

Universidade do Porto

FEUP Faculdade de
Engenharia

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES

GESTÃO DE CONTROLO DE ACESSOS

Pedro Alexandre Teixeira Moreira

Licenciado em Informática de Gestão
pela Universidade Portucalense, Infante D. Henrique

Dissertação submetida para satisfação parcial dos
requisitos do grau de mestre
em

Engenharia Electrotécnica e de Computadores
(Área de especialização em Tecnologias da Informação para Gestão Empresarial)

Dissertação realizada sob a orientação do
Professor Doutor Adriano da Silva Carvalho
do Departamento de Engenharia Electrotécnica e de Computadores
da Faculdade de Engenharia da Universidade do Porto
e

co-orientação do
Mestre Manuel José Mendes Pinto Machado
do Centro de Informática Prof. Correia de Araújo
da Faculdade de Engenharia da Universidade do Porto

Porto, Dezembro de 2008

Agradecimentos

Gostaria de manifestar os meus agradecimentos:

Ao Professor Doutor Adriano da Silva Carvalho e Mestre Manuel José Mendes Pinto Machado, não só por terem aceite a orientação desta dissertação, como também, pela disponibilidade de recursos que colocaram à minha disposição.

Aos colegas de estudo da sala I104 do DEEC da FEUP, pelo acolhimento demonstrado em diversas situações.

“If you cannot do great things, do small things in a great way”

Napoleon Hill (1883 – 1970)

Resumo

A implementação de sistemas de controlo de acessos físico tem vindo, progressivamente, a assumir uma especial importância nas organizações, quer em grandes instituições estatais e grupos multinacionais, quer em empresas de média e, mesmo, pequena dimensão. Este facto, consequentemente, tem conduzido à indispensabilidade do recurso a sistemas informáticos para que, de modo adequado, possam ser geridos todos os processos relacionados com os sistemas de controlo de acessos físico. É com base na constatação da crescente necessidade de desenvolvimento e implementação destes sistemas de *software* de gestão de controlo de acessos físico, bem como, da utilidade que prestam na eficácia da administração dos acessos, a recursos tangíveis das organizações, que o presente trabalho é justificado. Nesse sentido, procura efectuar o estudo de matérias relacionadas com essas áreas, tendo como objectivo principal, estabelecer as linhas gerais relativas à concepção, desenvolvimento e implementação de uma aplicação *web* de gestão de sistemas de controlo de acessos físico (*WebGPACS*), mais propriamente, adequada a um *campus* universitário.

Neste contexto, começa por abordar vários temas abrangidos na problemática dos sistemas de controlo de acessos físico e sua gestão, procurando, deste modo, caracterizar os principais conceitos e mecanismos relacionados com o processo de controlo de acessos físico, tecnologias utilizadas e sistemas correspondentes. Quanto às tecnologias, cada uma das tecnologias de identificação e autenticação é caracterizada singularmente, com especial relevo para a *RFID* e para os diferentes tipos de biometrias. Os sistemas de controlo de acessos físico são também caracterizados, em particular, os suportados por tecnologia *RFID*, tanto ao nível da arquitectura geral e principais componentes, como das comunicações e dados.

Em etapas subsequentes, dedicadas à concepção, desenvolvimento e implementação da aplicação informática, é definido o domínio do problema, são descritos os objectivos e impacto da aplicação a desenvolver, assim como, identificados os seus requisitos e funcionalidades gerais. Os principais requisitos funcionais são descritos textualmente e apresentados sob a forma de casos de utilização, em diagramas *UML*, assim como, o modelo de objectos do domínio. No desenho e implementação, para além de serem apresentadas as arquitecturas lógica, física e as tecnologias de suporte ao desenvolvimento, também são mencionados os aspectos mais relevantes da implementação, em especial, o modelo de gestão de dados hierárquicos utilizado (*modelo de diagramas de Venn*) e correspondentes interrogações *SQL* de acesso à base de dados. Para validação de resultados e requisitos funcionais da aplicação, é apresentado um caso de estudo, com base num cenário de gestão de controlo de acessos num *campus* universitário, em que são demonstradas *interfaces* e testadas algumas funcionalidades. Por fim, as conclusões, que retratam, genericamente, o trabalho desenvolvido nesta dissertação e, sobretudo, mencionam as funcionalidades da aplicação implementadas e as que poderão vir a sê-lo, em trabalhos futuros, finalizando com uma ideia prática de viabilização de serviços de “gestão de controlo de acessos”.

Abstract

The physical access control systems implementation has been coming to assume a particular importance in the organizations, either in large state institutions and multinational groups, or in medium and, even, small sized enterprises. This fact, has consequently led to the indispensability of the use of computer systems so that all the processes related to the physical access control systems can be properly managed. It is based on the perception of the increasing need for development and implementation of physical access control management software systems, as well as, their utility to the efficiency in the access administration to tangible resources in the organizations, that this work is justified. On this purpose, seeks the study of themes related to those areas, having as main objective, to set the outlines for the conception, development and implementation of a web application for management of physical access control systems (*WebGPACS*), rather, appropriate to a university campus.

In this context, it begins to approach various topics comprised in the scope of physical access control systems and management, thereby seeking to characterize the main concepts and mechanisms related to the physical access control process, used technologies and related systems. As for technologies, each one of the identification and authentication technologies is uniquely characterized, with emphasis on *RFID* and different types of biometric technologies. The physical access control systems are also characterized, in particular, supported by *RFID* technology, either the general architecture and key components or data and communications.

In subsequent stages, devoted to the conception, development and implementation of computer application, the problem domain is defined, the objectives and the impact application are described, as well as, its requirements and general functionalities are identified. The main functional requirements are textually described and presented in the form of use cases, in *UML* diagrams, as well as, the object domain model. In the design and implementation, in addition to present the logic and physical architectures, the relevant aspects of implementation are also mentioned, in particular, the hierarchical data management model (Venn diagrams model) and related database access SQL queries. For validation of results and functional requirements of the application, is presented a case study, scenario-based access control management in a university campus, in which are shown interfaces and tested some functionalities. Finally, the conclusion that describes, generically, the work in this dissertation, and mainly mentions the functionalities that were implemented and those that may become so in future works, ending with a practical idea to offer services for “access control management”.

Índice

Resumo.....	vii
Abstract	ix
Índice.....	xi
Índice de Figuras.....	xvii
Índice de Tabelas	xxi
Acrónimos e Siglas	xxiii

Capítulo 1

Introdução	1
1.1 Enquadramento e Motivação	1
1.2 Estrutura da Dissertação	2

Capítulo 2

Identificação e Autenticação (Conceitos, Mecanismos e Tecnologias).....	5
2.1 Introdução	5
2.2 Identificação, Autenticação e Autorização	5
2.2.1 Identificação.....	5
2.2.2 Autenticação	5
2.2.3 Autorização	6
2.3 Mecanismos de Autenticação e Factor Múltiplo	6
2.3.1 Mecanismos de Autenticação	7
2.3.1.1 No Conhecimento	7
2.3.1.2 Na Posse.....	8
2.3.1.3 Nas Características Pessoais	8
2.3.1.4 Na Localização.....	8
2.3.2 Autenticação de Factor Múltiplo	9
2.4 Tecnologias de Identificação e Autenticação	10
2.4.1 Crachás de <i>ID</i>	10
2.4.2 Código de Barras	11
2.4.3 Bandas Magnéticas	12
2.4.4 Bandas Ópticas	12
2.4.5 <i>USB</i>	13
2.4.6 Tecnologia <i>RFID</i>	13
2.4.6.1 Tecnologias <i>RFID</i> para o Controlo de Acessos Físico.....	14
2.4.6.1.1 Tecnologia <i>125 KHz</i>	14
2.4.6.1.2 Tecnologias <i>ISO 14443</i> e <i>15693</i>	14
2.4.6.2 Cartões com <i>Chip</i> e Tecnologia <i>Smart Card</i>	15
2.4.6.2.1 Cartões de Memória	15
2.4.6.2.2 Cartões de Tecnologia <i>Smart Card</i>	16
2.4.6.3 Cartões (<i>Smart Card</i>)	16
2.4.6.3.1 Cartões de Contacto.....	17
2.4.6.3.2 Cartões de Proximidade.....	18
2.4.6.3.3 Cartões Híbridos.....	18
2.4.6.3.4 Cartões de <i>Interface Dupla</i>	19
2.4.6.4 <i>Tags (Transponders)</i>	19

2.4.6.4.1 Passivas.....	20
2.4.6.4.2 Activas.....	20
2.4.6.4.3 Semi-Activas	20
2.4.6.4.4 Semi-Passivas	21
2.4.7 Tecnologias Biométricas	21
2.4.7.1 Classificação e Tipos de Biometrias.....	21
2.4.7.1.1 Impressão Digital.....	23
2.4.7.1.2 Geometria da Mão	25
2.4.7.1.3 Íris.....	27
2.4.7.1.4 Facial	30
2.4.7.1.5 Padrão Vascular da Mão.....	32
2.4.7.1.6 Voz	33
2.4.7.1.7 Caligrafia	35

Capítulo 3

Sistemas de Controlo de Acessos Físico (baseados em <i>RFID</i>).....	37
3.1 Introdução.....	37
3.2 Sumário do Controlo de Acessos	37
3.3 Arquitectura e Componentes do Sistema	38
3.3.1 Arquitectura dum Sistema baseado em <i>RFID</i>	39
3.3.2 Tendências Actuais da Arquitectura dum Sistema em Rede.....	40
3.4 Componentes no Processo de Controlo de Acessos.....	41
3.4.1 Subsistema <i>RF</i>	41
3.4.1.1 A Credencial de <i>ID</i>	42
3.4.1.1.1 Características das <i>Tags</i>	42
3.4.1.2 O Leitor	45
3.4.1.2.1 Características dos <i>Readers</i>	47
3.4.2 Subsistema Empresarial	49
3.4.2.1 O Painel de Controlo	50
3.4.2.1.1 O <i>Middleware</i>	52
3.4.2.2 Os Sistemas Analíticos (do <i>Host System</i>).....	52
3.5 Dados e Comunicações do Sistema.....	53
3.5.1 Infra-estrutura de Rede.....	53
3.5.1.1 Topologia Física e Lógica	54
3.5.2 Protocolos de Comunicação de Dados	56
3.5.2.1 Comunicação <i>Tag – Reader</i>	56
3.5.2.2 Comunicações da Infra-estrutura de Rede (Leitor – Painel – Servidor).....	59
3.5.3 Factor Operacional Crítico: Distância <i>Tag – Reader</i>	60
3.5.4 Controlos Técnicos de Segurança (mais relevantes).....	61
3.5.4.1 Encriptação dos Dados e das Comunicações.....	61
3.5.4.1.1 Autenticação da Credencial de <i>ID</i> e dos Dados.....	61
3.5.4.1.2 Protecção dos Dados da Credencial de <i>ID</i>	62
3.5.4.1.3 Protecção das Comunicações de Dados.....	62

Capítulo 4

Definição do Domínio do Problema.....	65
4.1 Introdução.....	65
4.2 A Gestão de Acessos (Físico) em Universidades.....	65
4.3 Conceitos Relevantes na Gestão de Controlo de Acessos (Físico)	68
4.3.1 A Estrutura dos Espaços Físicos	69
4.3.2 O Controlo de Acessos Baseado no Papel	69

4.3.2.1	Atribuição de Permissões (sobre Objectos Físicos) a Papéis	70
4.3.2.2	Controlo de Acessos baseado nos Papéis de Utilizadores	71
4.3.3	Políticas de Segurança no Controlo de Acessos	71
4.3.3.1	O Menor Privilégio	71
4.3.3.2	Autorização Implícita e Herança Reversa	72
4.3.3.3	Auditorias de Acessos e Responsabilidade Individual	72
4.3.3.4	Políticas Especiais	73
4.4	A Aplicação <i>WebGPACS</i>	73
4.4.1	Objectivos	73
4.4.2	Impacto Esperado	74
Capítulo 5		
Requisitos da Aplicação.....		77
5.1	Requisitos Gerais	77
5.1.1	Sumário da Aplicação	77
5.1.2	Alojamento em Servidor <i>Web</i>	77
5.1.3	Base de Dados	78
5.1.4	Funcionamento, Monitorização e Notificações (em Tempo Real)	79
5.1.4.1	Funcionamento (em Tempo Real)	79
5.1.4.2	Monitorização (em Tempo Real)	79
5.1.4.3	Notificações (em Tempo Real)	80
5.1.5	<i>Interface Web</i> e Autenticação	80
5.1.6	Funcionalidades Essenciais de Gestão / Administração	81
5.1.6.1	Utilizadores	81
5.1.6.2	Papéis	82
5.1.6.3	Espaços Físicos (controlados)	83
5.1.6.4	Permissões (a espaços físicos)	83
5.1.6.5	Consultas e Produção de “ <i>Reports</i> ”	84
5.1.6.5.1	Auditorias/Pesquisas sobre Acessos e Presenças	84
5.1.6.5.2	Auditorias sobre Administração e Segurança do Sistema	85
5.1.6.5.3	Consultas Gerais à Base de Dados	86
5.2	Modelo de Casos de Utilização	86
5.2.1	Visão Global do Sistema	87
5.2.2	Identificação dos Actores	90
5.2.3	Subsistema “Gestão de Controlo de Acessos”	92
5.2.3.1	Gestão de Utilizadores	93
5.2.3.2	Gestão de Papéis	97
5.2.3.3	Gestão de Espaços (Físicos)	98
5.2.3.3.1	Editar Espaços (formato detalhado)	99
5.2.3.4	Gestão de Permissões (a Espaços)	103
5.2.3.5	Auditar/Pesquisar Acessos e Presenças	104
5.2.4	Subsistema “Funcionamento do Controlo de Acessos Físico”	106
5.2.4.1	Aceder e Abandonar Espaço	107
5.2.4.2	Diagramas de Sequência	108
5.3	Modelo de Objectos do Domínio	111
5.3.1	Diagrama do Modelo de Objectos do Domínio	111
5.3.2	Descrição do Modelo e Definições das Classes	112
Capítulo 6		
Arquitectura		115
6.1	Introdução	115

6.2 Arquitectura Lógica.....	115
6.3 Arquitectura Física	117
6.4 Tecnologias de Suporte	119
6.4.1 Servidor <i>Web</i> (<i>Apache</i>)	119
6.4.2 <i>HTML</i>	120
6.4.3 <i>CSS</i>	120
6.4.4 <i>JavaScript</i>	121
6.4.5 <i>PHP</i>	121
6.4.6 <i>SGBD</i> (<i>MySql</i>).....	122

Capítulo 7

Implementação	123
7.1 Introdução.....	123
7.2 Instalação e Configuração do Sistema	123
7.3 Modelo Relacional da Base de Dados da Aplicação.....	124
7.3.1 Diagrama Entidade-Relação (<i>E-R</i>).....	124
7.3.2 Descrição das Tabelas e Atributos	125
7.4 Modelo de Gestão de Dados Hierárquicos da Tabela “Espaços”	127
7.4.1 Expressões <i>MySQL</i> para a Hierarquia de Espaços Físicos.....	130
7.4.1.1 Representação da Totalidade dos Espaços Físicos	130
7.4.1.2 Espaços Físicos (nodos) “Folha”	130
7.4.1.3 Caminho Mais Simples até um Espaço Físico.....	131
7.4.1.4 Profundidade (nível hierárquico) dos Espaços Físicos	131
7.4.1.5 Representação Hierárquica Indentada dos Espaços Físicos	132
7.4.1.6 Adição Hierárquica de Espaços Físicos.....	134
7.4.1.7 Eliminação Hierárquica de Espaços Físicos	138
7.4.1.8 Outros.....	141
7.4.2 Interrogações da Aplicação sobre a Tabela “Espaços”	141
7.4.2.1 Editar Espaços	141
7.4.2.2 Consultar Espaços	142
7.4.2.3 Consultar Caminho mais simples até um Espaço	142
7.4.2.4 Consultar Permissões (a Espaços) do Papel	143
7.4.2.5 Consultar Espaços (disponíveis) para Permissões do Papel	143
7.4.2.6 Consultar Permissões (a Espaços) de Utilizadores	143
7.4.2.7 Auditar Acessos de Utilizadores	144
7.4.2.8 Auditar Acessos por Utilizador a um Espaço	145

Capítulo 8

Caso de Estudo	147
8.1 Introdução.....	147
8.2 Apresentação do Caso de Estudo e Pressupostos.....	147
8.3 Validação de Funcionalidades da Aplicação.....	148
8.3.1 Criar ou Inserir um Utilizador	148
8.3.2 Criar ou Inserir Permissões a Papel.....	151
8.3.3 Modificar Permissões do Papel	152
8.3.4 Atribuir Papéis a Utilizadores	155
8.3.5 Auditar Acessos de Utilizadores	157
8.3.6 Auditar Acessos a Espaços.....	161
8.3.7 Auditar Acessos a um Espaço por Utilizador.....	163

Capítulo 9

Conclusões	167
9.1 Funcionalidades da Aplicação (Implementadas)	167
9.2 Perspectivas de Trabalho Futuro.....	169
9.2.1 Funcionalidades da Aplicação (a Implementar)	169
9.2.1.1 Outras Funcionalidades (Relacionadas)	172
9.2.2 Serviços de “Gestão de Controlo de Acessos”	173
Bibliografia	175
ANEXOS.....	179
Anexo A – Sistema Biométrico	181
A.1 – Modelo Conceptual dum Sistema Genérico	181
A.2 – Funcionamento: Processos Característicos	183
A.3 – Erros	185
A.4 – Critérios Base.....	185
Anexo B – Casos de Utilização (Descrição)	187
B.1 – Gestão de Papéis	187
B.2 – Gestão de Espaços (Físicos).....	189
B.3 – Gestão de Permissões (a Espaços)	191
B.4 – Auditar/Pesquisar Acessos e Presenças	193
Anexo C – Listagem Parcial do Código da Aplicação	197
C.1 – Código de “Editar Espaços (inserir, modificar, eliminar)”	197
C.2 – Código de “Auditar Acessos a um Espaço por Utilizador”	215
Anexo D – Interrogações à Base de Dados	231
D.1 – Utilizadores	231
D.2 – Papéis	232
D.3 – Espaços	233
D.4 – Permissões (a Espaços)	235
D.5 – Acessos e Presenças	236
Anexo E – Serviços de “Gestão de Controlo de Acessos”	239

Índice de Figuras

<i>Figura 2.1 – Relação da utilização de vários factores de autenticação com os níveis de segurança atingidos [29].....</i>	<i>9</i>
<i>Figura 2.2 – Etiqueta com código de barras</i>	<i>11</i>
<i>Figura 2.3 – Com a tecnologia RFID as soluções de identificação do futuro tornam-se realidade hoje [36]</i>	<i>13</i>
<i>Figura 2.4 – Estrutura interna do chip microcontrolador de um smart card.....</i>	<i>16</i>
<i>Figura 2.5 – Cartão de contacto (contact smart card) [29]</i>	<i>17</i>
<i>Figura 2.6 – Cartão de proximidade (contactless smart card) [29].....</i>	<i>18</i>
<i>Figura 2.7 – Tag ou Tansponder</i>	<i>19</i>
<i>Figura 2.8 – Reconhecimento da impressão digital [26]</i>	<i>23</i>
<i>Figura 2.9 – Terminação e divisão de sulcos [27]</i>	<i>23</i>
<i>Figura 2.10 – Reconhecimento geométrico da mão [26]</i>	<i>25</i>
<i>Figura 2.11 – Reconhecimento geométrico da mão [5]</i>	<i>26</i>
<i>Figura 2.12 – Verificação da íris humana [3].....</i>	<i>27</i>
<i>Figura 2.13 – Padrão e código da íris [5]</i>	<i>27</i>
<i>Figura 2.14 – Reconhecimento da íris.....</i>	<i>28</i>
<i>Figura 2.15 – Reconhecimento facial</i>	<i>30</i>
<i>Figura 2.16 – Extracção do padrão vascular da mão [5]</i>	<i>32</i>
<i>Figura 2.17 – Fluxo do processo de extracção do padrão vascular da mão [5].....</i>	<i>32</i>
<i>Figura 2.18 – Espectrografia da representação da voz humana.....</i>	<i>33</i>
<i>Figura 2.19 – Quatro imagens de espectros (de baixa resolução) para quatro padrões de vozes diferentes, na pronúncia duma mesma palavra [3]</i>	<i>34</i>
<i>Figura 2.20 – Reconhecimento caligráfico.....</i>	<i>35</i>
<i>Figura 2.21 – Exemplo duma assinatura.....</i>	<i>35</i>
<i>Figura 2.22 – Gráficos correspondentes à assinatura (posição da caneta, tipo de pressão exercida, ângulos da escrita) [3]</i>	<i>35</i>
<i>Figura 3.1 – Componentes de sistemas de controlo de acessos físico.....</i>	<i>38</i>
<i>Figura 3.2 – Arquitectura dum sistema de controlo de acessos (físico).....</i>	<i>39</i>
<i>Figura 3.3 – Um exemplo dum simples subsistema RF</i>	<i>39</i>
<i>Figura 3.4 – Arquitectura do subsistema empresarial (representada no interior do tracejado).....</i>	<i>40</i>
<i>Figura 3.5 – Exemplo dum sistema de controlo de acesso físico em rede [13].....</i>	<i>40</i>
<i>Figura 3.6 – Um exemplo dum simples subsistema RF</i>	<i>41</i>
<i>Figura 3.7 – Credencial de ID sob a forma de chaveiro de proximidade [34]</i>	<i>42</i>
<i>Figura 3.8 – Cartão de proximidade [34]</i>	<i>42</i>
<i>Figura 3.9 – Exemplo dum código de produto electrónico de 96 bits (96-bit EPC).....</i>	<i>43</i>
<i>Figura 3.10 – Leitor com interface para cartões de contacto</i>	<i>45</i>
<i>Figura 3.11 – Leitor biométrico (impressão digital).....</i>	<i>46</i>
<i>Figura 3.12 – Exemplo dum leitor de autenticação de factor múltiplo [29]</i>	<i>46</i>
<i>Figura 3.13 – Leitor fixo dum sistema de controlo de acessos físico</i>	<i>48</i>
<i>Figura 3.14 – Leitor móvel manual na leitura duma tag.....</i>	<i>48</i>
<i>Figura 3.15 – Vários tipos de antena: A – antena de desktop ou de parede, B – antena de HF, C – antena em portal</i>	<i>49</i>
<i>Figura 3.16 – Arquitectura do subsistema empresarial (representada no interior do tracejado).....</i>	<i>49</i>
<i>Figura 3.17 – Painel de controlo dum sistema de controlo de acessos (físico) [8].....</i>	<i>50</i>
<i>Figura 3.18 – Ligações do painel de controlo num sistema de controlo de acessos (físico) [2].....</i>	<i>50</i>
<i>Figura 3.19 – Esquema simplificado dum sistema de controlo de acessos físico [29].....</i>	<i>51</i>

<i>Figura 3.20 – Arquitectura do subsistema empresarial (representada no interior do tracejado).....</i>	<i>53</i>
<i>Figura 3.21 – Ligações (do subsistema empresarial) num sistema de controlo de acessos (físico) [2]....</i>	<i>54</i>
<i>Figura 3.22 – Painel de controlo (access controller) ligado a vários readers [2].....</i>	<i>55</i>
<i>Figura 3.23 – Espectro de radiofrequência.....</i>	<i>56</i>
<i>Figura 3.24 – Ligação Ethernet [2].....</i>	<i>59</i>
<i>Figura 3.25 – Encriptação por chave simétrica.....</i>	<i>62</i>
<i>Figura 3.26 – Segurança da transmissão de dados (de início ao fim) num sistema de controlo de acessos físico (com base em smart cards) [13].....</i>	<i>63</i>
<i>Figura 4.1 – Panorâmica geral dum campus universitário.....</i>	<i>65</i>
<i>Figura 4.2 – Diferentes níveis de protecção [28].....</i>	<i>66</i>
<i>Figura 4.3 – Planta dum piso universitário.....</i>	<i>67</i>
<i>Figura 4.4 – Planta do Piso 1 do Edifício I (Electrotecnia) da FEUP.....</i>	<i>68</i>
<i>Figura 4.5 – Espaços físicos contêm outros espaços físicos menores.....</i>	<i>69</i>
<i>Figura 4.6 – O Modelo de “Controlo de Acessos Baseado no Papel (RBAC)”.....</i>	<i>70</i>
<i>Figura 4.7 – Permissões do modelo RBAC associadas a objectos físicos (espaços físicos).....</i>	<i>70</i>
<i>Figura 5.1 – Exemplo de Diagrama de Casos de Uso.....</i>	<i>86</i>
<i>Figura 5.2 – Diagrama de pacotes da aplicação WebGPACS.....</i>	<i>87</i>
<i>Figura 5.3 – Diagrama de pacotes de casos de utilização do subsistema “Gestão de Controlo de Acessos”.....</i>	<i>89</i>
<i>Figura 5.4 – Diagrama de casos de utilização do subsistema “Funcionamento do Controlo de Acessos Físico”.....</i>	<i>89</i>
<i>Figura 5.5 – Reader de proximidade.....</i>	<i>91</i>
<i>Figura 5.6 – Sensores.....</i>	<i>91</i>
<i>Figura 5.7 – Diagrama de pacotes de casos de utilização do subsistema “Gestão de Controlo de Acessos”.....</i>	<i>92</i>
<i>Figura 5.8 – Diagrama de casos de utilização de “Gestão de Utilizadores”.....</i>	<i>93</i>
<i>Figura 5.9 – Diagrama de casos de utilização de “Gestão de Papéis”.....</i>	<i>97</i>
<i>Figura 5.10 – Diagrama de casos de utilização de “Gestão de Espaços (Físicos)”.....</i>	<i>98</i>
<i>Figura 5.11 – Diagrama de casos de utilização de “Gestão de Permissões (a Espaços)”.....</i>	<i>104</i>
<i>Figura 5.12 – Diagrama de casos de utilização de “Auditar/Pesquisar Acessos e Presenças”.....</i>	<i>105</i>
<i>Figura 5.13 – Diagrama de casos de utilização do subsistema “Funcionamento do Controlo de Acessos Físico”.....</i>	<i>106</i>
<i>Figura 5.14 – Diagrama de sequência normal de funcionamento para aceder um espaço físico.....</i>	<i>109</i>
<i>Figura 5.15 – Diagrama de sequência de funcionamento excepcional para aceder um espaço físico....</i>	<i>110</i>
<i>Figura 5.16 – Diagrama de sequência normal de funcionamento para abandonar um espaço físico</i>	<i>110</i>
<i>Figura 5.17 – Diagrama do modelo de objectos do domínio.....</i>	<i>111</i>
<i>Figura 6.1 – Diagrama de pacotes de classes do WebGPACS.....</i>	<i>116</i>
<i>Figura 6.2 – Arquitectura física do WebGPACS, adaptada de [23].....</i>	<i>117</i>
<i>Figura 6.3 – Diagrama de distribuição do WebGPACS.....</i>	<i>118</i>
<i>Figura 6.4 – Interação navegador (browser) e servidor Web.....</i>	<i>119</i>
<i>Figura 6.5 – Interação entre PHP, o servidor Web e o browser do utilizador.....</i>	<i>121</i>
<i>Figura 7.1 – Esquema da implementação da aplicação WebGPACS.....</i>	<i>123</i>
<i>Figura 7.2 – Página inicial da aplicação WebGPACS.....</i>	<i>124</i>
<i>Figura 7.3 – Diagrama entidade-relação da base de dados da aplicação WebGPACS.....</i>	<i>125</i>
<i>Figura 7.4 – Representação hierárquica dos espaços físicos em árvore (com nodos e linhas).....</i>	<i>127</i>
<i>Figura 7.5 – Representação hierárquica dos espaços físicos em modelo de conjuntos encaixados.....</i>	<i>128</i>
<i>Figura 7.6 – Representação hierárquica dos espaços físicos no modelo de conjuntos encaixados, com discriminação dos valores lft e rgt de cada espaço físico (ou nodo hierárquico).....</i>	<i>129</i>
<i>Figura 7.7 – Representação hierárquica dos espaços físicos em árvore (com nodos e linhas), com discriminação dos valores de lft e rgt de cada espaço físico (ou nodo da árvore).....</i>	<i>129</i>

<i>Figura 7.8 – Visualização da indentação da identificação dos espaços físicos na página de edição de espaços físicos da aplicação WebGPACS</i>	<i>133</i>
<i>Figura 7.9 – Visualização mais aproximada da indentação da identificação dos espaços físicos de parte da página de edição de espaços físicos da aplicação WebGPACS</i>	<i>133</i>
<i>Figura 7.10 – Visualização da indentação da identificação dos espaços físicos, com discriminação dos valores de “lft” e “rgt”, de parte duma página da aplicação WebGPACS</i>	<i>133</i>
<i>Figura 7.11 – Representação hierárquica dos espaços físicos no modelo de conjuntos encaixados depois de inserido o novo espaço I – Escadas 0 – 1, com discriminação dos valores lft e rgt de cada espaço físico (ou nodo hierárquico)</i>	<i>134</i>
<i>Figura 7.12 – Representação hierárquica dos espaços físicos no modelo de conjuntos encaixados depois de inserido o novo espaço físico I-119.1, com discriminação dos valores lft e rgt de cada espaço físico (ou nodo hierárquico)</i>	<i>135</i>
<i>Figura 7.13 – Visualização da identificação dos espaços físicos, depois de inserido o novo espaço físico I-119.1</i>	<i>137</i>
<i>Figura 7.14 – Visualização mais aproximada da identificação dos espaços físicos, depois de inserido o novo espaço físico I-119.1</i>	<i>137</i>
<i>Figura 7.15 – Visualização da identificação dos espaços físicos depois de inserido o novo espaço físico I-119.1, com discriminação dos valores de “lft” e “rgt”</i>	<i>137</i>
<i>Figura 7.16 – Visualização da identificação dos espaços físicos, depois de eliminados o espaço físico I-119 e a sub-árvore de espaços físicos filho (neste caso, constituída apenas pelo espaço físico I-119.1)</i>	<i>140</i>
<i>Figura 7.17 – Visualização mais aproximada da identificação dos espaços físicos, depois de eliminados o espaço físico I-119 e a sub-árvore de espaços físicos filho (neste caso, constituída apenas pelo espaço físico I-119.1)</i>	<i>140</i>
<i>Figura 7.18 – Visualização da identificação dos espaços físicos, com discriminação dos valores de “lft” e “rgt”, depois de eliminados o espaço físico I-119 e a sub-árvore de espaços físicos filho (neste caso, constituída apenas pelo espaço físico I-119.1)</i>	<i>140</i>
<i>Figura 8.1 – Página para inserção de dados do novo utilizador</i>	<i>149</i>
<i>Figura 8.2 – Mensagem relativa ao preenchimento dos campos de inserção</i>	<i>150</i>
<i>Figura 8.3 – Não inserção do utilizador, já existência da identificação do utilizador.....</i>	<i>150</i>
<i>Figura 8.4 – Inserção bem sucedida, com revelação dos dados inseridos.....</i>	<i>150</i>
<i>Figura 8.5 – Visualização parcial da página de inserção de permissões de acesso a um papel.....</i>	<i>151</i>
<i>Figura 8.6 – Lista das permissões do papel, depois de atribuição automática de permissões de acesso a espaços físicos, hierarquicamente ascendentes, que conduzem ao espaço físico da nova permissão. Disponibilidade para continuação da inserção de novas permissões ao papel.</i>	<i>152</i>
<i>Figura 8.7 – Lista das permissões a espaços físicos já atribuídas ao papel AlunoDocDEEC_IA e selecção da permissão ao espaço físico I-104 para alteração.....</i>	<i>153</i>
<i>Figura 8.8 – Visualização parcial da modificação da permissão de acesso ao espaço físico I-104 do papel AlunoDocDEEC_IA.....</i>	<i>154</i>
<i>Figura 8.9 – Alteração bem sucedida, com revelação dos dados da permissão de acesso</i>	<i>154</i>
<i>Figura 8.10 – Listas dos papéis já atribuídos ao utilizador e dos, existentes no sistema, que não lhe estão atribuídos, com selecção do papel AlunoDocDEEC_IA para consulta das suas permissões de acesso</i>	<i>156</i>
<i>Figura 8.11 – Visualização das permissões de acesso (a espaços físicos) correspondentes ao papel</i>	<i>156</i>
<i>Figura 8.12 – O sistema mostra de imediato o novo papel atribuído ao utilizador na lista de papéis do utilizador e lista os papéis disponíveis, existentes no sistema.....</i>	<i>157</i>
<i>Figura 8.13 –Menu da aplicação WebGPACS, Acessos → Auditar Acessos de Utilizadores.....</i>	<i>158</i>
<i>Figura 8.14 – Página Auditar Acessos de Utilizadores com selecção do utilizador a auditar</i>	<i>158</i>
<i>Figura 8.15 – Página de inserção das datas de início e fim, para parametrização da pesquisa de acessos</i>	<i>159</i>
<i>Figura 8.16 – Inserção de datas, pelo despoletar dum calendário ao lado de cada campo de inserção</i>	<i>159</i>
<i>Figura 8.17 – Visualização parcial e aproximada da inserção de datas</i>	<i>160</i>

