Faculdade de Engenharia da Universidade do Porto

Gestão Integrada de Controlo de Acessos

Filipe João Pereira Montenegro

Versão Final

Relatório de Projecto realizado no Âmbito do
Mestrado Integrado em Engenharia Informática e Computação

Orientador: Prof. Gabriel David
Co-orientador: Eng. Manuel Machado

Julho de 2008

Gestão Integrada de Controlo de Acessos

Filipe João Pereira Montenegro

Relatório de Projecto realizado no Âmbito do
Mestrado Integrado em Engenharia Informática e Computação

Aprovado em provas públicas pelo Júri:

Presidente: Prof. Rosaldo José Fernandes Rossetti

Arguente: Prof. José Carlos Ramalho

31 de Julho de 2008

Resumo

A problemática da gestão da informação de acesso e permissões de acesso às instalações de uma Instituição, são cada vez mais uma prioridade no planeamento da segurança. Neste sentido, com o desenvolvimento de um módulo para o SIGARRA, que permita gerir toda a informação de permissões de acesso, estatísticas de acesso e fazer a integração com os dispositivos físicos e humanos que controlam o acesso às instalações.

Este novo módulo do Sistema de Informação para a Gestão Agregada de Recursos e Registos (SIGARRA) vem permitir que exista a possibilidade de através do SI controlar, os dispositivos de acesso existentes, as pessoas com acesso a esses dispositivos e monitorizar com recurso a estatíticas os acessos efectuados. Para que todas essas funcionalidades fossem possiveis, foram criadas duas possibilidades de atribuição de novas permições de acesso, permições dadas a pessoas individualmente e permissões dadas a grupos. Os grupos de acesso são criados no SI e permitem a aglumeração de pessoas com permições de acesso iguais de modo a permitir uma mais fácil alteração de permições a um grande número de pessoas. De modo a ser possivel atribuir permições é também necessário registar no sistema de informação os dispositivos que controlam os pontos de acesso, para tal foi também criada a possibilidade de no SI inserir esta funcionalidade.

Para o controlo das entradas e saidas das intalações foi necessário interligar o SI com a aplicação que controla os dispositivos existentes, para recolher os dados que são lidos pelos dispositivos. Estes dados são despois tratados de modo a criar estatísticas de acesso, que servirão como indicativos do funcionamento dos pontos de acesso existentes.

Do mesmo modo que é importante o controlo dos acessos é também importante o controlo da distribuição dos cartões de acesso disponibilizados aos utilizadores das instalações da Faculdade de Engenharia da Universidade do Porto, para tal foi criada a possibilidade de pedir uma nova via do cartão de acesso apartir do SI e o controlo de todo o processo da criação do mesmo, isto tudo sem que seja necessário recurrer aos antigos requerimentos em papel.

Com o módulo concluído temos os diversos sistemas completamente integrados e o completo controlo sobre os pontos de acesso das instalações, todo reunido num único ponto, facilitando o bom funcionamento geral do controlo de acessos.

Abstract

The sistem called Sistema de Informação para a Gestão Agregada de Recursos e Registos (SIGARRA) gets together the information from varied faculties, one point that until now is not part of that information is the information relative to the acess control sistems that exist allover those institutions. As response to that situation, was created a now module for the information sistem that gets the data from all the access control aplications. My particular interest in the information sistems area and the oportunity of produting software to itegrate SIGARRA whore the most estimulating motivations to envolve in this project project.

In Faculdade de Engenharia da Universidade do Portocase, now we have the possibility to control from the information sistem all the data relative to access control sistems, allowing the users to get access to their accesses data and improving the existing processes concerning the delivery of access cards and access permitions.

For atributing permitions to people whore created two possibilities, the direct atribution to a person and the atribution to groups of people. To acomplish that was created in the possibility to manage groups of people and linking them to access control dispositives. To get access to the data collected from the dispositives it was necessarie to create a way to connect the information sistem to the aplication that directly connects to the dispositives, that was made with web services using SOAP protocol. For the atribution of acess permitions was also necessarie to create the possibilitie of inserting in the information sistem the list of all the active control dispositives.

With the data collected from the dispositives are create access statistics that allow to verify the viability of the sistens corrently controling the infrastutures of Faculdade de Engenharia da Universidade do Porto.

Agradecimentos

Agradeço ao Professor Gabriel David pela disponibilidade, interesse e acompanhamento ao longo de todo o projecto. Agradeço a toda a equipa do Projecto de Sistemas de Informação pela disponibilidade em ajudar sempre que foi necessário, em especial ao Eng. Manuel Machado que como co-orientador me deu um grande apoio. Agradeço à minha namorada Vera, pela compreensão e paciência demonstrada. Por fim mas não menos importante agradeço ao Artur Castro, Claudio Alves e Carlos Fernandes pela companhia nas noites de trabalho na FEUP sempre que tal foi necessário.

Filipe João Pereira Montenegro

"Pleasure in the job puts perfection in the work."

Aristotle

Conteúdo

Lista de Figuras

Abreviaturas e Símbolos

FEUP	Faculdade de Engenharia da Universidade do Porto
SI	Sistema de Informação
SIGARRA	Sistema de Informação para a Gestão Agregada de Recursos e Registos Académicos
SQL	Structured Query Language
PL/SQL	Procedural Language/Structured Query Language
XML	eXtensible Markup Language
SOAP	Simple Object Access Protocol
UML	Unified Modeling Language

Capítulo 1

Introdução

O projecto de Gestão Integrada de Controlo de Acessos é o trabalho final do mestrado integrado em engenharia informática e computação da Faculdade de Engenharia da Universidade do Porto do aluno Filipe João Pereira Montenegro. O projecto foi desenvolvido no Projecto de Sistemas de Informação da FEUP e teve como objectivo a criação de um novo módulo para o sistema SIGARRA que permitisse de uma forma simples e completa o controlo de todos os acessos às instalações da FEUP (ao ser integrado no SIGARRA este módulo pode à posteriori ser instalado em todas as escolas que usam o mesmo). O meu gosto particular pelos sistemas de informação e a sua gestão, bem como o conteúdo aliciante do projecto tornaram a motivação para o mesmo bastante elevada.

O projecto passou por diversas fases distintas, estas serão descritas em pormenor mais adiante neste relatório, nem todas as fases fazem parte do novo módulo do SIGARRA mas visto estarem relacionadas com o contexto global do projecto serão alvo de alguma atenção. O projecto contou então na sua totalidade com as seguintes fases:

- Estudo do sistema físico a aplicar nas novas portas rotativas;
- Estudo do suporte informático a utilizar;
- Criação e distribuição dos identificadores (neste caso cartões de banda magnética e chip RFid) pessoais aos utilizadores;
- Migração de dados dos utilizadores dos antigos para os novos identificadores (por razões de segurança os códigos magnéticos existentes foram alterados);
- Implementação do módulo do SIGARRA como agregador de toda a informação.

Este relatório é composto por sete capítulos, este primeiro (1) capítulo onde é feita a introdução ao projecto, descrição dos principais objectivos e uma breve informação da empresa onde decorreu o projecto. No capítulo 2 é analisado o estado actual do controlo de acessos na FEUP e as tecnologias utilizadas actualmente. No capítulo 3 é feita a especificação do projecto de modo a detalhar todos os pontos que serão implemantados. No capítulo 4 são detalhadamente descritos todos os componentes que fazem parte do projecto, ou serviram como apoio na construção do mesmo. No capítulo 5 é descrita em promenor toda a implementação efectuada. No capítulo 6 são descritos os testes efectuados e por fim no capítulo 7 são tiradas conclusões sobre o projecto e descritas quais as previsões de trabalho futuro sobre o módulo.

1.1 Contexto/Enquadramento

Este projecto foi devenvolvido no Projecto de Sistemas de Informação da FEUP, e integra-se na area dos sistemas de informação e de igual forma na área de segurança de intalações. O objectivo final é integrar complatamente o módulo com o sistema de informação SIGARRA que está já intalado em várias escolas pelo país fora.

O Projecto de Sitemas de Informação da FEUP é constituído por colaboradores da FEUP que pertencem maioritariamente aos quadros do CICA (Centro de Informática Professor Correia de Araújo). Depende funcionalmente da Direcção da Faculdade e tem por objectivo o desenvolvimento de produtos e serviços na área dos sistemas de informação. Actualmente os seus principais projectos são o desenvolvimento do SIGARRA, a Gestão Integrada de Contra-Ordenações para a Câmara Municipal do Porto e o Sistema de Informação do Sindicato de Trabalhadores da Função Pública do Norte.

1.2 Projecto

O projecto desenvolvido vem integrar o SIGARRA de modo a permitir a gestão de acessos às instalações das instituições que utilizam este sistema de informação. Desta forma a partir do SI é possivel gerir os dispositivos existentes, os espaços controlados por esses dispositivos, efectuar a gestão de grupos de acesso e controlar os acessos efectuados. No modulo é ainda incluída a gestão de atribuição e pedido de cartões de acesso as instalações.

Como os dispositivos de controlo possuem um software espacifico foram também implementadas mecanismos de sincronização e migração de dados entres os diversos sistemas.

1.3 Motivação e Objectivos

A grande motivação do projecto foi o meu gosto pessoal pelos sistemas de informação e ainda a possibilidade de trabalhar com algo com que nunca tinha trabalhado anteriormente (é o caso das aplicações de controlo de acesso que comunicam com os dispositos). Outro ponto motivante era a prespectiva de ligação entre os vários sistemas, pelo desafio que esta interacção poderia trazer. Os objectivos do projecto passavam por:

- gerir toda a informação de permissões de acesso
- estatísticas de acesso
- integração com os dispositivos físicos e humanos que controlam o acesso

Para a implementação dos objectivos estabelecidos foi necessário recurrer a diversas tecnologias das quais passo a listar as mais relevantes:

- Oracle
- Apache
- PLSQL
- HTML
- PHP
- Java

1.4 Estrutura da Dissertação

Para além da introdução, esta dissertação contém mais 6 capítulos. No capítulo 2, é descrito o estado actual existente relativamente ao controlo de acessos efectuado na Faculdade de Engenharia da Universidade do Porto. No capítulo 3, a especificação do projecto é descrita, é aborada a vista fisica e lógica do módulo, os casos de uso, requisitos e o modelo de dados que irá servir de suporte ao módulo. No capítulo 4, são descritos os componentes utilizados pelo módulo. No capítulo 5, é descrita em promenor toda a implementação efectuada. O capítulo 6, descreve a validação e testes ao módulo produzido. No capítulo 7, são apresentadas as conclusões e o trabalho futuro.

Capítulo 2

Contexto Actual

Neste capítulo é descrito o contexo actual da encontrado na Faculdade de Engenharia relativamente ao modo como os acessos às suas intalações eram efectuados e controlados. É também neste capitulo onde é feita uma revisão tecnologia das principais tecnologias e ferramentas utilizadas durante o projecto, relativamente as tecnologias é ainda apresentada a razão pela qual as tecnologias apresentadas foram escolhidas.

2.1 Controlo de acessos actual na FEUP

De modo a se compreenderem as necessidades do novo módulo foi estado o estado actual do controlo de acessos existente na FEUP.

Até ao momento a tecnologia utilizada para o controlo dos acessos era baseada numa rede única e separada da rede de intranet da faculdade, de leitores de banda magnética. Os leitores magnéticos estão ligados a controladores(SIEMENS) que permitem cada um a ligação de 8 leitores, estes controladores permitem que os leitores respondam de forma rápida aos pedidos e permitem que o servidor de controlo possa falhar, ou seja os controladores podem guardar um elevado número de acessos e alarmes(acessos não concedidos) internamente, para depois serem descarregados para o servidor.

O grande problema do sistema actual residia na sua distanciação do resto das aplicações, quer por estar fisicamente separado (por razões de segurança), quer por a aplicação que gere toda a informação ser já bastante antiga. Esta aplicação corre sobre um linux Red Hat versão 6.2 suportado por uma base de dados Unified. Nesta aplicação é feita toda a gestão das permissões actuais, nos pontos de acesso controlados por leitores magnéticos, sendo que o processo de pedido de novas permissões

basea-se no envio de mail para os serviços técnicos da faculdade de modo a que as novas permissões sejam concedidas.
Ligado também ao controlo de acessos temos a impressão e distribuição dos cartões para funcionários e alunos, estes são desde 2003 impressos e codificados nas instalações da faculdade. Estes cartões são entregues aos alunos no acto da inscrição e aos funcionários no inicio do seu contrato, sempre que estes eram perdidos ou roubados a segunda-via do cartão pressupunha o preenchimento de um requerimento pedindo um novo cartão. O problema no caso dos cartões residia no fraco controlo dos pedidos dos cartões e do seu respectivo levantamento, existindo actualmente bastantes cartões que foram pedidos, impressos mas que nunca foram levantados, levando em casos extremos ao pedido de um novo cartão sem que o anteriormente impresso seja levantado. Ainda relativamente à impressão dos cartões não existia um procedimento automático de criação do mesmo, este consistia na reunião dos dados a imprimir nos cartões serem recolhidos pelos funcionários responsáveis pela impressão dos mesmos através do SIFEUP. Estes dados eram depois inseridos num ficheiro excel que era reconhecido pelo software de impressão e codificação dos cartões, este processo era bastante moroso e mais sensível a erros que uma importação automática dos dados mesmo que no formato MSExcel. O controlo do final final da validade dos cartões era também deixada um pouco de lado, existindo actualmente cartões de utilizadores que já não frequentam a faculdade à alguns anos mas que continuam registados como activos.
Outro ponto analisado em paralelo com as necessidades de melhoramento do controlo de acesso residiu numa necessidade existente na Faculdade, esta passava por disponibilizar a toda a comunidade académica o acesso as instalações da mesma a qualquer hora. Actualmente as instalações estavam abertas durante o dia das sete da manha até à meia-noite passando depois a ser aberta de duas em duas horas para todas as entradas e saídas, durante o período de fecho e de modo a evitar a espera pela próxima hora de abertura começaram a ser utilizadas as portas de emergência para entrar e sair sem controlo. Esta situação de uso indevido das portas de emergência foi ainda agravada com a lei da proibição de fumar nos locais fechados, passando durante a noite as portas a estar mais tempo abertas que fechadas. Existia então uma necessidade real de implementar uma solução que permiti-se minorar este problema.

2.2 Revisão tecnológica

2.2.1 Tecnologias utilizadas actualmente

Como suporte para ao controlo de acessos actual é utilizado um sistema Siemens composto por um servidor ligado a controladores que por sua vez estão ligados

a dispositivos de controlo com leitura magnética. Toda esta infra-estrutura está conectada por uma rede única e distinta da rede da Faculdade, de modo a torna-se mais segura.

A aplicação servidor, StarGaze, corre num sistema Unix RedHat 6.2 e o sistema de base de dados utilizado é o Unify DataServer na versão 6.3. Esta aplicação permite registar os utilizadores através do seu código pessoal na faculdade e do código do seu cartão magnético, atribuir permissões ao diversos pontos de acesso, controlar os dispositivos existentes e adicionar novos dispositivos, controlar em tempo real os acessos (negados e concedidos) aos diversos dispositivos. Um dos pontos positivos desta aplicação é a estrutura do modelo de dados sobre o qual a mesma acenta, o que facilitou o reverse engineering que teve que ser feito para poder efectuar as migrações de dados necessárias para habilitar os novos cartões.

