''))
      exp_reg=inicio+'..'+fim;
  else if(inicio!='')
      exp_reg=inicio;
  else if(fim!='')
      exp_reg='^....'+fim;
  else{
      texto.value='NÃ£o foram introduzidos valores!';
      if(botao!='false')
            document.getElementById('botao').setAttribute('disabled','');
      return
  }

  texto.value=exp_reg;
}
</SCRIPT>
```

Anexo B – *Integração do Módulo de Autenticação Automática no Portal*

```
include ("classes/adLDAP.php");

if (!isset($_COOKIE['galleta']['logout']) && !isset($usuario)) {
  $ldap=new adLDAP($options);
  if(isset($_SERVER['REMOTE_USER']) &&
($_SERVER['PHP_SELF']=='/portal/index.php')){
    $username=$_SERVER['REMOTE_USER'];
    $pos = stripos($username, '@');
    $username = substr($username,0,$pos);
    $username = strtolower($username);

    // autentica o servidor (apenas para ter permissoes para obter os
dados do utilizador)
    $result=$ldap->authenticate('HTTP-retateste','retateste2008');

    if($result==true){
        #echo "<b>Autenticado na RIN com sucesso!</b><br><br>";
        $result=$ldap->user_info($username);
        #print_r($result);

        $displayname=$result[0]['displayname'][0];
        $mail=$result[0]['mail'][0];
      $mail2=str_replace  ('-','.',$mail);
        $departamento=$result[0]['department'][0];
        $telephonenumber=$result[0]['telephonenumber'][0];

        #echo "Nome: ".$displayname."<br>";
        #echo "E-Mail: ".$mail."<br>";
        #echo "Departamento: ".$departamento."<br>";
        #echo "Telefone: ".$telephonenumber."<br><br>";

      $qry=sql_consultar("SELECT * FROM YERBA_usuarios WHERE
alias_alt='$username'");
      if(!sql_cantidad($qry)) {
            #echo "O username $username (da RIN) ainda nÃ£o tem associa-
do uma conta no portal!<br><br>";
            if($mail!=null){
                  $qry=sql_consultar("SELECT * FROM YERBA_usuarios WHERE
correo='$mail' OR correo='$mail2'");
                  if(!sql_cantidad($qry)) {
                        #echo "NÃ£o existe nenhum user no portal com e-
mail $mail!";
                        $usuario[gid]=null;
                                ihtml();
                                imarco();

                        $var="
                        <select id=\"uid\">";
                        $qry=sql_consultar("SELECT uid,alias FROM
YERBA_usuarios where alias_alt IS null Order by alias");
                        $f=0;
                        while(list($uid,$nombre)=sql_tomar($qry,$f)) {
```

```
                                if($f-1==sql_cantidad($qry)) break; else
$f++;
                                ($c?$c=0:$c=1);
                                $var.="<option value=\"$uid\"> $nom-
bre</option>";
                        }
                        $var.="</select>";

                        $var.="<input type=\"button\" value=\"Associar
Contas\" class=\"boton\" on-
click=\"javascript:location.href='usuarios.php?us=associar&frm[nombre]=$
display-
name&frm[correo]=$mail&frm[icq]=$departamento&frm[web]=$telephonenumber&
frm[alias]=$username&uid='+getElementById('uid').value\">";
                        $var2="<input type=\"button\" value=\"Registar-
me\" class=\"boton\" on-
click=\"javascript:location.href='usuarios.php?us=agregar&frm[nombre]=$d
isplay-
name&frm[correo]=$mail&frm[icq]=$departamento&frm[web]=$telephonenumber&
frm[alias]=$username'\">";

                        mensaje("NÃ£o foi encontrado nenhum utilizador
no portal SGA que tivesse as mesmas caracterÃsticas da sua conta da
RIN.<br><br>Se jÃ¡ tem conta no portal SGA selecione o seu user do por-
tal e carregue em 'Associar Contas'.<br>SerÃ¡ enviado um e-mail ao admi-
nistrador do portal SGA para validar a situaÃ§Ã£o, sendo-lhe depois
comunicado por e-mail o resultado do pedido. AtÃ© lÃ¡ pode continuar a
utilizar o portal SGA normalmente, fazendo o login como antigamen-
te.<br><br>$var<br><br>Se ainda nÃ£o estÃ¡ registado no portal pode
criar uma conta nova, bastando para isso carregar em:<br><br>$var2");