<i>Figura 8.18 – Listagem dos acessos (a espaços físicos) do utilizador, entre as datas assinaladas.....</i>	<i>160</i>
<i>Figura 8.19 – Visualização parcial da listagem de acessos (direcção dos acessos; identificação, descrição, tipo e localização dos espaços acedidos, data e hora dos acessos).....</i>	<i>161</i>
<i>Figura 8.20 – Página Auditar Acessos a Espaços com selecção do espaço físico a auditar.....</i>	<i>162</i>
<i>Figura 8.21 – Visualização parcial com os dados do espaço físico a auditar entre duas datas</i>	<i>162</i>
<i>Figura 8.22 – Listagem dos acessos de utilizadores efectuados ao espaço físico, entre as datas assinaladas (ordenada por identificação do utilizador e data/hora do acesso).....</i>	<i>163</i>
<i>Figura 8.23 – Visualização parcial, com os dados do utilizador, listagem dos espaços físicos cujo utilizador tem permissão de acesso e selecção do espaço físico</i>	<i>164</i>
<i>Figura 8.24 – Página dos acessos do utilizador a um determinado espaço físico.....</i>	<i>165</i>
<i>Figura 8.25 – Visualização parcial, com enumeração dos principais atributos do utilizador e do espaço físico, datas de parametrização de pesquisa e lista dos acessos do utilizador efectuados ao espaço físico, entre as datas mencionadas</i>	<i>165</i>
<i>Figura 0.1 – Modelo conceptual dum sistema biométrico genérico e seus subsistemas [4].....</i>	<i>181</i>
<i>Figura 0.2 – A lógica dos passos dum sistema biométrico [30]</i>	<i>183</i>
<i>Figura 0.3 – Exemplo do processo de registo (enrollment) [11].....</i>	<i>183</i>
<i>Figura 0.4 – Exemplo do Processo de Verificação [6]</i>	<i>184</i>
<i>Figura 0.5 – Exemplo do Processo de Identificação [6]</i>	<i>184</i>
<i>Figura 0.6 – Gráfico representativo das alterações das taxas FRR e FAR consoante o valor crítico ERR</i>	<i>185</i>

Índice de Tabelas

<i>Tabela 1 – Sumário de códigos de barras standard e suas utilizações [7]</i>	<i>12</i>
<i>Tabela 2 – Resumo das Características Técnicas e Mecanismos de Segurança dos Standards RFID: ISO/IEC 14443 e ISO/IEC 15693</i>	<i>57</i>
<i>Tabela 3 – Características e Especificações dos Cartões de Proximidade (contactless smart cards) que utilizam os Protocolos ISO/IEC 14443 e ISO/IEC 15693 [13]</i>	<i>58</i>
<i>Tabela 4 – Resumo das Características Técnicas e Mecanismos de Segurança dos Standards RFID: EPCglobal Class-1 Generation-2 e ISO/IEC 18000-6C</i>	<i>58</i>
<i>Tabela 5 – Representação hierárquica dos espaços físicos, ...</i>	<i>128</i>

Acrónimos e Siglas

AIDC – *Automatic Identification and Data Capture*

CSS – Folhas de Estilo em Cascata (*Cascading Style Sheets*)

DEEC – Departamento de Engenharia Electrotécnica e de Computadores

EPC – Código Electrónico de Produto (*Electronic Product Code*)

ERR – Taxa de Erro Igual (*Equal Error Rate*)

FAR – Taxa de Falsa Aceitação (*False Acceptance Rate*)

FEUP – Faculdade de Engenharia da Universidade do Porto

FRR – Taxa de Falsa Rejeição (*False Rejection Rate*)

GUI – Interface Gráfica do Utilizador (*Graphical User Interface*)

HTML – Linguagem de Marcação de HiperTexto (*HyperText Markup Language*)

HTTP – Protocolo de Transferência de Hipertexto (*Hypertext Transfer Protocol*)

ICC – *Integrated Circuit Chip*

IEEE – *Institute of Electrical and Electronics Engineers*

IMAP – *Internet Message Access Protocol*

ID – Identificação (*Identification*)

IP – *Internet Protocol*

ISO/IEC – *International Organization for Standardization / International Electrotechnical Commission*

I&D – Investigação e Desenvolvimento

LAN – Rede de Área Local (*Local Area Network*)

LDAP – *Lightweight Directory Access Protocol*

NNTP – *Network News Transfer Protocol*

ODBC – *Open Data Base Connectivity*

PIN – Número de Identificação Pessoal (*Personal Identification Number*)

PKI – Infra-Estruturas de Chaves Públicas (*Public Key Infrastructures*)

POP3 – *Post Office Protocol*, 3 version

RF – Radiofrequência (*Radio Frequency*)

RFID – Identificação por Radiofrequência (*Radio Frequency Identification*)

RH – Recursos Humanos

SGBD – Sistema de Gestão de Base de Dados

SOAP – *Simple Object Access Protocol*

SMS – *Short Message Service*

SNMP – *Simple Network Management Protocol*

SQL – *Structured Query Language*

SSL – *Secure Sockets Layer*

TCP/IP – *Transmission Control Protocol / Internet Protocol*

TI – Tecnologia(s) de Informação

UML – Linguagem de Modelação Unificada (*Unified Modeling Language*)

USA – Estados Unidos da América (*United States of America*)

VLAN – Redes Virtuais de Área Local (*Virtual Local Area Network*)

XML-RPC – *Extensible Markup Language - Remote Procedure Call*

WAN – Rede de Área Alargada ou de Longa Distância (*Wide Area Network*)

WPA – *Wi - Fi Protected Access*

Capítulo 1

Introdução

Neste capítulo é apresentado o enquadramento deste trabalho, juntamente com as principais motivações associadas à sua realização. Seguidamente, apresenta-se a estrutura e organização desta dissertação.

1.1 Enquadramento e Motivação

Recentes alterações relacionadas com o mundo laboral têm vindo a intensificar os problemas que se prendem com a devida e conveniente identificação das pessoas. Os tempos da mão-de-obra estável, em que os empregados e colaboradores se reconheciam visualmente, estão tendencialmente a acabar. Na conjectura laboral e organizacional actual, as empresas e instituições estão, cada vez mais, com sérias dificuldades em realizar os seus trabalhos específicos, com a exigência constante e crescente de rotatividade dos seus empregados e consequente intensificação da necessidade de recorrer ao apoio de colaboradores externos. Esta dinâmica, tem provocado ambientes organizacionais que se caracterizam pela presença de novos colaboradores, de pessoal novo, estranho e pouco reconhecido, que para efectuarem os seus trabalhos necessitam, porém, de ter acesso a recursos e a informações das organizações. Ao acrescentar-se a isto, a dimensão e a complexidade de muitas destas organizações ou instituições, está criado o ambiente propício para que, no interior das mesmas, muitos dos seus utentes possam vir, impropriamente, a obter acessos indevidos a determinados recursos.

Com este cenário, a verificar-se, sobretudo, em grandes instituições estatais ou grupos multinacionais e, mesmo, em empresas de média dimensão, tem-se acentuado uma procura crescente de sistemas de segurança, que tem conduzido a que a questão da gestão dos acessos a recursos organizacionais, ultimamente, tenha vindo a assumir uma importância progressiva pelas mais diversas instituições. Actualmente, qualquer organização, por mais inócua ou imparcial que seja, reconhecerá dos perigos relacionados com as questões de segurança, ou sua omissão, concretamente, os que respeitam com a obtenção ou concessão de acessos aos seus recursos internos. A gestão de acessos nas organizações respeita, basicamente, à gestão e controlo dos acessos físico e lógico, geridos de modo independente ou integrado, com o intuito de impedir que os seus recursos físicos e “intelectuais” possam ser furtados ou comprometidos. O controlo de acessos físico é dirigido, em especial, à protecção dos acessos a recursos ou bens tangíveis da organização, enquanto, o lógico visa, essencialmente, limitar o acesso a dados informáticos, redes ou estações de trabalho. Mas, actualmente, a questão que se tem vindo a evidenciar como pertinente, é a necessidade de serem protegidas localizações, áreas ou espaços físicos no interior das organizações. Daí que a introdução de sistemas de controlo de acessos físico, que actuem selectivamente na permissão dos

acessos a determinadas instalações, são de grande importância, pois, quando aplicados adequadamente, permitem controlar, de modo eficaz, o acesso dos seus utentes a determinados espaços físicos de acesso restrito. Por via da necessidade de implementação destes sistemas, consequentemente, serão também indispensáveis os sistemas de informação que, de modo adequado, os possam gerir, os sistemas de *software* destinados a resolver a complexidade associada à gestão dos acessos e que facilitam a sua automatização e monitorização. Um sistema de gestão de controlo de acessos físico, utilizado na protecção de bens e recursos empresariais, será, portanto, uma ferramenta de segurança útil e de grande importância, em geral, suportando múltiplas funcionalidades de gestão e monitorização dos sistemas de controlo de acessos físico das organizações. É neste contexto e tomando por base a constatação da importância e utilidade, actuais, destes sistemas, que o presente trabalho procura, em síntese, não só caracterizar os principais conceitos associados à problemática dos sistemas de controlo de acessos físico e sua gestão, como também, estabelecer as linhas gerais relativas à concepção, desenvolvimento e implementação dum sistema de *software* de gestão de acessos físico em organizações, concretamente, de uma aplicação *web* de gestão de sistemas de controlo de acessos físico, adequada a um *campus* universitário. O desenvolvimento deste trabalho justifica-se, assim, pela premência e necessidade, actuais, do estudo deste tipo de sistemas e problemática associada, bem como, pelo significativo impacto que os resultados da sua implementação produzem nas organizações, tencionando, também, que os interessados, em geral, consolidem uma percepção mais clara das potencialidades relacionadas com as aplicações de *gestão de controlo de acessos físico*.

1.2 Estrutura da Dissertação

No Capítulo 2, são apresentados os conceitos de identificação, autenticação e autorização, utilizados no processo de controlo de acessos, sendo também caracterizados os principais mecanismos de autenticação e a sua principal forma, a autenticação de factor múltiplo. É dada uma visão global das principais tecnologias de identificação e autenticação, pela caracterização particular de cada tecnologia utilizada nos sistemas de controlo de acessos, com especial relevo para a tecnologia *RFID*, assente em *smart cards*, e para os diferentes tipos de tecnologias biométricas.

No Capítulo 3, é apresentada uma visão genérica dos sistemas de controlo de acessos físico, em particular, os suportados por tecnologia *RFID*, em que é definida a arquitectura geral destes sistemas e seus subsistemas. Ainda, nestes sistemas, são caracterizados os principais componentes, intervenientes no processo de controlo de acessos, os dados e comunicações, nomeadamente, ao nível da infra-estrutura de rede, dos protocolos de comunicação de dados, dos factores operacionais críticos de comunicação e dos controlos técnicos de segurança mais relevantes. É de salientar que, neste capítulo, as abordagens e análises são efectuadas segundo duas perspectivas, a dos sistemas de controlo de acessos físico e a dos sistemas *RFID*, que se relacionam e integram.

No Capítulo 4, é apresentado o problema concreto da gestão dos acessos (físico) em universidades. Para compreensão do domínio do problema são descritos e caracterizados os principais conceitos relativos à gestão de controlo de acessos físico, entre os quais, a estrutura dos espaços físicos das organizações, o modelo de controlo de acessos baseado no papel e as principais políticas de segurança. Também são apresentados os objectivos e o impacto esperado da aplicação *WebGPACS* (aplicação *web* de gestão de sistemas de controlo de acessos físico) a ser desenvolvida.

No Capítulo 5, são apresentados os requisitos gerais e funcionalidades essenciais que deverão ser satisfeitos por um sistema de *software* de gestão de sistemas de controlo de acessos físico, de âmbito alargado. Para uma primeira fase de desenvolvimento, no âmbito deste trabalho, é apresentado o modelo de casos de utilização do sistema e, por último, através dum diagrama de classes, o modelo de objectos do domínio e respectiva descrição.

No Capítulo 6, são definidas as arquitecturas do sistema de *software* e o seu suporte tecnológico. Inicialmente, a arquitectura lógica, em que são apresentados os pacotes de componentes e o diagrama respectivo. Seguidamente, a conceptualização da infraestrutura física (computadores e redes), a arquitectura física, que suporta a implementação do sistema. Um diagrama de distribuição em *UML* retrata o ambiente de *hardware*, no qual são executados os componentes de *software* da aplicação. Por fim, são apresentadas e caracterizadas, de modo genérico, as tecnologias de suporte, isto é, as tecnologias utilizadas para desenvolvimento da aplicação.

No Capítulo 7, são descritos os aspectos mais relevantes relativos à implementação da aplicação *WebGPACS*. Inicialmente, de modo sucinto, apresenta a estrutura e a configuração do sistema, utilizadas para implementação da aplicação, assim como, é mostrado o desenho de dados, através do diagrama *E-R* da base de dados e correspondente descrição das entidades e atributos. De seguida, é definido e caracterizado, em especial, o *modelo de gestão de dados hierárquicos* utilizado para lidar, em concreto, com a tabela de *espaços físicos* (dados hierárquicos) da aplicação, sendo expostas e explicadas, em detalhe, as principais expressões *MySQL* do modelo. Por fim, são apresentadas todas as interrogações da aplicação *WebGPACS* que foram utilizadas no acesso à tabela de *espaços físicos* (dados hierárquicos) da base de dados da aplicação.

No Capítulo 8, é apresentado um caso de estudo, com base num cenário de gestão de controlo de acessos (físico) num ambiente universitário, para validação de resultados de utilização da aplicação *WebGPACS*, desenvolvida neste projecto. São descritas e exemplificadas algumas das suas principais formas de utilização, testadas e validadas funcionalidades de vários casos de utilização, demonstrados resultados e *interfaces* da aplicação.

No Capítulo 9, as conclusões que retratam, genericamente, o trabalho desenvolvido e, mais detalhadamente, as funcionalidades implementadas da aplicação. Também são apresentadas perspectivas para trabalhos e desenvolvimentos futuros, nomeadamente,

funcionalidades da aplicação a implementar, igualmente, de modo discriminado, e uma ideia de prestação de serviços de gestão de controlo de acessos físico para organizações.

No Anexo A, em traços gerais, é apresentada a visão geral dum Sistema Biométrico (genérico) e suas principais características.

No Anexo B, são apresentadas as descrições textuais, em formato alto-nível, dos casos de utilização de diagramas do Modelo de Casos de Utilização da aplicação *WebGPACS*.

No Anexo C, é apresentada uma listagem parcial do Código da aplicação *WebGPACS*, que contempla a demonstração do código de, apenas, duas funcionalidades: “Editar Espaços” e “Auditar Acessos a Espaço por Utilizador”.

No Anexo D, são apresentadas as Interrogações *MySQL* de acesso à base de dados, utilizadas pela aplicação *WebGPACS*. Exceptuam-se as que foram utilizadas no acesso à tabela de *espaços físicos* (dados hierárquicos).

No Anexo E, é apresentado um aditamento ao Capítulo 9 “Conclusões” desta dissertação, em que são mencionados alguns dos benefícios e especificidades dos Serviços de “Gestão de Controlo de Acessos” para organizações.

Capítulo 2

Identificação e Autenticação (Conceitos, Mecanismos e Tecnologias)

2.1 Introdução

Neste capítulo são apresentados os conceitos de identificação, autenticação e autorização utilizados no processo de controlo de acessos, sendo também caracterizados os principais mecanismos e formas de autenticação. É dada uma visão global, pela caracterização particular, das principais tecnologias de identificação e autenticação utilizadas nos sistemas de controlo de acessos, com especial relevo para a tecnologia *RFID*, assente em *smart cards*, e para os diferentes tipos de tecnologias biométricas.

2.2 Identificação, Autenticação e Autorização

Esta secção apresenta os principais conceitos relativos à identificação, autenticação e autorização utilizados no processo de controlo de acessos.

2.2.1 Identificação

A *identificação* traduz-se pelos procedimentos de solicitação da identidade de um utilizador que deseje aceder a um serviço prestado. Por *identificação* entende-se o conjunto de técnicas que se utilizam para se obter o conhecimento da identidade de uma outra parte, no entanto, este processo não prova da identidade indicada pela parte. Quando se pede a identidade duma pessoa ou utilizador, pretende-se adquirir a garantia de que a pessoa ou utilizador que solicita o pedido do serviço terá o direito de aceder ao serviço que pretende. Este processo de *identificação* é realizado com o objectivo de se assegurar a *confidencialidade e integridade* da informação.

2.2.2 Autenticação

A *autenticação* é o processo pelo qual uma pessoa prova a sua identidade. A autenticação caracteriza-se pelo fazer-se genuíno, credível ou autorizado; é uma validação da identidade. Por exemplo, se a fotografia da face duma pessoa X foi emitida num determinado cartão de *identificação*, a autenticação dessa pessoa X verifica-se,

através do processo de demonstração que a sua face corresponde à face da fotografia do cartão. A autenticação é o processo de prova de que a pessoa *X* é a pessoa identificada no cartão de *identificação* [13].

Em geral, *identificação* e *autenticação* são utilizadas como dois conceitos sobrepostos, sendo a *autenticação* vista como fazendo parte da *identificação*. Este problema tem sido resolvido pela utilização dum nome de utilizador (*username*) e duma senha (*password*), que se utilizam respectivamente para identificar e autenticar uma pessoa. Por exemplo, quando uma pessoa *Y* se quer identificar a uma pessoa *Z*, envia o seu nome de utilizador (*username*) à pessoa *Z*. Agora, a pessoa *Z* vai pretender certificar-se se a pessoa *Y*, que se apresentou como sendo “*Y*”, é a verdadeira e não outra a fazer-se passar por ela., então, a pessoa *Z* solicita à pessoa *Y* que lhe mande a sua senha (*password*), pessoal e secreta. Se a pessoa *Y* souber a verdadeira senha (*password*), a pessoa *Z* pode considerar e ficar certa de que, realmente, está a comunicar com a verdadeira pessoa *Y*.

2.2.3 Autorização

A *autorização* é o processo pelo qual, a uma pessoa ou utilizador autenticado, é concedido o acesso autorizado a determinados recursos protegidos [13]. A *autorização* é o acto de conferir ou outorgar legalidade. O acesso autorizado a um recurso protegido, área ou sistema controlados, começa por requerer a identificação e a autenticação da pessoa ou utilizador que solicita esse acesso. A partir da efectiva autenticação do utilizador, o sistema de concessão de *autorização* deverá estar configurado de modo a validar se o mesmo utilizador está autorizado a aceder ao recurso em questão, para o qual solicitou o acesso. Este processo de autorização é, em parte, uma verificação ou validação da autorização de acesso – “*Tem, actualmente, permissão para fazer ou aceder ao que está a tentar fazer ou aceder?*” – e que pode ser implementado, tanto por métodos manuais, como automáticos [1].

Em geral, as permissões de acesso são atribuídas pelos administradores ou responsáveis do sistema de acesso, e podem ser, ao longo do tempo, alteradas, revogadas ou suspensas [9]. Para serem registados estes direitos ou permissões de utilizadores, podem ser utilizadas várias formas (entre as quais, “listas de controlo de acesso”,...) e o critério subjacente à atribuição, a um utilizador, duma autorização de acesso a um recurso protegido, não só envolve a avaliação da necessidade de acesso desse utilizador ao recurso, como também, o conhecimento da política de segurança da organização e sua conformidade [1].

2.3 Mecanismos de Autenticação e Factor Múltiplo

Esta secção apresenta os principais mecanismos de autenticação e a forma de autenticação de factor múltiplo utilizados no processo de controlo de acessos.

2.3.1 Mecanismos de Autenticação

A *identificação* e *autenticação* de utilizadores são dos principais aspectos a serem considerados para se garantir a segurança dum sistema operacional. O componente principal do processo do controlo de acessos é a *autenticação*, duma pessoa ou utilizador, pois garante que um utilizador é de facto quem alega ser, sendo uma das funções de segurança mais importantes que um sistema operacional deve possuir. Se não for confiável e um utilizador conseguir “enganar” o sistema de *autenticação*, fingindo ser outra pessoa, todos os demais itens relacionados com a segurança serão inúteis.

Existem vários *factores* ou *mecanismos de autenticação*, baseados fundamentalmente:

- No *Conhecimento* (algo ou alguma coisa que o utilizador sabe ou conhece)
 - *PIN*
 - senha (*password*)
- Na *Posse* (algo ou alguma coisa que o utilizador tem ou possui)
 - chave convencional
 - cartão magnético
 - *token* ou cartão - *smart card*
 - documentos visíveis e tangíveis (carta de condução, passaporte,...)
- Nas *Características* (algo ou alguma coisa que se é, uma ou mais características inerentes ao utilizador, que se possam verificar por comparação biométrica)
 - impressão digital
 - assinatura
 - voz
 - íris ou retina
 - geometria da mão
- Na *Localização* (algum lugar onde o utilizador se situa)

2.3.1.1 No Conhecimento

O *mecanismo de autenticação baseado no conhecimento*, em geral, constituído pelo nome de utilizador (*username*) e senha (*password*), é o *factor* mais antigo e mais utilizado. Possui uma série de deficiências que o tornam vulnerável, uma vez que se baseia na memória dos utilizadores e estes, por natureza, estão sujeitos a esquecimentos. Além disso, requer imaginação para se criar senhas (*passwords*) genuínas. Outros problemas não só advêm da forte possibilidade das mesmas poderem ser furtadas ou descobertas, como também, da sua difícil administração na utilização (se uma senha é

“fraca”, pode ser facilmente descoberta; se é “forte”, é facilmente esquecida),... Um sistema de *autenticação* que se baseie, somente, na utilização de senhas (*passwords*) não garante, por si só, a efectiva autenticidade do utilizador. Uma vantagem da utilização deste mecanismo é o seu baixo custo, uma vez que pode ser utilizado em qualquer tipo de ambiente e sem necessidade de qualquer equipamento especial.

2.3.1.2 Na Posse

O *mecanismo de autenticação baseado na posse* constitui-se, na maioria dos casos, pela usufruição ou detenção de cartões, *smart cards*, por parte de um determinado utilizador. Este método pode ser aperfeiçoado, através da utilização conjunta dos *PIN* e de senhas (*passwords*). Uma desvantagem, é os cartões, devido ao seu tamanho pequeno, poderem ser facilmente perdidos ou furtados e, outra, será a necessidade de equipamento especial para “leitura” dos mesmos, o que torna o sistema dispendioso. Um aspecto positivo revela-se pelo facto deste factor ou mecanismo poder adicionar um nível de protecção suplementar ao de utilização de senhas (*passwords*).

2.3.1.3 Nas Características Pessoais

O *mecanismo de autenticação baseado nas características pessoais* utiliza os factores biométricos da pessoa ou utilizador em causa. A biometria, sob o ponto de vista da segurança, refere-se a métodos automatizados de *identificação* de pessoas, baseados em características físicas ou aspectos comportamentais singulares. Esta tecnologia analisa características físicas e comportamentais humanas, tais como, as impressões digitais, a retina, face, padrão de voz, assinatura,... A impressão digital é a técnica de biometria mais utilizada, fundamentalmente, devido ao facto de ter um custo menos dispendioso e menor dificuldade de implementação. A vantagem da biometria em relação a outras tecnologias é que, através deste mecanismo, o utilizador é autenticado com base nas suas características pessoais, únicas e intransmissíveis, o que dispensa a utilização de senhas (*passwords*) e, mesmo, de cartões. Nos últimos tempos, a utilização da biometria tem crescido bastante, principalmente, devido à diminuição do custo dos dispositivos de *autenticação biométrica*. A principal desvantagem é a de requerer equipamento especial para aquisição de informação biométrica dos utilizadores e, em geral, esse equipamento, apesar da crescente diminuição do seu custo, ainda, é dispendioso.

2.3.1.4 Na Localização

O *mecanismo de autenticação baseado na localização* tem como base a localização geográfica do utilizador a ser autenticado. Devido à complexidade de implementação deste tipo de autenticação, são, ainda, poucos os sistemas que o utilizam. Por mero exemplo, cita-se a *autenticação*, através da comunicação *GPS*, da utilização de endereços *TCP/IP*, número de série de placas de rede,...

2.3.2 Autenticação de Factor Múltiplo

O nível de segurança obtido por um método de *autenticação* pessoal, tal como, um cartão (*smart card*), uma chave ou um *token*, é aumentado à medida que o número de *factores de autenticação* aumenta [1]. Assim, para se alcançar um nível elevado de segurança, utiliza-se uma autenticação que combina vários *tipos* ou *mecanismos de autenticação*, a *autenticação de factor múltiplo* [22]. A segurança da *autenticação* pessoal aumenta significativamente, quando se combinam as tecnologias e técnicas de *autenticação*, em especial, quando se combinam *diferentes factores de autenticação*. A autenticação pode ser efectuada por uma das seguintes formas:

- *um factor simples de autenticação* (utilização, apenas, de um dos *factores de autenticação*)
 - um *PIN* ou uma senha (*password*)
 - ...
- *dois factores de autenticação* (se forem utilizados na autenticação dois *factores de autenticação diferentes*)
 - um *PIN* e um cartão
 - uma senha (*password*) e um *token de ID*
 - um cartão e uma assinatura
 - ...
- *três factores de autenticação* (se todos os três *factores de autenticação* forem utilizados e *diferentes*)
 - um *PIN*, um *token de ID* e uma impressão digital
 - ...

A Figura 2.1 seguinte é elucidativa, quanto à relação da utilização de vários *factores de autenticação* com os níveis de segurança atingidos.

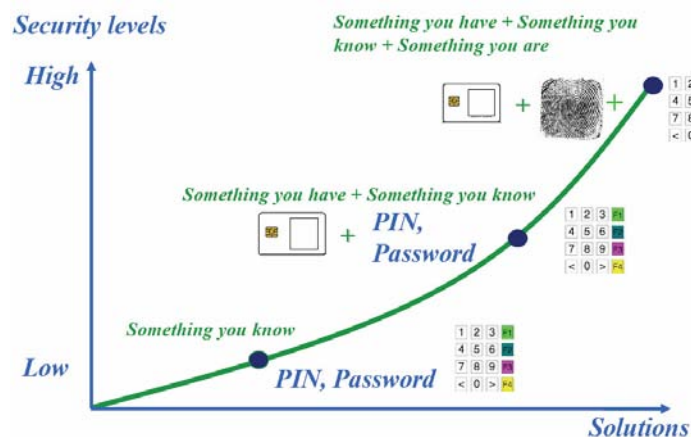


Figura 2.1 – Relação da utilização de vários factores de autenticação com os níveis de segurança atingidos [29]

Pela combinação de dois ou três *factores de autenticação*, pode-se atingir um tipo de autenticação “forte” que poderá, ou não, ser suficiente para as diferentes necessidades. Por exemplo, um cartão (*smart card*) poderá ser combinado com um *PIN* e serem apresentados conjuntamente. Neste caso, para se obter um método de autenticação mais seguro utilizaram-se *dois mecanismos de autenticação (algo possuído e algo conhecido)*.

A autenticação “forte” inclui no mínimo *dois mecanismos de autenticação diferentes*, geralmente, algo que se possui e algo que se conheça. É também apelidada de *autenticação de dois factores*, por serem utilizados *dois mecanismos de autenticação diferentes*. Um exemplo deste tipo de autenticação é a utilização do cartão multibanco, *algo possuído*, e do número de código pessoal, *algo conhecido*, utilizados nas transacções multibanco. Para uma autenticação “forte” é recomendado fazer uso de algo ou de alguma coisa que se conheça [33].

2.4 Tecnologias de Identificação e Autenticação

As secções que se seguem, vão proporcionar a visão global das principais tecnologias de identificação e autenticação. Cada uma destas tecnologias será caracterizada singularmente, dando-se especial relevo à tecnologia RFID, suportada por *smart cards*, e aos principais tipos de tecnologias biométricas.

2.4.1 Crachás de ID

Os *crachás de ID* são, frequentemente e essencialmente, utilizados como um meio de identificação visual dos seus utilizadores. Ao longo do tempo, muitas das suas características de impressão (por ex., hologramas, tintas ópticas, micro-impressões,...) têm vindo a ser desenvolvidas e adicionadas, permitindo que este tipo de identificadores seja mais facilmente verificado por inspecção visual [9].

Estes *crachás* podem ter várias formas e ser de tipo *personalizado*, *cores codificadas* e *enumerados*. Os de tipo *personalizado*, depois de prova de identidade do seu detentor, podem suportar diversos níveis de personalização, tal como, a inclusão de informação de identificação (nome, fotografia, assinatura,...) que será utilizada para autenticar o seu utilizador. Um crachá de *cores codificadas*, como a própria designação sugere, é um cartão colorido cuja diferenciação de cores pode servir para distinguir, por categorias, os seus utentes. São geralmente utilizados para identificação de visitantes, quando pretendem aceder ao interior duma determinada organização, edifício ou local de trabalho [1]. Os crachás *enumerados*, são numerados e costumam, também, ser entregues a visitantes, em locais de controlo de acessos, como troca de prova de identidade, depois da sua apresentação e devida autorização.

Os *crachás de cores codificadas*, *enumerados* e *personalizados* fornecem um nível de segurança mínimo de autenticação pessoal, podendo facilmente ser copiados, furtados

ou falsificados. Não obstante, seja necessário um nível de aptidão relativamente elevado para ser alterado ou falsificado um *crachá* personalizado, actualmente, com as tecnologias existentes, “que se estão a vulgarizar”, é relativamente fácil, acessível e pouco dispendioso. Para o incremento do nível de garantia de segurança, o *crachá* deverá ser combinado com métodos de autenticação adicionais [1].

2.4.2 Código de Barras

Um *código de barras* é uma imagem de linhas ou barras sequenciais, de largura e de espaço variado, que podem ser afixados em artigos comerciais, em cartões de *ID*, em correio postal,... Servem para a representação de números e outros símbolos, na identificação dum código de produto, duma pessoa ou duma localização. Os *códigos de barras* que armazenam informação pessoal podem ser impressos em cartões, geralmente de plástico, sendo os dados pessoais representados em *código de barras* e integrados no cartão, durante o processo de impressão. O cartão é depois “lido”, através dum leitor de código de barras que utiliza um feixe *laser* sensível às reflexões das linhas, da suas espessuras e à variação dos espaços entre as mesmas. Os *códigos de barras* podem ser copiados facilmente, através da utilização dum normal e simples fotocopiador, o que impossibilita a sua utilização em aplicações que exijam um nível de segurança mais elevado [7].