2.2.2 Tecnologias utilizavéis

De modo a implementar todas as componentes envolvidas no projecto foi necessário analisar diversas tecnologias de modo a optar pela que, ou por incutir maior segurança no seu uso, ou por existir um maior conhecimento sobre a mesma, se revelou como a opção mais viável.

Sistema de Base de Dados - Neste campo foi bastante fácil optar pela base de dados da Oracle na versão 10g, isto porque todo o SIGARRA assenta em tecnologia Oracle e como o módulo a desenvolver será integrado com o esse sistema não existiu realmente escolha relativamente a esta tecnologia.

Interfaces web, lógica de negocio e ligação a dados - Visto ter sido escolhida a base de dados Oracle para armazenamento dos dados era obrigatório (neste caso pelo menos) o uso da linguagem PLSQL para a implementação das camadas de lógica de negócio, de ligação a dados e de criação de interfaces. Comparativamente com outras possíveis linguagens o PLSQL tem como grande vantagem a seu favor o facto de estar embutido na própria base de dados, isto em termos de tempos de processamento apresenta ganhos enormes comparativamente com outras tecnologias.

Capítulo 3

Especificação

3.1 Arquitectura do Sistema

3.1.1 Vista Lógica

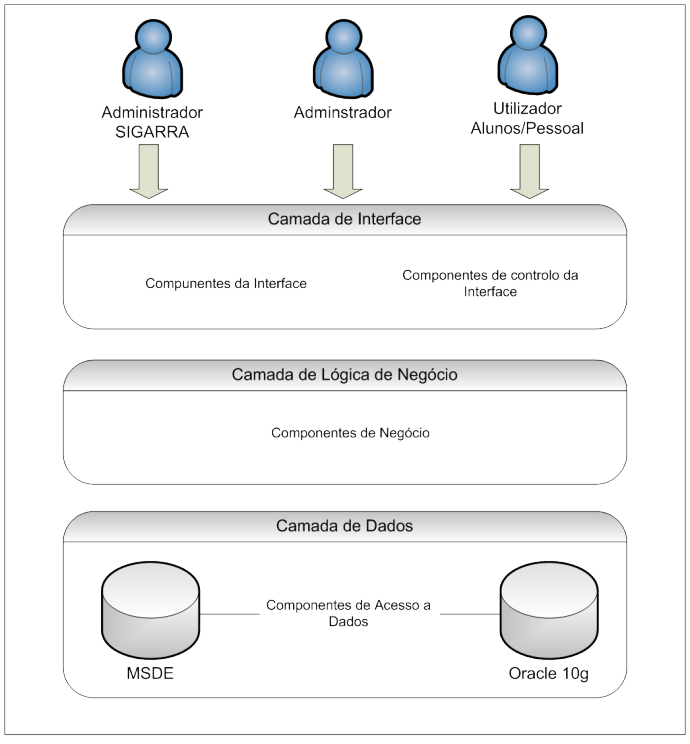

Figura 3.1: Vista Lógica

A vista lógica de uma arquitectura permite-nos conhecer os principais componentes funcionais da aplicação e as relações existentes entre eles. Esta visão é feita

de uma forma independente, tanto de detalhes técnicos, como do método usado para implementar as funcionalidades da aplicação.

O projecto será implementado usando uma arquitectura típica de três camadas lógicas: a camada de interface, a camada de lógica de negócio e a camada de dados. Este tipo de arquitectura permite uma correcta divisão modelar do sistema, com base nos seus componentes.

Camada de Interface

Esta camada é composta pelas sub camadas de componentes de interface e de controlo da interface. As componentes da interface encerram entre si a lógica de representação e aquisição de dados. As componentes de controlo da interface têm as funções de gestão do estado da interface e de realização de acções típicas da interface.

Camada de Lógica de Negócio

É composta pelas sub-camadas de componentes de lógica de negócio e por entidades de lógica de negócio. As componentes de lógica de negócio assumem a obrigação de definir e fazer prosseguir as regras de negócio. As entidades de lógica de negócio são simbolizadas por objectos, e apoiam as acções compreendidas nas componentes lógicas de negócio.

Camada de Dados

Esta camada é composta pelas sub-camadas de componentes de acesso a dados e pela base de dados. A primeira disponibiliza a interface para a camada de lógica de negócio, no sentido de modularizar o acesso a dados. A segunda sub-camada é composta pela base de dados.

3.1.2 Vista Fisica

O projecto seguiu uma arquitectura normal de uma aplicação web, onde o servidor disponibiliza online os seus conteudos através de páginas web do sistema de informação. Existe ainda a ligação através de web services com a aplicação de controlo de acessos StarWatch, está ligação permite a sincronização de dados entre estas duas partes do controlo de acessos.

Apesar de não estar representada na figura 3.2, por não existir uma ligação automáticamente establecida, a aplicação StarGaze descrita no anexo B está também ligada ao controlo de acesso, mas no presente a troca de dados entre os dois sistemas é feito manualmente, por esse motivo não foi includa no diagrama.

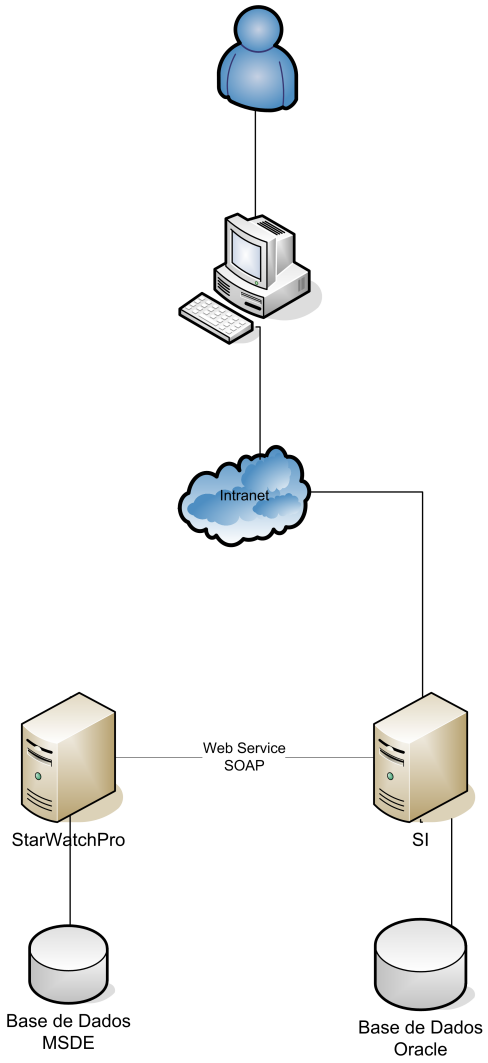

Figura 3.2: Vista Fisica

3.2 Casos de Uso

Para a descrição das necessidades a implementar serão de seguida descritos os casos de uso do módulo. Estes casos de uso correspondem ao que realmente é proposto implementar durante o projecto.

A figura 3.3 representa o pacote completo dos casos de uso a implementar, bem como os actores que terão interacção com o módulo.

Os actores deste módulo são:

- Administrador SIGARRA
- Administrador
- Alunos

- Pessoal (Docente e Não docente)

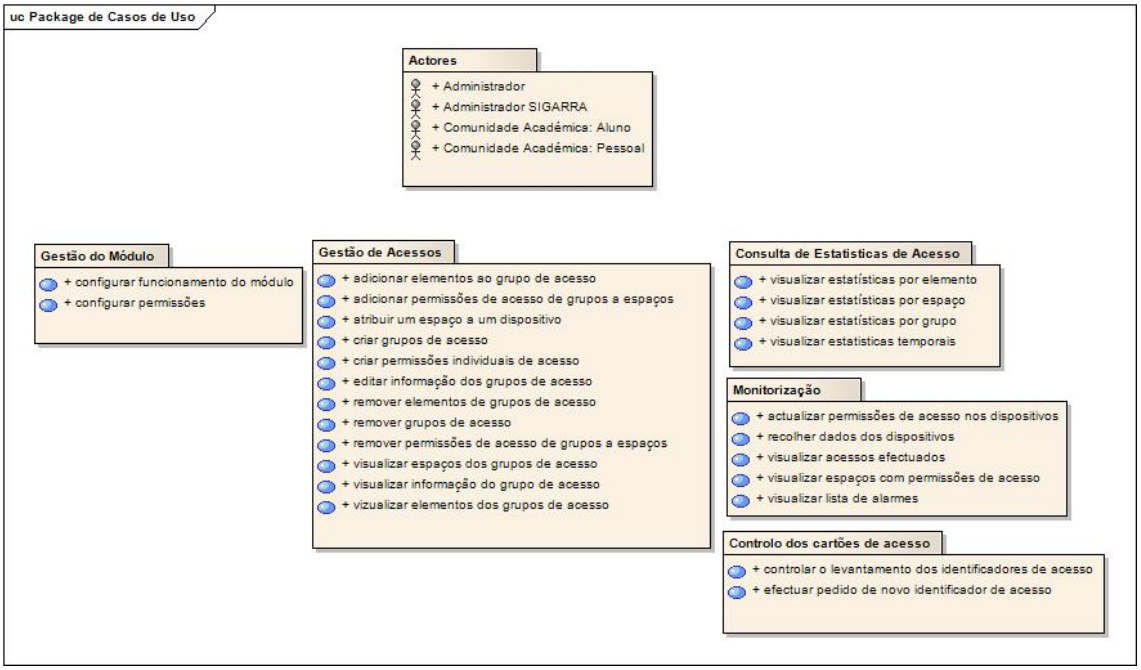

Figura 3.3: Package de casos de uso

Gestão do Módulo

- Configurar funcionamento do módulo

  Este caso de uso permite a cada instituição a configuração do módulo de controlo de acessos de modo a este se adequar da melhor forma às suas necessidades. Estas configurações têm como principal objectivo as configurações necessárias para a aplicação estar em concordância com os dispositivos utilizados.

- Configurar permissões

  Existem dois tipos de utilizadores do módulo os utilizadores que apenas podem consultar dados sobre os seus acessos e as suas permições e aqueles que para além de possuirem as permissões dos outros utilizadores ainda podem atribuir permições de acesso de pessoas e grupos a espaços.

Gestão de Acessos

- Criar grupos de acesso

  Permite a crição de novos grupos de acesso.

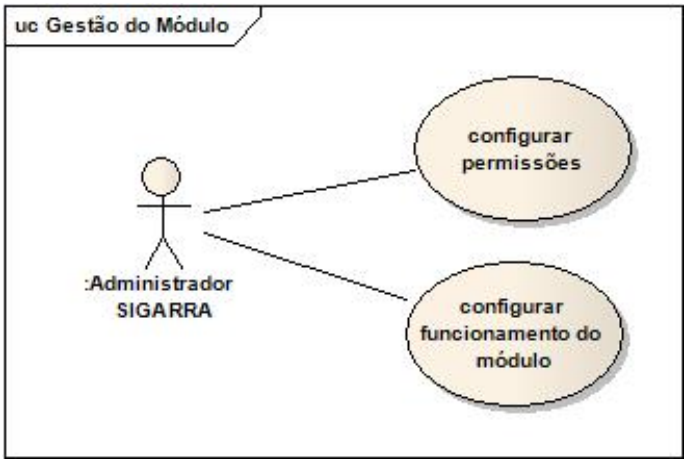

Figura 3.4: Pacote de Gestão do Módulo

- Adicionar elementos aos grupos de acesso

  Permite a adição de novos elementos aos grupos de acesso.

- Adicionar permissões de acesso de grupos a espaços

  Permite a adição de novas permissões de acesso aos grupos de acesso.

- Remover grupos de acessos

  Permite a remoção do sistema de grupos de acesso.

- Editar informação dos grupos de acessos

  Permite a edição da informação dos grupos de acesso.

- Remover elementos de grupos de acessos

  Permite a remoção de elementos dos grupos de acesso.

- Remover permissões de acessos de grupos a espaços

  Permite a remoção de permissões de acesso dos grupos de acesso a espaços.

- Visualizar informação dos grupos de acesso

  Este caso de uso permite a visualização da informação genérica dos grupos de acesso.

- Visualizar espaços dos grupos de acesso

  Os administradores e criadores de grupos de acesso podem visualizar os espaços aos quais os grupos de acesso existentes têm acesso.

- Visualizar elementos dos grupos de acessos

  Os administradores e criadores de grupos de acesso podem visualizar a constituição dos grupos de acesso existentes.

- Criar permissões individuais de acesso

  A partir do SI os utilizadores com permissões para tal podem atribuir permissões de acesso individuais de acesso a espaços.

- Atribuir um dispositivo a um espaço

  Permite a atribuição de um dispositivo a um espaço, de modo a este poder ser acedido.

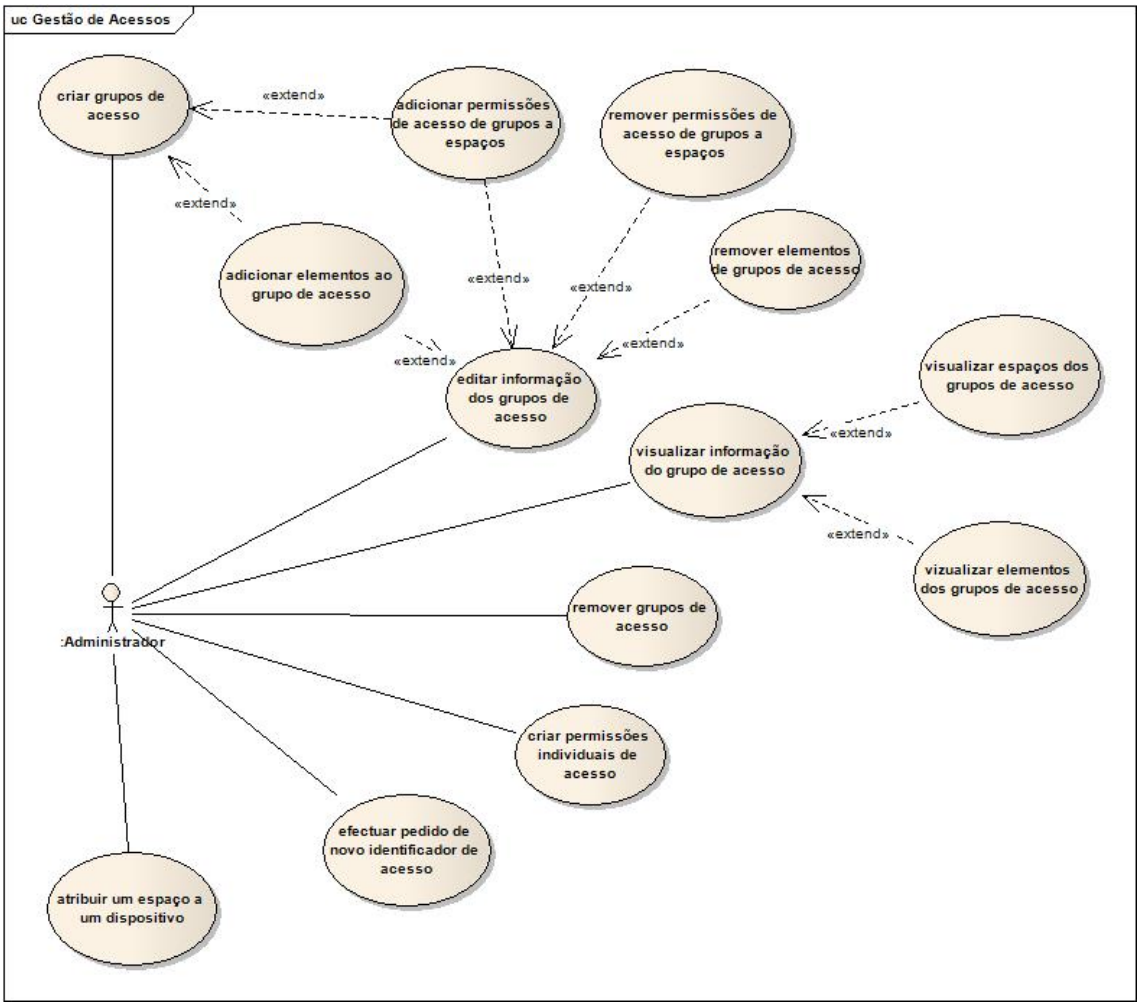

Figura 3.5: Pacote de Gestão de Acessos

Consultar estatísticas de acesso

Este caso de uso representa o grupo de casos de uso relativos às estatísticas geradas pelo módulo.