                        lado('d');
                        fmarco();
                                fhtml();
                                exit;
                } else if (sql_cantidad($qry)==1){
                        $usuario=sql_registro($qry);
                        #print_r($usuario);

                        if($usuario[alias_alt]!=null){
                                $usuario[gid]=null;
                                ihtml();
                                        imarco();
                                mensaje("Verifique a sua caixa de e-
mail.<br>Foi-lhe enviado um e-mail para associar a sua conta da RIN com
a sua conta do portal SGA.<br><br>Se nÃ£o recebeu nenhum e-mail, ou caso
o tenha apagado, contacte Guilherme AraÃºjo - 225008432");
                                fmarco();
                                fhtml();
                                exit;
                        } else {
                                $cod=md5(time());
                                $alias_alt=$cod."-".$username;
                                $qry=sql_consultar("update yerba_usuarios
set alias_alt='$alias_alt' where uid='$usuario[uid]'");


      $link="http://172.20.20.19/portal/usuarios.php?us=activate&uid=$us
uario[uid]&cod=$cod";

                                $to = $usuario[correo];
```

```
                                $subject = "ActivaÃ§Ã£o da conta SGA";
                                $message = "<br>A sua conta da RIN com
login <b>".$username."</b> estÃ¡ prestes a ser associada Ã Â  conta do
portal SGA com login <b>".$usuario['alias']."</b>.<br><br>Os dados refe-
rentes ao login <b>".$username."</b> na RIN sÃ£o:<br>Nome:
<i>".$displayname."</i><br>E-Mail: <i>".$mail."</i><br>Departamento:
<i>".$departamento."</i><br>Telefone:
<i>".$telephonenumber."</i><br><br>Os dados referentes ao login
<b>".$usuario['alias']."</b> no portal SGA sÃ£o:<br>Nome:
<i>".$usuario['nombre']."</i><br>E-Mail:
<i>".$usuario['correo']."</i><br>Departamento:
<i>".$usuario['icq']."</i><br>Telefone:
<i>".$usuario['web']."</i><br><br>Se estas contas forem realmente as
suas carregue no seguinte link:<br><a href=".$link.">Associar con-
tas</a><br><br>Se pelo contrÃ¡rio estes dados estÃ£o incorrectos pedimos
desculpa pelo engano e pedimos ainda que faÃ§a <i>reply</i> a este mail.
NÃ£o necessita de adicionar nenhum texto, basta enviar tal como
estÃ¡.<br><br>Muito obrigado,<br>SGA";
                                $headers = 'From: sga@telecom.pt' . "\r\n"
.
                                'Reply-To: carlos.g.araujo@telecom.pt' .
"\r\n" .
                                'X-Mailer: PHP/' . phpversion() . "\r\n" .
                                "MIME-Version: 1.0\r\n" .
                                "Content-Type: text/html; charset=UTF-
8;\r\n" .
                                "Content-Transfer-Encoding: 8bit\r\n\r\n";

                                mail($to, $subject, $message, $headers);

                                $to      = "carlos.g.araujo@telecom.pt";
                                      $subject = "AssociaÃ§Ã£o da conta da
RIN ".$username." Ã  conta do portal SGA ".$usuario['alias'];
                                $message = "<br>A conta da RIN com login
<b>".$username."</b> estÃ¡ prestes a ser associada Ã  conta do portal
SGA com login <b>".$usuario['alias']."</b>.<br><br>Os dados referentes
ao login <b>".$username."</b> na RIN sÃ£o:<br>Nome:
<i>".$displayname."</i><br>E-Mail: <i>".$mail."</i><br>Departamento:
<i>".$departamento."</i><br>Telefone:
<i>".$telephonenumber."</i><br><br>Os dados referentes ao login
<b>".$usuario['alias']."</b> no portal SGA sÃ£o:<br>Nome:
<i>".$usuario['nombre']."</i><br>E-Mail:
<i>".$usuario['correo']."</i><br>Departamento:
<i>".$usuario['icq']."</i><br>Telefone: <i>".$usuario['web']."</i>";
                                mail($to, $subject, $message, $headers);