Figura 2.2 – Etiqueta com código de barras

Os *códigos de barras lineares (de uma dimensão)* são utilizados para armazenar dados simples, alfanuméricos (por ex., em aplicações de comércio retalhista), e para facilitar a leitura automática de pequenos números ou dígitos decimais (por ex., números de série dum produto ou de identificação dum utilizador). Os *códigos de barras bidimensionais (2-D)* permitem armazenar uma quantidade maior e mais significativa de dados (até 1108 bytes) num pequeno espaço, preferivelmente, numa superfície de impressão lisa e de plástico [9]. A Tabela 1 seguinte, sumaria os *códigos de barras standards* e suas aplicações.

Tabela 1 – Sumário de códigos de barras standard e suas utilizações [7]

Código de barras “standard”	Utilizações
Uniform Product Code (UPC)	Armazéns de retalho para vendas caixa/saída; inventário
Code 39 (Code 3 of 9)	Identificação, inventário e rastreio de expedições
Code 128	Utilizado de preferência ao Code 39 por ser mais compacto
PDF417	Um novo código de barras de 2-D que pode codificar até 1108 bytes de informação e tornar-se, também, num ficheiro de dados (PDF) comprimido e portátil

2.4.3 Bandas Magnéticas

Desde os anos 70 que as *bandas magnéticas* têm vindo a ser utilizadas, em cartões, para um grande número de aplicações, nomeadamente, em cartões bancários (débito/crédito), cartas de condução, *cartões de controlo de acessos (físico/lógico)*,... A *banda magnética*, situada na parte detrás do cartão de *ID*, é composta por partículas magnéticas revestidas por uma fita de plástico. A informação de identificação é gravada, por comunicação magnética, e é adquirida ou lida, através de *leitores de banda magnética*. Os dados codificados em *bandas magnéticas* não só podem, facilmente, ser copiados e interpretados, através da utilização dum *leitor magnético*, como também, transferidos para um outro cartão. Este facto, proporciona que esta *tecnologia de banda magnética* seja mais aplicável em aplicações que não exijam grande segurança (de baixa segurança) [7].

Nos cartões de plástico podem ser utilizados diferentes tipos de *bandas magnéticas*. O *standard ISO/IEC 7811* define as várias opções para codificação interoperável da informação da *banda magnética* e, dependendo da densidade e da codificação utilizada, é possível armazenar entre 100 e 150 bytes de informação [9].

2.4.4 Bandas Ópticas

Inicialmente, esta tecnologia, similar à tecnologia de gravação laser de *CD*, foi projectada para ser utilizada em registos médicos portáteis, sendo a codificação óptica utilizada, em cartão de plástico (*ISO/IEC 7810 ID1*), apenas, quando se necessita de armazenar uma quantidade muito elevada de informação [9]. Esta informação é armazenada em disco compacto, tipo *CD*, em que se recomenda que esteja dentro dum revestimento protector para que, na utilização normal, sejam reduzidos possíveis danos no material de armazenamento óptico. Os *cartões de banda óptica* são uma tecnologia que necessita de equipamento externo para leitura, escrita e processamento de informação. Utilizam uma tecnologia semelhante à da leitura e escrita de *CD*, a tecnologia de gravação *WORM (Write Once Read Many)*, que permite, apenas, que os dados sejam lidos ou adicionados e, não, cortados ou apagados. Os *cartões de banda óptica* possuem uma elevada capacidade de memória (múltiplos *megabytes*) não volátil

e são utilizados na identificação, em serviços médicos, na gestão logística e noutras aplicações que requeiram armazenamento de grande quantidade de dados [7]. O custo elevado dos seus leitores, limita esta tecnologia, somente, a aplicações em que um leitor possa ser utilizado por dezenas de milhar de cartões [9].

2.4.5 USB

O *USB (Universal Serial Bus)* é uma interface “*plug-and-play*” que faz a ligação entre um computador e outros dispositivos (áudio, *joysticks*, teclados, telefones, digitalizadores, impressoras,...). Com o *USB*, um novo dispositivo pode ser ligado a um computador sem ter que ser adicionado um adaptador ou, mesmo, desligado o computador. Actualmente, todos os computadores e dispositivos periféricos estão equipados com *USB*, que permite suportar uma grande velocidade¹ [37] de dados e, por isso, acomodar uma grande gama de dispositivos. Os *tokens de segurança USB* são dispositivos utilizados na autenticação de utilizadores, especialmente, em controlo de acessos lógico (a um computador ou rede), proporcionando armazenamento para nomes de utilizadores (*usernames*), senhas (*passwords*), *templates* biométricos, chaves criptográficas,... [7]

2.4.6 Tecnologia RFID



Figura 2.3 – Com a tecnologia RFID as soluções de identificação do futuro tornam-se realidade hoje [36]

A tecnologia *RFID* é uma tecnologia de identificação automática. Os processos de identificação, suportados por este tipo de tecnologias (*AIDC technologies*)², são significativamente mais fiáveis e menos dispendiosos do que os de tecnologias não automáticas. A tecnologia *RFID* representa um considerável avanço tecnológico, a nível

¹ O USB suporta 3 velocidades de dados: *Low Speed USB* (1.5 Mbit/seg.), *Full Speed USB* (12 Mbit/seg.), *Hi-Speed USB 2.0* (480 Mbit/seg.).

Nota: actualmente, a *USB 3.0* está projectada para uma velocidade de 4.8 Gbit (10x *Hi-Speed USB*)

² Tecnologias de Aquisição de Dados e Identificação Automática (da expressão inglesa *Automatic Identification and Data Capture Technologies*). Os Sistemas ou Tecnologias de Identificação Automática são também conhecidas por Tecnologias *AIDC*.

da identificação automática, que contém enumeras vantagens, nomeadamente: na *comunicação e transmissão de dados*, que pode ocorrer sem linha de visão óptica, uma vez que as ondas electromagnéticas de radiofrequência podem atravessar diversos materiais; na *velocidade do processo*, dado que muitas *tags* e *smart cards* podem ser lidos mais rapidamente; na *distância de leitura de dados*, pois as diversas tecnologias de radiofrequência podem transmitir e receber sinais a maiores distâncias do que outras tecnologias. A capacidade da tecnologia *RFID* em comunicar sem linha de visão óptica e à distância, sem necessidade de contacto físico, reduz sensivelmente o envolvimento pessoal ou humano no processo de identificação. Além disso, a tecnologia *RFID* pode também suportar características funcionais, que outras tecnologias não possuem, tais como, memória regravável, funcionalidades de segurança, sensores ambientais,...

2.4.6.1 Tecnologias *RFID* para o Controlo de Acessos Físico

Para aplicações de controlo de acessos físico, existem três principais tecnologias de proximidade (*RFID*):

- *125 KHz*
- *ISO 14443*
- *ISO 15693*

2.4.6.1.1 Tecnologia *125 KHz*

A tecnologia de *125 kHz* é somente de leitura, é a mais antiga e, ainda, utilizada por muitos dos actuais sistemas de controlo de acesso físico baseados em *RFID* [10]. A tecnologia de *125 kHz* permite um único e seguro número de código, que será, depois, transmitido ao sistema do *host system*³ com o objectivo de poder ser processado e de se averiguar dos direitos e privilégios associados ao respectivo cartão.

2.4.6.1.2 Tecnologias *ISO 14443* e *15693*

A tecnologia de proximidade dos cartões *smart cards* está baseada nos standards *ISO 14443* e *ISO 15693* (ver secção §3.5.2.1 “Comunicação *Tag – Reader*”, pág. 56). Os cartões que atendem a estes *standards* são “inteligentes”, permitem a leitura/escrita, são capazes de armazenar diferentes tipos de dados e de operarem a diferentes distâncias. Têm capacidade de processamento, tanto para autenticar a identidade de uma pessoa, como para determinar o nível adequado do acesso, tudo isto, a partir dos dados armazenados no *chip* do cartão. Estes cartões podem, também, incluir factores adicionais de autenticação (tais como, modelos biométricos, números de identificação pessoais,...) e outras tecnologias associadas ao cartão, inclusive um *chip* de contacto,

³ Também referido por *head-end system* ou *back-end system*

para satisfação de exigências relacionadas com aplicações legadas ou outras, nas quais é mais apropriado a utilização de uma tecnologia diferente.

2.4.6.2 Cartões com *Chip* e Tecnologia *Smart Card*

Basicamente, um *smart card* poderá ser considerado um cartão que incorpora na sua estrutura um *chip de circuito integrado (ICC)*, o qual pode ser:

- *Apenas de Memória (somente memória)*
- *Um Microcontrolador com memória interna (Nota: o que inclui, efectivamente, o conceito de tecnologia smart card) [12].*

2.4.6.2.1 Cartões de Memória

Um *cartão de memória* é um cartão que contém um *chip apenas de memória*, não possuindo capacidades de execução lógica ou de cálculo, pois, simplesmente, armazena dados [7]. Estes cartões são mais económicos do que os cartões que contêm *chips microcontroladores*, mas possuem menor segurança, ao nível da sua informação, dependendo da segurança do leitor. Os cartões que utilizam *chip apenas de memória* possuem capacidade de armazenamento limitada e são utilizados, somente, em situações que requeiram um nível de segurança pequeno ou médio, não sendo convenientes em utilizações multi-aplicação [12].

Refere-se que um cartão com um *chip apenas de memória*, apesar de conter um *chip* na sua estrutura, funciona somente como um simples *cartão de memória* e, por isso, *não deverá ser considerado como um cartão smart card* ou de *tecnologia smart card*. Quando um cartão com *chip* é utilizado, apenas, como um repositório de informação, sem realizar quaisquer outras funções caracterizadoras da tecnologia *smart card* (*próprias dos chips microcontroladores*), como execução e processamento de informação (ver secção §2.4.6.2.2 “Cartões de Tecnologia *Smart Card*” seguinte, pág. 16), não deve ser considerado *cartão smart card*. Estes cartões acabam por ser, em funcionalidade, semelhantes aos “cartões de banda magnética”, proporcionando, somente, um pouco mais de segurança e uma capacidade mais elevada de armazenamento de dados [7]. *A diferença conceptual entre um cartão smart card e um cartão de memória, é que enquanto um cartão de memória, apenas, armazena dados, um cartão smart card, para além de armazenar dados, também os processa, tal como um simples computador [1].* Seguindo este conceito, deverão ser entendidos por *cartões de memória*, todos os cartões utilizados, puramente, para armazenamento de dados ou de informação, tais como os de:

- código de barras
- banda magnética
- banda óptica
- *chip (ICC - Integrated Circuit Chip) apenas de memória*
- ...

Todos estes *cartões*, “apenas de memória”, não processam informação, apenas, servem para seu repositório.

2.4.6.2.2 Cartões de Tecnologia *Smart Card*

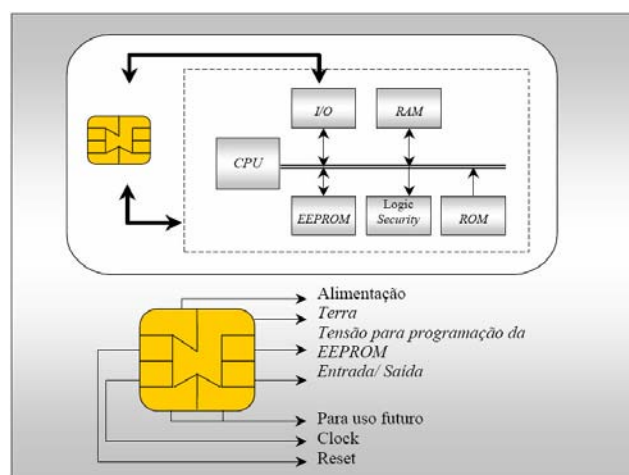


Figura 2.4 – Estrutura interna do chip microcontrolador de um smart card

Um cartão de tecnologia *smart card*, é um cartão que contém um *chip microcontrolador*, o qual pode adicionar, apagar e transferir informação na sua memória. Um *microcontrolador* é como um dispositivo computacional portátil em miniatura (com uma porta de entrada/saída, sistema operacional e disco rígido) que pode interagir com o leitor. Os *cartões smart card* com *microcontrolador* integrado têm a capacidade singular de poderem armazenar grandes quantidades de informação, realizar funções próprias (por ex., funções criptográficas ou de assinatura digital) e de interagir “inteligentemente” com um leitor de *cartões smart card* [12]. Os dados, armazenados no *chip microcontrolador* dum *cartão smart card*, oferecem muita segurança, pois são utilizados mecanismos de bloqueamento e de encriptação que executam complexos algoritmos criptográficos de protecção de confidencialidade da informação transportada, podendo ser utilizados para autenticar o utilizador [9]. Também podem executar complexas operações de computação interna, incluindo a capacidade de execução de operações de correspondência biométrica (ver Anexo A – Sistema Biométrico, pág. 181) no próprio cartão [7].

2.4.6.3 Cartões (*Smart Card*)

Dependendo do modo como se comunicam com os leitores, os cartões *smart card* podem ser categorizados em:

- *Cartões de Contacto* (quando a comunicação se efectua apenas por contacto físico directo – *contact smart card*)

- *Cartões Sem Contacto* (quando a comunicação se efectua por *interface* electromagnética de *RF – contactless smart card*) [7] [1]

Além das anteriores, ainda, existem duas categorias adicionais de cartões *smart card*:

- *Cartões de Interface Dupla*
- *Cartões Híbridos*

Todos estes cartões *smart card* podem ser utilizados em múltiplas aplicações relacionadas com diversas áreas:

- financeira
- telecomunicações
- transportes colectivos
- serviços de saúde
- segurança (*na identificação/autenticação em sistemas de controlo de acessos*)
- ...

2.4.6.3.1 Cartões de Contacto

Um *cartão de contacto* (*contact smart card*), é um cartão com *chip* que só pode ser utilizado depois de inserido num leitor de cartões, em que se estabelece uma ligação física directa entre o micromódulo condutor do cartão e o conector do leitor. A transmissão de comandos, informação e estado do cartão acontecem mediante estes pontos de contacto físico [12].

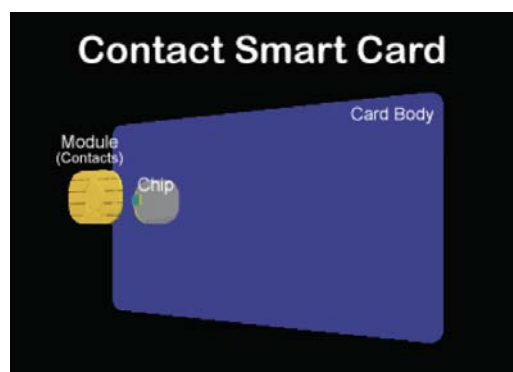


Figura 2.5 – Cartão de contacto (*contact smart card*) [29]

São geralmente utilizados em aplicações de:

- pagamentos financeiros
- telefones digitais celulares
- controlo de acessos lógico
- seguros
- identificação de estudantes [9]

2.4.6.3.2 Cartões de Proximidade

Um *cartão de proximidade ou sem contacto (contactless smart card)* para ser utilizado requer, apenas, uma aproximação a um leitor de proximidade. Tanto o cartão como o leitor possuem antenas internas para se comunicarem e trocarem dados sem contacto físico, simplesmente, através de radiação electromagnética de radiofrequência. A maioria destes *cartões* serve-se da energia, do sinal electromagnético criado pelo leitor, para a utilizar no seu *chip* interno. Existe uma variedade de tecnologias, associadas a esta categoria de cartões, com diferentes frequências de operação (*125 KHz*, a mais antiga, que não oferece interoperabilidade, e a de *13,5 Mhz*) e distâncias operacionais (ver secção §2.4.6.1 “Tecnologias *RFID* para o Controlo de Acessos Físico”, pág. 14 e secção §3.5.2.1 “Comunicação *Tag – Reader*”, pág. 56) [9].

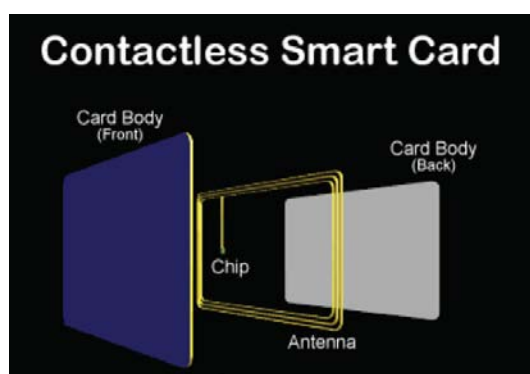


Figura 2.6 – Cartão de proximidade (*contactless smart card*) [29]

Estes *cartões de proximidade* são principalmente utilizados em aplicações de:

- *controlo de acessos físico*
- pagamento de transportes colectivos (ideal para este tipo de aplicações, que requer bastante rapidez) [12].
- pequenas transacções financeiras (porta-moedas electrónico)

2.4.6.3.3 Cartões Híbridos

Um *cartão híbrido (hybrid smart card)* possui dois *chips* não interligados:

- um que suporta uma *interface de contacto*
- outro que suporta *interface sem contacto* (de proximidade) [12]

Os dois *chips*, o de contacto e o de proximidade (*contactless*), são diferentes e estão colocados no cartão de modo distinto, não possuindo quaisquer interligações. Os *chips* estão separados de tal modo, que não existem quaisquer comandos comuns e, também, possuem características de segurança, de gestão e de estrutura de memória muito diferentes. Por tal, a informação do cartão necessita de ser sincronizada.

Como num mesmo cartão é bastante fácil a existência das tecnologias de contacto e de proximidade (sem contacto), estes cartões são, particularmente, úteis para aplicações em que seja necessário utilizar ambas as tecnologias (por ex., quando é necessário utilizar um cartão num sistema de controlo de acessos físico, que privilegia a tecnologia de proximidade, e num sistema de controlo de acessos lógico, que dá favorecimento à tecnologia de contacto) [9].

2.4.6.3.4 Cartões de *Interface Dupla*

Um *cartão de interface dupla* (*dual-interface chip smart card*) possui um único *chip* com *interface dupla*:

- de contacto
- sem contacto (de proximidade) [12].

Estes *cartões de interface dupla* fornecem, num só *chip*, ambas as funcionalidades, a de cartão de contacto e a de cartão de proximidade (*contactless*), sendo possível aos leitores, quer de contacto, quer de proximidade (sem contacto), acederem com elevada segurança ao *chip* e à sua informação [7]. Além de segurança muito elevada, em geral, possuem comportamento similar em cada uma das suas *interfaces de comunicação*, de contacto e sem contacto (*RF*), em que pode ser utilizada a mesma informação de memória, os mesmos programas aplicativos ou algoritmos de segurança. Como estes cartões possuem, somente, um único *chip*, não correm o risco da informação das diferentes aplicações estar dessincronizada [9].

São especialmente úteis em aplicações nas áreas:

- financeiras
- transportes colectivos

2.4.6.4 *Tags* (*Transponders*)



Figura 2.7 – Tag ou Tansponder

As *tags*⁴ são dispositivos electrónicos, transmissores e receptores, que comunicam com leitores *RFID*. São compostas por um *chip* ligado a uma antena, embutidos num dado

⁴ Também conhecidas por *Transponders*.

material, e possuem um mecanismo de armazenamento de informações. Cada *tag* possui um número de identificação único e, nalguns casos, *bits* (ou *kilobits*) adicionais de memória. As *tags* (ver também secção §3.4.1.1.1 “Características das *Tags*”, pág. 42), com base na sua *fonte de energia*, utilizada para comunicação ou qualquer outra funcionalidade, são categorizadas segundo quatro tipos [25]:

- *Passivas*
- *Activas*
- *Semi-Activas*
- *Semi-Passivas*

2.4.6.4.1 Passivas

Uma *tag passiva* utiliza a energia electromagnética recebida da transmissão dum *reader* para responder ao mesmo *reader*. O sinal de resposta duma *tag passiva* possui, apenas, uma fracção da energia recebida do sinal do *reader*. Esta limitação de energia restringe, significativamente, a distância operacional da *tag*, implicando que as *tags passivas* podem, somente, suportar dados de limitada complexidade. Em geral, as *tags passivas* são baratas, pequenas e mais leves do que os outros tipos de *tags*, que possuem vantagens mais consistentes, em muitas das aplicações de *RFID*.

2.4.6.4.2 Activas

Uma *tag activa* possui e baseia-se numa bateria interna para alimentar a sua energia, que é utilizada para comunicação com o *reader*, para funcionamento do seu circuito interno e execução doutras funções. As *tags activas* não só podem comunicar a maiores distâncias do que os outros tipos de *tags*, como também, responder a sinais mais fracos, uma vez que possuem um fornecimento interno de energia. São geralmente maiores, mais caras e a sua bateria tem tempo de vida finito.

2.4.6.4.3 Semi-Activas

Uma *tag semi-activa*, é uma *tag activa* que permanece inactiva até que receba um sinal do *reader* para se activar. As *tags semi-activas* podem usar a energia da sua bateria para se comunicarem com o *reader* e, tal como as *tags activas*, podem comunicar a maiores distâncias do que as *tags passivas*. A principal vantagem em relação às *tags activas* é que a sua bateria pode ter um tempo de vida mais longo. Uma desvantagem é demorarem a reagir, quando em vigília, algumas vezes, com um tempo inaceitável de demora, principalmente, quando passam pelos *readers* muito rapidamente ou quando muitas *tags* precisam de ser lidas num período de tempo muito pequeno (curto).

2.4.6.4.4 Semi-Passivas

Uma *tag semi-passiva*, é uma *tag passiva* que utiliza uma bateria para alimentar o seu circuito interno, mas não para produzir sinais de retorno. Quando a bateria é utilizada para accionar um sensor, são frequentemente chamadas *tags de sensor*. Geralmente são mais pequenas e mais baratas do que as *tags activas* e, também, possuem melhor funcionalidade do que as *tags passivas*, visto terem, em relação a estas, mais energia disponível.

2.4.7 Tecnologias Biométricas

A autenticação biométrica baseia-se no reconhecimento das características, fisiológicas e comportamentais, específicas de uma dada pessoa [35]. Desde há muito que tem sido objecto de interesse em questões de segurança, no entanto, até há pouco tempo atrás, a sua adopção restringia-se, apenas, quer por razões de natureza económica, quer tecnológica, a ambientes que exigiam níveis de segurança muito elevados (de alta segurança) e a casos de identificação criminal. Com o aperfeiçoamento contínuo desta tecnologia e, conseqüente, redução do custo dos seus dispositivos, que se tem verificado recentemente, cada vez mais, a biometria tem vindo a generalizar-se, sendo, actualmente, apontada como uma solução promissora para os processos de autenticação, nomeadamente, em sistemas de controlo de acessos físico [10]. Nas subsecções seguintes, apresenta-se uma visão geral desta tecnologia de identificação e autenticação, em que, inicialmente, se começa por abordar os principais tipos de tecnologias biométricas e sua classificação, para depois se caracterizar, singularmente, cada um dos principais ou mais utilizados tipos de biometrias (tanto fisiológicas, como comportamentais), seus respectivos benefícios e limitações (desvantagens).

2.4.7.1 Classificação e Tipos de Biometrias

As diversas tecnologias biométricas existentes podem ser classificadas em dois grupos, tendo por base as suas características: [16]

- *Fisiológicas* – grupo de tecnologias biométricas baseado em características *fisiológicas* ou *estáticas*. Traços fisiológicos que têm origem no potencial genético de cada pessoa e que variam pouco (ou nada) ao longo do tempo.
- *Comportamentais* – grupo de tecnologias biométricas baseado em características *comportamentais* ou *dinâmicas*. Características apreendidas ou desenvolvidas com a prática ou utilização contínuas e que podem variar, acentuadamente, com o passar do tempo. Também podem ser, facilmente, alteradas pela vontade ou estado físico e/ou emocional do utilizador.

Contudo, esta distinção, entre biometrias *fisiológicas* e *comportamentais*, é um tanto “artificial”, uma vez que as características comportamentais podem ser, parcialmente,

influenciadas pelas características fisiológicas e vice-versa. Algumas outras biometrias, como a voz e a assinatura, são influenciadas, tanto por características fisiológicas, como comportamentais (por ex., a voz é muito influenciada pelas estruturas fisiológicas, mas a tecnologia respectiva acentua-se bastante nas características comportamentais, tais como, a sua rapidez e pausas,...). O valor desta distinção é, no entanto, oferecer suporte relativo à compreensão funcional das tecnologias biométricas [6].

Biometrias Fisiológicas:

As principais ou mais utilizadas são:

- *Impressão Digital* (padrões da pele na ponta dos dedos)
- *Geometria da Mão* (tamanho e forma da mão)
- *Íris* (padrões do tecido à volta da pupila)
- *Face* (aparência facial, atributos geométricos do nariz, olhos, boca,...)

Outras, menos utilizadas ou em estados iniciais de pesquisa, são:

- *Retina* (padrão vascular da retina)
- *Veias* (padrão vascular das costas ou da palma da mão)
- *DNA*
- *Formato da Orelha* (tamanho e forma da orelha)
- *Odor* (odor corporal)
- *Pele* (reflectividade e padrões da pele)
- *Unhas* (tamanho e forma da unha)
- *Geometria do Dedo* (tamanho e forma dos dedos)
- *Palma da Mão* (impressão da palma da mão)
- *Estrutura Dentária* (padrão da estrutura dentária)
- *Termografia* (padrão da temperatura de partes corporais)

Biometrias Comportamentais:

As principais ou mais utilizadas são:

- *Voz* (padrão ou características da voz – por ex., frequência, pausas, rapidez)
- *Assinatura / Caligrafia* (dinâmica da assinatura ou da escrita manual – por ex., rapidez, pressão, aceleração da escrita,...)

Outras, menos utilizadas ou em estados iniciais de pesquisa, são:

- *Dinâmica de Digitação* (dinâmica da batida de teclado – por ex., duração, pausas, rapidez e aceleração da batida)
- *Andar ou Movimento* (modo ou maneira de andar)
- *Movimento Facial* (movimento da face – por ex., lábios)
- *Gestos* (movimento das mãos e braços)
- ...

2.4.7.1.1 Impressão Digital

O reconhecimento da *impressão digital* é a biometria mais antiga e conhecida. As impressões digitais formam-se, ainda, no útero materno e, salvo lesões, continuam única e consistentemente ao longo da vida. As impressões digitais, desde há 150 anos atrás, têm constituído uma parte importante nas investigações criminais e na identificação de pessoas.



Figura 2.8 – Reconhecimento da impressão digital [26]



Figura 2.9 – Terminação e divisão de sulcos [27]

O reconhecimento da *impressão digital* consiste na aquisição da formação dos sulcos da pele dos dedos. Estes sulcos possuem determinadas terminações e divisões que diferem de pessoa para pessoa.

Neste tipo de identificação, a aquisição de imagens da *impressão digital* faz-se, basicamente, por quatro tipos de tecnologias:

- *óptica* (com base na reflexão de um feixe de luz)
- *capacitiva* (baseada na criação de diferentes acumulações de carga)
- *térmica* (baseada na alteração da temperatura provocada na superfície do sensor)
- *ultra-sónica* (com base na reflexão de radiações ultra-som)

A utilização da *impressão digital* é uma das formas ou tecnologias de identificação e autenticação mais utilizadas.

Vantagens (reconhecimento da *Impressão Digital*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Cada pessoa dispõe de *impressões digitais* únicas. A *impressão digital* é uma característica distintiva inata, não existindo, praticamente, possibilidade de falsa correspondência [6]. Elevada fiabilidade, pois nunca foram encontradas duas pessoas com a mesma *impressão digital*.
- Existe uma longa tradição legal na utilização da *impressão digital* como identificador imutável. As impressões digitais não se modificam de modo natural e esta tecnologia é aceite pela maioria das autoridades institucionais.
- É um método mais estável do que outras formas de identificação e autenticação, (por ex., o reconhecimento de *íris*, da *voz*, *face*) e uma tecnologia já bastante comprovada.
- Os dispositivos utilizados para o reconhecimento são pouco dispendiosos (baixo custo), quando comparados com outros, utilizados noutras tecnologias e sistemas biométricos, tendo vindo o custo dos sensores de *impressão digital* a diminuir, significativamente, nos últimos anos. Os dispositivos de *impressão digital* em comparação com os de outras tecnologias biométricas, são bastante pequenos, requerem menos energia e menos vulneráveis às alterações ambientais (por ex., à luz e temperatura), proporcionando que esta tecnologia, cujos investimentos em I&D têm sido elevados, seja flexível e adequada para operar em ambientes difíceis e massivos.
- Tecnologia que é bastante precisa e muito comprovada. A história, já longa, desta tecnologia tem apurado a precisão técnica e proporcionado confiança pública.
- Existem grandes bases de dados legadas de *impressões digitais*.
- Conveniente para os utilizadores, sendo os sistemas de *impressão digital* fáceis de manusear.

Desvantagens (reconhecimento da *Impressão Digital*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Vulnerabilidade a distorções provocadas por sujidade e poeiras, com aumento de falhas (rejeição) pela utilização de dedos bastante sujos ou danificados. Pode ser difícil efectuar o reconhecimento de dedos poeirentos, secos, molhados ou

oleosos, para além doutras dificuldades dependentes do ângulo e pressão de colocação do dedo [6].

- As pessoas, algumas pertencentes a determinadas culturas, podem ser relutantes a colocarem os seus dedos sobre sítios, onde muitas outras o fizeram. Nalgumas culturas as *impressões digitais* não são bem aceites, uma vez que são conotadas a criminosos e questões penais (estigma criminal), pessoas iletradas ou, então, por questões higiénicas.
- Algumas pessoas não têm *impressões digitais* ou têm-nas danificadas. As linhas do dedo são frequentemente influenciadas pelas actividades manuais (por ex., na construção civil, cujas pessoas utilizam intensivamente as mãos), que podem dar origem a sujidade, escoriações ou lesões das linhas do dedo. A qualidade das *impressões digitais* varia muito no interior duma população, sendo sabido que as linhas do dedo das pessoas mais idosas se tornam mais confusas e, conseqüentemente, mais difíceis de reconhecer pelo sensor. Estima-se que cerca de 2% das pessoas têm deficientes “linhas” no dedo.
- Os sensores mais baratos podem ser comprovadamente objecto de fraude.

2.4.7.1.2 Geometria da Mão

O tamanho e forma das mãos são características particulares de cada pessoa. No processo de reconhecimento da *geometria da mão* é utilizado um dispositivo (leitor) que efectua a digitalização da geometria tridimensional da mão e dedos, uma imagem matemática digitalizada (*template*) que, depois, pode ser comparada com outra, previamente, registada numa base de dados. Os leitores que efectuem este reconhecimento da *geometria da mão* são relativamente grandes, o que os torna adequados, principalmente, para o controlo de acessos.

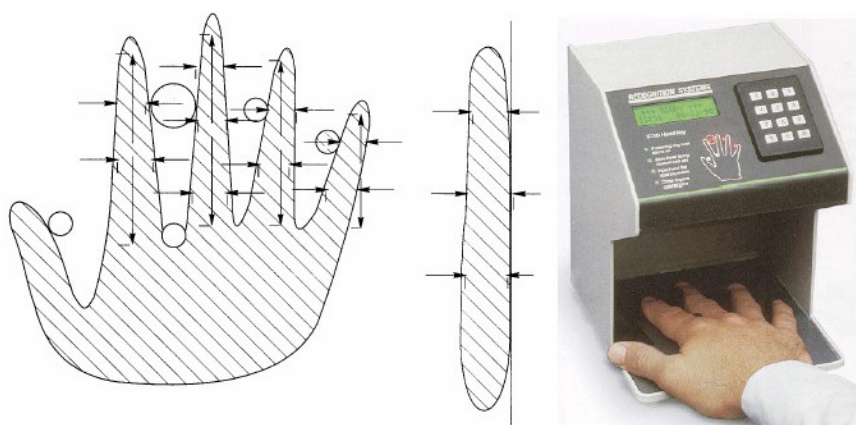


Figura 2.10 – Reconhecimento geométrico da mão [26]

Uma fonte de luz sobre dois espelhos perpendiculares faz com que a luz reflectida seja adquirida por um sensor. Quando a mão é introduzida numa posição apropriada,

apoiada em cavilhas de orientação, obstrui parcialmente a luz reflectida dos espelhos, criando-se, então, uma silhueta da imagem superior e lateral da mão no sensor de reconhecimento [5].