- Estatísticas por espaço

  Os utilizadores podem consultar estatísticas por espaço.

- Estatísticas por grupo

  Os utilizadores podem consultar estatísticas por grupo.

- Estatísticas por elemento

  Os administradores podem consultar estatísticas de utilização de todos os elementos, os restantes utilizadores apenas podem visualizar as estatísticas dos seus acessos.

- Estatísticas temporais

  Os utilizadores podem consultar estatísticas temporais.

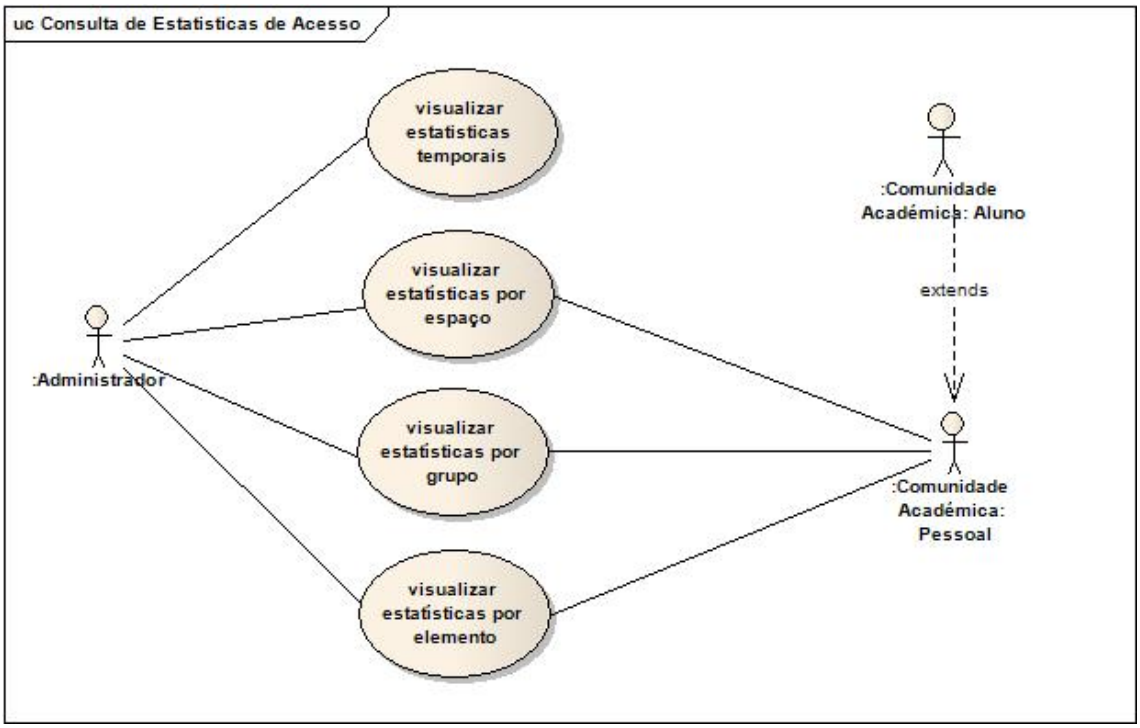

Figura 3.6: Pacote de Consulta de Estatísticas de Acesso

Monitorização

Este caso de uso engloba todos casos de uso relativos à monitorização de dados.

- Recolher dados dos dispositivos

  Permitir a recolha de dados dos dispositivos, os dados são recolhidos da aplicação que estabelece a ligação aos dispositivos (StarWath Pro).

- Actualizar permissões de acesso nos dispositivos

  Permite a sincronização entre os acessos atribuídos no sistema de informação e a aplicação que faz a conexão com os dispositivos.

- Consultar acessos efectuados

  Os utilizadores podem consultar no SI os acessos efectuados.

- Consultar lista de espaços com acesso

  A partir do SI os utilizadores registados podem consultar os espaços aos quais têm acesso atribuído.

- Visualizar lista de alarmes

  Os administradores do módulo podem consultar os alarmes gerados, dando a possibilidade de consultar o número de tentativas de acesso por parte de cartões não registados.

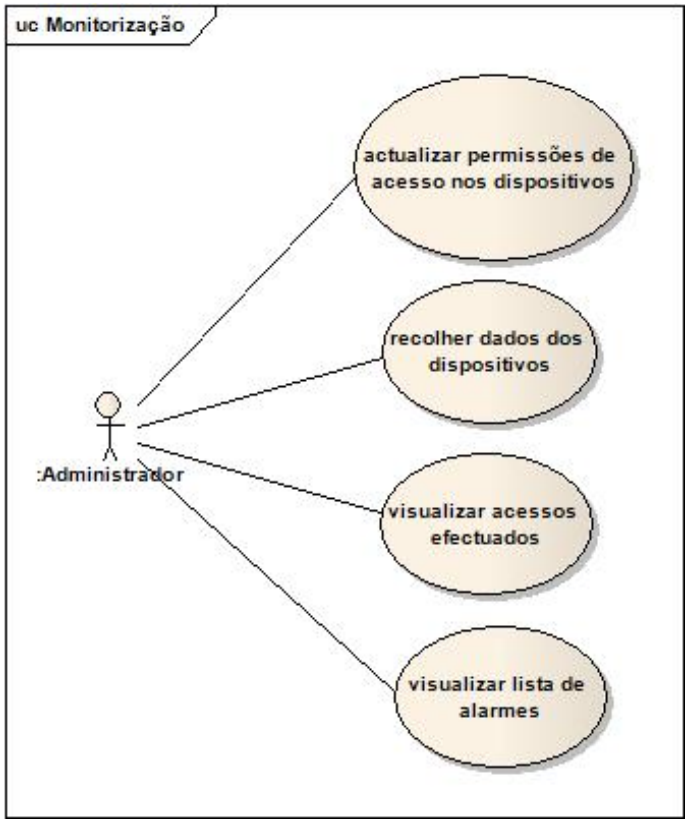

Figura 3.7: Pacote de Monitorização

Controlo dos cartões de Acesso

- Efectuar pedido de novo identificador de acesso

Os utilizadores podem pedir através do SI uma segunda via dos seus cartões de acesso em caso de perda ou roubo dos mesmos.

- Controlar o levantamento dos identificadores de acesso

  Quando um utilizador levanta o seu cartão é possível controlar no SI a entrega do mesmo de modo a ficar registada a data de entrega e confirmar a mesma.

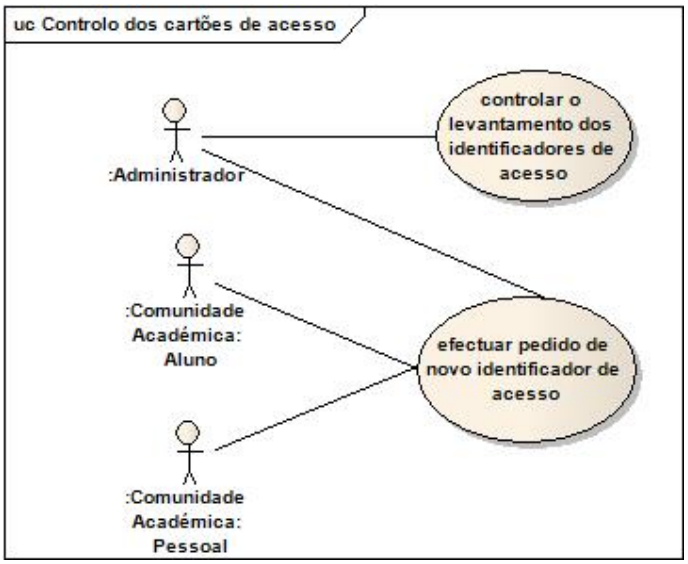

Figura 3.8: Pacote de Controlo dos Cartões de Acesso

3.3 Requisitos

Após a elaboração dos casos de uso foi importante definir os requisitos que iriam definir mais em concreto a implementação dos mesmos. Os requisitos criados são apresentados de seguida, de uma forma hierárquica de modo a melhorar o seu entendimento e permitir uma melhor organização em termos de planeamento do trabalho que ia ser desenvolvido.

- Grupos de validação

  Criação de três grupos de validação; Grupo de administração (CACESSOS-ADM), constituído pelos responsáveis do módulo; Grupo de manutenção (CACESSOS-CONTROL), constituído pelos funcionários (docentes e não docentes) que podem atribuir permissões de acesso; Grupo geral (CACESSOS-GERAL), constituído por todos os utilizadores (docentes, não docentes e alunos) do sistema de informação.

- Criar grupos de acesso

  Os administradores e o pessoal da manutenção podem criar grupos de acesso. Os grupos de acesso representam um conjunto de utilizadores com permissões de acesso iguais. O criador do grupo é considerado o responsável do mesmo.

- Adicionar elementos a um grupo de acesso

  Depois de criado o grupo de acesso permitir a adição de elementos a esse grupo.

- Permissões de acesso de grupos a espaços Com o grupo de acesso criado é possibilitar a adição de permissões de acesso a espaços. Só é possível adicionar permissões a espaços com um dispositivo atribuído.

- Formulário de criação de grupos de acesso

  O formulário de criação de grupos permite a criação de novos grupos de acesso no SI, este formulário contém os seguintes campos:

  Nome - nome do grupo;

  Tag - Abreviatura do nome do grupo;

  Estado - Estado actual do grupo (Activo ou Inactivo);

  Descrição - Observações descrevendo informação relevante sobre o grupo;

  Responsável - Pessoa responsável pelo grupo.

- Condições de criação de grupos de acesso

  Para a criação com sucesso do grupo de acesso os campos, Nome, Tag, Estado e Responsável não podem ser nulos.

- Visualização de grupos de acesso

  Este requisito engloba requisitos de interfaces relativas aos grupos de acesso e a visualização da informação principal do grupo de acesso.

- Visualização dos elementos do grupo

  Interface que permite a visualização dos elementos de um grupo de acesso.

- Visualização dos espaços atribuídos ao grupo

  Interface de visualização dos espaços com permissão de acesso de um grupo.

- Pesquisa de elementos do grupo

  Interface do formulário de pesquisa de elementos de um grupo de acesso.

- Pesquisa de espaços do grupo

  Interface de pesquisa de espaços a que o grupo tenha acesso.

- Edição de grupos de acesso

  Requisito que representa a interface de edição dos dados principais de um grupo de acesso.

- Eliminar elementos dos grupos

  Possibilitar a remoção de elementos de um grupo de acesso.

- Remover permissões de acesso dos grupos

  Retirar a permissão de acesso a espaços por parte de um grupo.

- Pesquisa de elementos

  Permite a pesquisa de elementos de modo a atribuir a estes permissões de acesso.

- Criar permissões de acesso individuais

  Atribuir permissões de acesso a uma pessoa singular

- Eliminar permissões de acesso individuais

  Apagar permissões de acesso individuais existentes.

- Pesquisa de espaços

  Permitir a pesquisa de espaços e a visualização dos elementos e grupo com acesso ao mesmo.

- Exportação de dados dos identificadores pedidos

  Permitir a exportação dos dados necessários à criação de novos cartões de acesso. Estes dados têm que ser facilmente disponibilizados aos elementos da equipa que irá efectuar a impressão dos cartões.

- Registo da entrega dos identificadores

  Controlar a entrega dos cartões à medida que estes vão sendo impressos.

- Tipos de dispositivos (controladores)

  Permitir a criação no SI dos tipos de dispositivos que estão a controlar os espaços. Até à data existem dispositivos de leitura magnética e leitura de RFid.

- Inserir no sistema um novo dispositivo

  Criar no SI novos dispositivos a medida que estes vão sendo montados. Para a inserção do novo dispositivo é necessário inserir a seguinte informação: Código - código interno atribuído ao dispositivo; Tipo de dispositivo - é necessário

especificar o tipo de dispositivo a ser criado; IP - no caso dos novos dispositivos de RFid que estão montados na intranet da faculdade pode inserir.se o ip que lhe está atribuído; Data de Aquisição - data em que o dispositivo foi comprado; Responsável - Pessoa responsável pelo dispositivo.

- Atribuir um dispositivo a um espaço

  Após a criação dos dispositivos no SI estes podem agora ser atribuídos a espaços, passando esse espaço a ser controlado pelo dispositivo indicado.

- Eliminar dispositivo

  Permitir que por motivos ou de avaria ou de eliminação definitiva os dispositivos existentes possam ser eliminados do SI. Para tal apenas devemos ter que escolher o dispositivo a remover e seguir as regras definidas para que um dispositivo possa ser removido.

- Regras de remoção do dispositivo

  Para que um dispositivo possa ser removido tem que obedecer às seguintes regras: O espaço controlado pelo dispositivo não pode ter permissões de acesso de grupo; O espaço também não pode ter permissões de acesso individuais que usem o dispositivo a remover.

- Recolha de dados de acessos recolhidos pelos dispositivos

  Os dados recolhidos pelos dispositivos têm que ser recolhidos da(s) aplicações de controlo de acessos e passados para o SI de modo a serem tratados da forma necessária.

- Sincronização das permissões dos dispositivos com o SI

  Tal como na recolha de dados, é igualmente necessário implementar um mecanismo que permita enviar os dados registados no SI para os dispositivos, passando estes a estar assim activos nas aplicações de controlo de acessos.

- Consultas de Informação

  Este requisito reúne todos os requisitos onde é consultada a informação recolhida dos dispositivos de controlo.