                                        $usuario[gid]=null;
                                        ihtml();
                                        imarco();
                                        mensaje("Obrigado por visitar o
portal do SGA.<br>Visto ser a primeira vez que o faz, foi-lhe enviado um
e-mail para associar a sua conta da RIN com a sua conta do portal
SGA.<br>Por favor siga as intruÃ§Ãµes do e-mail.");
                                        fmarco();
                                        fhtml();
                                        exit;
                        }
                } else {   #caso o mesmo e-mail esteja associado a
mais q um utilizador
                        $usuario[gid]=null;
                                ihtml();
```

```
                                imarco();

                                $var="
                                <select id=\"uid\">";
                                $qry=sql_consultar("SELECT uid,alias
FROM YERBA_usuarios where alias_alt IS null AND correo='$mail' OR cor-
reo='$mail2' Order by alias");
                                $f=0;

while(list($uid,$nombre)=sql_tomar($qry,$f)) {
                                        if($f-1==sql_cantidad($qry))
break; else $f++;
                                        ($c?$c=0:$c=1);
                                        $var.="<option value=\"$uid\">
$nombre</option>";
                                }
                                $var.="</select>";

                                $var.="<input type=\"button\"
value=\"Associar Contas\" class=\"boton\" on-
click=\"javascript:location.href='usuarios.php?us=associar&frm[nombre]=$
display-
name&frm[correo]=$mail&frm[icq]=$departamento&frm[web]=$telephonenumber&
frm[alias]=$username&uid='+getElementById('uid').value\">";

                                mensaje("Foram encontrados mais do que
um utilizador do portal SGA que correspondem Ã s suas caracterÃsticas.
Assim sendo, selecione o seu user do portal e carregue em 'Associar Con-
tas'.<br>SerÃ¡ enviado um e-mail ao administrador do portal SGA para
validar a situaÃ§Ã£o, sendo-lhe depois comunicado por e-mail o resultado
do pedido. AtÃ© lÃ¡ pode continuar a utilizar o portal SGA normalmente,
fazendo o login como antigamente.<br><br>$var");

                                lado('d');
                                fmarco();
                                fhtml();
                                exit;
                        }
                }
        } else {
                $ip=getenv('REMOTE_ADDR');
                  $usuario=sql_registro($qry);
                sql_consultar("UPDATE YERBA_estado SET
uid='$usuario[uid]',tipo='u',refresco=now() WHERE ip='$ip'");
                  $se-
sion="$usuario[uid]:$usuario[gid]:$usuario[nombre]:$usuario[alias]:$usua
rio[clave]:$usuario[pais]";
                  $sesion=base64_encode($sesion);
                setcookie('galleta[sesion]',$sesion,time()+(3600*24));

                  # Log de sessoes abertas
                $Handle = fopen('/home/retadm/log/sessoes_portal.log', 'a');
                  fwrite($Handle, date('Y-m-d H:i')." uid=$usuario[uid]
$usuario[alias],\tgid=$usuario[gid] $usuario[pais],\t$ip\n");
                fclose($Handle);

                  header("Location: index.php");
        }
        sql_liberar($qry);
      }
      else if(isset($username)){
```

```
      $usuario[gid]=null;
      ihtml();
        imarco();
        mensaje("Erro! Credenciais da RIN erradas!<br>Se preferir faÃ§a
o login manual.$username");
      lado('d');
      fmarco();
        fhtml();
        exit;
    }
  }
}
```

Anexo C – *Módulo para gerar os menus visíveis a cada utilizador*

```
<?

include('config.inc.php');
global $color;
global $usuario;

if(isset($usuario['pais'])){
  $opr="USR=$usuario[alias]&GRP=$usuario[pais]&GID=$usuario[gid]";
  $p = popen("psql --host $MAQ_BD_LOC --username $USR_BD --dbname
$NOME_BD -F' ' -At -c \"SELECT domorg FROM grupo WHERE
nome_grupo='$usuario[pais]'\"", "r");
  $usuario['domorg'] = trim(fgets($p));
  pclose($p);
}else{