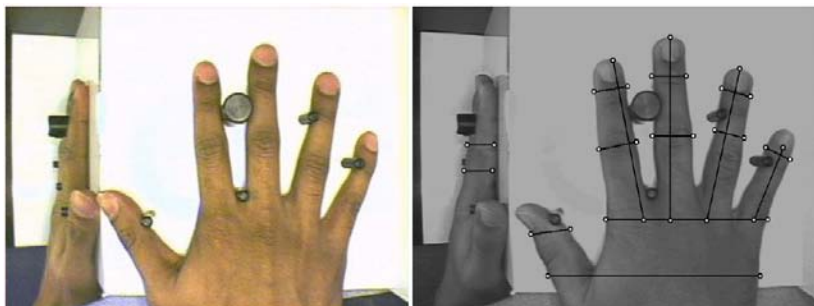


Figura 2.11 – Reconhecimento geométrico da mão [5]

O reconhecimento da *geometria da mão* é um processo de utilização simples, rápido e não invasivo, mas é incapaz de estabelecer certas diferenças (por ex., entre uma mão verdadeira e uma falsificada). A *geometria da mão* humana não é também uma característica unicamente exclusiva para cada pessoa, como o são as *impressões digitais* ou a *íris*, proporcionando que este processo de identificação não seja tão fiável como os demais. Com este método deve-se poder aplicar outros em complementaridade [33].

Este tipo de *reconhecimento biométrico* é utilizado, principalmente, em aplicações de controlo de acessos físico e em sistemas ou áreas que não sejam consideradas “críticas”, porventura, onde não seja necessário identificar o utilizador mas apenas autenticá-lo [5].

Vantagens (reconhecimento da *Geometria da Mão*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- A aquisição da característica biométrica é fácil e não invasiva.
- É um método robusto, de fácil utilização e baixo custo.
- O sistema computacional é bastante simples e, uma vez que o tamanho de cada “perfil” digitalizado é reduzido (9 a 35 bytes), as necessidades de armazenamento são baixas.
- Adequada para integração com outras biometrias, em particular, com a impressão digital.
- Não está conotada a registos de natureza policial ou criminal.
- Eficiência adequada para aplicações de reduzida complexidade.

Desvantagens (reconhecimento da *Geometria da Mão*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- A *geometria da mão*, tal como a tecnologia de impressão digital, é adquirida quando o utilizador pressiona uma superfície e este contacto pode causar preocupações às pessoas, no que respeita a questões de higiene.
- Não é suficientemente precisa e distintiva para a identificação, sendo apenas adequada para aplicações de verificação (ver Anexo A – Sistema Biométrico, A.2 – Funcionamento: Processos Característicos, pág. 183).[16]. A sua precisão é inadequada para aplicações onde não se utilizem outros métodos complementares de identificação.
- A utilização de adornos nos dedos da mão (por ex., anel, aliança,...) pode causar problemas de eficiência no processo de reconhecimento.

2.4.7.1.3 Íris

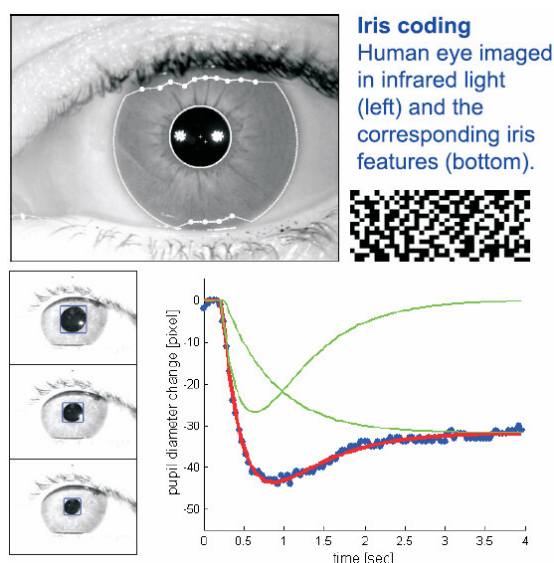


Figura 2.12 – Verificação da íris humana [3]

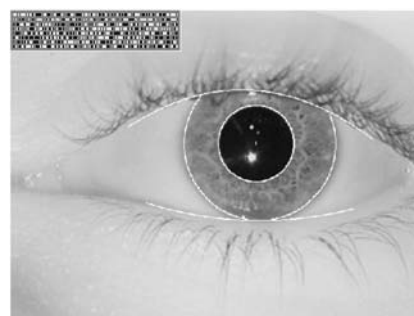


Figura 2.13 – Padrão e código da íris [5]

Esta tecnologia baseia-se na leitura dos anéis coloridos existentes em torno da pupila do olho. Dado as combinações destes anéis formarem uma “imagem” bastante complexa, faz com que este método seja um processo de reconhecimento equivalente ou mais preciso que o da *impressão digital*. Esta vantagem também é consolidada pelo facto da *íris* praticamente não mudar durante a vida duma pessoa. Este processo não precisa de verificar o fundo do olho, tal como o do reconhecimento da *retina*, o que o torna um método mais rápido e cómodo.

A leitura da *íris* efectua-se através de câmaras estrategicamente colocadas em locais de acesso. A imagem obtida é comparada com um *template* existente numa base de dados e, consoante o resultado, o acesso será permitido ou recusado. Existem pequenos equipamentos que funcionam autonomamente, mas a maioria liga-se a computadores em rede que, em segundos, relacionam as imagens obtidas com as da base de dados.



Figura 2.14 – Reconhecimento da *íris*

Estes sistemas de reconhecimento da *íris* pressupõem cooperação dos utilizadores, uma vez que o dispositivo para efectuar, devidamente, a leitura necessita que estes se imobilizem durante breves momentos e, ao mesmo tempo, mantenham o seu olhar fixo num determinado ponto. Recentemente, já se encontram em desenvolvimento sistemas de reconhecimento da *íris* para utilizadores em movimento, em que os utilizadores passam pelo dispositivo de leitura sem adoptarem, em especial, qualquer postura, em que é, apenas, necessário manterem os olhos abertos e nalguns casos retirarem os óculos.

Vantagens (reconhecimento da *Íris*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- A *íris* desenvolve-se na sua totalidade muito precocemente (ao fim dos primeiros dezoito meses de vida) e dispõe de protecções biológicas naturais contra eventuais agressões ambientais. A sua estrutura e forma, praticamente, não se modificam ao longo da vida, o que garante uma elevada fiabilidade. É uma característica fisiológica que, salvo algumas excepções motivadas por doenças raras, é estável, inata e distintiva (mesmo os padrões da *íris* de gémeos idênticos são diferentes) [6].
- Actualmente, o reconhecimento da *íris* é considerado entre as principais tecnologias biométricas (*impressão digital, face, geometria da mão, dinâmica da assinatura, padrão de voz,...*) a mais precisa, muito em especial, no que respeita às baixas taxas de falsa aceitação (*FAR*) (ver Anexo A – Sistema Biométrico, A.3 – Erros, pág. 185), o que representa um aspecto importante nas questões de segurança. [16]. Será uma boa tecnologia para procedimentos destinados, unicamente, à identificação.

- Tem um desempenho elevado, na análise de imagem e sua codificação (um segundo, em média) e no processo de identificação (pode comparar 100.000 registos/segundo num *CPU* de 300 *MHz*).
- A tecnologia de *reconhecimento da íris* tem sido apoiada (desde o 11 de Setembro de 2001) pelas autoridades internacionais.

Desvantagens (reconhecimento da *Íris*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Os utilizadores consideram que este método é extremamente invasivo, provocando-lhes reacções de desagrado e receios com possíveis danos nos olhos. Existe o conceito de que os olhos são sujeitos a um feixe *laser*, o que é um equívoco comum, pois, na realidade, é apenas luz que ilumina a *íris* no procedimento da sua leitura [6].
- Choque com algumas culturas e/ou religiões “não ocidentais”.
- Custo elevado dos dispositivos de reconhecimento. O custo unitário, nomeadamente, o das câmaras dos sistemas de reconhecimento da *íris* é, ainda, elevado.
- A *íris* não é um alvo de aquisição fácil, não só por ser pequeno (1 cm) para ser percebido a uma distância de cerca de um metro, mas também, por ser móvel, que está localizado sob uma superfície reflectora húmida, curvada e, parcialmente, oculto pelas pálpebras que estão frequentemente a piscar. Além do mais, a *íris* pode também estar obscurecida por óculos, lentes e estar sujeita a reflexos, bem como, a deformações causadas pela dilatação da pupila [16]. A distância entre os olhos e os sensores tem de ser curta, geralmente, 1 metro ou menos. Lentes de contacto coloridas, riscos em óculos ou movimentos das pestanas dos olhos podem causar falhas no seu reconhecimento [6].
- Está dependente das condições de luminosidade.
- Devido ao processo de pausa, necessário para uma leitura eficiente, esta tecnologia não será apropriada para o reconhecimento massivo de pessoas.
- O *reconhecimento da íris* pode ser problemático para as pessoas que sofrem de epilepsia, glaucoma ou de olhos molhados. Além disso, as pessoas cegas, obviamente, têm dificuldades em encontrar e olhar para o sítio correcto (onde a câmara está instalada).
- É uma tecnologia, ainda, relativamente recente, que esteve patenteada até 2005, o que impediu novos desenvolvimentos e aperfeiçoamentos.

2.4.7.1.4 Facial

Neste método, a definição dos traços do rosto duma pessoa é utilizada para *reconhecimento facial*. É um processo que se assemelha, parcialmente, com o da geometria da mão, só que este considera o formato do nariz, do queixo, das orelhas,... São utilizadas câmaras de filmar digitais para adquirir registos da estrutura facial global, inclusive a distância entre olhos e sua profundidade, comprimento do nariz, boca, dos ossos da *face*, maxilar e queixo. Um utilizador coloca-se diante duma câmara e, frequentemente, é-lhe solicitado que execute algum movimento facial, como sorrir ou pestanejar, tentando-se, deste modo, impedir que o sistema identifique, positivamente, uma *face* falsificada num molde [33]. Estes sistemas poderão apresentar falhas, quando em presença de gémeos idênticos.

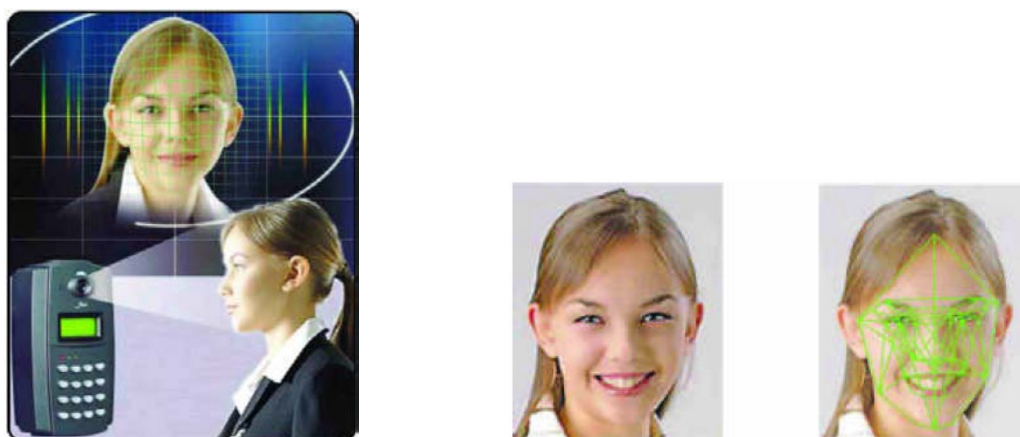


Figura 2.15 – Reconhecimento facial

O *reconhecimento facial*, tal como outros métodos de reconhecimento, traduz a imagem obtida para um código digitalizado único que, subsequentemente, é comparado a outros, registados na base de dados. Quanto mais sofisticada e maior for a base de dados, mais avançado e eficaz será o suporte a esta tecnologia.

Vantagens (reconhecimento *Facial*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Tecnologia pouco invasiva, em que não existe qualquer contacto físico entre o utilizador e o dispositivo de leitura e, por isso, qualquer sensação de desconforto, o que conduz a uma elevada aceitação por parte dos seus utilizadores. Esta tecnologia não exige também grande colaboração destes [16], uma vez que não têm de esperar ou de se colocar numa determinada posição, por grandes períodos de tempo [6].

- Nalgumas situações particulares, por imposições legais, a imagem da *face* é o único modo aceite para identificar um determinado utilizador.
- Não necessita de dispositivos de leitura demasiado dispendiosos, sendo necessária, apenas, a utilização duma câmara de vídeo. Desde que as câmaras *web* se tornaram acessíveis, qualquer entidade pode instalar um sistema desta natureza, pois os dispositivos de aquisição de imagens (2D) são de baixo custo.
- Integração com as soluções de segurança convencionais, já existentes em muitas infra-estruturas (locais de trabalho,...) que possuem sistemas de videovigilância e outras tecnologias vídeo, *webcams* [6].
- Existe grande aceitação pública para este tipo de identificador biométrico, dado as fotos de *faces* serem, rotineiramente, utilizadas em documentos. A imagem facial é social e culturalmente aceite, as pessoas já a utilizam, regularmente, em processos de reconhecimento.
- Precisão e eficiência, relativamente, elevadas. As *faces* de pessoas de raça ou cultura diferentes (por ex., asiáticas) podem ser mais facilmente distinguidas através desta tecnologia do que, propriamente, pelos seres humanos.
- É uma tecnologia extremamente simples, em comparação com outras biometrias, e adequada para aplicações de “conveniência”.
- Reconhecimento fácil, nenhuma outra tecnologia biométrica é tão bem sucedida no reconhecimento de pessoas à distância.
- A legislação dos *USA* (desde o 11 de Setembro que as autoridades estatais têm dado uma atenção especial a esta tecnologia) e Europeia têm apoiado fortemente o *reconhecimento facial*.

Desvantagens (reconhecimento *Facial*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Imprecisões que podem ocorrer devido a resoluções insuficientes da câmara, movimentos faciais e influências externas (por ex., condições de luminosidade) [6].
- O sistema poderá ser ludibriado pela utilização de disfarces.
- Ferimentos ou inchaços no rosto podem prejudicar o processo de reconhecimento.
- Alterações da *face* ocorrem com a idade.

- A percepção pública do *reconhecimento facial* pode ser negativamente influenciada por temores relacionados com a sensação de se estar a ser monitorizado por meio de câmaras.

2.4.7.1.5 Padrão Vascular da Mão

O *reconhecimento vascular* é um sistema de identificação fiável, uma vez que o padrão vascular, espessura e posições das veias, é único para cada pessoa. Para este reconhecimento é necessário que as veias, das costas ou da palma da mão, apareçam realçadas numa fotografia, cuja imagem será, depois, processada e interpretada. Para fotografar as veias da mão, existem dois métodos: reflexão e transmissão. O método de reflexão ilumina a mão e faz a aquisição da luz que é reflectida, enquanto o método de transmissão adquire a luz que passa através da mão. Ambos os métodos utilizam emissões próximas da gama de infravermelhos, emitidas por um *scanner* que executa, também, o processo de digitalização vascular [33].

A *Figura 2.16* e *Figura 2.17* seguintes demonstram a obtenção e o fluxo do processo de extracção do *padrão vascular* duma mão.

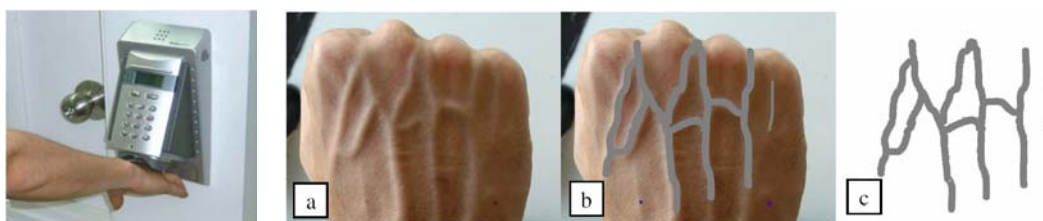


Figura 2.16 – Extracção do padrão vascular da mão [5]

- Imagem das costas da mão já fotografada
- Imagem das veias processada por *software*
- A impressão da imagem das veias

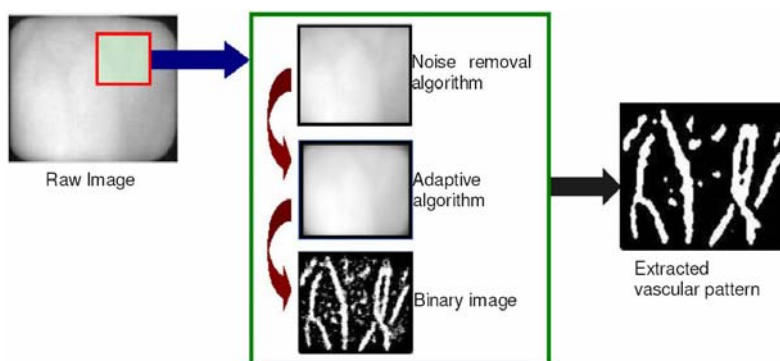


Figura 2.17 – Fluxo do processo de extracção do padrão vascular da mão [5]

Este tipo de reconhecimento pode ser utilizado em aplicações diversas, que requeiram identificação e autenticação, concretamente, em sistemas de controlo de acessos físico e

lógico. Actualmente, é utilizado em aplicações (por ex., acesso a cofres) de muitas instituições financeiras do Japão.

Vantagens (reconhecimento *Vascular da Mão*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Segurança, uma vez que a informação está no interior corporal, abaixo da pele, sendo difícil ser imitada.
- Bastante precisa (com taxas muito baixas de *FAR* 0,0001% e *FRR* 0,1%) (ver Anexo A – Sistema Biométrico, A.3 – Erros, pág. 185) e distintiva, dado o padrão vascular da mão ser complexo e único para cada pessoa.
- Facilidade na utilização e não invasiva.
- Higiénica, uma vez que para a aquisição da imagem do padrão vascular não é necessário um contacto físico com qualquer superfície.

Desvantagens (reconhecimento *Vascular da Mão*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- A *mão* é susceptível a sofrer lesões ou alterações.
- Custos, ainda, elevados dos dispositivos de reconhecimento.

2.4.7.1.6 Voz

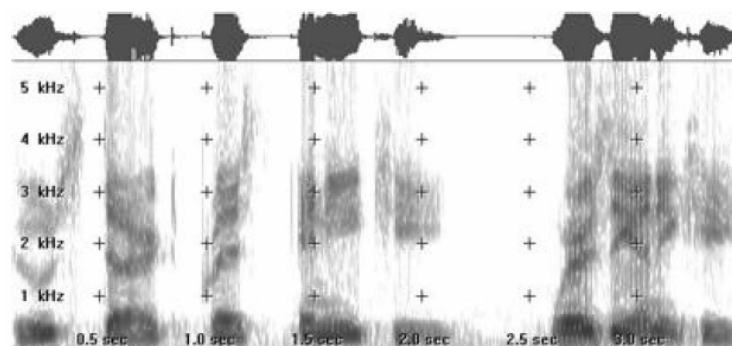


Figura 2.18 – Espectrografia da representação da voz humana

O reconhecimento do *padrão de voz* funciona através da dicção duma frase que actua como se fosse uma senha (*password*). O entrave desta tecnologia é que tem ou deve ser

utilizada em ambientes sem ruídos, pois estes podem influenciar o bom funcionamento do seu processo de reconhecimento. Também se uma pessoa estiver rouca ou gripada, a sua *voz* será diferente, o que poderá provocar transtornos na sua validação. Por estas razões, a identificação ou reconhecimento do *padrão de voz* é, ainda, pouco aplicado.

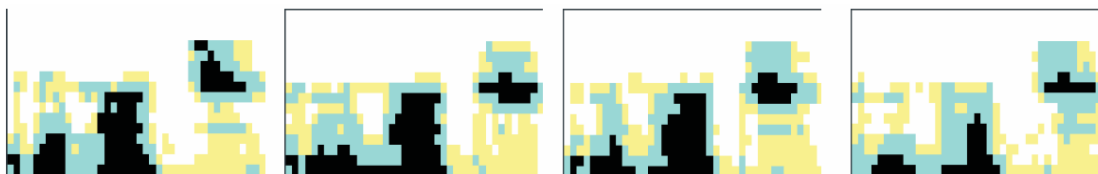


Figura 2.19 – Quatro imagens de espectros (de baixa resolução) para quatro padrões de vozes diferentes, na pronúncia duma mesma palavra [3]

Vantagens (reconhecimento do *Padrão da Voz*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- A *voz*, tal como a *face*, já é uma biometria instintivamente utilizada pelas pessoas para mútua autenticação.
- Os sistemas de telefone são há muito tempo objecto de reconhecimento de *voz*. A fala como objectivo único de autenticação (autenticação activa) pode ser um tanto anti-natural, mas em situações em que o utilizador tem mesmo de falar, este tipo de autenticação torna-se passivo, amigável e não invasivo.
- Tecnologia que utiliza dispositivos baratos e implementada sobre infra-estruturas existentes, amplamente utilizadas (por ex., os sistemas de telefone).
- Permite protocolos de autenticação de segurança incremental, pois quanto mais se exigir do nível de confiança necessário, tanto mais o sistema poderá esperar e receber dados adicionais de *voz*.

Desvantagens (reconhecimento da *Padrão da Voz*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Sistema fácil de ludibriar, pois é susceptível a imitações ou à utilização de gravações de *voz* do utilizador legítimo.
- A qualidade do sinal de áudio é sensível ao ruído ambiente e, além disso, são introduzidas distorções, tanto na aquisição do sinal (pelo microfone), como na sua transmissão (pelo meio de transmissão) [16]. A *performance* e precisão do reconhecimento da *voz* dependem, em muito, da qualidade da infra-estrutura de comunicação e das condições de ruído.

- Nem todas as pessoas estão habilitadas a falar.
- Antes mesmo de poder ser avaliado, o sistema tem de ser muito experimentado, o que requer dispêndio de muito tempo e inabilita a tecnologia para utilizações massivas [6].
- O *padrão de voz* é uma característica biométrica bastante “frágil”, pois pode ser alterado pelo estado de saúde e/ou emocional do utilizador,...

2.4.7.1.7 Caligrafia



Figura 2.20 – Reconhecimento caligráfico

O *reconhecimento caligráfico* analisa não só a forma dos caracteres mas também a forma de escrita, em que são testadas as diferentes pressões e a sequência de construção das letras. O equipamento de *reconhecimento caligráfico* constitui-se por uma base sensível ao toque e por um instrumento (“caneta”) de escrita provido de sensores, em que são detectados o ângulo, a pressão e a direcção da escrita. Grande parte dos *softwares* utilizados, neste método de reconhecimento, registam as pequenas alterações próprias da evolução da escrita de cada pessoa.

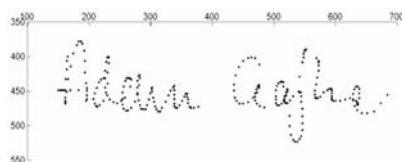


Figura 2.21 – Exemplo duma assinatura [3]

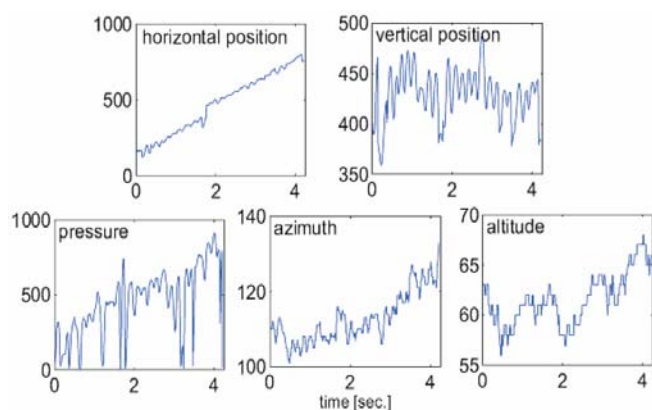


Figura 2.22 – Gráficos correspondentes à assinatura (posição da caneta, tipo de pressão exercida, ângulos da escrita) [3]

É um dos mecanismos mais usados em instituições financeiras, embora não se trate, completamente, dum método biométrico.

Vantagens (reconhecimento *Caligráfico*)

As principais vantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- Grande aceitação por parte do utilizador [16], desde tempos longínquos que a assinatura tem sido utilizada e socialmente aceite [6].
- O *reconhecimento da assinatura* oferece elevada segurança, devido não só à grande quantidade de dados existentes num *template* caligráfico, como também, à grande dificuldade em se imitar, num período curto de tempo, a dinâmica duma assinatura.
- Nenhuma escrita manual é similar a outra; mesmo entre gémeos idênticos, as suas escritas são sempre distintas.
- A assinatura é uma característica muito activa, que é transmitida pela vontade e conhecimento da pessoa [6].
- O custo dos dispositivos de *reconhecimento da assinatura* tem diminuído, nos últimos anos.
- Os bancos e seguradoras têm grande interesse neste tipo de reconhecimento.

Desvantagens (reconhecimento *Caligráfico*)

As principais desvantagens da utilização desta tecnologia de identificação e autenticação biométrica são:

- O custo dos dispositivos de aquisição é elevado
- É uma característica biométrica sujeita a variabilidade elevada, existindo, ainda, muitas pessoas com assinaturas inconsistentes [16], principalmente, aquelas que não as utilizam muito frequentemente ou que sofrem de doenças musculares. Também pode ser objecto de variações dependentes do facto da pessoa estar sentada ou em pé, sob pressão ou relaxada, do seu estado emocional e ao longo do tempo,... [6].
- Nem todas as pessoas são capazes de escrever

Capítulo 3

Sistemas de Controlo de Acessos Físico (baseados em *RFID*)

3.1 Introdução

Este capítulo apresenta uma visão geral dos sistemas de controlo de acessos físico, em especial, os suportados pela tecnologia *RFID*, em que são definidos a arquitectura geral e os principais componentes que intervêm no processo de controlo de acessos. Também são efectuadas considerações acerca dos dados e das comunicações destes sistemas, nomeadamente, a infra-estrutura de rede, os protocolos de comunicação de dados, factores operacionais críticos de comunicação e controlos técnicos de segurança mais relevantes. É de salientar que, ao longo do capítulo, as abordagens e análises são efectuadas segundo duas perspectivas, a dos sistemas de controlo de acessos físico e a dos sistemas *RFID*, que se relacionam e integram.

3.2 Sumário do Controlo de Acessos

Os *Sistemas de Controlo de Acessos Físico* actuais utilizam, fundamentalmente, *RFID* para identificarem automaticamente uma pessoa e, conseqüentemente, verificarem se está autorizada a aceder a um determinado espaço físico (por ex., um edifício ou uma sala no interior dum *campus* universitário). Actualmente, na implementação destes sistemas utilizam-se cartões de proximidade (sem contacto) *RFID*, em substituição das chaves tradicionais. Cada pessoa ou utilizador tem de transportar consigo uma credencial de *ID* (geralmente um cartão *smart card*), pois os espaços físicos estão protegidos por portas ou torniquetes que, para se abrirem, exigem que estas credenciais de *ID* sejam apresentadas a, ou próximo de, um leitor (*reader*) apropriado. A porta ou torniquete destravar-se-á depois do utilizador se autenticar e do sistema o autorizar, pois o sistema estará configurado de tal modo que, somente, para determinados cartões e respectivos utilizadores se destravam certas portas. Para segurança adicional nestes acessos, à posse das credenciais deve, também, estar associada uma senha (*password*), *PIN* ou, mesmo, uma característica biométrica (ver secção §2.4 “Tecnologias de Identificação e Autenticação”, pág. 10 e secção §2.3.2 “Autenticação de Factor Múltiplo”, pág. 9).

3.3 Arquitectura e Componentes do Sistema

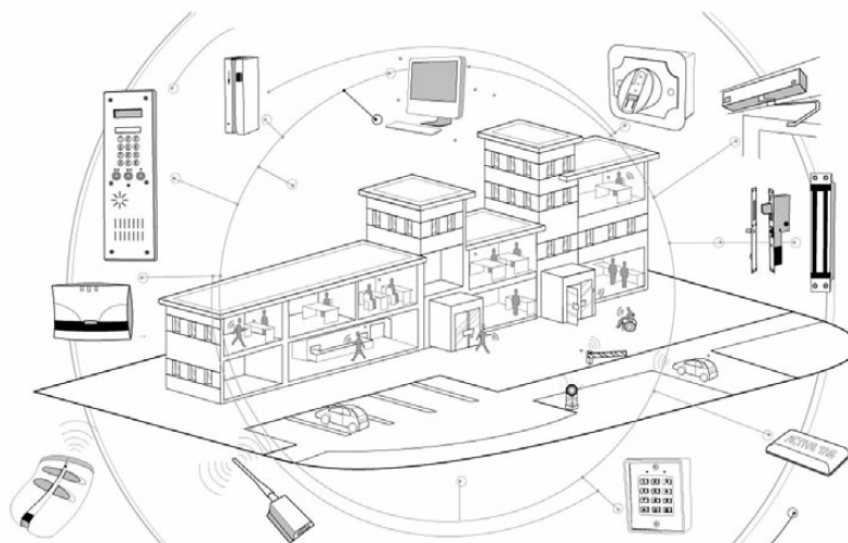


Figura 3.1 – Componentes de sistemas de controlo de acessos físico

Dum modo geral, um *sistema de controlo de acessos físico* típico (*online*⁵) é composto pelos seguintes *componentes* [13]:

- *Credencial de ID* (cartão ou *token ID* que se apresenta a um leitor de cartões no local de acesso, à entrada dum espaço físico)
- *Leitor* (leitor de cartões, *reader*, no local de acesso ou à entrada dum espaço físico, que “lê” a credencial de *ID* e indica se o acesso é permitido)
- *Porta com fecho* ou *Torniquete* (que se abrem quando o acesso é autorizado)
- *Painel de controlo* (ponto de comunicação entre os *readers* e o servidor)
- *Servidor de Controlo de Acessos*
- *Software* (programas apropriados ao sistema de controlo de acessos)
- *Base de Dados* (dados actualizados referentes ao sistema de controlo de acessos)

⁵ Existem dois tipos comuns de sistemas de controlo de acesso: *online* e *offline*.

Os *sistemas online* possuem leitores (*readers*) ligados a um computador central e a cada cartão (*credencial de ID*) está vinculada uma pessoa ou utilizador em particular. A cada leitor (*reader*), ligado em rede com o computador central, é fornecido, pelo computador central, listas de acesso actualizadas das pessoas ou utilizadores que podem aceder à correspondente área ou espaço controlado.

Os *sistemas offline*, por oposição, não têm os leitores (*readers*) ligados a qualquer computador central, pois actuam autonomamente. Nestes sistemas, é o próprio cartão (*credencial de ID*) que contém o conjunto de áreas ou espaços controlados que o seu utilizador pode aceder, possivelmente, também incluindo uma data de validade correspondente a cada uma dessas permissões. Quando uma pessoa ou utilizador tenta aceder a uma área ou espaço controlado, apresenta o cartão ao leitor e este, autonomamente, antes de permitir ou negar o acesso, verifica se o cartão (*credencial de ID*) contém, ou não, os identificadores da permissão referentes à área ou espaço solicitado.

Estes *componentes* interligam-se e interagem entre si, segundo uma *arquitectura* expressa pela *Figura 3.2* seguinte.