- Consulta de Estatísticas

  Interface que permite consultas de variados tipos de estatísticas sobre os dados recolhidos pelos dispositivos

- Consultar espaços com acesso

  Listar os espaços com dispositivos de controlo e o tipo dos mesmos.

- Consultar lista de acessos

  Para os administradores deve ser possível obter a lista de acessos aos diversos espaços da faculdade. Estes dados sobre os acessos podem depois ser visualizados de várias formas, por espaço, por elemento ou por espaços de tempo.

- Consulta de tentativas de acesso negadas

  Apenas como mero dado estatístico deve ser permitido visualizar as tentativas de acessos por parte de utilizadores não registados, nos espaços em questão.

3.4 Modelo de Dados

A figura 3.9 mostra o modelo de dados criado para suportar o módulo de controlo de acessos. De seguida serão descritas as tabelas utilizadas:

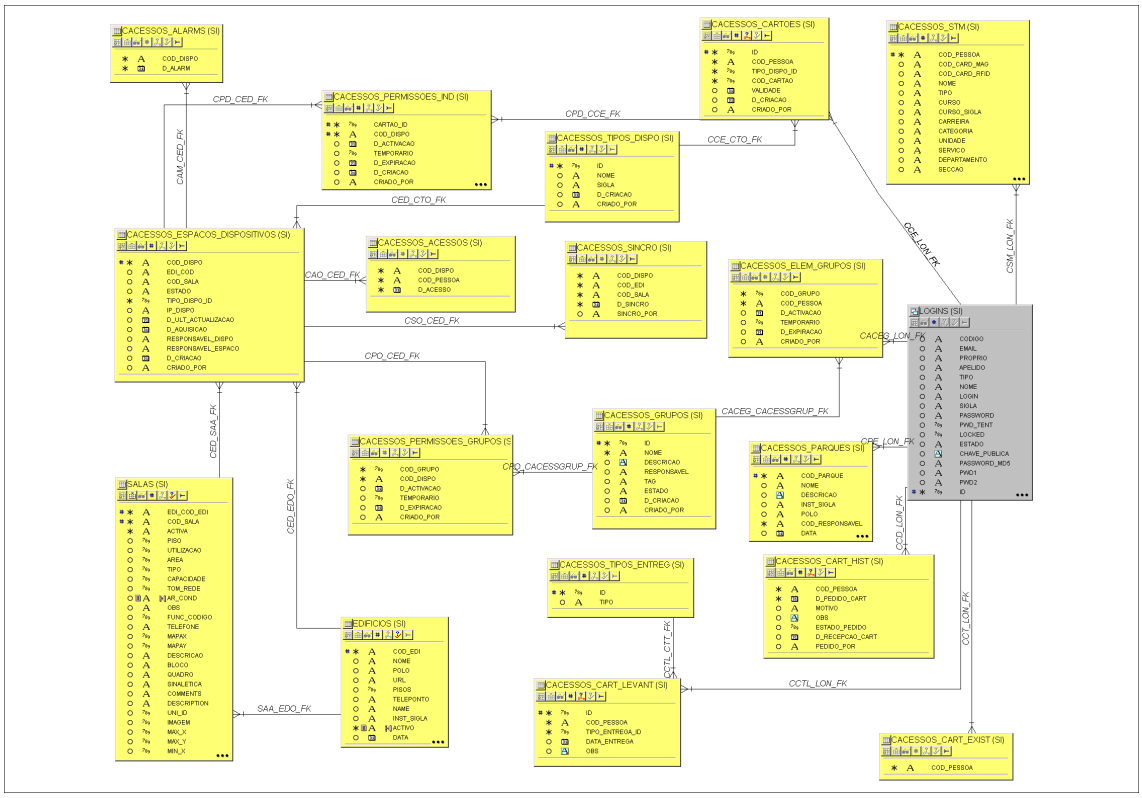

Figura 3.9: Modelo de dados do módulo

- CACESSOS_ACESSOS - Tabela que regista a informação dos acessos às instalações da Faculdade de Engenharia da Universidade do Porto

- CACESSOS_ALARMS - Tabela que regista as tentativas de acessos por parte de utilizadores não registados.

- CACESSOS_CARTOES - Tabela que regista a informação pessoal dos utilizadores, contém um utilizador pode existir várias vezes nesta tabela porque cada registo contém informação relativa a cada tipo de cartão ou identificador.
- CACESSOS_CART_EXIST - Tabela que regista os cartões existentes
- CACESSOS_CART_HIST - Tabela que regista novos pedidos de cartões e o seu estado de criação.
- CACESSOS_CART_LEVANT - Tabela que regista o levantamento de novos cartões.
- CACESSOS_ELEM_GRUPOS - Tabela que contém a indicação de quem pertence a cada grupo de acesso.
- CACESSOS_ESPACOS_DISPOSITIVOS - Tabela que regista os dispositivos que estão existentes e que espaços controlam.
- CACESSOS_GRUPOS - Tabela que regista a informação dos grupos de acesso existentes.
- CACESSOS_PARQUES - Tabela que regista os parque existentes.
- CACESSOS_PERMISSOES_GRUPOS - Tabela que regista as permissões que cada um dos grupos de acessos tem.
- CACESSOS_PERMISSOES_IND - Tabela que regista as permissões que cada pessoa tem a nivel individual.
- CACESSOS_SINCRO - Tabela que regista as datas de sincronização dos disposivos com o SI.
- CACESSOS_STM - Tabela que regista a informação a exportar para os serviços tecnicos, para que estes possam imprimir os cartões de identificação.
- CACESSOS_TIPOS_DISPO - Tabela que regista os tipos de dispositivos existentes.
- CACESSOS_TIPOS_ENTREG - Tabela que regista o tipo de entrega de cartão realizada.

Capítulo 4

Componentes

Para a elaboração deste projecto foram usadas diversas tecnologias e linguagens de programação. Neste capítulo serão descritas ao pormenor as mesmas e explicada a razão da sua escolha.

Posso começar por referir a utilização da base de dados de Oracle, esta foi imposta dado que todo o SIGARRA é suportado por tecnologias da Oracle por isso a sua adopção foi uma escolha simples. Ainda ligada a base de dados, toda a programação foi feita em PLSQL (linguagem de procedimentos para SQL). Esta permite alcançar bons desempenhos nas camadas de acesso a dados, podendo apenas perder ligeiramente em termos de performance na geração de interfaces, visto que todas as interfaces em HTML são criadas através de comandos de PLSQL.

A aplicação de controlo de acessos STARWATCH usa como repositório de dados uma base de dados MSDE, deste modo após o estudo da mesma era necessário criar uma ligação entre os dados existentes no SI em oracle e os da aplicação. Para tal a opção escolhida foi usar web services para efectuar a troca de dados. Os web services foram implementados em PHP que corre num servidor de HTTP Apache e são depois chamados via PLSQL.

Ainda durante o projecto foi usada para uma pequena implementação a linguagem Java, esta foi utilizada para gerar automaticamente ficheiros. Zip no servidor. A escolha da linguagem java foi também pesada pela possibilidade de inclusão e chamada de classes Java através de bases de dados Oracle.

Outra adaptação de tecnológica que teve de ser feita foi a criação de ficheiros Excel através de PLSQL para tal foi utilizado o formato XML Spreedsheet.

Foi igualmente necessário estudar o funcionamento de algumas a aplicações de modo a ser possível a interligação dos dados existentes. Estas aplicações foram

a StarGaze e a StarWath Pro. A aplicação StarGaze está instalada na faculdade de engenharia desde que se iniciou o funcionamento do novo pólo. Esta controla os acessos de praticamente todas as portas existentes na faculdade através de leitores magnéticos, todos acessos recolhidos pelos leitores são armazenadas em controladores, sendo estes que depois descarregam os dados para a aplicação. Esta aplicação corre num servidor com uma rede especifica da qual apenas fazem parte, o servidor, os controladores e os leitores, esta rede oferece vantagens inegáveis em termos de segurança, mas dificulta o trabalho de manutenção das maquinas que apenas permitem o seu controlo local, não existindo a possibilidade de trabalhar remotamente para esta máquina. Deste modo o acesso aos dados recolhidos quer para efeitos estatísticos, quer para cópia de segurança, tem obrigatoriamente que ser feito localmente, ou através de discos externos, ou através de ligação de um portátil em rede. Por ser usada uma versão já bastante antiga deste software este corre actualmente sobre um sistema operativo Linux (RedHat 6.2) e apresenta uma interface já bastante desactualizada, apresentando apenas a informação essencial. Essencial nesta aplicação foi o estudo do seu modelo de dados de modo a poderem ser feitas transferências de dados de outros sistemas.

Relativamente ao StarWatch na versão Profissional esta é uma aplicação bastante mais recente, desenvolvida unicamente para a plataforma Windows e já permite a utilização de além dos leitores magnéticos, leitores de RFid e de dados Biométricos. Com um nível de complexidade bastante superior ao StarGaze (pelo maior número de funcionalidades disponibilizadas), a interacção com esta aplicação é inicialmente mais complicada (embora ajudada por uma interface bem mais intuitiva). Relativamente à sua interacção com os leitores esta é basicamente igual à antiga aplicação existindo leitores ligados a controladores que depois comunicam com o software. O tipo de comunicação também é outra vantagem já que os novos controladores permitem o seu controlo através do protocolo TCP/IP o que facilita a sua gestão (se for necessário é possível desenvolver uma aplicação que interaja com os controladores sem ter que passar pela aplicação principal). Em relação aos dados a aplicação é suportada actualmente por uma base de dados MSDE da Microsoft, que por ser gratuita apresenta algumas limitações em termos de tamanho, o que provavelmente irá levar à sua migração para uma base de dados SQL Server que também é suportada pela aplicação. Uma vez mais teve que ser feito o estudo da estrutura de dados utilizada, para poder manter aos dados actualizados com o novo módulo do SIGARRA.

Para efectuar gestão de páginas e as permissões da ferramenta de gestão de projectos é usada a aplicação de Gestão do Sistema de Informação (GESSI). O GESSI está conceptualmente dividido em duas componentes: uma aplicação de configurações onde estão definidos ficheiros CSS, grupos de utilizadores e respectivas

permissões de acesso às páginas, páginas activas no sistema de informação e uma estrutura que, baseada nas configurações referidas, disponibiliza serviços de construção de páginas web dinâmicas.

4.1 Ferramentas Utilizadas

Ferramenta de Gestão de Projectos do Projecto de Sistemas de Informação

A ferramenta de gestão de projectos existente no PSI foi desenvolvida internamente pela unidade e apoia todas as fases de um projecto. É composta por cinco grupos funcionais, Administração, Requisitos, Problemas, Testes e Módulos. O módulo de administração permite a gestão de toda a informação dos projectos, a gestão de permissões e de recursos, os restantes grupos permitem tal como o nome indica a gestão da informação dos requisitos, problemas, testes e módulos.

A GP corre sobre uma base de dados Oracle 10g e dispõe de um servidor web que recebe os pedidos HTTP dirigidos ao sistema, no caso de serem pedidos que impliquem acessos a procedimentos PL/SQL, são passados ao servidor da base de dados que executa o código e passa o resultado do mesmo novamente ao servidor web que, por sua vez, o passa ao utilizador.

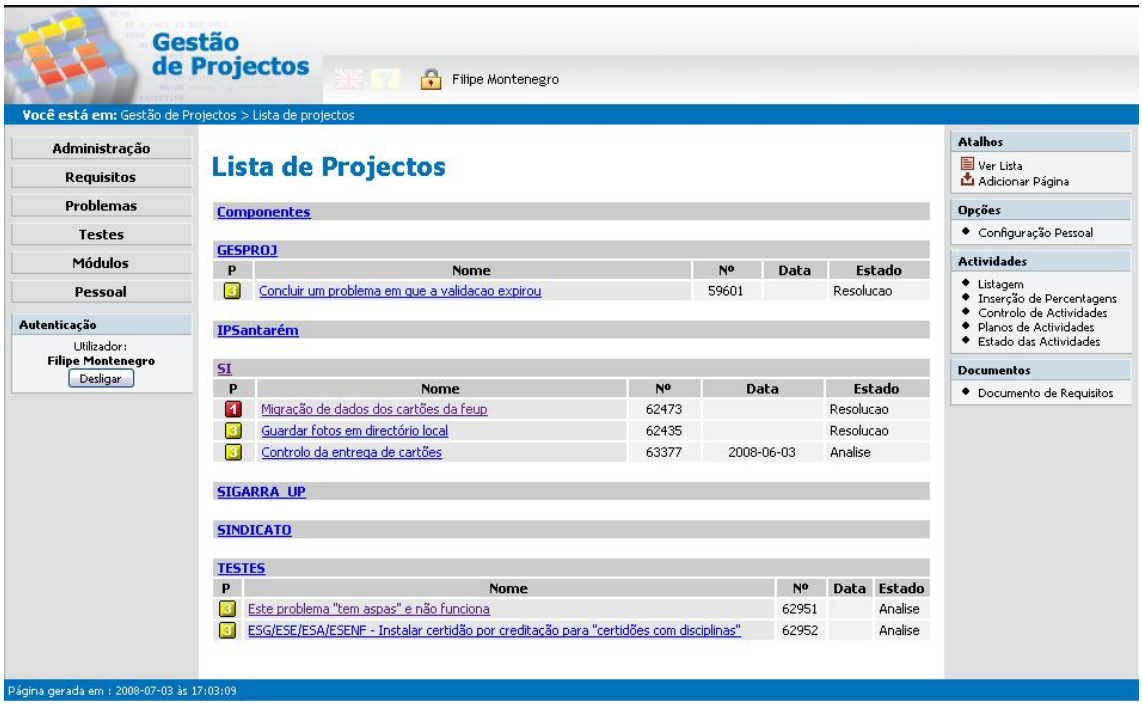

Figura 4.1: Ferramenta de Gestão de Projectos

SQL Navigator

Como ferramenta de codificação em PL/SQL foi escolhido o SQL Navigator desenvolvido pela Quest Software que mostrou ser a melhor ferramenta para esta linguagem oferecendo bastantes mais funcionalidades que por exemplo o SQL Developer da Oracle. O SQL Navigator possui diversas funcionalidades bastante úteis como a formatação automática do código, a obtenção de modelos de dados visuais da base de dados, entre outras. O principal senão, o facto de só estar disponível para o sistema operativo windows, outro dos motivos para a utilização desta ferramenta foi o facto de já ser usada pela maioria dos elementos da unidade.

Oracle Designer

Para a modelação da base de dados e mais uma vez porque já era a ferramenta mais usada pela equipa com este objectivo, foi escolhido o Oracle Designer. Desta ferramenta apenas foi utilizada uma pequena parte das suas funcionalidades, pois esta ferramenta para além da modelação de dados e criação automática de api's, que foram utilizadas, permite por exemplo a criação automática de formulários para um dado modelo de dados.

JDeveloper

Esta ferramenta foi utilizada numa parte reduzida do projecto onde foi utilizada a linguagem java e esta fui a ferramenta escolhida principalmente devido ao anterior conhecimento da mesma.