$usuario['gid']=$usuario['domorg']=$usuario['alias']=$usuario['pais']=nu
ll;
}

if(!isset($opr))
  $opr=null;

$tabla['ti']="Menu";

// Codigo para o menu vertical
global $dirlm, $wwwlm;
$dirlm='/var/www/html/portal/phplayersmenu/';

echo '
<SCRIPT LANGUAGE="JavaScript">
function bb(loc)
{
jbb=window.open(loc,"jbb","toolbar=no,location=no,directories=no,status=
no,menubar=no,scrollbars=no,resizable=yes,width=800,height=600")
}
</SCRIPT>';

$descmv="";

$tabla['co']="
<b><center>Alarmes Activos</center></b>
<hr>";

$descmv.=".|<b>Geral</b>\n";
$descmv.="..|Consulta|javascript:blank('/cgi-
bin/wasga.cgi/alm_arq0?$opr&tit=Rede',710,480,10,50,'consulta')|InformaÃ
§Ã£o que se ver ao passar o rato por cima|\n";

if($usuario['domorg'] & 1 || $usuario['gid'] & 1){   # Caso o utilizado
tenha o bit 0 do dominio organizacional a 1, ou root
  if($usuario['gid'] & 2 || $usuario['gid'] & 1){ # SÃ³ para operadores
registados, com bit 2 no gid ou root
```

```
     $descmv.="..|Janela de Alar-
mes|javascript:blank_ja('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=1&quant=1',800,550,10,50)|InformaÃ§Ã£o que se
ver ao passar o rato por cima|\n";
       $descmv.="..|Janela Alarmes
Dupla|javascript:blank_ja_unica('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=1&quant=2',800,550,10,50,'geral_ja_dupla')|Info
rmaÃ§Ã£o que se ver ao passar o rato por cima|\n";
       $descmv.="..|Mensagens da
JA|javascript:blank('/portal/log.php?instancia=1',710,480,20,70,'msg_ja'
)|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
  }


if((strncmp($usuario['pais'],"cngr",4)==0)||(!strcmp($usuario['alias']," 
jpmorais"))||(!strcmp($usuario['alias'],"3030988")))  # So para o opera-
dor com grupo cngr
    $descmv.="..|Janela com
Mapas|javascript:blank_ja('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=1&quant=1&mapas=1',800,550,10,50,'ja_mapas')|In
formaÃ§Ã£o que se ver ao passar o rato por cima|\n";
}

$descmv.="."|<b>Megabit</b>\n";
$descmv.="..|Consulta|javascript:blank('/cgi-
bin/wasga.cgi/alm_arq1?$opr&tit=Circuito',710,480,10,50,'consulta')|Info
rmaÃ§Ã£o que se ver ao passar o rato por cima|\n";

if($usuario['domorg'] & 2 || $usuario['gid'] & 1){   # Caso o utilizado
tenha o bit 1 do dominio organizacional a 1, ou root
  if($usuario['gid'] & 2 || $usuario['gid'] & 1){ # SÃ³ para operadores
registados, com bit 2 no gid ou root
   $descmv.="..|Janela de Alar-
mes|javascript:blank_ja('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=2&quant=1',800,550,10,50)|InformaÃ§Ã£o que se
ver ao passar o rato por cima|\n";
       $descmv.="..|Janela Alarmes
Dupla|javascript:blank_ja_unica('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=2&quant=2',800,550,10,50,'megabit_ja_supla')|In
formaÃ§Ã£o que se ver ao passar o rato por cima|\n";
       $descmv.="..|Mensagens da
JA|javascript:blank('/portal/log.php?instancia=2',710,480,20,70,'msg_ja'
)|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
  }
}

$descmv.="."|<b>Redes de Dados</b>\n";
$descmv.="..|Consulta|javascript:blank('/cgi-
bin/wasga.cgi/alm_arq2?$opr&tit=Dados',710,480,10,50,'consulta')|Informa
Ã§Ã£o que se ver ao passar o rato por cima|\n";

if($usuario['domorg'] & 4 || $usuario['gid'] & 1){   # Caso o utilizado
tenha o bit 2 do dominio organizacional a 1, ou root
      if($usuario['gid'] & 2 || $usuario['gid'] & 1){ # SÃ³ para opera-
dores registados, com bit 2 no gid ou root
   $descmv.="..|Janela de Alar-
mes|javascript:blank_ja('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=3&quant=1',800,550,10,50)|InformaÃ§Ã£o que se
ver ao passar o rato por cima|\n";
       $descmv.="..|Janela Alarmes
Dupla|javascript:blank_ja_unica('http://172.20.20.26/cgi-
```