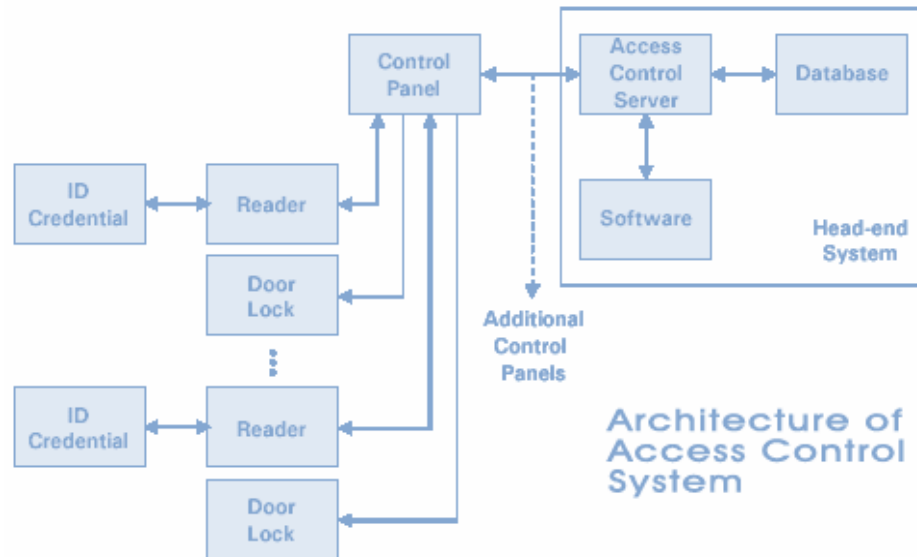


Figura 3.2 – Arquitectura dum sistema de controlo de acessos (físico)

3.3.1 Arquitectura dum Sistema baseado em *RFID*

Um *sistema de controlo de acessos físico* baseado em *RFID* pode ser composto, em geral, por dois⁶ *subsistemas*:

- *Subsistema RF* – composto pelo *reader* e *tags*, que executa, através de comunicação *wireless* (ver secção §3.5.2.1 “Comunicação Tag – Reader”, pág. 56), a identificação e transacções relacionadas.

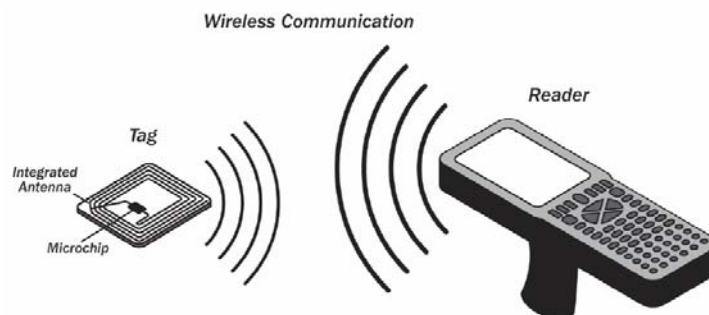


Figura 3.3 – Um exemplo dum simples subsistema RF

⁶ poderá existir ainda um terceiro *subsistema*, denominado *inter-empresarial*, que faz a ligação de vários *subsistemas empresariais* quando a informação precisa de ser partilhada para além duma única unidade empresarial. Mas este caso, em princípio, não se insere na tipicidade dum *sistema de controlo de acessos físico*.

- *Subsistema empresarial* – composto por computadores que executam *software* especializado para armazenar, processar e analisar os dados adquiridos e provenientes do *subsistema RF*. As suas características são muito semelhantes às dos *sistemas em rede*, tanto ao nível dos computadores necessários, como dos protocolos e questões de segurança [25].

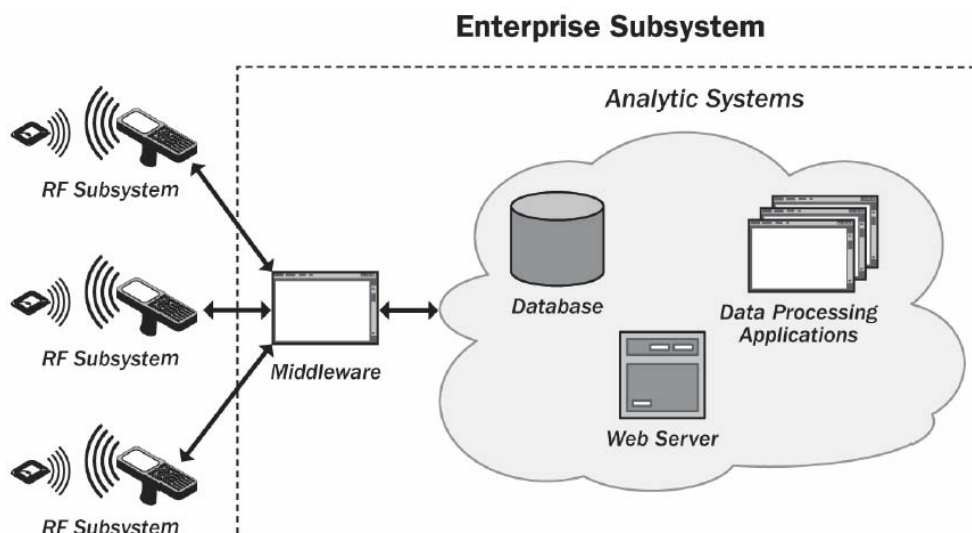


Figura 3.4 – Arquitectura do subsistema empresarial (representada no interior do tracejado)

3.3.2 Tendências Actuais da Arquitectura dum Sistema em Rede

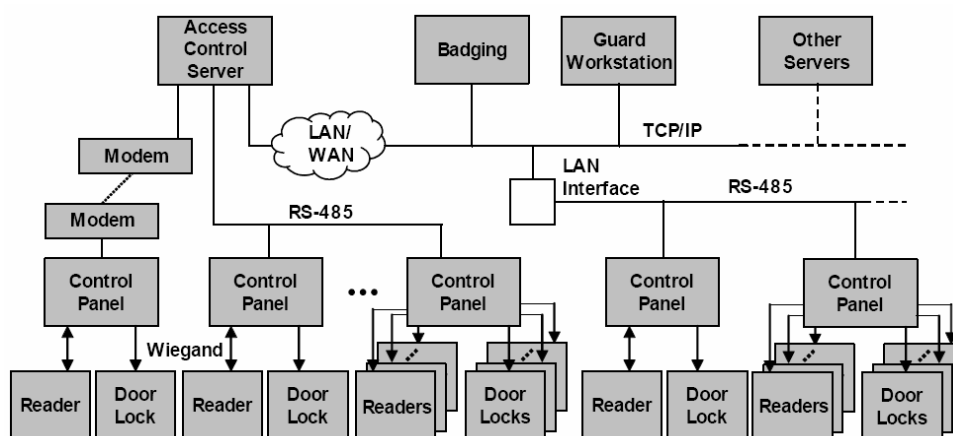


Figura 3.5 – Exemplo dum sistema de controlo de acesso físico em rede [13]

O advento dos sistemas e tecnologias de informação assentes em redes *Internet* e *TCP/IP* (ver secção §3.5.2.2 “Comunicações da Infra-estrutura de Rede (Leitor – Painel – Servidor)”, pág. 59) proporcionou que os *sistemas de controlo de acessos físico* tivessem vindo a evoluir para *arquitecturas de sistemas em rede* que integram outras funções e permitem envolver diversos departamentos das organizações. Estes sistemas, mais actuais, para além de executarem as *funções típicas de controlo de acessos*,

também, podem incluir funções relacionadas com outros sectores da organização (por ex., um leitor à entrada dum espaço físico poderá, também, servir e actuar como um relógio de ponto, o que envolverá departamentos como os de *RH*, contabilidade,...). A *arquitectura em rede dos sistemas de controlo de acessos físico* poderá ter múltiplas aplicações e envolver vários departamentos da organização.

3.4 Componentes no Processo de Controlo de Acessos

Nas secções seguintes, para cada subsistema, são analisados e caracterizados os principais componentes, já discriminados anteriormente (ver secção §3.3 “Arquitectura e Componentes do Sistema”, pág. 38), que intervêm no processo de controlo de acessos.

3.4.1 Subsistema *RF*

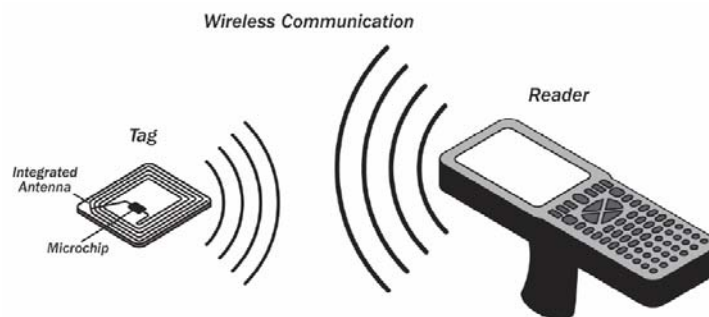


Figura 3.6 – Um exemplo dum simples subsistema *RF*

Um *subsistema RF* dum sistema baseado em *RFID* é composto por dois componentes:

- *Tags⁷ RFID*

Uma *tag* é um pequeno dispositivo electrónico que possui:

- um identificador único

e pode possuir outras características, como:

- memória para armazenar dados adicionais
- sensores ambientais
- mecanismos de segurança

- *Leitores (Readers) RFID*

Um *reader* é um dispositivo que comunica, por *wireless*, com as *tags* com o objectivo de as identificar. Podem adquirir o *identificador único* associado com cada *tag* e, possivelmente, relacioná-lo com outros dados

⁷ *Tags RFID* são por vezes apelidadas de *Transponders*.

Tanto a *tag* como o *reader* são rádio emissores/receptores que têm uma antena e são capazes de modular ou desmodular sinais rádio [25].

3.4.1.1 A Credencial de *ID*

São múltiplas as *tecnologias de ID* (ver secção §2.4 “Tecnologias de Identificação e Autenticação”, pág. 10) que podem ser utilizadas em *sistemas de controlo de acessos físico*. Podem-se apresentar sob uma grande variedade de formatos, sendo utilizadas para o armazenamento de dados que vai permitir a identificação e autenticação da *credencial de ID* e do seu utilizador.



Figura 3.7 – Credencial de *ID* sob a forma de chaveiro de proximidade [34]



Figura 3.8 – Cartão de proximidade [34]

Uma *tecnologia de ID* ajustada aos *sistemas de controlo de acessos físico* é a tecnologia *smart card*, em especial, os cartões de proximidade (*contactless smart card*) definidos pelos protocolos *ISO/IEC 14443* e *ISO/IEC 15693* (ver secção §3.5.2.1 “Comunicação Tag – Reader”, pág. 56), com capacidades de leitura, escrita e armazenamento de dados. As *credenciais de ID* que utilizam este tipo de tecnologia podem armazenar vários tipos de informação, tais como permissões, registos de assiduidade, números de identificação pessoais e *templates* biométricos que possibilitam a autenticação de factor múltiplo (ver secção §2.3.1 “Mecanismos de Autenticação”, pág. 7 e secção §2.3.2 “Autenticação de Factor Múltiplo”, pág. 9) [13].

3.4.1.1.1 Características das *Tags*

Como observado anteriormente (ver secção §3.4.1 “Subsistema RF”, pág. 41), as *tags* são um dos componentes do *subsistema RF*, cujas *principais características* [25] baseiam-se em:

- *Formato do Identificador*
- *Fonte de Energia*
- *Frequências de Operação*
- *Funcionalidade*
- *Forma*

Formato do Identificador:

Cada *tag* possui um *identificador* único que é utilizado exclusivamente para a sua identificação. Existem vários *formatos* para codificação de identificadores de *tags* mas, em geral, utilizam-se identificadores de estrutura *standard*, com grupos de *bits* específicos para representarem, também, campos específicos. Um *formato de identificador* de *tag* muito utilizado é o *EPC* (*Electronic Product Code*).



Figura 3.9 – Exemplo dum código de produto electrónico de 96 bits (96-bit EPC)

O *formato de identificador EPC* possui quatro campos de dados:

- *Cabeçalho* (especifica o tipo de *EPC*)
- *ID do Gestor EPC* (identifica a organização responsável pela atribuição da classe de objectos e do número de série – frequentemente o fabricante do artigo)
- *Classe de Objecto* (identifica uma classe de objectos – por ex., um modelo específico de computadores)
- *Número de Série* (descreve a instância duma classe de objectos – por ex., um computador específico, em particular)

Fonte de Energia:

As *tags* não só precisam de executar diversas funções, como emissão de sinais rádio para um *reader*, armazenamento e recuperação de dados, como também, outros processos computacionais (por ex., relativos a mecanismos de segurança). Para tal, podem obter energia (corrente eléctrica) proveniente, quer duma bateria própria, quer através das ondas electromagnéticas emitidas pelos *readers*. Os requisitos inerentes à energia duma *tag* dependem de vários factores:

- distância entre a *tag* e o *reader*
- radiofrequência utilizada
- funcionalidade da *tag*

Em geral, nas funções que uma *tag* executa, a característica mais evidente e complexa respeita à sua energia (por ex., *tags* que suportam criptografia ou autenticação precisam de mais energia do que as que se limitam a transmitir um simples identificador).

Com base na sua *fonte de energia*, para comunicação ou qualquer outra funcionalidade, as *tags* são categorizadas em quatro tipos (já mencionados e abordados na secção §2.4.6.4 “Tags”, pág. 19):

- *Passivas*
- *Activas*
- *Semi-Activas*
- *Semi-Passivas*

Frequências de Operação:

Também a radiofrequência de transmissão e recepção de sinais de uma *tag*, traz implicações para:

- as características de desempenho da *tag*, incluindo:
 - a distância operacional
 - a velocidade de leitura da *tag*
 - o rácio de transferência de dados
- a capacidade do sinal da *tag* atravessar materiais
- a possibilidade de rádio interferência nas comunicações
- a sua portabilidade (internacional).

Funcionalidade:

A principal função duma *tag* é facultar um *identificador* específico a um *leitor*, mas para certas actividades, muitos tipos de *tags* podem suportar vantajosas capacidades adicionais, como:

- memória
- sensores ambientais
- funcionalidades de segurança (protecção de senhas – *passwords* – e criptografia)
- mecanismos de protecção de privacidade

Forma:

Existem numerosos e diferentes tipos de *tags* que podem diferir bastante quanto a:

- forma, tamanho e peso
(por ex., as *tags activas*, porque possuem uma bateria interna, são maiores e mais pesadas do que as *tags passivas*; as *tags* que integram sensores ambientais também são maiores e mais pesadas do que aquelas que não possuem essa funcionalidade)
- embalagem
(as *tags* podem aparecer sob diversas embalagens – por ex., embebidas sob cartões *smart cards*, o que as torna menos vulneráveis e mais resistentes às condições ambientais)
- manuseamento

- desempenho
- mecanismos de segurança
- custo (quanto mais funcionalidades integrarem maior é o seu custo; a energia ou a sua fonte também influenciam no seu custo)
- ...

3.4.1.2 O Leitor

O *leitor* no local de acesso ou à entrada dum espaço físico pode ter uma ou mais *interfaces*, nomeadamente para:

- *Cartões de Contacto*



Figura 3.10 – Leitor com interface para cartões de contacto

O leitor para ser utilizado por *cartões de contacto* possui uma abertura ou conector para ser inserido o cartão. Neste tipo de leitura estabelece-se um contacto físico directo entre o micromódulo condutor do cartão e o conector do leitor.

- *Cartões de Proximidade*

O leitor utilizado para *cartões de proximidade* actua como um emissor/receptor de baixa potência que transmite ininterruptamente um campo electromagnético de *RF*. Quando um *cartão de proximidade* está sob o seu campo de alcance, a energia do campo é recebida através da antena interna do cartão e convertida para activação do seu *chip* interno que, em seguida, transmite pela antena os dados ao leitor.

- *Teclado para introdução dos PIN*

Os leitores podem possuir também um teclado para digitação de *PIN*

- *Leitura Biométrica*



Figura 3.11 – Leitor biométrico (impressão digital)

Os que possuem um dispositivo para leitura de características biométricas (normalmente, um leitor de impressão digital ou de geometria da mão)

Os leitores que possuem um teclado para digitação de *PIN* e leitura biométrica suportam geralmente dois ou três *factores de autenticação* em simultâneo (ver secção §2.3.2 “Autenticação de Factor Múltiplo”, pág. 9).



Figura 3.12 – Exemplo dum leitor de autenticação de factor múltiplo [29]

Quando o leitor acaba de receber todos os dados solicitados, em geral, sucede-se um dos dois modos seguintes, em que os dados são:

- enviados imediatamente ao *painel de controlo*

Os *leitores* mais simples não avaliam os dados ou a legitimidade da *credencial de ID*, logo, enviam-nos directamente ao *painel de controlo*. São geralmente leitores genéricos, dum *único factor de autenticação* e, actualmente, já obsoletos.

- primeiramente analisados pelo leitor e, só depois, enviados ao *painel de controlo*

Os *leitores* podem interpretar, tratar os dados provenientes do cartão e, a seguir, transmiti-los ao *painel de controlo*, numa forma mais utilizável. Oferecem um nível de segurança mais elevado, uma vez que o *leitor* pode validar a legitimidade da *credencial de ID* apresentada, efectuar comparações de dados biométricos (ver Anexo A – Sistema Biométrico, pág. 181),... Para efectiva segurança, deverão ser estes os leitores a utilizar nos actuais *sistemas de controlo de acessos físico*.

3.4.1.2.1 Características dos *Readers*

Como referido atrás (na secção §3.4.1 “Subsistema RF”, pág. 41), os *readers*, tal como as *tags*, são outro dos componentes do *subsistema RF* e, independentemente das características das *tags*, as suas principais características [25] são:

- *Potência de Saída e Ciclo de Função*
- *Interface para o Subsistema Empresarial*
- *Mobilidade*
- *Desenho e Colocação da Antena*

Potência de Saída e Ciclo de Função:

Na maioria dos casos, existem *standards* e regulamentos que determinam a *potência de saída* (permitida) e o *ciclo de função* dos leitores.

O *ciclo de função* corresponde à relação de tempo de emissão de energia pelo leitor, num período específico (por ex., um leitor que emita durante 30 segundos em cada minuto, tem um ciclo de função de 50%).

Os *leitores* que se comunicam com *tags* passivas necessitam de maior *potência de saída* do que os que se comunicam com *tags* activas, dado o sinal ter de ser suficientemente forte para alcançar a *tag* e permitir que esta adquira a energia suficiente para emitir o sinal de retorno ao leitor.

Em geral, os leitores com *poder de saída* e *ciclo de função* maiores, para além de poderem interceptar e “ler” as *tags* com mais precisão, mais rapidamente e a maiores distâncias, podem potenciar, também, um nível de escuta indesejado.

A Interface para o Subsistema Empresarial:

Todos os *leitores* para se comunicarem com as *tags* não só possuem, necessariamente, uma *interface* para o *subsistema RF*, mas também, no caso dos *sistemas de controlo de acessos físico (online)*⁸, uma outra *interface* para comunicação com o *subsistema empresarial* (ver *Figura 3.3* e *Figura 3.4* da secção §3.3.1 “Arquitectura dum Sistema baseado em RFID”, pág. 39 e/ou secção §3.4.2 “Subsistema Empresarial”, pág. 49). A *interface do subsistema empresarial* além de suportar a transferência dos dados, desde o *leitor* até ao *middleware* e/ou *sistemas analíticos*, onde se processam e analisam os dados, também pode ser utilizada para gestão remota dos leitores. Pode estar ligada por:

- cabos (por ex., *Ethernet*)

⁸ Os *sistemas online* possuem leitores (*readers*) ligados a um computador central e a cada cartão (*credencial de ID*) está vinculada uma pessoa ou utilizador em particular. A cada leitor (*reader*), ligado em rede com o computador central, é fornecido, pelo computador central, listas de acesso actualizadas das pessoas ou utilizadores que podem aceder à correspondente área ou espaço controlado.

- *wireless* (por ex., *Wi-Fi* – protocolo 802.11x do *IEEE*)

(Nota: Sobre os dois tipos de comunicação anteriores, ver secção §3.5.2.2 “Comunicações da Infra-estrutura de Rede (Leitor – Pannel – Servidor)”, pág. 59).

Muitos sistemas utilizam o protocolo *SNMP* (*Simple Network Management Protocol*) para monitorização dos *leitores* e alerta dos administradores de determinadas condições que o justifiquem.

A Mobilidade:

Como se referiu no ponto anterior, “A *Interface* para o Subsistema Empresarial”, a *interface* dum *leitor* com o *subsistema empresarial* pode ser por cabos ou por *wireless*. A maioria dos leitores com ligação por cabo estão em posições fixas, suportam aplicações nas quais as *tags* para serem lidas têm de se aproximar dos leitores, caso geral dos *sistemas de controlo de acessos físico*, e, obviamente, estes leitores possuem limitações ao nível da mobilidade.



Figura 3.13 – Leitor fixo dum sistema de controlo de acessos físico

Por oposição, os leitores *wireless* suportam grande mobilidade para efectuarem a leitura das *tags*. A Figura 3.14 seguinte, mostra um exemplo de um *leitor* móvel e manual no processo de leitura duma *tag*.

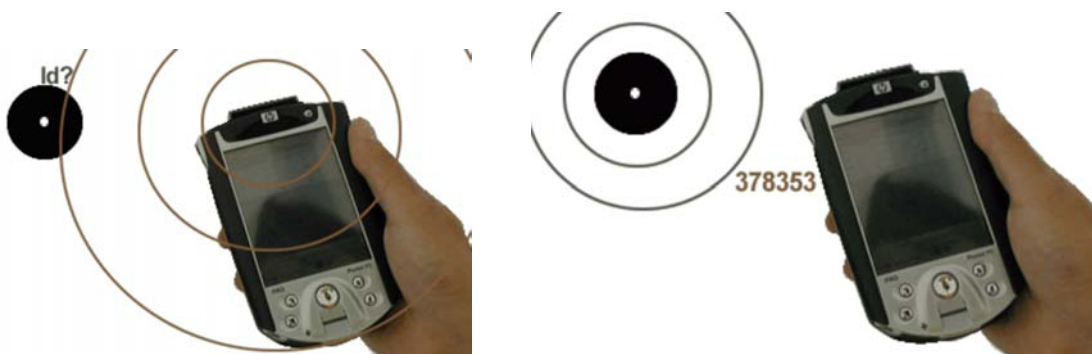


Figura 3.14 – Leitor móvel manual na leitura duma *tag*

Em geral, um *leitor* móvel utiliza diferentes protocolos de comunicação para as *interfaces* do *subsistema RF* e *empresarial*, mesmo sendo ambas por *wireless*. O protocolo 802.11 do *IEEE* (conhecido também como *Wi-Fi*) é um protocolo comum

para a *interface de subsistema empresarial*, se bem que, também, seja utilizado para *interface RF* nalgumas implementações de *tags* activas. Os protocolos mais comuns de *interface RF* são definidos pelos *standards ISO/IEC* (ver secção §3.5.2.1 “Comunicação *Tag – Reader*”, pág. 56).

O Tipo e Colocação da Antena:

Os leitores utilizam uma ampla variedade de tipos da *antena*, cada um possuindo um padrão de cobertura diferente. Para se reduzir a probabilidade de escutas e interferências indesejadas, a cobertura da *antena* deve estar dentro dum parâmetro suficiente para que haja apenas comunicação com as *tags* pretendidas.



Figura 3.15 – Vários tipos de antena: A – antena de desktop ou de parede, B – antena de HF, C – antena em portal

As *antenas* podem ser destacáveis ou integradas no *leitor*. Os leitores que suportam *antenas* destacáveis são mais convenientes em aplicações que requeiram áreas específicas de cobertura, dado a *antena* poder ser seleccionada e customizada no sentido de corresponder às exigências. As *antenas* devem poder ser montadas consoante as exigências específicas duma aplicação.

3.4.2 Subsistema Empresarial

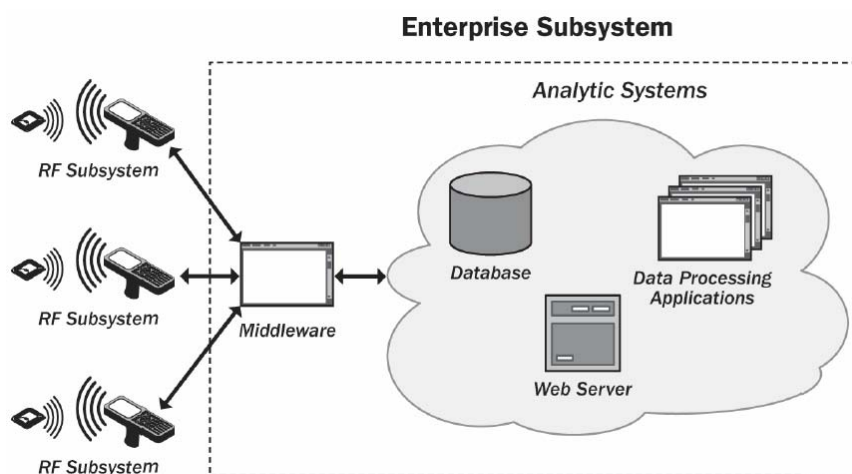


Figura 3.16 – Arquitectura do subsistema empresarial (representada no interior do tracejado)

O *subsistema empresarial* é composto de três principais componentes:

- *Middleware*
- *Sistemas Analíticos*
- *Infra-estrutura de Rede*

O *subsistema empresarial* interliga os *readers* aos computadores centrais, que executam o *software* para armazenar, processar e analisar os dados adquiridos nas transacções do *subsistema RF*. No caso concreto dum *sistema de controlo de acessos físico baseado em RFID*, existe um *subsistema RF* que faz a leitura do identificador dum cartão ou *tag* pertencente a cada um dos utilizadores. O *subsistema empresarial*, por sua vez, fará a correspondência desse *identificador*, associado a cada utilizador, com registos correlativos na *base de dados*, para determinar as permissões e outros atributos correspondentes. Alguns *sistemas de controlo de acessos físico baseado em RFID*, mais simples (*offline*⁹), apenas, possuem um *subsistema RF* (por ex., sistemas em que os *readers* decidem, por si, acerca das permissões do controlo de acessos, não necessitando de aceder aos computadores centrais). No entanto, a maioria dos *sistemas de controlo de acessos físico baseado em RFID* possui os dois subsistemas: o *subsistema RF* e o *subsistema empresarial* [25].

3.4.2.1 O Painel de Controlo



Figura 3.17 – Painel de controlo dum sistema de controlo de acessos (físico) [8]

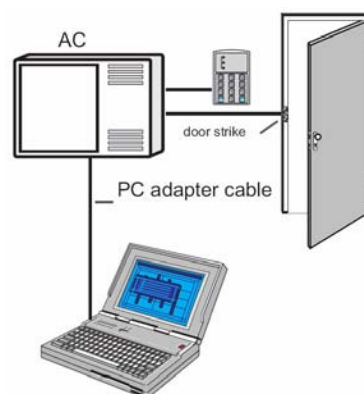


Figura 3.18 – Ligações do painel de controlo num sistema de controlo de acessos (físico) [2]

O *painel de controlo (controlador)* é o ponto de comunicação central num *sistema de controlo de acessos físico*. Interage e comunica com os múltiplos leitores, nos diferentes locais de acesso dos espaços físicos, com os *fechos* electromecânicos das portas de

⁹ Os *sistemas offline*, ao contrário dos *online*, não têm os leitores (*readers*) ligados a qualquer computador central, pois actuam autonomamente. Nestes sistemas, é o próprio cartão (*credencial de ID*) que contém o conjunto de áreas ou espaços controlados que o seu utilizador pode aceder, possivelmente, também incluindo uma data de validade correspondente a cada uma dessas permissões. Quando uma pessoa ou utilizador tenta aceder a uma área ou espaço controlado, apresenta o cartão ao leitor e este, autonomamente, antes de permitir ou negar o acesso, verifica se o cartão (*credencial de ID*) contém, ou não, os identificadores da permissão referentes à área ou espaço solicitado.

acesso ou com os mecanismos de desbloqueio dos *torniquetes*, podendo abri-los ou destravá-los, assim como, com o *servidor de controlo de acessos*.

O *painel de controlo* começa por validar o *leitor* e aceitar os dados transmitidos por este. Em seguida, o processo vai depender do *sistema de controlo de acessos* ser:

- *Centralizado*¹⁰
- *Distribuído*¹¹ (*Descentralizado*)

Dependendo do sistema, o *painel de controlo* tanto pode processar os dados provenientes do *leitor* e do *servidor de controlo de acessos* e decidir sobre as permissões dos acessos (*sistema distribuído*), como pode enviar os dados para que o *servidor do controlo de acessos* tome essa decisão (*sistema centralizado*).

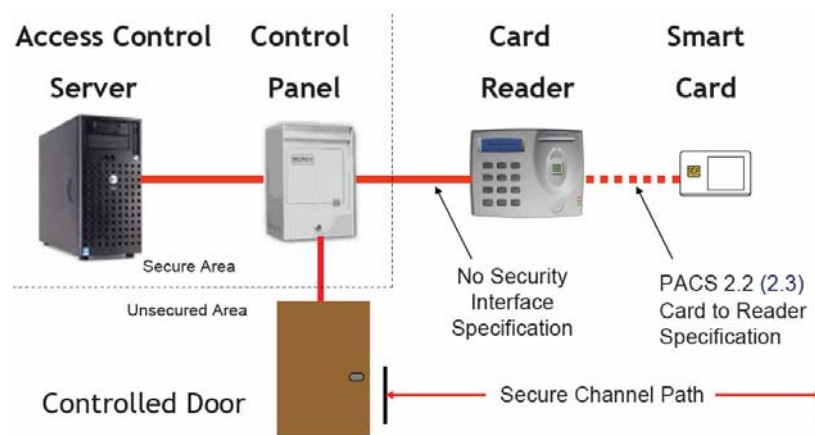


Figura 3.19 – Esquema simplificado dum sistema de controlo de acessos físico [29]

Por questões de segurança, é importante que seja o *painel de controlo* e não o *leitor* a efectuar a gestão do sinal de desbloqueio do *fecho* da porta do local de acesso. Isto, porque o *painel de controlo* está localizado no interior da organização, em princípio, numa área ou espaço seguro, enquanto o *leitor* poderá estar localizado numa área desprotegida ou insegura [13].

¹⁰ Num *sistema centralizado*, o *painel de controlo* transmite os dados, enviados pelo *leitor (reader)*, ao *servidor do controlo de acessos* que, por sua vez, através dum *software de controlo de acessos* apropriado, analisa as *permissões* de acesso e outras questões relativas ao utilizador, com base na informação armazenada na *base de dados*. Em seguida, o *servidor do controlo de acessos* envia uma mensagem ao *painel de controlo* no sentido deste, consoante a decisão relativa à permissão do acesso, poder, ou não, destravar a porta. Nessa mensagem, o *painel de controlo* emite dois sinais: um para o *fecho* adequado da porta do local de acesso, no sentido de o poder, ou não, destravar; outro para o *leitor (reader)* referente ao local de acesso (entrada do espaço físico controlado), o qual emitirá uma mensagem (audível ou visual) ao utilizador, correspondente à decisão do acesso.

¹¹ Num *sistema distribuído ou descentralizado*, é da competência do *painel de controlo* decidir acerca do acesso do utilizador. Nestes sistemas, o *servidor do controlo de acessos* fornece, periodicamente, aos *painéis de controlo*, os dados necessários para o *software do painel (middleware)* poder determinar se um acesso será, ou não, concedido. O *painel de controlo*, neste tipo de sistemas, executa as funções do *servidor de controlo de acessos* (do *sistema centralizado*, descritas em nota anterior) e decide acerca das permissões de acesso. Dotar ou capacitar os *painéis de controlo* no exercício destas funções, traz a vantagem de se obter um menor tráfego de comunicação entre os *painéis de controlo* e o *servidor de controlo de acessos central*, o que, deste modo, melhora o desempenho e a fiabilidade do sistema.