PHPEdit

Para a criação dos web services do lado da aplicação de controlo de acessos foi escolhida a linguagem PHP. Para a edição dos ficheiros php criados foi usada a ferramenta PHPEdit que para além da preciosa indentação do código, possui também um auto complete de funções php bastante completo o que em termos de rapidez de produção de código se mostrou bastante útil.

Excel Neste projecto o excel foi utilizado como modo de migração de listagens de cartões de acesso a imprimir. Isto porque a aplicação de impressão de cartões (ver mais em detalhe nos anexos), recebia dos dados a imprimir nos mesmos neste formato.

Enterprise Architect Este software foi utilizado para a criação dos diagramas UML dos casos de uso.

4.2 Tecnologias

Neste ponto é feita a descrição das tecnologias e linguagens de programação utilizadas no projecto.

PLSQL

Todo SIGARRA é desenvoldido sobre uma base de dados Oracle, por esse motivo a linguagem de manipulação de dados e de criação de interfaces foi automaticamente

escolhida. Visto já ter alguma experiencia com PLSQL esta era sem duvida a melhor opção.

O PL/SQL é uma linguagem de procedimentos lançada pela oracle que serve de extensão ao SQL. Foi lançada em 1991 como uma extensão opcional ao Oracle 6, estando hoje em dia presente em todos os servidores oracle.

HTML

Visto que a aplicação desenvolvida é uma aplicação web o HTML é com naturalidade uma linguagem essencial. Embora o desenvolvimento tenha sido feito em PL/SQL o conhecimento de HTML é vital, visto que para a criação das interfaces o PL/SQL apenas serve para criar outputs de HTML.

HTML é uma linguagem de marcação utilizada para produzir páginas na Internet com códigos que são interpretados pelos browsers para exibir essas mesmas páginas, teve o seu surgimento no inicio da década de 1990 e hoje em dia é a umas das linguagens mais utilizadas na web.

UML

Como linguagem de modelação dos objectos foi usada a linguagem universal de modelação UML.

O UML nasceu pelas mãos de um consórcio internacional chamado UML Paterns que propôs a sua versão do UML 1.0 à OMG em Janeiro de 1997 e só no fim de 1997 o UML foi então aceite como um standard do OMG (Object Management Group). É hoje em dia o método de modelação considerado universal.

Java

A linguagem java foi utilizada no projecto para criar em tempo real ficheiros. Zip contendo as fotografias dos utilizadores que pediram cartão de acesso. Deste modo é permitido aos produtores dos cartões efectuar através do SI o download das fotografias necessárias para a impressão de um grupo de cartões. A escolha de java para realizar esta tarefa foi a possibilidade de integração de classes java na em bases de dados oracle, estas podem depois ser chamadas a partir do PLSQL, deste modo é possível controlar todo o procedimento através de uma linguagem só.

JavaScript

De modo criar interfaces com maior interactividade do que a permitida apenas utilizando HTML e ainda para efectuar computação do lado do cliente foi usada a linguagem de scripting Javascript.

O Javascript foi criado em 1995 pela Netscape sendo usado maioritariamente utilizado como linguagem de validação de formulários do lado do cliente e como modo de interacção em tempo real e sem necessidade de acesso ao servidor entre uma aplicação web e o seu utilizador.

Web Services SOAP

Como os dados recolhidos estão distribuídos por dois sistemas de bases de dados diferentes existia a necessidade de criar uma ligação entre ambos, para tal a tecnologia escolhida foram os web services, quer pela sua base em standards (HTTP e XML), quer pela facilidade de configuração e criação dos mesmos. Dos vários tipos de protocolos existentes o implementado foi o SOAP (Simple Object Acess Protocol), este protocolo foi projectado para invocar aplicações remotas por RPC (Remote Procedure Calls) ou efectuar trocas de mensagens, num ambiente independente da plataforma e da linguagem de programação. Uma mensagem SOAP bem construída em consonância com as definições do W3C, é constituída pelos seguintes elementos:

- Envelope - envelope é a raiz do documento XML criado e pode conter a declaração de namespaces, estilo de codificação e ainda atributos adicionas.
- Header - é o primeiro elemento depois da raiz e contém informações adicionais, especificas do web service em questão.
- Body - no campo body é onde a informação pretendida é transportada para o seu destino.

PHP

Os Web Services foram implementados na linguagem PHP que é uma linguagem script do lado do servidor usado tal como o javascript para criar páginas web dinâmicas. A escolha desta linguagem deveu-se ao facto de poder ser usada recorrendo apenas a recursos open source, já que para correr os web services em php foi usado um servidor de HTTP Apache.

XML SpreadSheat

Para a exportação de certas listagens web foi escolhido o formato MSExcel, após essa escolha foi efectuado um estudo dos métodos disponíveis para a criação de ficheiros Excel de um modo não muito pesado. Deste modo e como eu já possuía conhecimentos de XML o formato escolhido para essas exportações foi o formato XML Spreadsheet, que para a além da fácil interpretação do XML criado, permitia por exemplo a criação de estilos de formatação o que se mostrou bastante útil. Este formato XML Spreadsheet está disponível desde o Office 2000 e permite a interpretação por parte do Excel de um ficheiro XML que compra as regras do schema XML Spreadsheet.

Apache HTTP Server

Como servidor de HTTP escolhido para colocar disponiveis online os webservices foi escolhido o Apache por ser uma opção open source e por estar já bastante madura e trazer consigo poucas falhas.

Capítulo 5

Implementação

Neste capitulo vão ser descritas todas as funcionalidades implementadas e explicadas as opções ao longo do projecto. Para uma melhor organização do relatório a descrição das funcionalidades vai seguir a estrutura dos casos de uso de modo a tentar aprofundar melhor cada um dos pacotes criados. O primeiro pacote de casos de uso a ser descrito será o de gestão do módulo, seguido do de gestão de acessos, consulta de estatísticas , monitorização e finalmente o pacote de controlo dos cartões de acesso.

Antes de falar especificamente de cada pacote convém destacar a estrutura de código PL/SQL utilizada no desenvolvimento da aplicação que é geral a todos os módulos visto seguir as normas de programação utilizadas no PSI. O PL/SQL pode estar contido em procedimentos ou funções que podem existir directamente na base de dados ou podem estar agrupados em pacotes. Assim segundo as normas de programação utilizadas no PSI cada módulo é dividido em pacotes que devem apresentar no seu nome os seguintes sufixos:

- _GERAL - implementação das páginas principais do módulo;
- _ADM - implementação das páginas de administração do módulo;
- _UTIL - implementação de funções de utilidade do módulo e API, nestes pacotes não devem ser produzidas páginas web;
- _WEB - funções de geração de código HTML;
- _DM - funções de acesso a dados geradas automaticamente.

Depois da apresentação das regras utilizadas podemos então fazer a descrição dos principais pacotes criados de modo a suportar a implementação dos pacotes:

- CACESSOS_GERAL - Pacote contendo a maior parte do codigo do módulo, foi neste pacote que foram cridas as principais interfaces do módulo, bem como a mair parte da lógica associada aos módulo.

- CACESSOS_ADM - Este pacote contém as páginas de acesso restrito do módulo, páginas de administração e páginas de configuração de módulo.

- CACESSOS_DM - O pacote -DM é gerado automaticamente e permite de uma forma generica aceder a todas os dados do módulo (esta geração é feita escolhendo todas as tabelas que fazem parte do modelo de dados do módulo).

- CACESSOS_UTIL - Neste pacote estão as funções de acesso a dados que complementas as funções existentes no pacote _DM mas que são necessidas especificas do módulo. Estão ainda neste pacote outras funções de processamento auxiliares ao módulo.

- CACESSOS_WEB - No pacote web estão as funções de geração de codigo HTML, no caso deste módulo este package é usado para criar o código principalmente das comboxs mais utilizadas.

5.1 Gestão do Módulo

Na secção de gestão módulo é onde os administradores podem controlar os acessos às páginas do módulo. Essa gestão de permissões é efectuada no GESSI, onde são criados grupos de acesso às páginas e opções disponíveis nessas páginas. Isto é possível pois todas as páginas e atalhos (nos menus direito e esquerdo) criados para o módulo têm que ser registadas no GESSI para estarem disponíveis online, deste modo quando são registados é inserido (opcionalmente) quem tem acesso quer às páginas, quer às opções. Para tal os utilizadores ficam distribuídos por grupos, cada um com o seu conjunto de permissões, estes apresentam ainda uma estrutura hierárquica onde os pais/filhos herdam as permissões dos pais/filhos, a estrutura seguida é apresentada de seguida:

- Grupo de administração (CACESSOS_ADM), constituído pelos responsáveis do módulo, estes podem visualizar todas as páginas do módulo e ainda atribuir a utilizadores permissão de gestão dos controlos de acessos, passando estes utilizadores a poder igualmente atribuir permissões de acesso.

- Grupo geral (CACESSOS_GERAL), constituído por todos os utilizadores (docentes, não docentes e alunos) do sistema de informação, estes podem visualizar todos os seus acessos e controlar os espaços a possuem permissão de entrada.

É ainda nesta parte do módulo onde algumas configurações de funcionamento podem ser feitas, estas estão disponíveis apenas para os administradores do SI, a principal função das configurações aqui existentes são relativas aos dispositivos existentes permitindo a adição de tipos de dispositivos bem como a configuração do seu tipo, ip, entre outras informações relevantes.

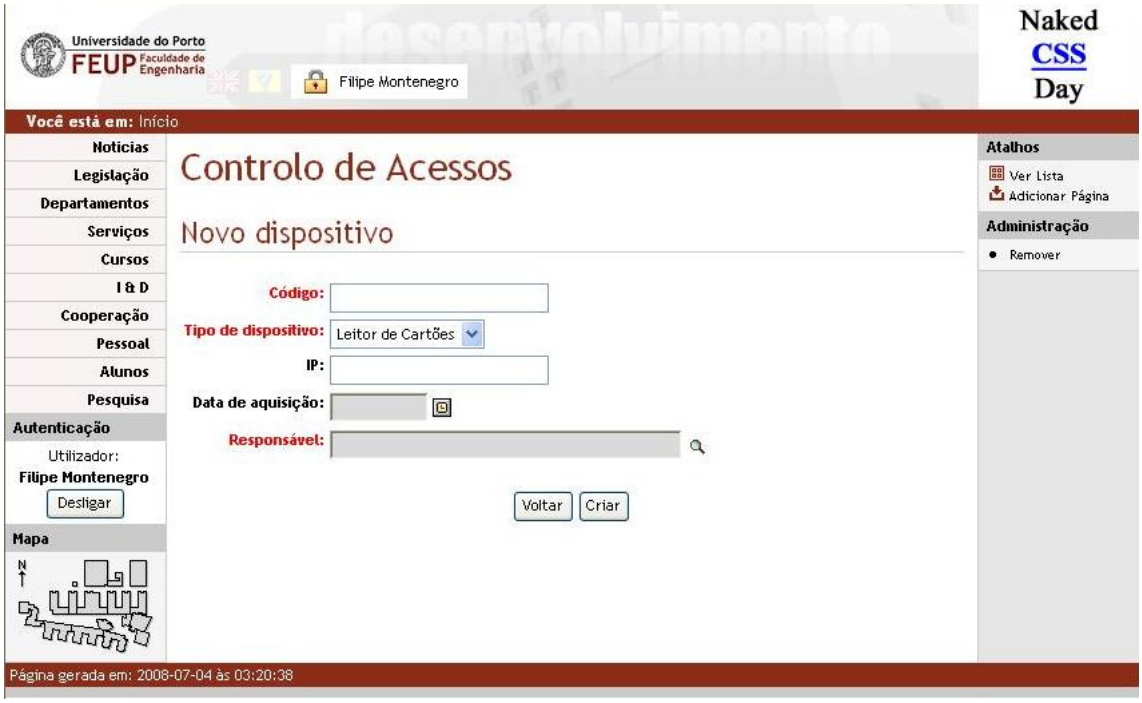

Figura 5.1: Criação de novo dispositivo

Outro ponto controlado apenas por administradores é a situação dos parques de estacionamento existentes nas instituições que utilizam o SI, isto porque, actualmente (irá ser disponibilizada em breve um nova versão do módulo de instalações onde os parque já serão também controlados) os parques não fazem parte do módulo de instalações existente, tendo assim que ser criada temporariamente a possibilidade de gerir os parque através deste módulo, possibilitando assim a atribuição de permissões de acesso a esses parques.

5.2 Gestão de Acessos

Este é ponto do módulo onde grande para da implementação foi feita, este é o tronco que suporta as restantes funcionalidades criadas.

De modo a permitir uma maior eficácia na gestão dos acessos e evitar o envio de emails com o pedido de permissões de acesso para algum utilizador das instalações da faculdade, é disponibilizada agora através do SI essa possibilidade.

Figura 5.2: Atribuição de dispositivos aos parques

Existem no sistema dois modos de atribuir permissões, através de grupos de acesso ou através da atribuição individual de permissões, cada um dos modos tem as suas vantagens e desvantagens mas quando utilizados em conjunto tornam-se uma boa solução. Para a criação de um grupo de acesso é necessário inserir a seguinte informação, o nome a dar ao grupo, a tag que irá caracterizar o mesmo, o seu estado (activo ou não activo) e o responsável, é registada ainda, mas de forma automática, a data de criação do grupo e o seu criador.

A partir deste momento o grupo já se encontra registado no sistema e de seguida pode ser efectuada uma das seguintes acções, atribuir permissões de acesso ao grupo ou atribuir elementos ao grupo, estas duas opções podem ser escolhidos por ordem aleatória, podendo assim ser atribuídas permissões de acesso ao grupo sem este ter elementos ou atribuir elementos sem que o grupo tenha qualquer permissão de acesso.