```
bin/ja.pl?$opr&instancia=3&quant=2',800,550,10,50,'dados_ja_supla')|Info
rmaÃ§Ã£o que se ver ao passar o rato por cima|\n";
       $descmv.="..|Mensagens da
JA|javascript:blank('/portal/log.php?instancia=3',710,480,20,70,'msg_ja'
)|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
  }
}

$descmv.="|<b>ServiÃ§os</b>\n";
$descmv.="..|Consulta|javascript:blank('/cgi-
bin/wasga.cgi/alm_arq3?$opr&tit=ServiÃ§os',710,480,10,50,'consulta')|Inf
ormaÃ§Ã£o que se ver ao passar o rato por cima|\n";

if($usuario['domorg'] & 8 || $usuario['gid'] & 1){   # Caso o utilizado
tenha o bit 3 do dominio organizacional a 1, ou root
      if($usuario['gid'] & 2 || $usuario['gid'] & 1){ # SÃ³ para opera-
dores registados, com bit 2 no gid ou root
   $descmv.="..|Janela de Alar-
mes|javascript:blank_ja('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=3&quant=1',800,550,10,50)|InformaÃ§Ã£o que se
ver ao passar o rato por cima|\n";
       $descmv.="..|Janela Alarmes
Dupla|javascript:blank_ja_unica('http://172.20.20.26/cgi-
bin/ja.pl?$opr&instancia=3&quant=2',800,550,10,50,'servicos_ja_dupla')|I
nformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
       $descmv.="..|Mensagens da
JA|javascript:blank('/portal/log.php?instancia=3',710,480,20,70,'msg_ja'
)|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
  }
}

if($usuario['gid'] & 2 || $usuario['gid'] & 1) { # So para operadores
registados, com bit 2 no gid, ou root
 $descmv.="|<b>Anomalias</b>\n";
 $des-
cmv.="..|Activas|javascript:blank('anm_pal.php?func=msg&estado=A&GRP=$us
uario[pais]',710,480,20,70,'janela')|InformaÃ§Ã£o que se ver ao passar o
rato por cima|\n";
 $des-
cmv.="..|Resolvidas|javascript:blank('anm_pal.php?func=msg&estado=R&GRP=
$usuario[pais]',710,480,20,70,'janela')|InformaÃ§Ã£o que se ver ao pas-
sar o rato por cima|\n";
}

require_once $dirlm.'lib/treemenu.inc.php';
$treemid = new TreeMenu();
$treemid->setMenuStructureString($descmv);
$treemid->setIconsize(10, 10);
$treemid->parseStructureForMenu('treemenu1');
$treemid->replaceStringInUrls('treemenu1','Vusr',$opr);
$treemid->setSelectedItemByUrl('treemenu1', basename(__FILE__));

$tabla['co'].=$treemid->newTreeMenu('treemenu1');
$descmv="";

if($usuario['gid']) { # So para operadores registados
 $tabla['co'].="
 <br><b><center>Arquivo</center></b>
 <hr>";

 $descmv.="|<b>Rede e Infraestruturas</b>\n";
```

```
 $descmv.="..|Pontos Alarme
(Novo)|javascript:blank('/portal/hista.php?it=_r&$opr',710,480,20,70,'ar
quivo')|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
 $descmv.="..|Pontos de Alarme|javascript:blank('/cgi-
bin/wdbi.cgi/retadm/histr/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";

 if($usuario['gid'] & 1)  # Administrador do Sistema
  $descmv.="..|NÃ£o Arquivados|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/actr/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã£
o que se ver ao passar o rato por cima|\n";