3.4.2.1.1 O *Middleware*

O *middleware* é responsável pela preparação dos dados adquiridos pelos *readers* do *subsistema RF* e pela sua transferência, imediata ou posterior, para os *sistemas analíticos*. O *middleware* “esconde” dos *sistemas analíticos* a complexidade e os detalhes do *subsistema RF*, permitindo que os utilizadores (analistas) destes *sistemas analíticos* se concentrem, preferencialmente, noutros tipos de tarefas (por ex., na gestão e administração do sistema) e não, propriamente, em questões de maior detalhe (por ex., comunicações *wireless*). O *middleware* filtra a informação, proveniente dos *readers*, que possa estar duplicada, incompleta ou errada, o que é especialmente útil em aplicações, com um grande número de *tags* e estas muito próximas (ambientes de grande exigência de *RF*), o que, seguramente, não se encaixa na tipicidade dos *sistemas de controlo de acessos físico*.

Os administradores de sistemas utilizam o *middleware* para efectuarem, também, a gestão e monitorização dos *readers* (por ex., ajustar a *potência de saída* e o *ciclo de função*). A existência de ficheiros de *log* de transacções, no *middleware*, ajuda à identificação e detecção de comportamentos anormais e/ou utilizações não autorizadas [25].

3.4.2.2 Os Sistemas Analíticos (do *Host System*)

Os *sistemas analíticos do host system*¹² são compostos por:

- *Servidores Web* (*Servidor de controlo de acessos*)
- *Software* (*Aplicações de processamento de dados*)
- *Base de Dados* (*Dados actualizados do sistema de controlo de acessos: permissões, utilizadores, acessos, ...*)

Os *sistemas analíticos* processam os dados, provenientes do *middleware*, com base na lógica, instruções e requisitos do processo de negócio suportado pelo sistema em questão (por ex., os *sistemas analíticos* dum *sistema de controlo de acessos físico* tratam da lógica inerente a este sistema: permissões de acesso aos espaços físicos, informação referente aos utilizadores, seus papéis, espaços físicos controlados,...). Incluem as aplicações que não só integram os dados provenientes do *subsistema RF*, como também, os de outras fontes (por ex., alguns *sistemas* podem complementar ou coexistir com outros sistemas de *AIDC* já existentes, como os de tecnologia de código de barras), podendo correlacionar dados importados de diversas bases de dados.

Dum modo geral, num *sistema de controlo de acessos físico centralizado* (ver secção §3.4.2.1 “O Painel de Controlo”, pág. 50), o *servidor de controlo de acessos* recebe, através do *painel de controlo*, os dados provenientes da leitura da *credencial de ID* pelo

¹² Também referido por *head-end system* ou *back-end system*

leitor. O *software de controlo de acessos* correlaciona estes dados com os dados existentes numa *base de dados*, analisa as permissões ou privilégios de acesso correspondentes ao utilizador e indica ao *painel de controlo* se o utilizador pode ser admitido ao espaço físico solicitado.

A maioria dos *sistemas de controlo de acessos físico* são *descentralizados (distribuídos)* (ver secção §3.4.2.1 “O Pannel de Controlo”, pág. 50) e, nestes casos, o *servidor do controlo de acessos* envia, periodicamente, aos *painéis de controlo*, informação actualizada sobre o controlo de acessos, permitindo que os *painéis de controlo* operem independentemente e tomem, com base nos dados armazenados, as correspondentes decisões de permissão de acesso dos utilizadores [13].

3.5 Dados e Comunicações do Sistema

Os dados e as comunicações são um factor crítico nestes sistemas, nomeadamente, na eficácia do seu desempenho e no que respeita à fiabilidade e segurança dos dados transmitidos. Nas secções seguintes, começa-se por fazer uma caracterização da infra-estrutura de rede e dos principais protocolos de comunicação de dados utilizados nos sistemas de controlo de acessos físico, suportados por *RFID*. Seguidamente, refere-se um ponto crítico na operacionalidade destes sistemas, a distância operacional entre a credencial de *ID* e o leitor, assim como, os controlos técnicos mais relevantes para minimizar os riscos de segurança associados aos dados e sua transmissão.

3.5.1 Infra-estrutura de Rede

A *infra-estrutura de rede* permite a comunicação entre:

- o *subsistema RF* e o *subsistema empresarial*
- os próprios *componentes do subsistema empresarial*

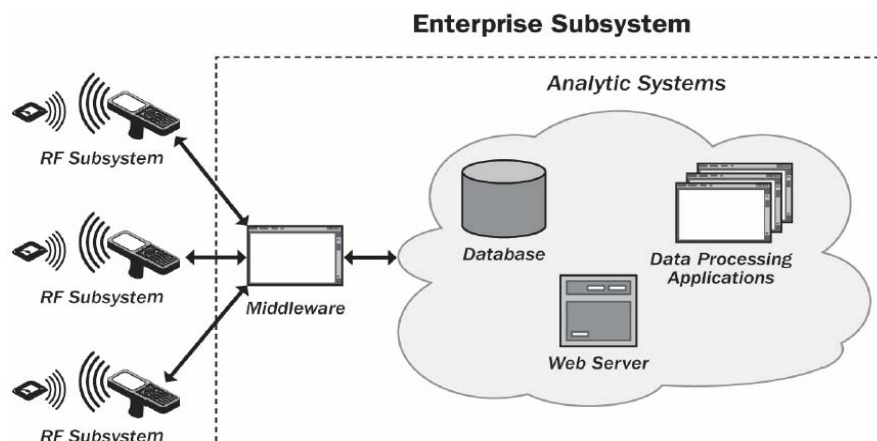


Figura 3.20 – Arquitectura do subsistema empresarial (representada no interior do tracejado)

Algumas características importantes [25] da *infra-estrutura de rede* são:

- *Topologia Física e Lógica da Rede*
- *Protocolos de Comunicações de Dados*

3.5.1.1 Topologia Física e Lógica

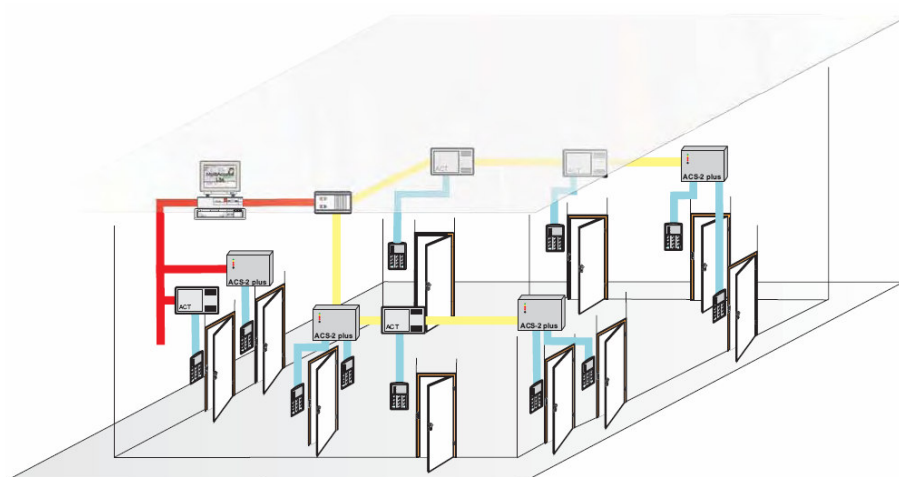


Figura 3.21 – Ligações (do subsistema empresarial) num sistema de controlo de acessos (físico) [2]

A *topologia* duma rede descreve como os vários elementos da rede estão *física* e *logicamente* interligados.

- *Topologia Física* (refere o posicionamento das interligações da rede, quer por cabo, quer por *interfaces wireless*)
- *Topologia Lógica* (descreve como as ligações de comunicação entre os dispositivos da rede se efectuam)

A *topologia física* duma *infra-estrutura de rede* dum *sistema* baseado em *RFID* depende fundamentalmente da localização física dos componentes do seu *subsistema empresarial* (ver Figura 3.20 da secção §3.5.1 “*Infra-estrutura de Rede*” anterior, pág. 53). Quando estes componentes se distribuem ao longo da rede da organização podem dar origem a *topologias físicas* complexas.

A localização física dos servidores de *middleware* (painéis de controlo) depende do nível de tráfego gerado pelos *readers*:

- Se as transacções são relativamente pouco frequentes, como num *sistema de controlo de acessos físico*, com número reduzido de utilizadores, a localização dos painéis de controlo e subjacente *middleware* não é um aspecto crítico. Neste

contexto, os painéis de controlo (*middleware*) poderão estar situados numa localização que possa servir múltiplos *readers*.

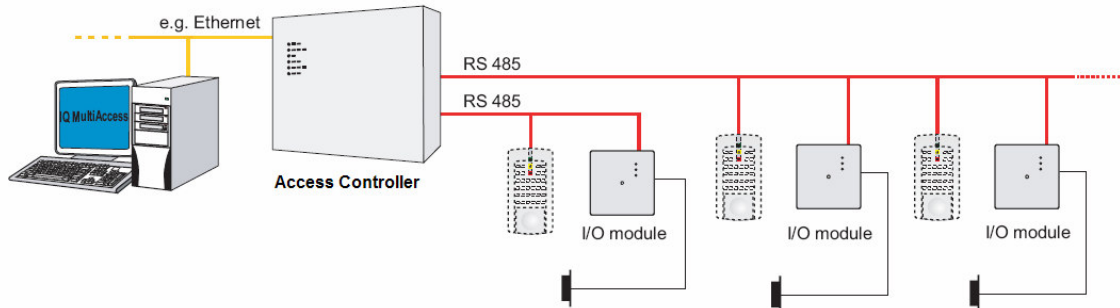


Figura 3.22 – Painel de controlo (*access controller*) ligado a vários *readers* [2]

- Se um número elevado de *tags* precisa de ser lido rapidamente, o *middleware* será colocado perto dos *readers*, evitando-se deste modo problemas de latência e restrições no débito de dados.

A localização física dos *sistemas analíticos* (ver Figura 3.20 da secção §3.5.1 anterior, pág. 53), normalmente, depende do modo como a organização gere a totalidade das suas aplicações:

- Se os *sistemas analíticos* estiverem dedicados exclusivamente a aplicações relacionadas com *RFID*:
 - frequentemente são colocados perto dos *readers* e do *middleware*
 - mas também poderão estar situados em unidades remotas de processamento e tratamento de dados, obtendo-se vantagens relacionadas com:
 - segurança física
 - existência de pessoal técnico
 - proximidade a infra-estruturas várias, já existentes
- Se os *sistemas analíticos* integrarem outros sistemas de informação para além dos de *RFID*, é improvável que a localização do *subsistema RF* condicione, de modo significativo, a localização dos *sistemas analíticos*.

Dependente da configuração de rede, a *topologia lógica* pode ser relativamente simples. Muitas organizações utilizam redes virtuais de área local (*VLAN*) para as interligações dos diversos componentes do *subsistema empresarial*. As *VLAN*, em redes com elevado número de transacções, reduzem a latência e isolam o tráfego doutros sistemas, o que elimina problemas de desempenho da rede e contribui para melhorar a segurança [25].

3.5.2 Protocolos de Comunicação de Dados

Os *protocolos de comunicação de dados* são um componente crítico no desempenho, fiabilidade e segurança, tanto nas comunicações do subsistema *RF* (*tag* – *reader*), como nas do subsistema empresarial ou infra-estrutura de rede (leitor – painel de controlo – servidor de controlo de acessos). As secções que se seguem, vão referenciar os protocolos de comunicação de dados mais utilizados nesses dois subsistemas.

3.5.2.1 Comunicação *Tag* – *Reader*

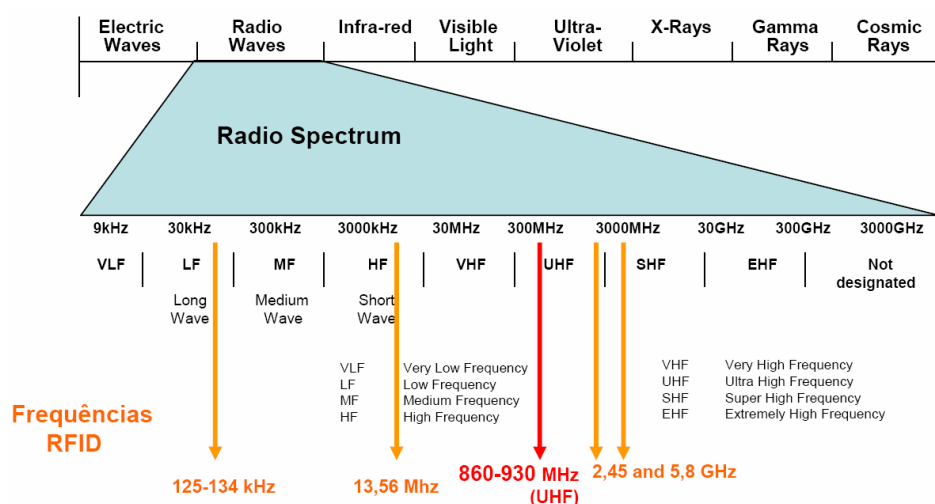


Figura 3.23 – Espectro de radiofrequência

A comunicação das *tags* com o *reader* faz-se pela utilização dum *protocolo de comunicação* comum¹³. Existem vários *protocolos de comunicação tag – reader* [25], tanto para as aplicações que utilizam *cartões de proximidade*, como *tags*, e estão especificados por *standards RFID* internacionais. As aplicações que utilizam:

- cartões de proximidade (*contactless smart cards*), como é o caso típico dos *sistemas de controlo de acessos físico* (ver secção §2.4.6.1 “Tecnologias *RFID* para o Controlo de Acessos Físico”, pág. 14), os *protocolos* mais utilizados¹⁴ são:

- *ISO/IEC 14443*

(define as *interfaces*, incluindo a de radiofrequência (*RF*) e a eléctrica, para cartões *smart card* “de grande proximidade”, bem como, os

¹³ Tanto a *tag* como o *reader* devem obedecer a um mesmo protocolo para se comunicarem entre si. Nos casos de utilização de *tags* patenteadas por um fornecedor, o *reader* para se comunicar com as *tags*, tem de suportar o mesmo protocolo de comunicação. Muitas vezes estas *tags* utilizam protocolos proprietários, o que implica que somente *readers* do mesmo fornecedor, que utilizam os mesmos protocolos, possam ser utilizados para se efectuar ou estabelecer a comunicação com as mesmas.

¹⁴ Os principais *standards* para cartões *smart card* são: *ISO/IEC 7816*, *ISO/IEC 14443*, *ISO/IEC 15693* e *ISO/IEC 7501*. Apenas se mencionam os mais utilizados, *ISO/IEC 14443* e *ISO/IEC 15693*.

protocolos de comunicações e anti-colisão. Permite os cartões operarem a uma frequência de 13,56 MHz e a distâncias superiores a 10 cm. É o principal *standard* dos cartões *smart card* de proximidade utilizados nas aplicações de transporte colectivo, financeiras e de *controlo de acessos*. Também é utilizado nos passaportes electrónicos e em cartões de verificação de identidade pessoal)

- tem duas variantes, tipo A e tipo B, com *interfaces* de comunicação diferentes¹⁵
- distância operacional entre 7 e 15 cm (aproximadamente)
- frequência de operação 13,56 MHz

• *ISO/IEC 15693*

(estabelece as normas para cartões de proximidade com distâncias operacionais até 1 metro, nomeadamente, características físicas, sinal de radiofrequência e *interface*, protocolos de transmissão e anti-colisão)

- distância operacional até 1 metro (aproximadamente)
- frequência de operação 13,56 MHz

Tabela 2 – Resumo das Características Técnicas e Mecanismos de Segurança dos Standards *RFID*: *ISO/IEC 14443* e *ISO/IEC 15693*

Características Técnicas:	<i>ISO/IEC 14443</i>	<i>ISO/IEC 15693</i>
Banda	HF	HF
Distância	≈ entre 7 e 15 cm	≈ 1 m
Dados	Tipo A: Identificador de 32, 56 ou 80 bits Tipo B: Identificador de 32 bits	Identificador de 64 bits e até 8 Kbytes de memória de leitura/escrita
Mecanismos de Segurança:		
Confidencialidade	Não ¹⁶	Não possui protecção no comando de leitura. Não tem encriptação ou autenticação.
Integridade	Detecção de erro <i>CRC</i> (<i>Cyclic Redundancy Check</i>)	Característica de fecho permanente da memória de protecção de escrita. Detecção de erro <i>CRC</i> (<i>Cyclic Redundancy Check</i>).

¹⁵ Os *readers* compatíveis com o *ISO/IEC 14443* têm de ser capazes de se comunicarem nas duas variantes: tipo A (*ISO/IEC 14443A*) e tipo B (*ISO/IEC 14443B*).

¹⁶ O *ISO/IEC 14443* não fornece serviços de confidencialidade, mas estes serviços estão disponíveis em muitas aplicações que o utilizam em comunicações *wireless*.

Tabela 3 – Características e Especificações dos Cartões de Proximidade (*contactless smart cards*) que utilizam os Protocolos ISO/IEC 14443 e ISO/IEC 15693 [13]

Características e Especificações (<i>contactless smart cards</i>)	ISO/IEC 14443	ISO/IEC 15693
Frequência de Operação	13,56 MHz	13,56 MHz
Distância Operacional	Até 10 cm	Até 1 m
Tipos de <i>Chip</i>	Microcontrolador c/ memória lógica	Memória lógica
Funções ¹⁷ de Encriptação e Autenticação	Vários	Alguns
Capacidade de Memória	De 64 até 64K bytes	De 256 até 2K bytes
Capacidade de Leitura/Escrita	Leitura/Escrita	Leitura/Escrita
Taxa de Transferência de Dados (Kb/seg)	Até 106 (<i>ISO</i>) Até 848 (disponível)	Até 26,6
Anti-Colisão	Sim	Sim
Autenticação do Cartão ao Leitor	Desafio/Resposta	Desafio/Resposta
Capacidade de Cartão Híbrido	Sim	Sim
Suporte para <i>Interface</i> de Contacto	Sim	Não

- *tags*, mais utilizadas em aplicações de gestão de materiais e cadeia de fornecimento, com os protocolos:

- *ISO/IEC 18000-series* (para gestão de materiais)
- *EPCglobal Class-1 Generation-2* (mais recente e equivalente ao *standard ISO/IEC 18000-6C*) (para cadeia de fornecimento)

Tabela 4 – Resumo das Características Técnicas e Mecanismos de Segurança dos Standards *RFID*: *EPCglobal Class-1 Generation-2* e *ISO/IEC 18000-6C*

Características Técnicas:	<i>EPCglobal Class-1 Generation-2</i> e <i>ISO/IEC 18000-6C</i>
Banda	UHF
Distância	3 m
Dados	Suporta identificadores até 496 bits, memória definida pelo utilizador, memória de leitura/escrita
Mecanismos de Segurança:	
Confidencialidade	Cobertura de código para proteger as comunicações <i>tag-reader</i> . <i>Readers</i> endereçam as <i>tags</i> utilizando números aleatórios de 16 bits.
Integridade	Áreas de memória podem ser fechadas, cuja escrita protege essas áreas. Áreas de memória podem também ser permanentemente fechadas. Detecção de erro <i>CRC</i> (<i>Cyclic Redundancy Check</i>).

¹⁷ Os *standards ISO/IEC* não especificam funções de segurança (como se pode observar na Tabela 2).

3.5.2.2 Comunicações da Infra-estrutura de Rede (Leitor – Painei – Servidor)

Os *protocolos de comunicação de dados* são um componente crítico no desempenho, fiabilidade e segurança duma rede. Para se entender como a *infra-estrutura de rede* do *subsistema empresarial* actua, deve-se distinguir entre:

- *Protocolos de ligação de camada* (especificam como os dispositivos se comunicam num meio de comunicação ou de ligação comum):

- *Ethernet (IEEE 802.3)*

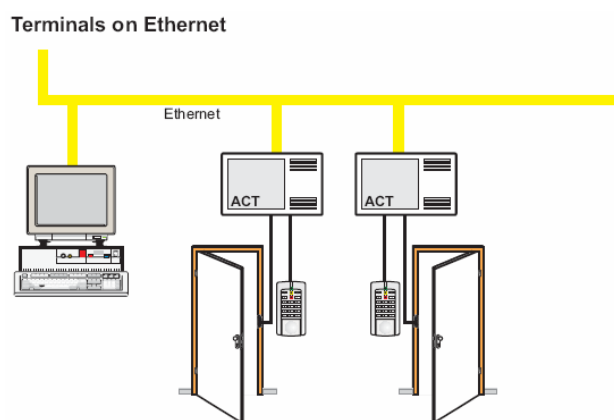


Figura 3.24 – Ligação Ethernet [2]

O *protocolo de ligação de camada* mais comum para ligar os componentes do *subsistema empresarial*. É o mesmo que o utilizado nas ligações na maioria dos computadores das redes locais por fio. Não inclui nenhuma funcionalidade de segurança, o que implica que outros protocolos complementares de comunicação de dados a tenham de fornecer.

- *Wi-Fi (Wireless Fidelity) (IEEE 802.11)*

Protocolo wireless que se aplica, sobretudo, à comunicação de dados dos *readers* móveis com o *subsistema empresarial* (*interface do subsistema empresarial*). Também pode ser utilizado nas comunicações entre *readers* e alguns tipos de *tags* activas, mas as suas características são significativamente diferentes dos *protocolos de ligação de camada*, na comunicação entre as *tags* e *readers*, em particular, do WPA (*Wi-Fi Protected Access*) que inclui numerosas características de segurança (autenticação forte e encriptação).

- *Protocolos de ligação de rede* (descrevem como o tráfego de dados é encaminhado ao longo das múltiplas ligações da rede, possivelmente, sobre vários meios de comunicação):

- *IP (Internet Protocol)*

O *protocolo de ligação de rede* mais comum para comunicação do *subsistema empresarial*. Desde que a maioria dos computadores começou a utilizar o *IP*, também os componentes (*middleware* e *sistemas analíticos*) do *subsistema empresarial* começaram a poder comunicar-se, facilmente, por redes internas e externas, tal como a *Internet*. Os componentes do *subsistema empresarial* que utilizam este protocolo estão sujeitos aos ataques e riscos de segurança típicos da sua utilização.

3.5.3 Factor Operacional Crítico: Distância *Tag* – *Reader*

Em *sistemas de controlo de acessos físico* que utilizam cartões de contacto, a distância operacional, *distância entre a credencial de ID e o leitor para uma comunicação eficaz*, obviamente, não faz sentido, uma vez que os cartões têm de ser inseridos no leitor. Mas nos sistemas que utilizam cartões e leitores de proximidade, a *distância operacional* não só é uma característica importante, que está relacionada com a operacionalidade do *sistema de controlo de acessos físico*, como também, um ponto crítico na implementação destes sistemas, que deve ser tomado em consideração pelas políticas e requisitos de segurança da organização. O alcance do sinal de transmissão/recepção entre as credenciais de *ID (tags)* e um leitor, pode ser, significativamente, maior do que os mencionados pelos protocolos (de *interface RF*) *standards* de comunicação de dados *ISO/IEC* (ver secção §3.5.2.1 “Comunicação *Tag* – *Reader*”, pág. 56 e respectivas *Tabela 2*, *Tabela 3* e *Tabela 4*), dependendo, em muito, da força do campo magnético induzido pelo leitor (*reader*). Este campo magnético poderá ser influenciado por vários factores, tais como:

- *tipo e colocação da antena do leitor* (ver na secção §3.4.1.2.1 “Características dos *Readers*”, pág. 47, o item “O Tipo e Colocação da Antena”).
 - *ambiente físico circundante da localização da antena*
(por ex., a proximidade da antena a objectos metálicos, colocação sobre metais ou perto de portas metálicas, pode distorcer ou impedir o campo de radiação que se gera entre o *leitor* e a *credencial de ID*, implicando que a *distância operacional* seja muito reduzida ou nula; mesmo a orientação da credencial em relação ao leitor,...)
 - *tipo de antena*
(a forma, material e tamanho da antena do leitor influenciam o campo magnético e, conseqüente, *distância operacional*)
- *potência de saída e ciclo de função do leitor*
(os leitores com maior *poder de saída* e *ciclo de função* podem interceptar e “ler” as *tags* com mais precisão, mais rapidamente e a maiores distâncias) (ver

na secção §3.4.1.2.1 “Características dos *Readers*”, pág. 47, o item “Potência de Saída e Ciclo de Função”)

- *frequências de operação (transmissão/recepção) das credenciais de ID ou das tags* (ver secção §3.4.1.1.1 “Características das Tags”, pág. 42, o item “Frequências de Operação” e secção §2.4.6.4 “Tags”, pág. 19).
- ...

3.5.4 Controlos Técnicos de Segurança (mais relevantes)

A tecnologia *RFID* associada aos sistemas de controlo de acessos físico, como qualquer outra tecnologia de informação, também apresenta riscos de segurança e privacidade, que podem ser reduzidos ou atenuados através de vários controlos, nomeadamente, técnicos. As secções seguintes, apresentam alguns dos mais relevantes controlos técnicos de segurança, utilizados para minimizar esses riscos.

3.5.4.1 Encriptação dos Dados e das Comunicações

A segurança e a fiabilidade da informação que serve para identificar os utilizadores e as suas permissões de acesso aos espaços físicos, é uma questão chave para o sucesso dum *sistema de controlo de acessos físico*. A capacidade de se poder utilizar *dados encriptados* ao nível:

- do *Chip do Cartão (smart card)*
- e da *Transmissão de Dados*

é um dos pontos fortes na *protecção dessa informação*.

3.5.4.1.1 Autenticação da Credencial de *ID* e dos Dados

Para incremento da segurança dum *sistema de controlo de acessos físico*, deve também garantir-se a *autenticidade*:

- da *Credencial de ID* (apresentada ao leitor)¹⁸
- dos *Dados* (contidos na credencial).

¹⁸ Nalguns casos, pode ser importante verificar também a *autenticidade do leitor* e, deste modo, evitar-se a usurpação de dados que pode ser levada a efeito pela utilização de terminais falsificados.

Para se provar a *autenticidade da credencial de ID e dos seus dados*, os cartões do tipo *smart cards*, a nível do seu *chip* interno, têm a capacidade exclusiva de possuir soluções com *características de autenticação*, baseadas em mecanismos de *encriptação* simétrica ou assimétrica. Por intermédio destes mecanismos e técnicas de encriptação, a credencial pode responder aos “desafios” impostos pelo leitor, no sentido desta revelar e provar a sua *autenticidade* e, assim, *autenticar-se* perante o mesmo [13].

3.5.4.1.2 Protecção dos Dados da Credencial de *ID*

As *credenciais de ID* que podem suportar *técnicas de encriptação*, asseguram uma substancial *protecção dos seus dados*. *Chaves múltiplas de encriptação simétrica e assimétrica* podem ser armazenadas no *chip* duma credencial, com o objectivo de se atender a diversos requisitos de segurança, em várias utilizações e aplicações.

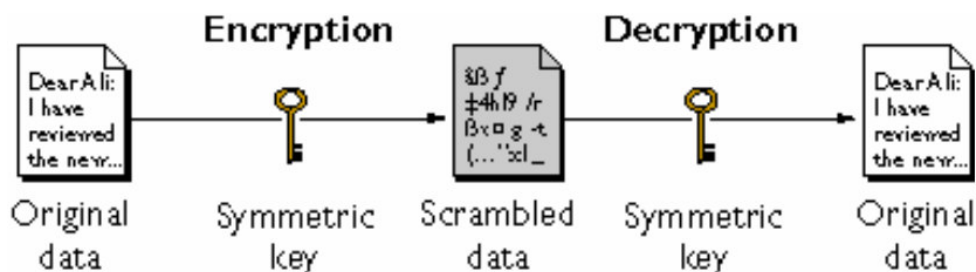


Figura 3.25 – Encriptação por chave simétrica

A *chave simétrica* é amplamente utilizada em *sistemas de controlo de acessos físico*, tanto na *encriptação*, como na *desencriptação* de dados, com tempo de processamento reduzido e fiabilidade. Já em *sistemas de controlo de acessos lógico* e privilégios *PKI*, em que o tempo de processamento não é tão importante, pode ser utilizada *encriptação assimétrica*.

3.5.4.1.3 Protecção das Comunicações de Dados

Num *sistema de controlo de acessos físico*, devido à transmissão de dados ao longo dos seus diversos componentes, devem ser avaliados:

- *o ambiente físico*
(se as áreas estão devidamente protegidas ou desprotegidas a ponto de, por exemplo, alguém poder interceptar, através dum dispositivo qualquer, o sinal transmitido e efectuar a leitura e a cópia do fluxo de dados)
- *o risco* (a probabilidade real destes ataques ou outros, se poderem concretizar)

Esta avaliação é importante para que os dados enviados, pelas *credenciais de ID* (cartões de contacto ou de proximidade) e pelos leitores, não possam vir a ser interceptados e a originar, consequentemente, acessos “indevidos” a espaços físicos

controlados. Para se neutralizar estas ameaças, à segurança da transmissão de dados e outras, deve-se providenciar que as ligações, principalmente, da credencial de *ID* para o leitor e deste para o painel de controlo, sejam seguras.

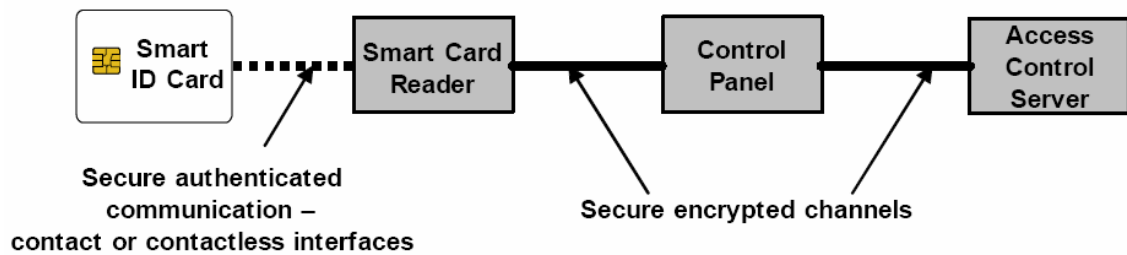


Figura 3.26 – Segurança da transmissão de dados (de início ao fim) num sistema de controlo de acessos físico (com base em smart cards) [13]

Para tal, os cartões (*smart cards*) podem suportar *técnicas e mecanismos de encriptação*, para garantir a segurança da *comunicação de dados* entre a credencial e o leitor. De forma análoga, a *comunicação de dados* entre o leitor e o painel de controlo deverá ser assegurada por *técnicas de encriptação de dados* e, mesmo, para maior segurança, quer o leitor, quer o painel, poderão ser autenticados durante a transacção. Já a ligação do painel de controlo ao servidor do sistema de controlo de acessos, em princípio, sendo interna (no interior dum edifício ou em espaços seguros), não é, normalmente, tão susceptível a ataques. Contudo, a *segurança nessa comunicação* pode, também, ser melhorada pela utilização das mesmas *técnicas de encriptação*, proporcionando-se assim, a todo o sistema do início ao fim, uma *comunicação de dados* devidamente segura.

Capítulo 4

Definição do Domínio do Problema

4.1 Introdução

Neste capítulo, é apresentado o problema concreto da gestão dos acessos (físico) em universidades. Para compreensão do domínio do problema são também descritos e caracterizados conceitos essenciais relativos à gestão de controlo de acessos físico, nomeadamente, a estrutura dos espaços físicos das organizações, aspectos importantes do modelo controlo de acessos baseado no papel e as principais políticas de segurança utilizadas no controlo de acessos. Por último, são apresentados os objectivos e impacto da aplicação *WebGPACS* a desenvolver.