Já na atribuição dos elementos e das permissões existem algumas pré condições que têm que ser cumpridas obrigatoriamente. Na adição de elementos é necessário que o elemento a adicionar cumpra as seguintes imposições:

- Estar registado no SI
- Possuir um cartão de identificação válido

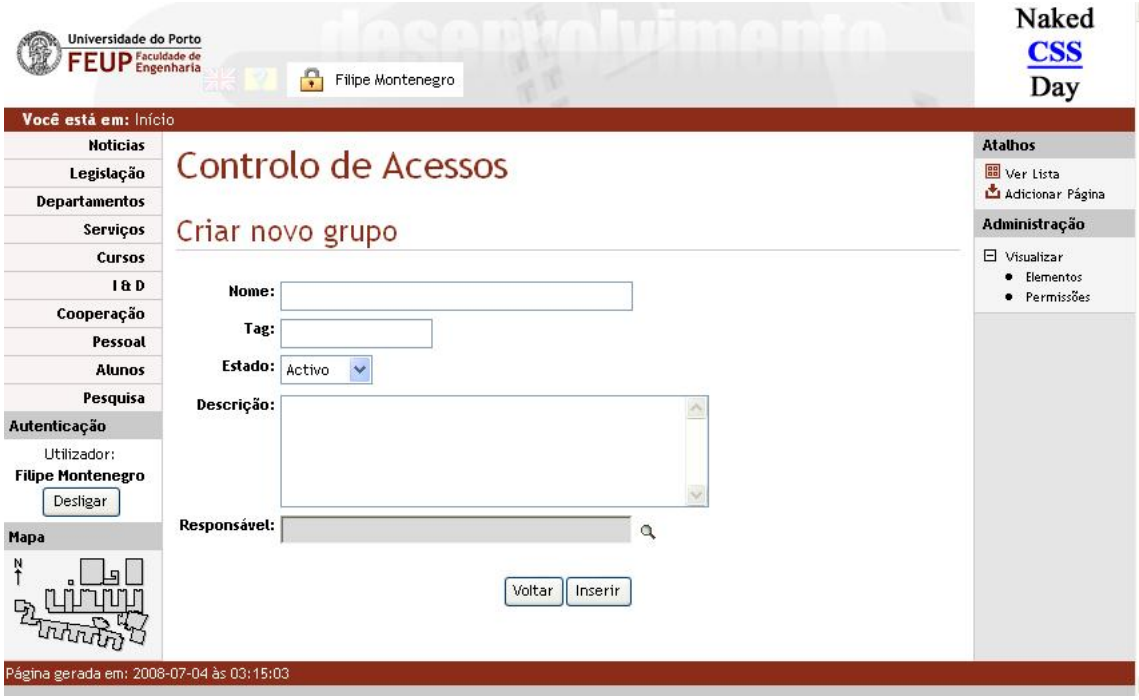

Figura 5.3: Criação de novo grupo de acesso

- No caso de serem usados dispositivos de controlo biométrico, este deve juntamente com a sua informação pessoal ter registado o elemento necessário para a sua validação junto destes dispositivos.

figura atribuição de permissões individuais

Em relação às permissões de acesso estas podem ser atribuídas a três tipos de espaços físicos, edifícios, espaços (designados pela combinação de um edifício com uma sala) e aos parques, estas atribuições têm tal como no caso dos elementos restrições, neste caso apenas uma, o espaço físico escolhido tem obrigatoriamente de ter atribuído um dispositivo de controlo registado no sistema. Para que estas regras possam ser cumpridas existe a possibilidade de atribuir uma identificação o elemento e de atribuir dispositivos a espaços. A questão de identificação dos elementos será descrita em pormenor no ponto Controlo dos cartões de acesso deste relatório, no caso da atribuição dos dispositivos aos espaços está disponível na página do SI que descreve o espaço a pagina de atribuição e consulta do dispositivo utilizado para controlar esse espaço. Assim se um espaço ainda não possui um dispositivo de controlo quando a opção referida acima é escolhida vai ser possível atribuir um dispositivo para controlar o mesmo, isto se existirem dispositivos livres para atribuição, esta restrição é rapidamente visível pois apenas são dados como opção de escolha dispositivos que ainda não estão a controlar nenhum espaço. Ainda para a atribuição do

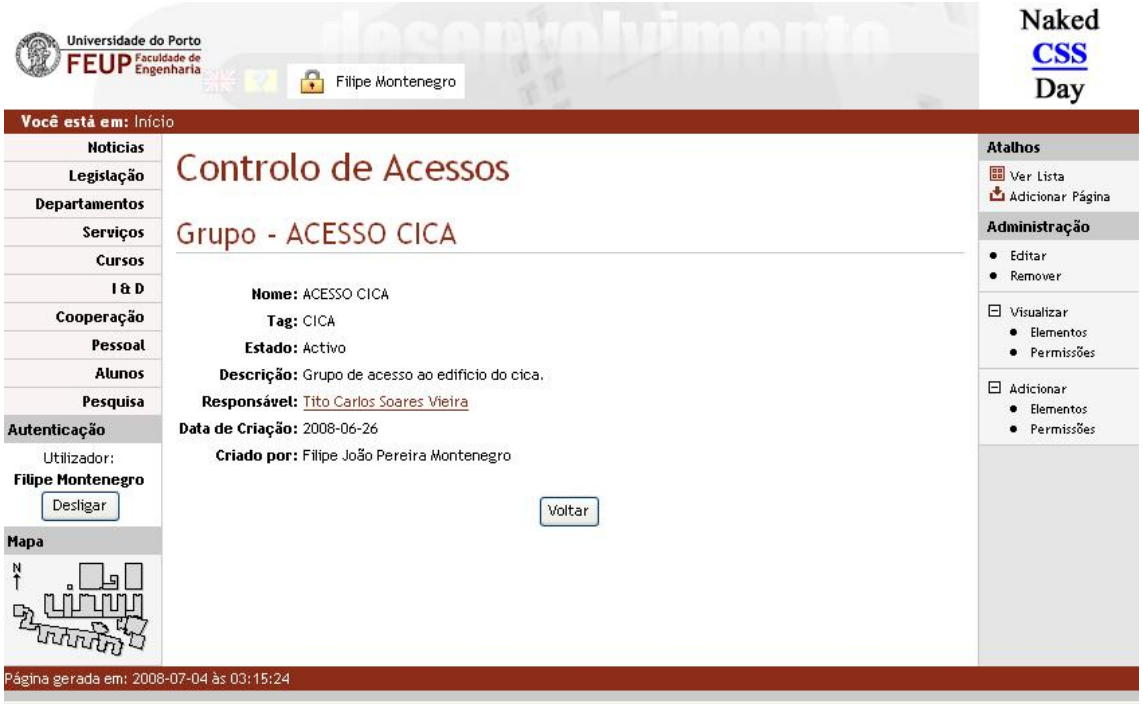

Figura 5.4: Descrição do grupo de acessos

dispositivo é necessário escolher se este está actualmente no estado activo ou não activo e quem é o responsável pela ligação entre o espaço e o dispositivo escolhidos. Se o utilizador for um administrador pode a partir desta interface aceder à inserção de novos dispositivos no sistema, isto para que no caso de este querer criar uma ligação entre espaços e dispositivos e não existirem dispositivos disponíveis no sistema mas disponíveis para a inserção no mesmo, este possa de uma forma mais directa inserir um novo dispositivo no sistema.

No caso das permissões individuais o método é bastante mais directo, bastando pesquisar pelo utilizador e escolher o espaço ao qual é desejado dar permissão, as restrições de criação desta permissão são equivalentes às existentes nos grupos, ou seja, o elemento escolhido deve possuir no registo no sistema dos seus meios de acesso e o espaço físico escolhido tem que ter atribuído um dispositivo de controlo. Aos elementos é dada toda a liberdade de estarem inseridos em grupos e de possuírem permissões individuais, no entanto é controlada a sobreposição de espaços aos quais este tem permissão, de modo a impedir que o elemento de um grupo com acesso ao espaço x não tenha também uma permissão individual ao espaço x.

5.3 Consulta de Estatísticas

Neste ponto do módulo é dada ao utilizador a possibilidade de visualizar estatísticas dos seus acessos às instalações da faculdade, se o utilizador possuir permissões de administração este pode consultar não só estatísticas dos seus acessos como pode consultar estatísticas sobre os acessos gerais, ou de um utilizador em particular.

Os tipos de estatísticas disponibilizadas são:

- Estatísticas por grupo de acesso
- Estatísticas por espaço
- Estatísticas temporais
- Estatísticas por elemento

As estatísticas por grupo permitem aos administradores visualizar os espaços com maior quantidade de acessos dentro dos espaços a que este tem acesso, permite ainda a comparação de utilização entre grupos, saber quais os grupos com mais acessos efectuados e a que espaços. As estatísticas por espaços permitem visualizar quais os elementos e grupos que utilizam com maior frequência o espaço escolhido, permitindo esta análise determinar se o meio de acesso ao espaço é o mais adequado. Com as estatísticas temporais é possível obter os a relação entre os acessos e o horário em que este é efectuado, sendo depois mostrado o número de acessos por horas durante um dia e em termos semanais e mensais quais os dias com maior afluência, tendo o acesso a esta estatística podemos tirar elações sobre quais as horas de pico, dias de pico em cada semana e quais os meses com maior número de acessos. Por fim a estatística por elemento, a única disponível a todos os utilizadores que permite a junção das anteriores estatísticas mas todas apenas para o utilizador validado no SI, apenas os administradores podem variar o elemento sobre o qual desejam ver as estatísticas em questão. (imagem das estatísticas)

5.4 Monitorização

Relativamente à monitorização dos acessos esta é feita através das aplicações que gerem a ligação com os dispositivos de controlo, para os dispositivos de RFid o controlo e troca de informação é gerida pela aplicação StarWatch Pro onde devem ser criadas todos os utilizadores, as suas permissões e ainda os dispositivos que controlam cada ponto de acesso. De forma a não ser necessária a inserção manual de informação no SI a também no StarWatch foram criados web services para permitir a troca de informação entre os dois sistemas. Os web services estão a correr na

máquina servidor onde está instalado o StarWatch e permite através de chamadas do SI, inserir, actualizar e remover dados existentes na aplicação. A opção dos web services foi escolhida porque os dados no SI estão numa base de dados Oracle 10g e no StarWatch num base de dados MSDE. Para esta troca de dados existia uma funcionalidade da Oracle, o Oracle Heterogenios Service, que fazia exactamente o que era necessário permitindo através de uma base de dados Oracle aceder a uma base de dados de outro tipo de forma totalmente transparente. O grande senão que impediu a utilização deste serviço foi só existir para sistemas Oracle de 32bits e na FEUP os servidores todos utilizam já Oracle na versão 64bits inviabilizando totalmente esta opção, dai a escolha dos web services.

Os web services foram implementados em PHP e são suportados por um servidor de HTTP Apache, a escolha recaiu nestas duas tecnologias, por serem gratuitas, bastante estáveis e por eu já ter alguma experiência em PHP. Para implementar as mensagens a trocar foi escolhido o protocolo SOAP, que permite através mensagens em xml enviar e receber por HTTP de modo a os resultados returnados serem válidados pelo proprio xml (a estrutura e exemplo das mensagens trocadas ésta descrino no anexo D. A figura 5.5 representa o funcionamento dos web services,

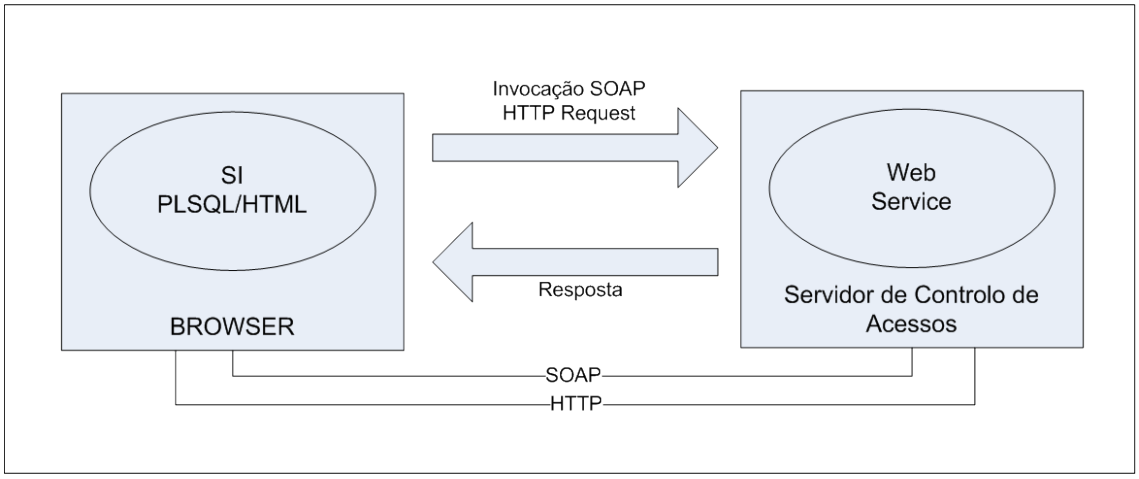

Figura 5.5: SOAP

depois de serem colocados online, estes são chamados a através de pedidos HTTP em PLSQL, obetendo a resposta desde que o xml enviado corresponda ao que o web service deve receber. Em termos de segurança, foi pensada a hipotese de incluir um certificado nas messagens de modo a poder verificar a veracidade do pedido, no entanto visto o Apache poder ser configurado o de modo a só permitir o acesso por parte de certos Ip's, foi configurado para só aceitar pedidos vindos dos servidores que suportam o SI. No web service criado estão disponiveis duas funcões *getData* e *setData*, em que a função *getData* é utilizada para ir buscar dados ao servidor

do StarWatch, esta função cria uma query SQL (são passados como parametros os campos a retornar, a tabela a ser questionada e os argumentos da clausula *where* se existentes) a ser executada sobre a base de dados da aplicação e retorna os resultados obtidos no formato XML, a função *setData* serve para inserir e actualizar os dados existentes na base de dados da aplicação, para tal recebe a query a executar em formato livre, retornando a *string* ok no caso de sucesso.

Agora que temos a ligação entre dos dois pontos de dados estabelecida, foi necessário criar interfaces que permitissem a utilização das funções de envio e recepção de dados. (imagem do estados dos dispositivos)

Após os dados recolhidos estes podem ser visualizados pelos utilizadores, não só os dados de acessos permitidos, mas também os dados relativos aos alarmes que apenas permitem saber em quando é que alguem tentou aceder aos pontos de acesso sem estar registado.

5.5 Controlo dos Cartões de Acesso

Para que exista um real controlo dos cartões disponibilizados quer a alunos, quer a funcionarios da Faculdade de Engenharia da Universidade do Portofoi implementado no SI um sistema que permite no acto da entrega do cartão registar facilmente a sua entrega, sendo assim possivel a qualquer momento determinar quem possui cartão de identificação e quem não possui.

Outro dos pontos melhorados foi o procedimento de pedido de cartões que passou agora a ser completamente gerido através do sistema de informação, evitando o preenchiimento de requerimentos para a obtenção de uma nova via do cartão. O único ponto que o sistema de informação ainda não trata é o processo de pagamento do novo cartão. O novo processo é representado pelas figuras seguintes.

Na figura 5.6 podemos ver os cartões pedidos que ainda não foram processados. Para que os cartões sejam impressos é disponibilizado no link *download dados* um ficheiro excel com os dados dos utilizadores que efectuaram o pedido do cartão, de modo a que os sevições que fazem a impressão dos cartões tenham acesso aos dados a imprimir nos cartões. Visto ser impossivel inserir as fotos no excel e ligá-las ao utilizador em questão é disponibilizador um ficheiro .zip com as fotos de todos os cartões pedidos. Este ficheiro tal como o excel é gerado automáticamente na altura em que é requesitado.