 $descmv.="..|NotificaÃ§Ãµes|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/ntffr/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";
 $descmv.="..|Registos Arq.
Geral|javascript:blank_arq('/portal/arqact/index.php?$opr&instancia=1&ti
po=1',800,600,10,50,'arquivo')|InformaÃ§Ã£o que se ver ao passar o rato
por cima|\n";
 $descmv.="..|Registos Arq.
Dados|javascript:blank_arq('/portal/arqact/index.php?$opr&instancia=3&ti
po=1',800,600,10,50,'arquivo')|InformaÃ§Ã£o que se ver ao passar o rato
por cima|\n";
 $descmv.="..|EstatÃstica|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/alres/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";

 if($usuario['gid'] & 1) # Administrador do Sistema
       $des-
cmv.="..|Componentes|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/compr/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";


 $descmv.=".|<b>Circuitos Alugados</b>\n";

 $descmv.="..|Pontos Alarme
(Novo)|javascript:blank('/portal/hista.php?it=_c&$opr',710,480,20,70,'ar
quivo')|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
 $descmv.="..|Pontos de Alarme|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/histc/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";

 if($usuario['gid'] & 1)  # Administrador do Sistema
  $descmv.="..|NÃ£o Arquivados|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/actc/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã£
o que se ver ao passar o rato por cima|\n";

 $descmv.="..|NotificaÃ§Ãµes|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/ntffc/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";
 $descmv.="..|Registos Arquiva-
dos|javascript:blank_arq('/portal/arquivo.php?instancia=2',800,600,10,50
,'arquivo')|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
 $descmv.="..|EstatÃstica|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/alces/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";

 if($usuario['gid'] & 1) # Administrador do Sistema
```

```
       $des-
cmv.="..|Componentes|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/compc/form?$opr',710,480,20,70,'arquivo')|InformaÃ§Ã
£o que se ver ao passar o rato por cima|\n";


      $descmv.=".|<b>Outras Consultas</b>\n";
      $descmv.="..|Elementos de
Rede|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/sub/form',710,480,20,70,'arquivo')|InformaÃ§Ã£o que
se ver ao passar o rato por cima|\n";

      if($usuario['gid'] & 1) # Administrador do Sistema
       $descmv.="..|Tipos de Alar-
me|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/tipo_alm/form',710,480,20,70,'arquivo')|InformaÃ§Ã£o
que se ver ao passar o rato por cima|\n";

      $descmv.="..|Detalhe do
DG|javascript:blank('/portal/pdg.php',710,480,20,70,'arquivo')|InformaÃ§
Ã£o que se ver ao passar o rato por cima|\n";

      if($usuario['gid'] & 4) # So para operadores registados, com bit 4
no gid
       $des-
cmv.="..|ObservaÃ§Ãµes|javascript:blank('/portal/msg_pal.php?USR=$usuari
o[alias]',710,480,20,70,'arquivo')|InformaÃ§Ã£o que se ver ao passar o
rato por cima|\n";

      $descmv.="..|Alarmes Exter-
nos|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/conf_esp1/form?$opr',710,480,20,70,'arquivo')|Inform
aÃ§Ã£o que se ver ao passar o rato por cima|\n";

      if($usuario['gid'] & 4) { # So para operadores registados, com bit
4 no gid
   $descmv.=".|<b>Monitoria de Pontos de Alarme</b>\n";

       $des-
cmv.="..|ConfiguraÃ§Ã£o|javascript:blank('pasa.php?USR=$usuario[alias]',
710,480,20,70,'arquivo')|InformaÃ§Ã£o que se ver ao passar o rato por
cima|\n";
       $descmv.="..|Consulta|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/pasa/form?USR=$usuario[alias]',710,480,20,70,'arquiv
o')|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
  }

      if($usuario['gid'] & 1 or $usuario['gid'] & 4) # Administrador do
Sistema ou operadores registados com gid&4
       $descmv.="..|DomÃnios de Ges-
tÃ£o|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/dg_grp/form?USR=$usuario[alias]',710,480,20,70,'arqu
ivo')|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";

      if($usuario['gid'] & 1) # Administrador do Sistema
       $descmv.="..|MÃ¡quinas e Sub-
sist|javascript:blank('http://$MAQ_BD_LOC/cgi-
bin/wdbi.cgi/retadm/tab_ms/form?USR=$usuario[alias]',710,480,20,70,'arqu
ivo')|InformaÃ§Ã£o que se ver ao passar o rato por cima|\n";
}
```