4.2 A Gestão de Acessos (Físico) em Universidades

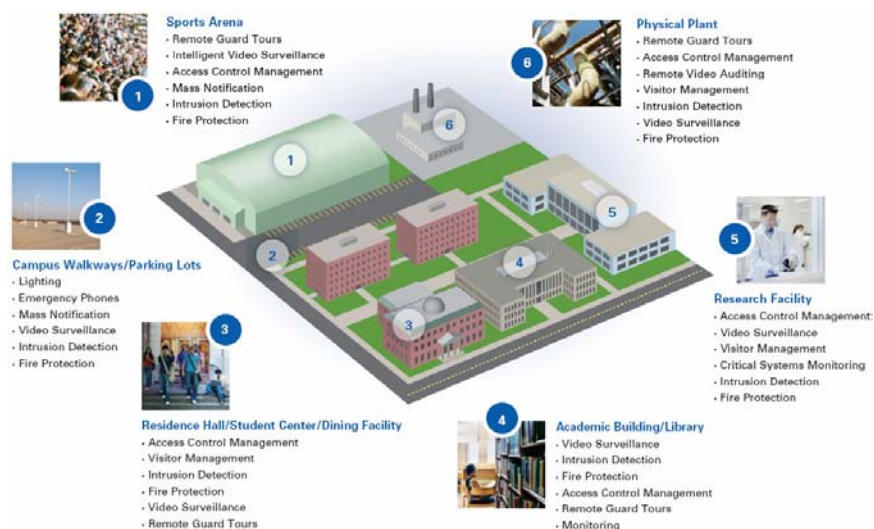


Figura 4.1 – Panorâmica geral dum campus universitário

A gestão dum *campus* universitário não só devida à complexidade dos seus múltiplos edifícios, departamentos, serviços, cursos, profissionais e alunos, como também, a cuidados relativos com a segurança, nomeadamente, os que correspondem aos acessos de pessoas a instalações, é complexa e difícil. Um *campus* universitário, em princípio, é constituído por um conjunto de edifícios, anfiteatros, secções administrativas, laboratórios, salas de aula, gabinetes, lugares de estacionamento, ..., que se localizam geograficamente no interior de um grande perímetro, que pode estar, ou não, vedado por muros, sebes ou ser, mesmo, uma zona ampla, totalmente aberta.

Muitas universidades controlam os seus acessos, apenas, pela entrada principal do edifício (*hall* de entrada), através do qual funcionários, alunos, colaboradores e visitantes obtêm acesso. Duma maneira geral, estes acessos são regulados, somente, por seguranças ou recepcionistas, não adoptando, as universidades, quaisquer outras medidas de segurança, nomeadamente, no que respeita a controlo de acessos em áreas e espaços físicos do seu interior. Mas, nem todas as áreas no interior dum *campus* podem ter os mesmos critérios ou requisitos de segurança, pois alguns espaços terão de ser acessíveis (por ex., a visitantes), enquanto outros, destinados a funções mais específicas (por ex., laboratórios ou armazéns de produtos químicos,...) deverão ter o acesso mais restringido e, obviamente, com um nível de protecção mais exigente e elevado. Constata-se, então, que um único critério de segurança, que possa servir a todas as áreas ou espaços físicos dum *campus*, será uma política desajustada da realidade e que dificultará, mesmo, o nível de desempenho da segurança.

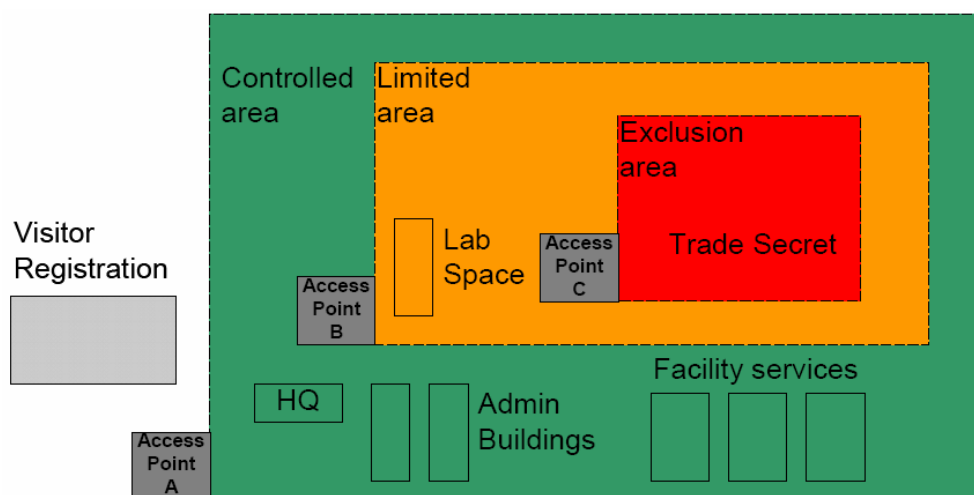


Figura 4.2 – Diferentes níveis de protecção [28]

Daí que sistemas de controlo de acessos físico que actuem selectivamente na permissão dos acessos a áreas e determinados espaços, no interior dum *campus*, são de grande importância, pois, quando aplicados adequadamente, permitem controlar, de modo selectivo e eficaz, o acesso dos utentes a áreas e espaços físicos controlados e de acesso restrito. Por via da implementação destes sistemas de controlo de acessos físico, consequentemente, serão necessários e essenciais os sistemas que os possam gerir, que possam resolver a complexidade associada à gestão dos acessos a instalações e que facilitem a automatização e monitorização dos mesmos [31].

Com o intuito de proporcionar uma visão, mais real, do que representará a gestão e o controlo de acessos em ambientes universitários, seguem-se dois cenários que, também, poderão servir para exemplos de demonstração relativos a subseqüentes considerações de matérias abordadas nesta dissertação.

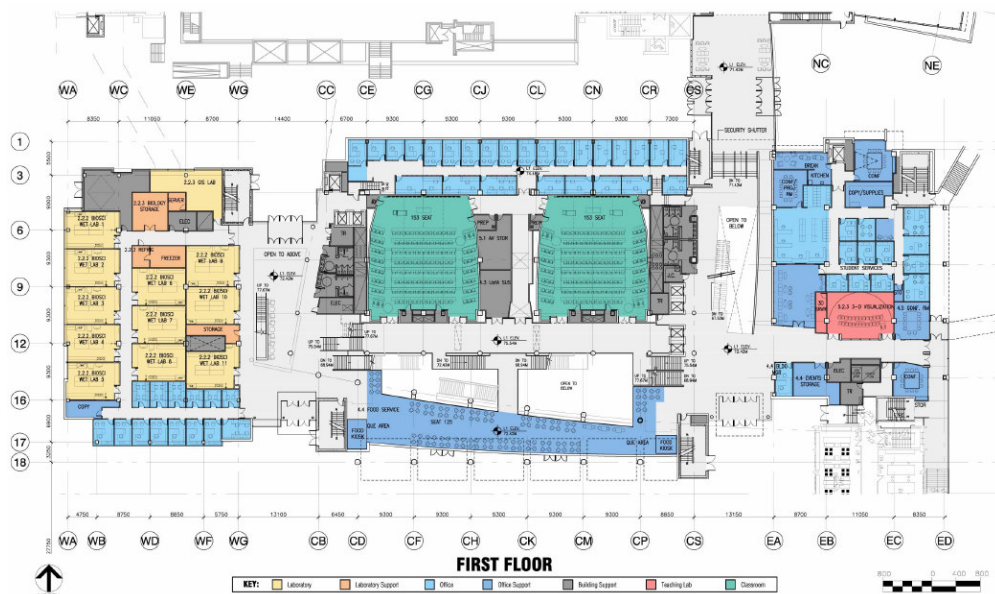
Cenário 1:

Figura 4.3 – Planta dum piso universitário

Um cenário genérico de gestão de controlo de acessos a instalações universitárias, que poderia ser colocado em prática, a partir do átrio de entrada dum *campus* universitário. A partir deste átrio, em princípio, acessível ao público em geral, poder-se-ia conceder a cada visitante, apenas, permissões de acesso a determinadas áreas do seu interior, tais como, serviços académicos e administrativos, certos corredores e bares. Já os estudantes, poderiam ter permissões para aceder ao interior da universidade (ver Figura 4.3 acima) mas, somente, aos edifícios, salas de aula e laboratórios correspondentes aos departamentos do ramo ou área de estudo individuais (por ex., estudantes do curso de “engenharia electrotécnica e de computadores” terão permissão para aceder, unicamente, a edifícios desse ramo e não aos de “engenharia civil”...). Entre estudantes dum mesmo curso ou departamento poderia, também, ser concedido ou restringido o acesso a determinados espaços físicos (por ex., em laboratórios de estudo), consoante as necessidades individuais de desenvolvimento de trabalhos ou projectos académicos. Em contraposição, numa perspectiva oposta, a todos os estudantes, professores e funcionários, independentemente das suas áreas de formação ou trabalho, ser-lhes-ia permitido aceder livremente a diversos espaços do interior do *campus*, tais como, bibliotecas, bares, salas de estudo,...

Cenário 2:

Outro cenário elucidativo de gestão de controlo de acessos (físico) num ambiente universitário, poderá ser o que, hipoteticamente, se verifica com a gestão dos acessos ao espaço físico I-104 do Piso-1 do Edifício-I, no interior do *campus* universitário da FEUP. O Piso-1 situa-se no interior do Edifício-I e está acessível a todos os utentes deste edifício, sendo, concretamente, um grande espaço físico aberto, constituído por vários laboratórios e gabinetes (ver Figura 4.4 anterior) de acesso restrito, espaços

físicos fechados. Um desses espaços físicos é o identificado por *I-104* (laboratório de automação e informática industrial) que é um laboratório de acesso restrito e controlado, sobre o qual é assumido que, apenas, professores da área de “informática e automação” e alunos de mestrado ou doutoramento a realizar trabalhos (projectos) nessa área de estudo, o podem aceder. No seu interior existirá, também, um outro espaço de protecção, *I-104.1* (por ex., um grande armário contendo equipamentos), que poderá ser acedido, somente, pelo professor principal e responsável pela área de estudo referida, ou, quiçá, por um funcionário especificamente delegado para tarefas de apoio aos trabalhos correntes neste laboratório, para tal, necessitando de possuir uma permissão especial de acesso.



Figura 4.4 – Planta do Piso 1 do Edifício I (Electrotecnia) da FEUP

4.3 Conceitos Relevantes na Gestão de Controlo de Acessos (Físico)

Nesta secção, são apresentados e caracterizados alguns conceitos relevantes a considerar para a gestão de controlo de acessos físico, nomeadamente, a estrutura dos espaços físicos das organizações, o modelo de controlo de acessos baseado no papel e as principais políticas de segurança utilizadas.

4.3.1 A Estrutura dos Espaços Físicos

Um *campus* universitário é caracterizado por ser um grande perímetro que contém outros mais pequenos no seu interior, os quais, por sua vez, podem conter outros, ainda, menores e assim sucessivamente. As diferentes áreas ou espaços físicos dum *campus* encaixam-se uns nos outros, em que espaços maiores englobam outros mais pequenos. Para uma visão mais aproximada da realidade da *estrutura dos espaços físicos*, refere-se o exemplo demonstrativo dum edifício, no interior dum *campus* universitário, que inclui pisos, certamente, contendo salas, gabinetes,... No interior destes espaços (salas, gabinetes,...) poderão, ainda, existir outros espaços físicos, tais como, divisões ou armários fechados,...

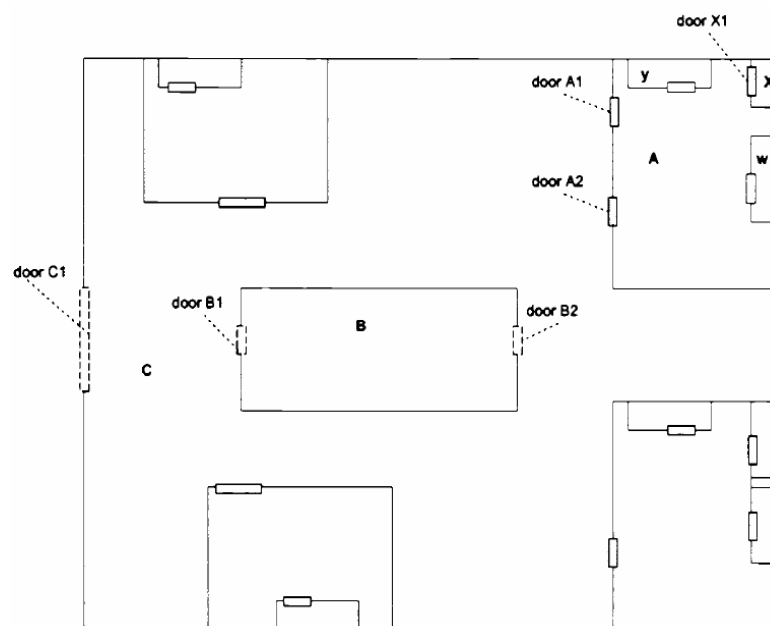


Figura 4.5 – Espaços físicos contêm outros espaços físicos menores

Através da Figura 4.5 acima, pode-se observar que um dado espaço físico é composto por uma multiplicidade de espaços físicos, podendo, cada um destes, cingir outros espaços no seu interior,... Na constatação desta *estrutura dos espaços físicos*, deve-se realçar que a *gestão de controlo de acessos físico* para ser eficaz deverá ser capaz de lidar convenientemente com este *conceito de espaços físicos encaixados*, isto é, com o facto de os espaços físicos poderem conter outros espaços físicos.

4.3.2 O Controlo de Acessos Baseado no Papel

As próximas secções apresentam considerações relevantes acerca modelo de *controlo de acessos baseado no papel*, utilizado para gestão de controlo de acessos físico.

4.3.2.1 Atribuição de Permissões (sobre Objectos Físicos) a Papéis

Na gestão de controlo de acessos físico vai ser necessário determinar quem pode aceder a um determinado espaço físico controlado. Como neste tipo de organizações, *campus* universitários, em princípio, existem vários e diferentes tipos ou perfis de pessoas que poderão aceder a diversos espaços físicos (ver secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65) o modelo de “Controlo de Acessos Baseado no Papel” (RBAC)¹⁹ surge como um modelo convenientemente apropriado a utilizar [32], pois permite que *permissões sobre objectos sejam atribuídas a papéis*.

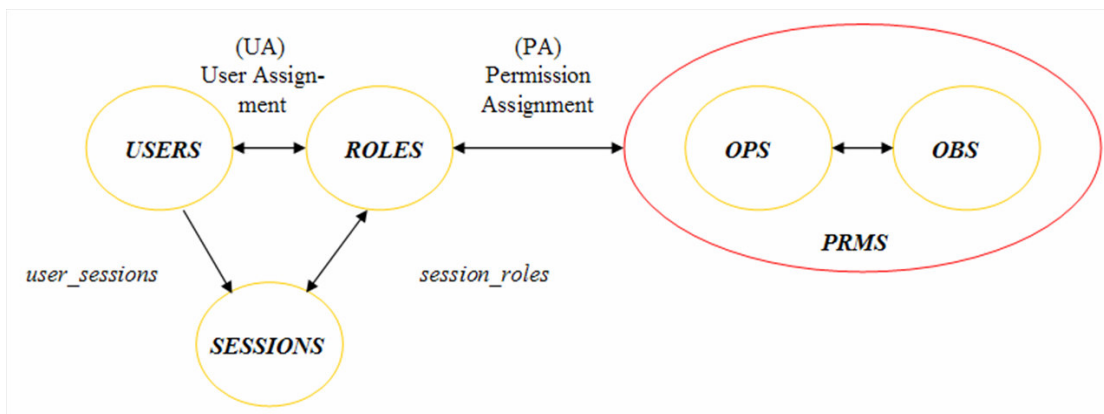


Figura 4.6 – O Modelo de “Controlo de Acessos Baseado no Papel (RBAC)”

Neste modelo, as *permissões estão associadas à protecção de objectos* que, no caso concreto do controlo de acessos físico, são *objectos físicos*, ou seja, os espaços físicos a serem controlados (por ex., edifícios, pisos com um conjunto de salas, laboratórios, gabinetes,...)

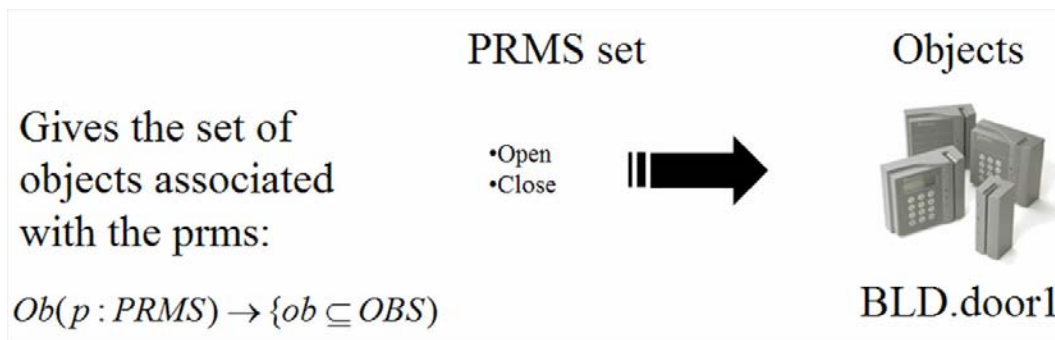


Figura 4.7 – Permissões do modelo RBAC associadas a objectos físicos (espaços físicos)

Estes objectos de protecção ou espaços físicos, como já referido anteriormente (ver secção §4.3.1 “A Estrutura dos Espaços Físicos”, pág. 69), podem ser compostos por espaços mais pequenos. Um piso num determinado edifício é um espaço físico que pode incluir outros espaços físicos, sobre os quais pode ser restringido o acesso.

¹⁹ Controlo de Acessos Baseado no Papel (da expressão inglesa *Role Based Access Control*).

4.3.2.2 Controlo de Acessos baseado nos Papéis de Utilizadores

Conforme se constata pelos cenários descritos anteriormente (ver secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65), os *utentes ou utilizadores obtêm permissões de acesso aos espaços físicos, com base nos perfis ou papéis que possuem no interior da organização (instituição)* [24], em detrimento das suas identidades individuais. Um papel poderá corresponder a uma categoria profissional, a uma função ou grupo de funções que o utilizador possui ou pode exercer na organização [22]. Uma pessoa ou utilizador pode também ter mais do que um papel, pois facilmente se conclui, por exemplo, que um aluno de mestrado em engenharia electrotécnica e computadores possa não só ter o papel de *aluno do MEEC*²⁰, de certo modo genérico, que lhe permite um conjunto de permissões atribuídas ao papel e associadas a espaços físicos da universidade (por ex., entrar em determinados edifícios e salas de aula pertencentes ao *DEEC*²¹), como também, o papel de *aluno de mestrado na área de “informática e automação”*, mais específico, que lhe permitirá um outro conjunto, mais particular, de permissões (por ex., a obtenção de acesso ao espaço físico *I-104*, laboratório permitido, unicamente, a alunos de mestrado e doutoramento a realizar trabalhos e projectos na área de informática e automação) (ver cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65).

4.3.3 Políticas de Segurança no Controlo de Acessos

Nas secções seguintes são caracterizadas algumas das principais *políticas de segurança* utilizadas para gestão de controlo de acessos físico.

4.3.3.1 O Menor Privilégio

Com vista à prevenção dos utilizadores não abusarem dos seus privilégios, deve-lhes ser concedido um conjunto mínimo de permissões a espaços físicos controlados ou restritos, apenas, necessário para levarem a efeito as suas funções ou trabalhos na instituição – *política do menor privilégio* [24] [31]. Um exemplo, em conformidade com esta política, é o da gestão de acessos ao *laboratório I-104*, apresentado anteriormente (ver cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65), em que se constata que os alunos que o podem aceder são, unicamente, os de mestrado e doutoramento a realizarem trabalhos e projectos na área de “informática e automação”. Outros alunos, mesmo de mestrado ou doutoramento, mas a desenvolverem estudos em áreas diferentes, não poderão aceder ao espaço físico citado. Para estes, ser-lhes-ão definidos e atribuídos outros papéis com um conjunto mínimo de permissões necessário a garantir-lhes a realização das suas tarefas, não abrangendo, certamente, o direito de acesso ao *laboratório I-104*.

²⁰ Mestrado em Engenharia Electrotécnica e de Computadores.

²¹ Departamento de Engenharia Electrotécnica e de Computadores.

4.3.3.2 Autorização Implícita e Herança Reversa

A gestão de controlo de acessos físico deverá ser capaz de lidar com o facto de os espaços físicos poderem possuir ou conter outros espaços físicos – *conceito de espaços físicos encaixados* (ver secção §4.3.1 “A Estrutura dos Espaços Físicos”, pág. 69). A partir desta realidade, não se pode ignorar que os utilizadores que acedem a um determinado espaço físico, também podem ter necessidade de aceder a um outro contido no interior do mesmo espaço físico. Para suporte desta necessidade, salienta-se a ideia ou *princípio do acesso ou autorização implícita*, isto é, de que o acesso a espaços físicos deve ser hereditário. Basicamente, este princípio refere que, se um utilizador tem acesso a um determinado espaço físico, implicitamente, terá acesso a espaços físicos contidos ou encaixados no mesmo. Um exemplo ilustrativo pode ser dado pelo *laboratório I-104*, apresentado anteriormente (ver cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65), que agora, para exemplo deste caso, poderá incluir outros dois compartimentos além do armário *I-104.1* (o que pode ser acedido, apenas, pelo professor principal e, eventualmente, por um funcionário). Para conformação com este princípio, deve subentender-se que os novos compartimentos ficarão, em princípio, acessíveis a todos os que têm permissão de acesso ao *laboratório I-104*.

Adicionalmente, a gestão de controlo de acessos físico deve, também, utilizar o *conceito de herança reversa*. Genericamente, este conceito significa que um utilizador que tem acesso a um determinado espaço físico, deve ter, igualmente, acesso aos espaços físicos que conduzem ao primeiro. Voltando ao exemplo do *laboratório I-104* (ver cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65), deve-se verificar que todos os utilizadores que têm permissão para o poder aceder, necessariamente, deverão ter permissão para aceder a espaços físicos que conduzem ao mesmo laboratório (no caso concreto, ao *Edifício-I* e *Piso-I*, que conduzem ao espaço físico *I-104*) e, assim, verificar-se a conformidade com o *conceito ou regra da herança reversa*. Por oposição, em caso de desconformidade, obviamente, seria impossível os utilizadores poderem alcançar o laboratório referido.

4.3.3.3 Auditorias de Acessos e Responsabilidade Individual

A partir do momento em que um determinado espaço físico pode ser acedido e utilizado por vários utilizadores, também será necessário fazer o controlo e rastreio dos seus acessos, nomeadamente, saber-se *quem* o acede, *quando* é acedido e do *tempo* de permanência do acesso. Este procedimento traduz-se, concretamente, pela realização de *auditorias sobre os acessos* [31] dos utilizadores aos espaços físicos controlados, que podem ser dirigidas, tanto a *utilizadores* (onde têm estado), como a *espaços físicos* controlados (quem os tem acedido). Estas auditorias contribuem, significativamente, para a *responsabilização dos utilizadores* nos seus diversos acessos pelos espaços físicos controlados e funcionam como efeito dissuasor de comportamentos e incidentes menos próprios. Outros meios ou *políticas de responsabilização individual* são também utilizados, traduzidos pela exigência de *identificação, autenticação e autorização* (ver

secção §2.2 “Identificação, Autenticação e Autorização”, pág. 5) ou de permissão de cada utilizador que requer acesso a um qualquer espaço físico controlado. Isto, implica que em todos os processos de acesso e saída dum utilizador dum espaço físico, a informação de identificação do utilizador e do espaço físico, a data e hora do acesso sejam registadas no sistema. Posteriormente, os auditores podem verificar estes registos no sentido de não só determinarem ou inspeccionarem, *quem* acedeu, *quando* e *durante* quanto tempo a um determinado espaço físico, num período qualquer de tempo, como também, *quais* os espaços físicos acedidos por um determinado utilizador.

4.3.3.4 Políticas Especiais

A gestão de controlo de acessos físico também deverá ser capaz, para além das políticas anteriormente citadas (nas secções anteriores), de utilizar e implementar outras *políticas especiais*. Entre estas, a título meramente exemplificativo, refere-se a simples concessão ou autorização de permanência num determinado espaço físico, apenas, durante um pré-determinado período de tempo específico (por ex., a um aluno pode ser permitido permanecer num laboratório, somente, durante um determinado número de horas por dia, ou por semana,...). Outra, poderá ser a dependência, da concessão ou restrição do acesso a espaços físicos, da verificação dum conjunto de condições ou pré-requisitos (por ex., um utilizador ou grupo de utilizadores só poder efectuar acessos, a um determinado espaço físico controlado, a partir de certa hora do dia, certos dias da semana,...).

4.4 A Aplicação WebGPACS

A gestão dos acessos num *campus* universitário, quer devido à complexidade e variedade de edifícios, quer aos cuidados relativos à segurança das suas instalações, é complexa e difícil. Sistemas de informação dirigidos à *gestão de sistemas de controlo de acessos físico* podem contribuir, de modo efectivo, para a melhoria da segurança nos complexos universitários. Neste contexto, procura-se desenvolver uma aplicação, *WebGPACS*, cujos objectivos e impacto se descrevem a seguir.

4.4.1 Objectivos

A aplicação *WebGPACS* – *aplicação web de gestão de sistemas de controlo de acessos físico*, tem como objectivo principal proporcionar que por via remota (*internet* ou *intranet*) se possa fazer a gestão e monitorização do sistema de controlo de acessos físico duma organização, em particular, dum *campus* universitário.

Uma particularidade importante dessa gestão, é a capacidade de suportar uma gama de funcionalidades essenciais de administração ou gestão de sistemas de controlo de acessos físico numa organização, nomeadamente, a gestão relacionada com os utilizadores, papéis, espaços físicos controlados, permissões (a espaços físicos) e várias

consultas (*reports*) afins, entre estas, de auditoria. Auditorias ou rastreio acerca dos acessos, num determinado período de tempo, dos diversos utilizadores aos diferentes espaços físicos controlados da organização, assim como, a pesquisa ou localização, em tempo real, de utilizadores nas instalações.

Outro dos objectivos é a gestão do funcionamento do sistema de controlo de acessos físico da organização, concretamente, o controlo das operações do processo de acessos (entradas e saídas) aos espaços físicos controlados e seu registo automático. Com base nas permissões do utilizador, do local de acesso e do tempo (data e hora), o sistema pode decidir, autorizando ou não, acerca do acesso dum utilizador a um determinado espaço físico controlado e, subseqüentemente, efectuar o registo do mesmo na base de dados.

Pretende-se também que a aplicação possa facilmente ser integrada, quer no sistema de informação da organização, quer, inclusive, com sistemas de automação, além de poder vir a incluir outros módulos de funcionalidades adicionais, como:

- registo de eventos de sistema ou rede e de actividades de administração
- funcionamento, monitorização (em tempo real) e customização do sistema
- notificações (por via electrónica) sobre ocorrências específicas de acessos, de eventos de sistema e de actividades de administração
- atribuição de privilégios de operação ou gestão
- customização de consultas à base de dados.

4.4.2 Impacto Esperado

Sendo uma plataforma de *software* baseada na *web*, cujo acesso remoto à aplicação é facilitado através dum simples navegador *web*, este sistema contribui para o aumento da eficácia e qualidade das actividades de gestão do sistema de controlo de acessos físico da organização (instituição) e, conseqüentemente, para o incremento da segurança das suas instalações, neste caso, as universitárias. A aplicação de gestão de sistemas de controlo de acessos físico será, assim, uma ferramenta de segurança bastante útil para a protecção de pessoas e, em especial, de recursos organizacionais, contribuindo nomeadamente para:

- uma maior eficácia da segurança da organização (instituição), oferecendo a garantia de uma maior segurança no acesso ao interior das suas instalações e evitando que muitos dos seus utentes possam aceder indevidamente (acessos “impróprios”) a determinados recursos ou instalações organizacionais.
- facilitar os acessos às instalações da organização, automatizando, monitorizando e elevando o nível geral de eficiência e eficácia do sistema de controlo de acessos físico da organização.
- contribuir para o aumento da qualidade e eficácia das actividades de gestão de segurança da organização (instituição), satisfazendo as necessidades concretas

dos administradores que actuam nessa área funcional da organização, proporcionando:

- suporte à tomada de decisões, em que a informação resultante das auditorias de controlo e rastreio de acessos de utilizadores aos diferentes espaços físicos controlados, constitui informação relevante para apoiar as políticas de planeamento e de gestão de segurança da instituição
- facilidade e rapidez das operações de gestão de controlo de acessos, assegurando as condições necessárias à manutenção e actualização dos registos de utilizadores, papéis, permissões e espaços físicos controlados.

Capítulo 5

Requisitos da Aplicação

O desenvolvimento de sistemas de informação envolve mais do que a compreensão do domínio do problema específico da aplicação. Este capítulo começa por apresentar os requisitos gerais e funcionalidades essenciais que deverão ser satisfeitos por um sistema de *software* de gestão de sistemas de controlo de acessos físico, de âmbito alargado. Seguidamente, já numa concepção mais restrita (no âmbito deste trabalho), os actores e os casos de utilização (requisitos funcionais, na óptica dos actores) do sistema, são descritos textualmente e apresentados, graficamente, por diagramas de casos de utilização, em diagramas *UML*. Por último, através dum diagrama de classes, é apresentado o modelo de objectos do domínio e feita a sua descrição.

5.1 Requisitos Gerais

Esta secção identifica e descreve os principais requisitos gerais e funcionalidades essenciais que deverão ser satisfeitos por um sistema de *software* de gestão de sistemas de controlo de acessos físico, de âmbito alargado.

5.1.1 Sumário da Aplicação

O *WebGPACS* deverá ser uma aplicação de *software* alojada num servidor *web* para estar disponível na *Internet* ou *Intranet* da organização, permitindo que, através dum navegador *web*, se faça a *gestão do seu sistema de controlo de acessos físico*. Deverá ser um sistema conduzido ou accionado ao evento, de dados intensivos, bastante escalável e concebido para funcionar em tempo real. O *WebGPACS* será composto por uma base de dados e por módulos aplicativos de *software*.

5.1.2 Alojamento em Servidor *Web*

O *WebGPACS* tanto poderá ser utilizado para, através das infra-estruturas *WiFi* ou *Ethernet* existentes na organização, gerir um sistema de controlo de acessos físico com, apenas, um espaço físico a ser controlado (com um só local de acesso e um correspondente dispositivo de identificação/autenticação), como poderá ser configurado para, através de uma *WAN*, gerir um sistema de controlo de acessos físico numa organização de grande dimensão, cuja implementação pode abranger múltiplos espaços físicos ou locais de acesso, situados em áreas geograficamente dispersas.

Por ser uma aplicação que será alojada num servidor *web*, vai utilizar os protocolos *standard* de comunicações e as infra-estruturas *Internet* da organização, proporcionando que as organizações, mesmo as que possuem um grande número de instalações ou espaços físicos a serem controlados, não precisem de qualquer *hardware* ou *software* adicional. Assim, poderão ser continuamente acrescentados, ao sistema, localizações ou espaços físicos a serem controlados, bem como, os correspondentes aumentos de comunicações de dados.

O *WebGPACS* ao estar alojado no “*host system*”²² (ver secção §3.4.2.2 “Os Sistemas Analíticos (do Host System)”, pág. 52), localizado em instalações seguras da organização, permitirá que os seus utilizadores (no caso concreto deste projecto, o administrador e gestor/auditor de espaços) efectuem a *gestão do sistema de controlo de acessos físico*, a partir dum local remoto qualquer, desde que exista um computador com ligação à *Internet*, o que proporcionará que a solução seja facilmente utilizável e eficaz em organizações que pretendam usufruir dos benefícios dum *software* de gestão de controlo de acessos físico.