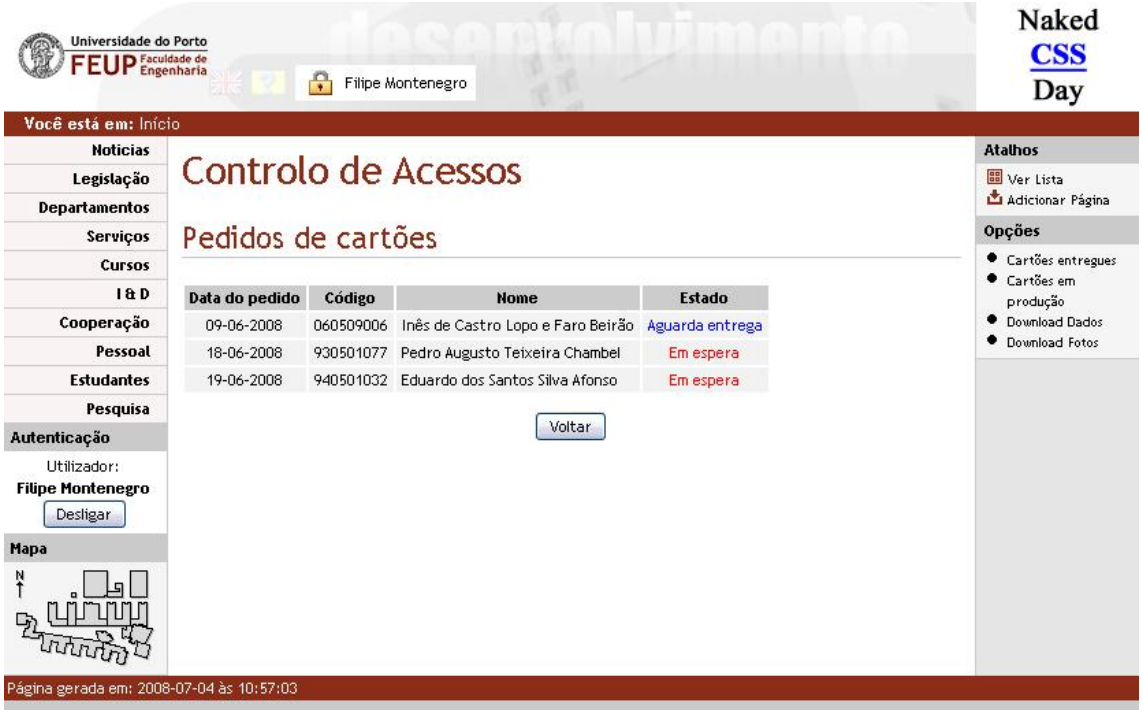

Figura 5.6: Cartões pedidos

Na figura 5.7 é demonstrado o passo seguinte do processo, onde após ter sido efectuado o download dos dois ficheiros contendo os dados a imprimir os cartões pendentes passam automáticamente para o estado de *Em produção*, ficando neste estado até estarem prontos, momento em que são marcados como produzidos. Ao serem marcados como produzidos os utilizadores que os requesitaram são notificados por email para irem levantar o seu novo cartão.

Figura 5.7: Cartões em produção

Quando os utilizadores levantam o seu novo cartão o levantamento é registado e é actualizada a sua informação dos dispositivos de controlo (no caso de perda ou roubo do cartão, o antigo codigo do cartão é inutilizado).

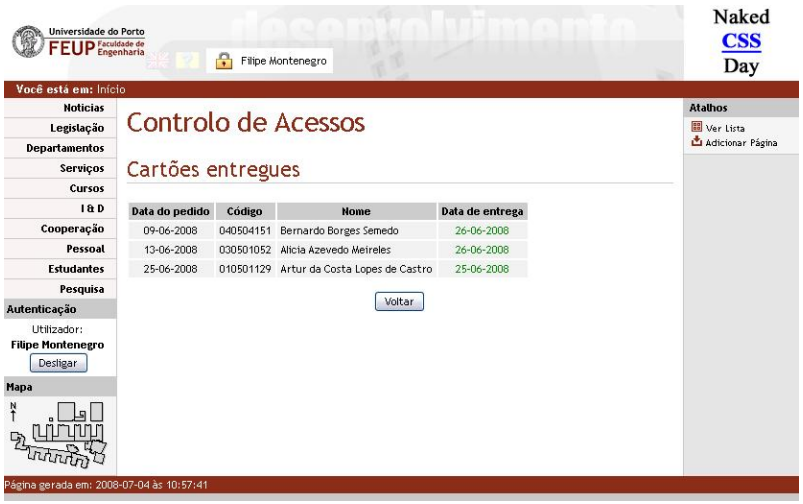

Figura 5.8: Cartões entregues

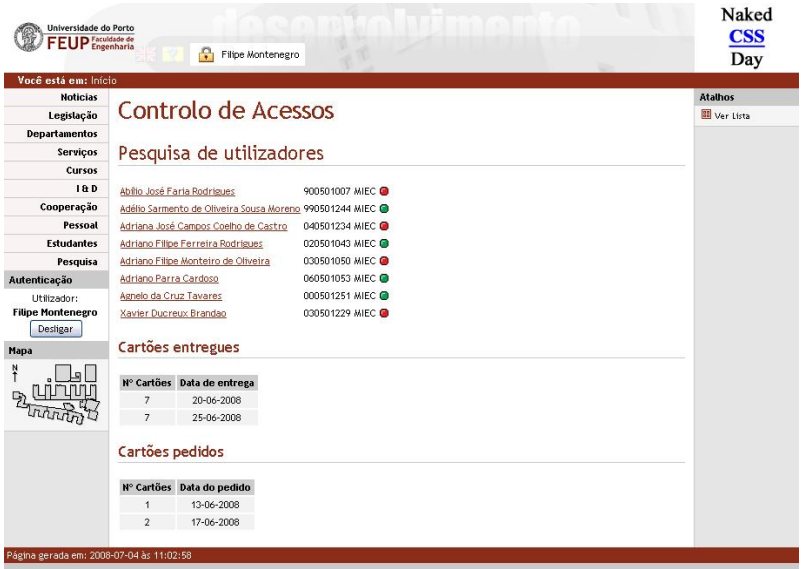

Figura 5.9: Controlo do estado dos cartões

Capítulo 6

Validação e Testes

De modo a ser testado o módulo procedeu-se à validação de cada um dos requisitos através de tudo que foi implementado. Para estes testes é utilizada a ferramenta de gestão de projectos existente no Projecto de Sistemas de Informação, que ao aglomerar todos os objectos criados permite enviar para testes estes objectos de modo a serem testados por outro elemento da equipa.

Como o tempo foi limitado os testes por outros elementos da equipa ainda não foram realizados pelo que os testes foram apenas realizados por mim e o encadeamento utilizado foi o seguinte:

- Validação da interface - todas as interfaces devem seguir os padrões do SI;
- Validação de formulários - os formulários devem conter os campos necessários e especificados;
- Tratamento de erros - os formulários são testados com a inserção de todo o tipo de valores de modo a testar se existe algum valor que leve a situações de erro não controlado;
- Validação dos dados inseridos - após cada inserção é verificada na base de dados a integridade dos dados inseridos.
- Validação multi-browser - é testada cada página em diversos browsers, o resultado deve ser igual em todos eles.
- Apenas após todos os testes o módulo terem passado satisfatoriamente pode ser criada uma versão do módulo. Neste ponto entra novamente a ferramenta de gestão de projectos que ao juntar todos os objectos testados do módulo cria uma nova versão instalavél do mesmo.

Capítulo 7

Conclusões e Previsões Futuras

Como conclusões a tomar depois do projecto estar terminado posso dizer que os objectivos foram cumpridos. As vantagens deste módulo irão trazer às instituições em que o módulo seja instalado uma maior facilidade em gerir a informação relativa ao controlo de acessos, e às actividades envolventes. O controlo dos cartões de identifição também apresenta agora melhorias substanciais, quer na altura da produção dos cartões, quer no registo da entrega dos cartões, deixando de existir multiplos pedidos do mesmo cartão, que até ao momento era impresso sem a certificação do utilizador já possuia ou não cartão. Agora é igualmente mais facil controlar a remoção dos acessos a utilizadores que abandonaram a faculdade.

Em termos de trabalho futuro existem já algumas ideias para pôr em prática. A principal delas que apenas ainda não implementada por falta de disponibilidade de tempo, é a ligação directa via tcp/ip aos controladores de modo a tentar evitar ao máximo a interacção humana no momento de atribuir uma permissão de acesso na aplicação StarWatch. Isto porque até ao presente momento, após a passagem dos dados do SI para a base dados da aplicação é necessária a intervenção humana para que estes dados sejam transmitidos para os controladores desejados. Neste campo já foi feito algum estudo e é disponibilizado pela empresa criadora do software um sdk contendo funções que permitem a criação de rotinas VB que através do protocolo acima referido interagem directamente com os controladores.

Outro as aspecto a ser melhorado no futuro é a ligação à aplicação StarGaze, que por até ao momento estar fisicamente separada da rede da faculdade não permite uma interacção directa com os controladores dos leitores magnéticos. Esta é uma possibilidade interessante, mas no entanto, à que ter atenção ao previsível futuro abandono deste tipo de leitores, dai esta possibilidade tenha que ser extremamente bem planeada. Por fim e como revisão do trabalho feito julgo que algumas das

interfaces podem vir a ser melhoradas através da interacção com um maior número de utilizadores, que com a sua utilização podem fazer sugestões úteis, de modo a tornar este módulo cada vez mais robusto e simples de utilizar.

Referências e Bibliografia

[CIC] CICA. Informações sobre o centro de informática prof. correia de araújo na feup. http://www.fe.up.pt/si/web_base.gera_pagina?P_pagina=2406.

[dJ] API de JAVA. Api de java 1.4. http://java.sun.com/j2se/1.4.2/docs/api/.

[FEU] FEUP. Página principal da faculdade de engenharia da universidade do porto. http://www.fe.up.pt/si/web_page.inicial.

[IDT] IDTECK. Site da empresa idteck. http://www.idteck.com/.

[OMG] OMG. Página principal da object management group. http://www.uml.org/.

[Ora] Oracle. Página principal da oracle. http://www.oracle.com/index.html.

[PHP] PHP. Página sobre a linguagem php. http://www.php.net.

[PL/] Oracle PL/SQL. Informações sobre pl/sql oracle. http://www.techonthenet.com/oracle/index.php.

[SOA] SOAP. Soap. http://conferences.codegear.com/article/32170.

[Spr] XML SpreadSheet. Informações sobre a notação xml spreadsheet. http://msdn2.microsoft.com/en-us/library/aa140066(office.10).aspx.

[SQL] Oracle SQL. Informações sobre sql oracle. http://www.adp-gmbh.ch/ora/sql/index.html.

[W3C] W3C. Página do world wide web consortium. http://www.w3.org/.

[W3S] W3Schools. Página do world wide web consortium. http://www.w3schools.com/default.asp.

Anexo A

StarWatch Pro

A aplicação StarWatch Pro foi adquirida em conjunto com os controladores e dispositivos montados para controlar as portas rotativas de acesso ao bloca B da Faculdade de Engenharia da Universidade do Porto. Esta aplicação foi desenvolvida pela IDTECK [IDT] até ao momento é através dela que as permições de acesso às novas portas rotativas são controladas. Esta aplicação é bastante completa, servindo não só para controlar os acessos como também para controlo de ponto dos funcionários (esta funcionalidade não é utilizada na feup). Para o controlo de acessos permite a criação de grupos de acesso, atribuição temporaria de acessos, visualização gráfica dos mapas referentes às instalações controladas entre muitas outras funcionalidades.

O únicio senão detectado por mim é relativo aos grupos de acessos e permissões individuais, não sendo possivel na aplicação uma pessoa pertencer a um grupo de acesso e ao mesmo tempo possuir permissões de acesso individuais. Esta particularidade é ultrapassada passando as permissões aos grupos existentes no SI como permissões individuais.

A figura A.1 mostra o ecrã de visualização dos acessos apresentado no StarWatch PRO.

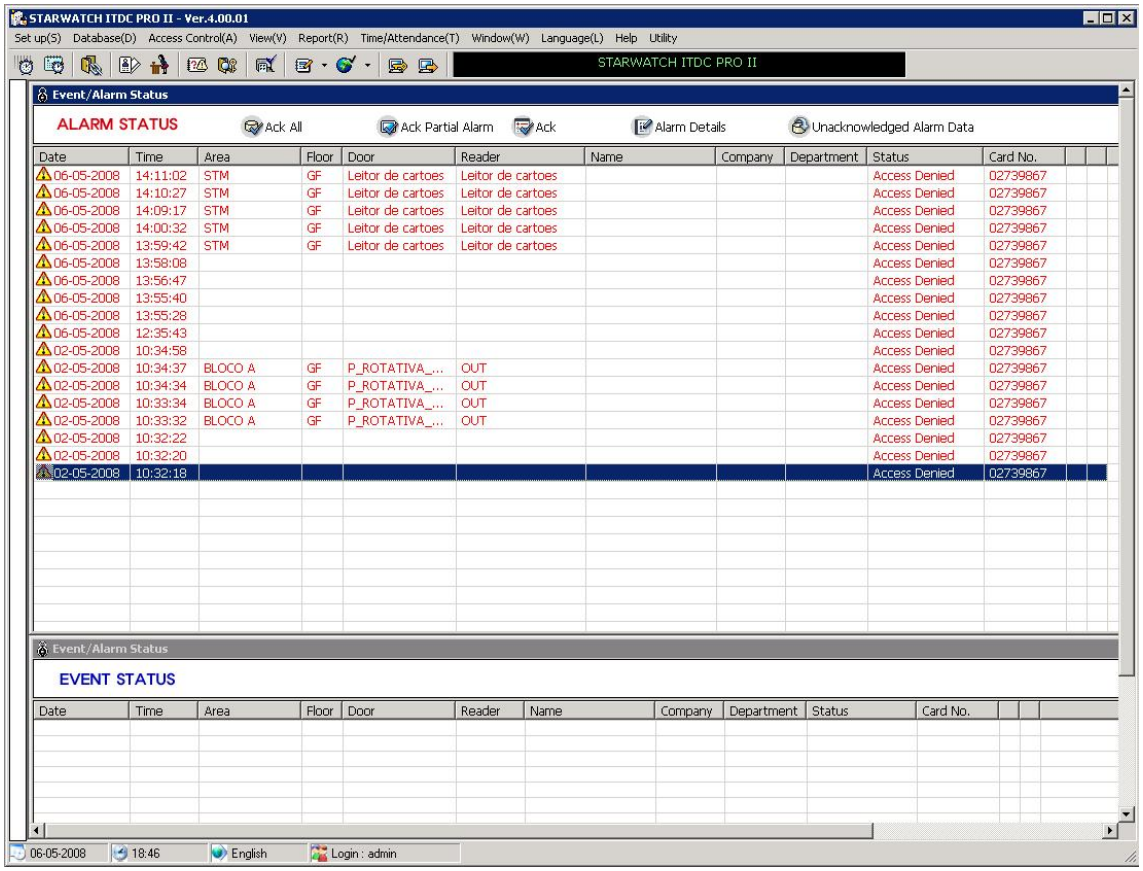

Figura A.1: Aplicação de Controlo de Acessos

Anexo B

StarGaze

StarGaze é a aplicação de controlo de acesso que existia para controlar os dispositivos magnéticos existentes. Esta aplicação é já bastante antiga no entanto funciona relativamente bem, tendo como principais contras a interface já desactualizada e pouco *user friendly* e ser muito pouco intuitiva. Esta aplicação é suportada por uma base de dados Unify que apesar de já bastante antiga apresenta bons resultados em termos de performance, tendo em conta a maquina em que está montada.