```
if($descmv){
  $treemid->setMenuStructureString($descmv);
  $treemid->setIconsize(10, 10);
  $treemid->parseStructureForMenu('treemenu1');
  $treemid->replaceStringInUrls('treemenu1','Vusr',$opr);
  $treemid->setSelectedItemByUrl('treemenu1', basename(__FILE__));

  $tabla['co'].=$treemid->newTreeMenu('treemenu1');
}


if($usuario['gid'] & 1) { # Administrador do Sistema
$tabla['co'].="
<br><b><center>Administrar</center></b>
<hr>";

$tabla['co'].="
<img src=\"graficos/sistema.gif\" hspace=\"3\"><a
href=\"javascript:blank('administrar.php?us=acessos',900,350,200,50,'jan
ela_admin')\">Grupos de Acesso</a><br>
<img src=\"graficos/sistema.gif\" hspace=\"3\"><a
href=\"javascript:blank('administrar.php?us=mdomo',600,500,75,200,'janel
a_admin')\">Dom. Organizacionais</a><br>
<img src=\"graficos/sistema.gif\" hspace=\"3\"><a
href=\"javascript:blank('administrar.php?us=gestao',1000,600,7,7,'janela
_admin')\">Dom. de GestÃ£o</a><br>
<img src=\"graficos/sistema.gif\" hspace=\"3\"><a
href=\"usuarios.php?us=perfis&popup=true\">Perfis Operadores</a><br>
<img src=\"graficos/sistema.gif\" hspace=\"3\"><a
href=\"javascript:blank('administrar.php?us=tec',820,300,200,100,'janela
_admin')\">Tecnologias</a><br>
<img src=\"graficos/sistema.gif\" hspace=\"3\"><a
href=\"javascript:blank('administrar.php?us=sub',1000,280,220,5,'janela_
admin')\">Sub-Sistemas</a><br>";
}


if($usuario['gid'] & 1) { # Administrador do Sistema
  $tabla['co'].="
  <br><b><center>Diversos</center></b>
  <hr>";

  $tabla['co'].="<img src=\"graficos/estadistica.gif\" hspace=\"3\">
  <a href=\"javascript:nulo()\"
  onclick=\"javascript:janela('/stats.html',710,480,20,70,'stats')\">
  Estat&iacute;sticas Servidor</a><br>";

  $tabla['co'].="<img src=\"graficos/estadistica.gif\" hspa-
ce=\"3\">\n".enl('Estat&iacute;stica Portal','contador.php')."<br>\n";
  $tabla['co'].="<img src=\"graficos/mas.gif\" hspa-
ce=\"3\">\n".enl(LOSMAS,'contador.php?cr=losmas')."<br>\n";
}


$tabla['co'].="
<br><b><center>Contactos</center></b>
<hr>";

$tabla['co'].="<img src=\"graficos/sugerir.gif\" hspa-
ce=\"3\">\n".enl('Admin. Sistema','index.php?ix=contacto')."<br>\n";
```

```
$tabla['co'].="<img src=\"graficos/profile.gif\" hspace=\"3\">
<a href=\"javascript:nulo()\"
on-
click=\"javascript:janela('usuarios.php?us=lista',710,480,20,70,'contact
os')\">
Registados</a><br>";


$tabla['co'].="<img src=\"graficos/profile.gif\" hspace=\"3\">
<a href=\"javascript:nulo()\"
onclick=\"javascript:janela('http://172.27.140.96/private/ListaResp.xls'
,710,480,20,70,'contactos')\">
Operacionais</a><br>";

$tabla['co'].="<img src=\"graficos/profile.gif\" hspace=\"3\">
<a href=\"javascript:nulo()\"
onclick=\"javascript:janela('http://ptsgps-
aplica-
tion.telecom.pt/estrutura/asp/Directorio.asp',710,480,20,70,'contactos')
\">
Lista Interna PT</a><br>";

$tabla['co'].="<img src=\"graficos/profile.gif\" hspace=\"3\">
<a href=\"javascript:nulo()\"
onclick=\"javascript:janela('http://tel118.telecom.pt/pesqmenu.php',710,
480,20,70,'contactos')\">
Lista 118</a><br>";

tabla($tabla);
?>
```