Uma situação a ser resolvida no futuro é a integração desta aplicação com a restante rede interna da faculdade de modo a poder ser interligada a informação desta aplicação de forma directa.

A figura B.1 demonstra a arquitectura da aplicação StarGaze.

Figura B.1: Arquitectura do StarGaze

Anexo C

Processos Paralelos ao Projecto

Neste capitulo de anexos vou falar inicialmente de uma parte deste projecto que decorreu paralelamente ao mesmo mas que o seu enquadramento se distancia dos objectivos do projecto enquanto trabalho integrado no curso.

O primeiro ponto a referir foi o meu trabalho durante a montagem da nova infra-estrutura de portas rotativas a funcionar actualmente na faculdade, esta esteve sobre a minha responsabilidade em termos de especificação do seu funcionamento. Esta especificação passou por estudar o funcionamento das portas de modo a permitir dentro do possível a entrada a uma só pessoa de cada vez, isto levou a que fossem feitas algumas experiências no modo como as folhas das portas eram posicionadas na posição de descanso. Foi de igual modo necessário estudar a melhor localização para o conjunto de câmaras a colocar de modo a poder detectar infracções e abusos na utilização das portas. Outro dos pontos em que estive envolvido foi a escolha do tipo de dispositivo a ser usado como controlador para essas mesmas portas, se se manteria leitores magnéticos ou iniciava uma alteração para leitores de RFid. Inicialmente a escolha recaiu sobre leitores magnéticos, mas esta opção cedo se tornou problemática, isto porque os novos leitores para serem compatíveis com os leitores já existentes (possibilitando assim a continuação do uso dos cartões magnéticos já existentes) não eram compatíveis com os controladores montados juntamente com as portas. Este problema consistia em os leitores antigos permitirem uma codificação seguindo a norma ISOII e os controladores apenas funcionarem com leitores que efectuassem a leitura seguindo a codificação de Weigand, deste modo se fossem usados leitores magnéticos compatíveis com os antigos e tendo em conta o funcionamento das duas normas, apenas iríamos ter a possibilidade de ler 100 cartões diferentes porque apenas eram detectados pelo leitor 2 dígitos de cada cartão. A partir deste ponto qualquer solução passava sempre pela distribuição de novos cartões, o que levou a que se opta-se por montar leitores de RFid por estes serem mais actuais e mais cómodos na sua utilização.

Após ter sido decidida a utilização dos leitores de RFid era então necessário distribuir novos cartões compatíveis os novos leitores mas que continuassem a ser de igual forma compatíveis com os antigos leitores magnéticos. Para tal era necessário replicar os dados existentes na aplicação de controlo dos leitores magnéticos para a aplicação de controlo dos leitores de RFid e manter em funcionamento durante um certo período de tempo os cartões antigos. Visto só existir o um servidor a correr esta aplicação foi necessário criar uma replica do disco desta maquina e monta-lo

numa maquina semelhante para poder efectuar testes de viabilidade desta migração. Os scripts SQL criados, depois de devidamente testados foram corridos no servidor de produção, estão neste momento atribuídos temporariamente dois cartões a cada utilizador que já possuía cartão e foram registados os utilizadores que iriam ter cartão pela primeira vez.

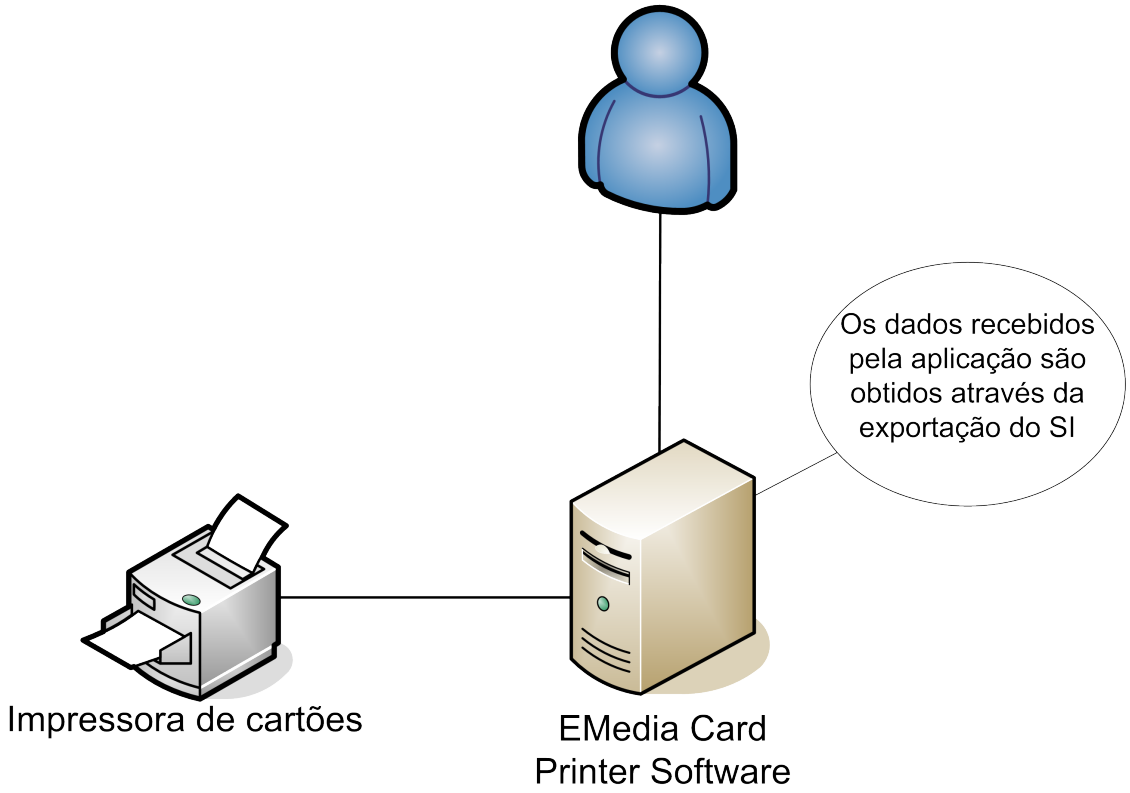

Figura C.1: Arquitectura do servidor de impressão de cartões

Estando terminada a fase de migração de dados foi iniciada a fase de criação dos cartões, esta começou pela montagem de uma nova impressora de cartões e o estudo do software que acompanhava a mesma. Este software (EMedia Card Designer) foi estado por mim de modo a saber quais os tipos de dados recebidos pela mesma e para dar formação aos funcionários que iriam trabalhar com a mesma. A aplicação permitia a importação de ficheiros excel para impressão em serie dos cartões de modo que foi necessário criar a partir do SI um excel contendo os campos necessários para a impressão dos cartões. Uma das limitações deste software era a impossibilidade de recolher a foto de um local remoto, desta forma as fotos a colocar nos cartões teriam que ser passadas para a maquina onde corria o software de impressão.

Com o novo módulo a geração do ficheiro de excel a ser importado pelo EMedia passou a ser automática facilitando bastante a troca de dados entre o SI e os serviços responsaveis pela impressão dos cartões. As fotos são agora transferidas em ficheiro zip, o qual também é gerado por pedido dos utilizadores.

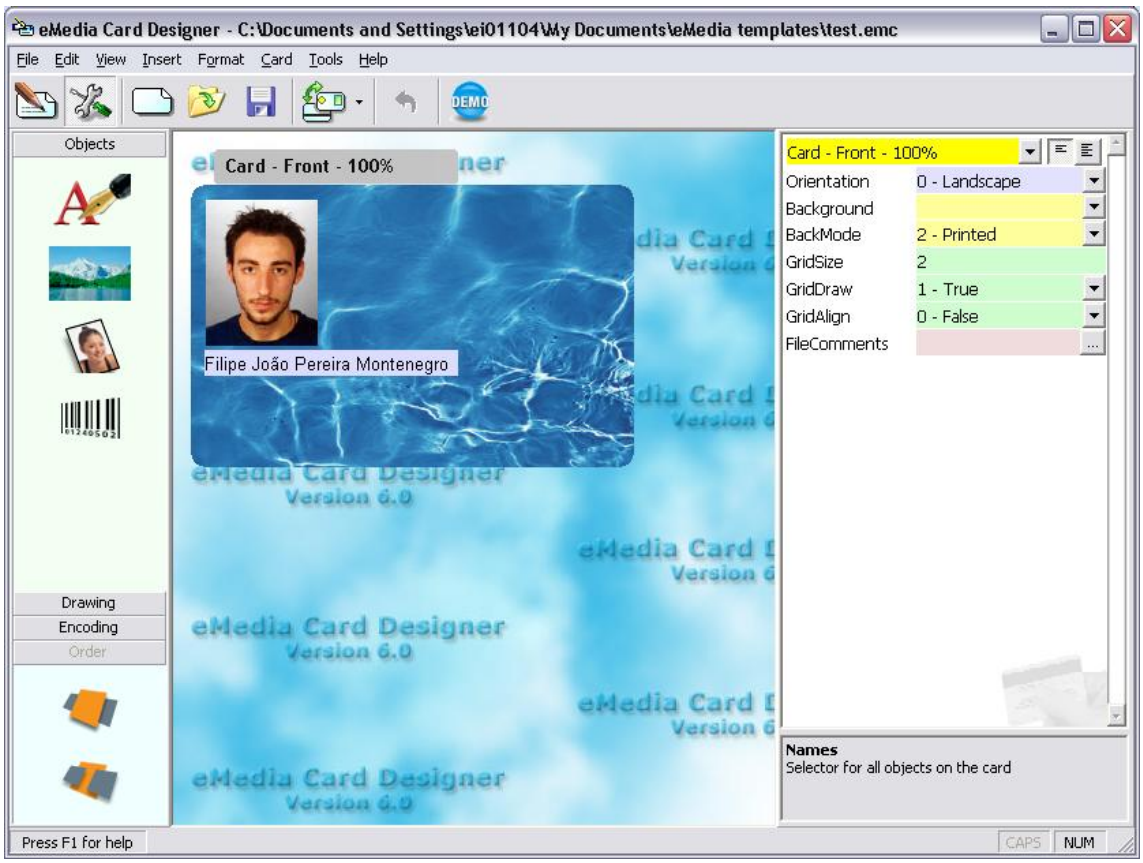

Figura C.2: Aplicação de impressão de cartões

Anexo D

PHP SOAP

Nesta secção vou mostrar as mensagens trocadas entre os dois servidores usando o protocolo SOAP através de HTTP.

As mensagens SOAP enviadas seguem a estrutura demonstrada na figura D.1.

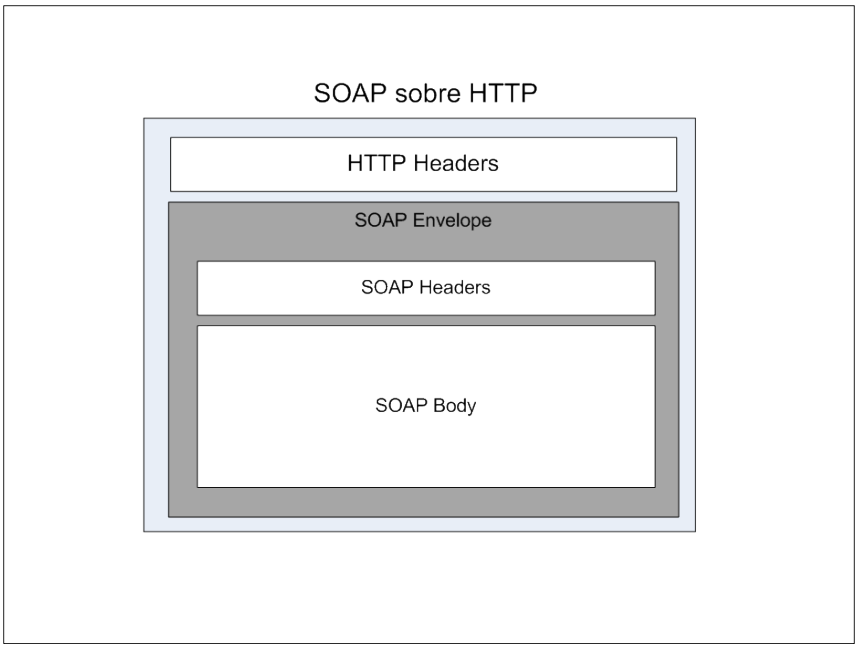

Figura D.1: SOAP sobre HTTP

Enviado

HTTP Header

```
POST /web_services/server.php HTTP/1.1
Host: itdc.fe.up.pt
Connection: Keep-Alive
User-Agent: PHP-SOAP/5.2.0-8+etch11
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://itdc.fe.up.pt/web_services/#getDados"
```

```
Content-Length: 791
```

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://itdc.fe.up.pt/web\_services/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
   <SOAP-ENV:Body>
      <ns1:getDados>
         <param0 xsi:type="xsd:string">itdc.fe.up.pt</param0>
         <param1 xsi:type="xsd:string">sa\<param1>
         <param2 xsi:type="xsd:string">portas.2008</param2>
         <param3 xsi:type="xsd:string">ITDC\_PRO\_II\_ACS\</param3>
         <param4 xsi:type="xsd:string">*\</param4>
         <param5 xsi:type="xsd:string">T_DOOR</param5>
         <param6 xsi:type="xsd:string"></param6>
      </ns1:getDados>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Recebido

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://itdc.fe.up.pt/web_services/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
   <SOAP-ENV:Body>
      <ns1:getDadosResponse>
         <return xsi:type="xsd:string">
            <RESULT>
               <ROW number="1">
                  <PORTID>01</PORTID>
                  <BOARDID>000</BOARDID>
                  <DOORID>1</DOORID>
                  <DOORNAME>P_ROTATIVA BL B</DOORNAME>
                  <DOORAREA>0002</DOORAREA>
                  <DOORLOCATIONGF></DOORLOCATION>
                  <LOCKTYPE>NO</LOCKTYPE>
                  <CONTACTTYPE>NO</CONTACTTYPE>
                  <APBVALUE>0</APBVALUE>
```

```
                  <DURESSPIN>00</DURESSPIN>
                  <UPDATEDATE>Jan 4 2008  3:24PM</UPDATEDATE>
               </ROW>
               <ROW number="2">
                  <PORTID>02</PORTID>
                  <BOARDID>000</BOARDID>
                  <DOORID>1</DOORID>
                  <DOORNAME>P_ROTATIVA_BL A</DOORNAME>
                  <DOORAREA>0001</DOORAREA>
                  <DOORLOCATION>GF</DOORLOCATION>
                  <LOCKTYPE>NO</LOCKTYPE>
                  <CONTACTTYPE>NO</CONTACTTYPE>
                  <APBVALUE>0</APBVALUE>
                  <DURESSPIN>00</DURESSPIN>
                  <UPDATEDATE>May 6 2008  2:58PM</UPDATEDATE>
               </ROW>
            </RESULT>
         </return>
      </ns1:getDadosResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```