5.1.3 Base de Dados

A aplicação deverá utilizar uma base de dados bastante escalável, pois todos os dados de eventos ou ocorrências relacionados com acessos, serão aí registados e armazenados. As consultas à base de dados deverão ser efectuadas duma maneira simples, bem como, ser possível efectuar uma grande variedade de consultas ou relatórios. O *WebGPACS* tentará disponibilizar uma gama ampla de consultas, como eventos registados nos locais de acesso, acessos (*logs*) de utilizadores aos espaços físicos, permissões de utilizador,... Também poderá ser conceptualizado para proporcionar outras capacidades de pesquisa avançada e para a produção de relatórios definidos pelo utilizador.

É importante salientar que o funcionamento do sistema deverá ser tolerante a falhas de operação. Em casos de falhas de rede, cada *reader* ou leitor do local de acesso deverá continuar a funcionar, sendo todos os dados referentes a ocorrências de acessos, registados e armazenados no próprio leitor e, posteriormente, após as comunicações de rede serem restabelecidas, reenviados para o servidor, onde está alojada a aplicação e a base de dados. Deste modo, preservar-se-á a integridade dos dados correspondentes a todos os acessos ocorridos, bem como, de todas as auditorias suportadas nesses dados.

Para além dos eventos de acessos, cada evento relacionado com a rede poderá também vir a ser registado na base de dados da aplicação, inclusive, as falhas de energia ou de ligação a um local de acesso, as tentativas de comunicação falhada e outros eventos específicos do funcionamento do próprio sistema. Quaisquer destes eventos, poderão servir de base para o sistema poder despoletar acções de notificação (por ex., notificações por *e-mail*, página *web*, *sms*,...), concretamente, para responsáveis ou administradores.

²² Também referido por *head-end system* ou *back-end system*

Para além dos eventos anteriores, todas as actividades ou operações relacionadas com a gestão do sistema de controlo de acessos (ocorrências de administração do sistema) poderão ser gravados na base de dados da aplicação e registados temporalmente (por ex., o caso de um administrador criar um novo utilizador ou modificar as suas permissões de acesso, é uma acção que deverá ser registada na base de dados, proporcionando que, em futuras auditorias dirigidas à administração ou gestão do sistema, se possa averiguar e avaliar a segurança do mesmo). Acrescenta-se que estes eventos de administração do sistema, poderão vir a ser utilizados para o envio de novas acções de notificação do sistema (por ex., de cada vez que um dado administrador regista um novo utilizador, os departamentos de RH, Segurança,... poderão vir a receber um *e-mail* a indicar as permissões desse novo utilizador,...).

5.1.4 Funcionamento, Monitorização e Notificações (em Tempo Real)

A aplicação deverá proporcionar funcionalidades de gestão do sistema, em *tempo real* (descritas nas secções que se seguem), quer ao nível do seu *funcionamento* e *monitorização*, quer no que respeita ao envio de *notificações* por comunicação electrónica.

5.1.4.1 Funcionamento (em Tempo Real)

O *WebGPACS* deverá ser um sistema de *software* conduzido ao evento, que actua em tempo real. Cada evento referente a acessos, como entrada ou saída de utilizadores, ocorrido num determinado local de acesso a um espaço físico controlado, deve ser comunicado ao servidor central, assim como, todas as operações de funcionamento do sistema de controlo de acessos físico, relativas ao controlo de acessos (por ex., de cada vez que um utilizador se autenticar num dispositivo de identificação / autenticação, por meio de um cartão ou de uma impressão digital, com o objectivo de aceder a um espaço físico, este evento deverá ser comunicado ao servidor central e, posteriormente, registado o respectivo acesso na base de dados). Deste modo, é fornecida informação suficiente para que se possa efectuar posteriores auditorias sobre a actividade, em tempo real, do sistema de controlo de acessos físico, nomeadamente, em cada local de acesso ou espaço físico controlado.

5.1.4.2 Monitorização (em Tempo Real)

Adicionalmente, o registo de eventos (ver secção §5.1.4.1 “Funcionamento (em Tempo Real”, pág. 79) permitirá também a possível monitorização ou controlo do sistema, em tempo real, permitindo que qualquer local de acesso a um espaço físico controlado possa ser gerido, a partir dum local remoto. A aplicação poderá, mesmo, vir a ser integrada com sistemas de *software* de automação, comunicando-os acerca de

determinados tipos de eventos de acessos e proporcionar que os mesmos (acessos) possam ser monitorizados, em tempo real, em conjunto com sistemas de alarme e/ou de videovigilância (por ex., o sistema poderá ser combinado com um sistema de videovigilância – CCTV²³ – para que, a partir da confirmação visual dum determinado utilizador, uma determinada porta de um local de acesso a um espaço físico, possa ser remotamente aberta). Para tal, a aplicação deverá permitir que seja efectuada a devida customização do sistema de controlo de acessos, no sentido de se poder designar como objecto de monitorização, um qualquer tipo de evento relacionado com acessos (por ex., porta deixada aberta, porta forçada, tentativa de utilização de um cartão furtado ou perdido,...) que, ao ocorrer, será transmitido ao “*host system*”²⁴ (ver secção §3.4.2.2 “Os Sistemas Analíticos (do Host System)”, pág. 52). Também ocorrências de sistema (por ex., falhas de energia ou das comunicações,...) poderão ser designadas como objectos de monitorização e encaminhados para o mesmo “*host system*”, caso sucedidos, onde serão tomadas as acções necessárias.

5.1.4.3 Notificações (em Tempo Real)

Quaisquer dos eventos referidos anteriormente (ver secção §5.1.4.1 “Funcionamento (em Tempo Real”, pág. 79 e secção §5.1.4.2 “Monitorização (em Tempo Real”, pág. 79), referentes, quer a acessos, quer ao sistema e, mesmo, à administração do sistema (ver secção §5.1.3 “Base de Dados”, pág. 78) poderão fazer actuar uma série de notificações de comunicação electrónica (por ex., *e-mail*, *sms*, *página web*,...), customizadas e dirigidas a determinadas pessoas – *stakeholders* – interessadas em resultados da aplicação. Por exemplo, uma notificação referente a acessos, poderia ser o envio duma notificação de aviso, a um qualquer director da instituição ou de um seu departamento, relativa à entrada de determinada pessoa ou colaborador numa determinada instalação da organização. Outro exemplo, agora, duma notificação relativa ao sistema, poderia ser uma notificação *e-mail* para o administrador de rede, avisando-o de uma falha nas comunicações de rede, das portas ou locais de acesso afectados, isto é, a funcionar sem ligação à rede ou autonomamente. Já para uma falha de corrente eléctrica ou para uma porta deixada aberta, poderia ser enviado um alerta para o respectivo funcionário de segurança e/ou correspondente gestor/director,...

5.1.5 Interface Web e Autenticação

A aplicação *WebGPACS* será utilizada através de um navegador *web* e deverá funcionar em qualquer máquina cliente (*desktops*, *laptops*,...), desde que tenha instalado um *browser* no seu sistema operativo. O acesso à aplicação far-se-á através duma *interface web* da aplicação disponível, tanto na *Intranet* da organização (*LAN / WAN*), como na *Internet*. A utilização e administração do sistema só deverão ser permitidas a utilizadores devidamente autorizados (administradores) e, após, registo ou autenticação por meio duma senha (*password – SSL*) segura e protegida. A aplicação deverá permitir

²³ Televisão em Circuito Fechado (da expressão inglesa *Closed Circuit Television*)

²⁴ Também referido por *head-end system* ou *back-end system*

que possam ser atribuídas ou concedidas permissões, a outros utilizadores, para determinados conjuntos de funcionalidades de administração ou gestão do sistema.

5.1.6 Funcionalidades Essenciais de Gestão / Administração

O administrador do sistema poderá atribuir privilégios especiais de operação ou de utilização a determinados utilizadores da aplicação e, em conformidade com a *política do menor privilégio* (ver secção §4.3.3.1 “O Menor Privilégio”, pág. 71), permitir-lhes o acesso, apenas, a áreas específicas e directamente relacionadas (por ex., algumas pessoas das *TI* acedem, somente, a páginas relacionadas com a gestão de rede e comunicações *IP*, enquanto outras, dos *RH*, poderão ter permissão, apenas, para registar utilizadores, mas nunca a quaisquer funções de auditorias de acessos de utilizadores em espaços físicos controlados).

A aplicação *WebGPACS*, numa primeira fase de desenvolvimento (âmbito deste trabalho), vai suportar as principais funcionalidades *standard* e essenciais de *administração ou de gestão de sistemas de controlo de acessos (físico)*, que se relacionam directamente com a gestão de:

- utilizadores
- papéis
- espaços físicos (controlados)
- permissões
- consultas e produção de “*reports*”, em particular, de auditorias de acessos

5.1.6.1 Utilizadores

A aplicação deverá permitir que sejam efectuadas as funcionalidades essenciais referentes à *gestão de utilizadores* do sistema de controlo de acessos:

- *Inserção, Modificação e Remoção de Utilizadores*
Efectuar a inserção, modificação de dados e eliminação de utilizadores que utilizam o sistema de controlo de acessos.
- *Atribuição e Eliminação de Papéis a Utilizadores*
Efectuar a atribuição e eliminação de papéis a utilizadores.
 - Um mesmo utilizador pode ter mais do que um papel.
- *Listagem de Utilizadores*
Efectuar a listagem de todos os utilizadores do sistema de controlo de acessos.
- *Consultar Papéis de Utilizadores*

Consultar para cada utilizador do sistema de controlo de acessos, os papéis que lhe estão atribuídos.

- *Consultar Permissões de Utilizadores*
Consultar para cada utilizador do sistema de controlo de acessos, as permissões a espaços que o mesmo tem acesso, isto é, o conjunto de espaços físicos que um determinado utilizador tem permissão a aceder.
- *Consultar Papéis e Permissões de Utilizadores*
Consultar para cada utilizador do sistema de controlo de acessos, os seus papéis e as permissões (a espaços físicos) que cada um dos papéis atribuídos lhe dá acesso.

5.1.6.2 Papéis

A aplicação deverá suportar a definição de um conjunto de papéis de utilizador, aos quais são atribuídos privilégios ou permissões de acesso aos espaços físicos controlados. Um papel corresponde a uma categoria profissional, a uma função ou grupo de funções que o utilizador possui ou pode exercer na organização. Uma pessoa ou utilizador pode ter mais do que um papel.

A aplicação deverá permitir efectuar as funcionalidades essenciais referentes à *gestão de papéis* dos utilizadores do sistema de controlo de acessos.

- *Inserção, Modificação e Remoção de Papéis*
Efectuar a inserção, modificação de dados e eliminação de papéis utilizados na gestão de controlo de acessos.
- *Atribuição e Eliminação de Utilizadores a Papéis*
Efectuar a atribuição e eliminação de utilizadores a papéis do sistema de gestão de controlo de acessos.
- *Listagem de Papéis*
Efectuar a listagem de todos os papéis utilizados na gestão do sistema de controlo de acessos.
- *Consultar Utilizadores de Papéis*
Efectuar a listagem de todos os utilizadores do sistema de controlo de acessos com um mesmo papel atribuído.
- *Consultar Permissões de Papéis*
Consultar para cada papel criado no sistema de gestão de controlo de acessos, as permissões de acesso a espaços físicos atribuídas ao papel.

5.1.6.3 Espaços Físicos (controlados)

Uma aplicação de gestão de sistemas de controlo de acessos eficaz deverá ser capaz de lidar convenientemente com a *estrutura física dos espaços físicos* da organização, em conformidade com o facto de os espaços físicos conterem outros espaços e satisfazendo o *conceito de espaços físicos encaixados* (ver secção §4.3.1 “A Estrutura dos Espaços Físicos”, pág. 69).

A aplicação deverá permitir efectuar as funcionalidades essenciais referentes à *gestão de espaços físicos* que são utilizados e controlados pelo sistema de controlo de acessos.

- *Inserção, Modificação e Remoção de Espaços (físicos)*
Efectuar a inserção, alteração de dados e eliminação *hierárquicas* de espaços físicos controlados pelo sistema de controlo de acessos
(Listagem do código desta funcionalidade no Anexo C.1 – Código de “Editar Espaços (inserir, modificar, eliminar)”, pág. 197).
- *Listagem de Espaços (físicos)*
Efectuar a listagem hierárquica de todos os espaços físicos controlados pelo sistema de controlo de acessos físico.
- *Consultar Utilizadores de Espaços (físicos)*
Consultar para cada espaço físico controlado pelo sistema de controlo de acessos, o conjunto de utilizadores que tem permissão de acesso ao mesmo.

5.1.6.4 Permissões (a espaços físicos)

A aplicação deverá poder controlar quem (e quando) poderá aceder a um espaço físico controlado, com base no modelo de *controlo de acesso baseado no papel – RBAC*²⁵ (ver secção §4.3.2 “O Controlo de Acessos Baseado no Papel”, pág. 69), o qual permite que permissões de acesso sobre objectos, neste caso, espaços físicos, sejam atribuídas a papéis. Os utilizadores do sistema de controlo de acessos obtêm acesso, preferencialmente, com base nos papéis que possuem, em detrimento das suas identidades individuais ou próprias, o que para tal, é atribuído a cada papel, em particular, direitos ou permissões de acesso a espaços físicos e o conjunto de utilizadores que o poderão usufruir, em consonância com os critérios ou a política de permissões seguida pela organização, ajustados à sua realidade e à eficácia da sua segurança.

Para a aplicação de gestão de controlo de acessos ser eficaz deverá, também, satisfazer o *conceito ou regra da herança reversa* (ver secção §4.3.3.2 “Autorização Implícita e Herança Reversa” pág. 72), significando que ao atribuir-se a um papel, uma permissão de acesso para um determinado espaço físico da organização, a aplicação verifica as permissões, do papel, de acesso aos espaços físicos ascendentes que conduzem ao

²⁵ Controlo de Acessos Baseado no Papel (da expressão inglesa *Role Based Access Control*).

espaço físico em causa e, se necessário, de modo automático, atribui as permissões em falta. De modo inverso, ao remover-se uma permissão de acesso a um espaço físico, a aplicação verifica e remove automaticamente ao papel, se necessário, as permissões de acesso aos espaços físicos hierarquicamente descendentes do espaço físico, ao qual foi removida a permissão de acesso.

A aplicação deverá permitir efectuar as funcionalidades essenciais referentes à *gestão de permissões* (a espaços físicos) de papéis de utilizadores do sistema de controlo de acessos:

- *Gestão de Permissões, a Espaços (físicos), de Papeis (de Utilizadores)*
Efectuar a atribuição, alteração de dados e eliminação de permissões (a espaços físicos) dos papéis utilizados no sistema.
 - Deverá ter por base o modelo de *controlo de acessos baseado no papel*
 - Deverá satisfazer o *conceito ou regra da herança reversa*

5.1.6.5 Consultas e Produção de “Reports”

A aplicação deverá possibilitar efectuar consultas ou produzir *reports* (*standard* ou customizados) de auditoria, a partir de eventos ocorridos na gestão ou com a utilização do sistema de controlo de acessos físico da organização. Essas consultas ou relatórios, primeiramente, são geradas numa página da aplicação e, depois, poderão ser impressos ou transferidos por *download* (em formatos *excel*, *pdf*,...).

5.1.6.5.1 Auditorias/Pesquisas sobre Acessos e Presenças

A funcionalidade de auditorias sobre acessos é extremamente importante, uma vez que pode gerar *reports* que proporcionam um visionamento geral dos acessos dos utilizadores efectuados às instalações ou espaços físicos controlados da organização. Podem mostrar, em detalhe, o rastreio ou fluxo de todos os acessos efectuados, num período de tempo, quer por um determinado utilizador, quer a um espaço físico em particular.

A aplicação deverá permitir efectuar as funcionalidades essenciais referentes a *auditorias sobre acessos* de utilizadores (também, *pesquisas sobre as suas presenças*) aos espaços físicos controlados pelo sistema de controlo de acessos:

- *Auditar/Consultar Acessos (de Utilizadores e a Espaços)*
Efectuar várias consultas e listagens sobre auditoria de acessos de utilizadores, fluxos de entrada/saída dos espaços físicos controlados pelo sistema de controlo de acessos, com registo do tempo, do espaço e do utilizador.
- *Auditar Acessos de Utilizadores*

Consultar ou listar todos os acessos, entre duas datas, dum determinado utilizador aos espaços físicos controlados pelo sistema de controlo de acessos.

- *Auditar Acessos a um Espaço por Utilizador*

Consultar os acessos, entre duas datas, efectuados por um determinado utilizador a um espaço físico controlado pelo sistema de controlo de acessos

(Listagem do código desta funcionalidade no Anexo C.2 – Código de “Auditar Acessos a um Espaço por Utilizador”, pág. 215).

- *Auditar Acessos a Espaços (físicos)*

Consultar ou listar todos os acessos, entre duas datas, efectuados pelos utilizadores do sistema de controlo de acessos a um determinado espaço físico controlado.

- *Pesquisar/Localizar Presenças de Utilizadores em Espaços*

Efectuar várias consultas e listagens sobre a localização, em tempo real, dos utilizadores em quaisquer dos espaços físicos controlados pelo sistema de controlo de acessos.

- *Pesquisar/Localizar Presenças de Utilizadores*

Pesquisar ou localizar, em tempo real, a presença dum determinado utilizador em qualquer um dos espaços físicos controlados pelo sistema de controlo de acessos.

- *Consultar Presenças em Espaços*

Consultar ou listar todas as presenças de utilizadores, em tempo real, num determinado espaço físico controlado pelo sistema de controlo de acessos.

5.1.6.5.2 Auditorias sobre Administração e Segurança do Sistema

Todas as actividades relativas à administração ou gestão do sistema podem ser auditadas ou rastreadas [14]. Para tal, podem ser produzidos “*reports*” detalhados em que se mostram as actividades dos administradores do sistema, em cada uma das sessões em que estiveram autenticados (“logados”) na aplicação de gestão de sistemas de controlo de acessos físico. Estes relatórios mostram o tempo de utilização ou de permanência dos administradores na aplicação e quais as operações que efectuaram (por ex., quais os utilizadores que criaram ou registaram, quais as permissões de acesso que foram atribuídas ou removidas,...).

Adicionalmente, poderão também ser realizadas auditorias relativas à segurança do sistema de controlo de acessos físico [31], em que se mostra todas as tentativas de acesso a espaços físicos (tentativas de intrusão) efectuadas por utilizadores não

autorizados (sem permissão, com senhas – *passwords* – inválidas,...) ou, até mesmo, os momentos de falha de energia ou de comunicações ocorridos em cada local de acesso.

5.1.6.5.3 Consultas Gerais à Base de Dados

A partir dos múltiplos dados armazenados na base de dados e da informação que podem proporcionar, a aplicação deverá permitir a possibilidade de se efectuar e, mesmo, customizar vários tipos de consultas e listagens de suporte à gestão de controlo de acessos, algumas já explicitadas em secções anteriores (sobre utilizadores, papéis e espaços físicos controlados, auditorias, ...).

5.2 Modelo de Casos de Utilização

Nesta secção, começa-se por fazer uma breve introdução sobre os modelos de casos de utilização, no intuito de proporcionar os conceitos a uma leitura mais fácil dos respectivos diagramas. Segue-se o contexto e a visão global do sistema, por forma a apresentar as suas fronteiras, a enumerar os actores e, sobretudo, a realçar os subsistemas e funcionalidades essenciais da aplicação. Por fim, são descritos os actores identificados para a aplicação, bem como, a forma como a totalidade dos casos de utilização foram organizados em pacotes, de acordo com o subsistema e a área funcional que abrangem, sendo cada pacote de casos de utilização descrito em separado.

Breves Noções sobre Casos de Utilização

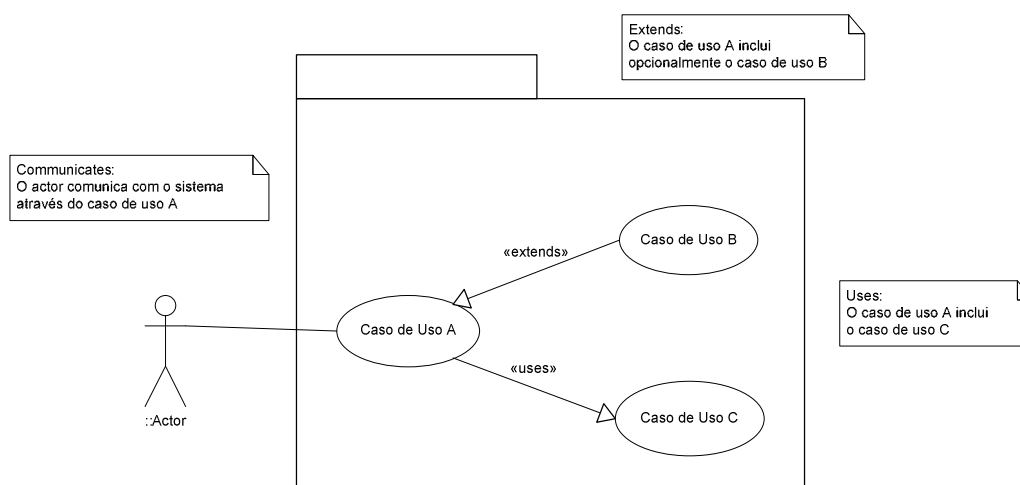


Figura 5.1 – Exemplo de Diagrama de Casos de Uso

Todas as aplicações de *software* de interesse interagem com pessoas ou com outras aplicações, *actores*, que as utilizam com o propósito de obter um determinado resultado previsível. Um *caso de uso ou de utilização* permite especificar o comportamento de uma aplicação, e consiste numa descrição de um conjunto de sequências de acções,

incluindo variantes, que uma aplicação realiza para conseguir obter um resultado observável para o actor que iniciou esse caso de uso (ver *Figura 5.1* anterior). Um caso de utilização descreve o que uma aplicação faz, mas sem especificar como tal é conseguido, o que é importante para ajudar a separar a visão externa de uma aplicação da sua visão interna. Os casos de uso podem-se associar entre si, de modo que um caso de uso poder incluir outro, associação *uses*, ou um caso de uso poder estender outro, associação *extends* (ver *Figura 5.1* anterior). Um actor representa um conjunto de funções que os utilizadores desempenham quando interagem com estes casos de uso. Normalmente, um actor representa uma função que uma pessoa, um periférico, ou outra aplicação desempenha com a aplicação. Uma pessoa normalmente acumula diferentes actores. A interacção de um actor com um caso de uso representa-se com uma associação entre estes – *communicates* (*Figura 5.1* anterior).

Uma aplicação normalmente tem diversos casos de uso que, de modo a poderem ser mais facilmente compreendidos, devem ser organizados e divididos em áreas funcionais de acordo com a funcionalidade que oferecem. Esta divisão pode ser representada agrupando os casos de uso em pacotes.

5.2.1 Visão Global do Sistema

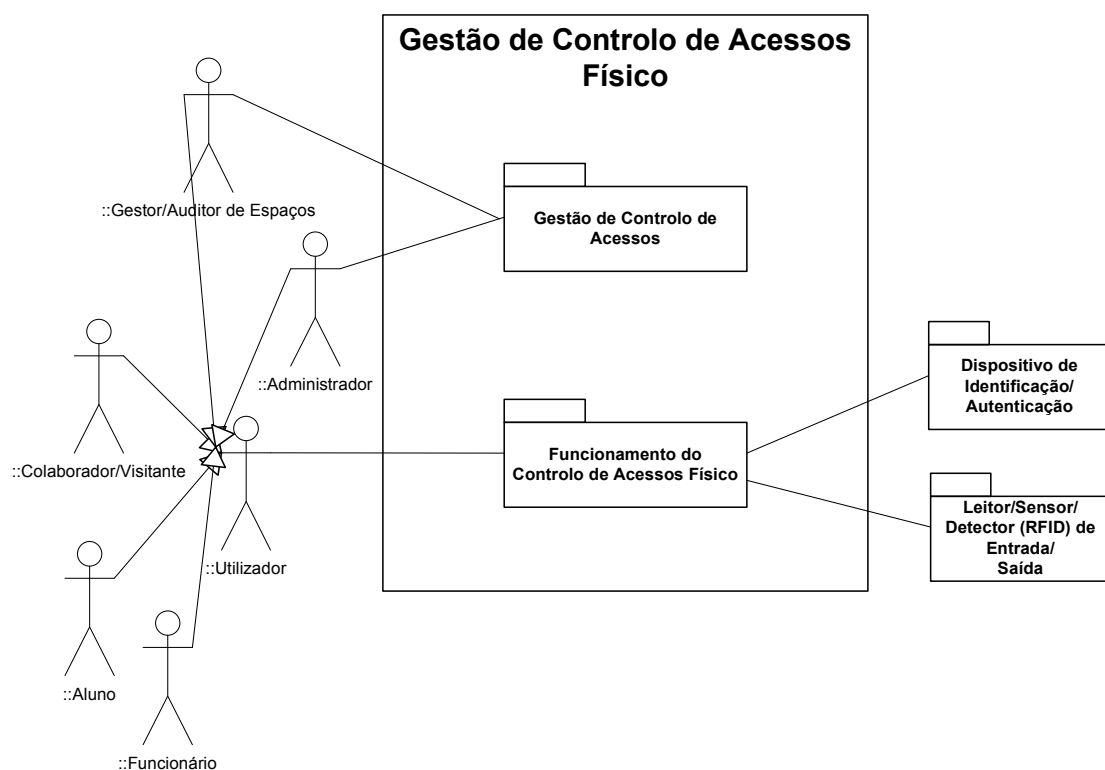


Figura 5.2 – Diagrama de pacotes da aplicação WebGPACS

A aplicação terá como objectivo proporcionar, remotamente, a gestão e a monitorização do sistema de controlo de acessos físico da organização. Esta aplicação de gestão de sistemas de controlo de acessos físico, numa primeira fase de conceptualização (no âmbito deste trabalho), está decomposta em dois subsistemas:

- o de *gestão de controlo de acessos*
- e o de *funcionamento do controlo de acessos físico*.

Estes dois subsistemas interagem entre si, partilhando a informação de gestão, que é armazenada numa base de dados relacional. Cada um dos subsistemas trata de um aspecto diferente da gestão do sistema de controlo de acessos físico.

O subsistema de *gestão de controlo de acessos* inclui as principais *funcionalidades standards essenciais de administração ou de gestão de controlo de acessos* (ver secção §5.1.6 “Funcionalidades Essenciais de Gestão / Administração”, pág. 81), nomeadamente, as relacionadas não só com a gestão de utilizadores, papéis, espaços físicos (controlados), permissões, como também, com a efectuação de auditorias sobre os acessos dos utilizadores aos espaços físicos controlados e a pesquisa/localização de presenças de utilizadores. Os actores que interagem com este subsistema resumem-se, basicamente, ao administrador e, de modo parcial, ao gestor/auditor de espaços.

O subsistema de *funcionamento do controlo de acessos físico* inclui as principais funcionalidades de gestão do sistema, ao nível do seu *funcionamento (em tempo real)* (ver secção §5.1.4.1 “Funcionamento (em Tempo Real”, pág. 79), nomeadamente, as operações de funcionamento do sistema de controlo de acessos físico, relativas ao controlo de acessos (entradas e saídas) dos utilizadores aos espaços físicos controlados. Os actores que interagem com este subsistema são todos os utilizadores registados que podem aceder a espaços físicos controlados, assim como, os dispositivos e sensores/detectores utilizados nos espaços físicos para os processos de identificação, autenticação e detecção de movimentos dos utilizadores.

As *Figuras* que se seguem (*Figura 5.3* e *Figura 5.4* da página seguinte) mostram os dois subsistemas que, numa primeira fase, são necessários ao suporte da aplicação de gestão de controlo de acessos físico.

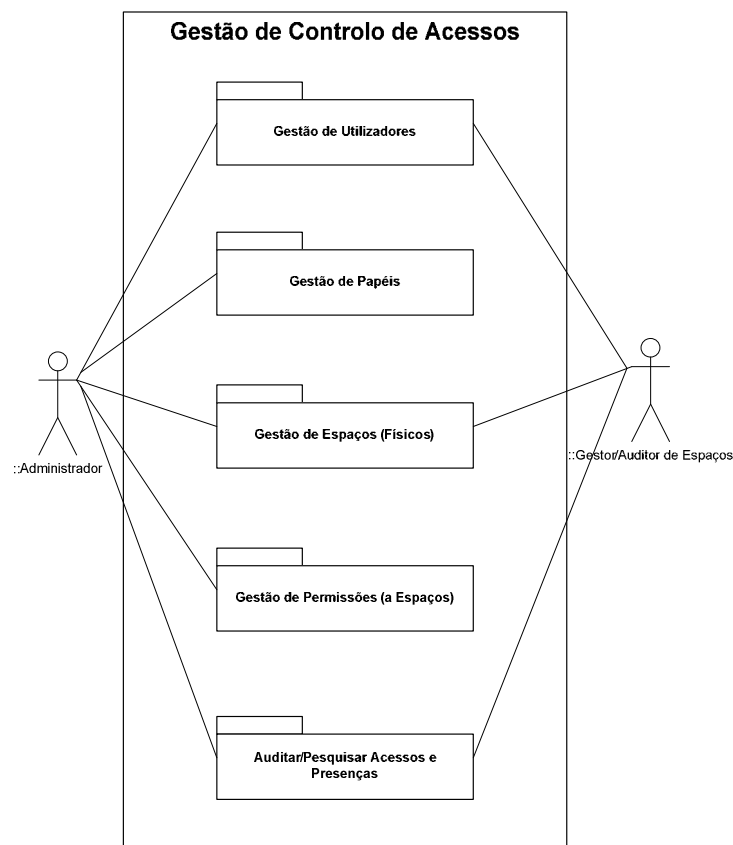


Figura 5.3 – Diagrama de pacotes de casos de utilização do subsistema “Gestão de Controlo de Acessos”

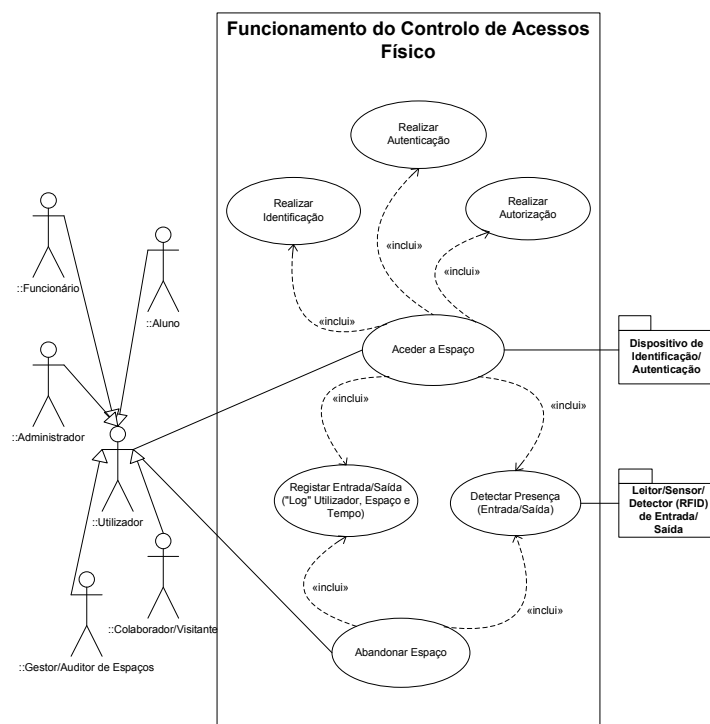


Figura 5.4 – Diagrama de casos de utilização do subsistema “Funcionamento do Controlo de Acessos Físico”

5.2.2 Identificação dos Actores

Os exemplos de actores correspondem a perfis de utilizadores e a outros sistemas, informáticos ou não, com os quais a aplicação irá interagir. A totalidade dos actores que comunicam ou interagem com a *aplicação de gestão de sistemas de controlo de acessos físico – WebGPACS* – são as seguintes: o administrador, o gestor/auditor de espaços, os utilizadores do sistema de controlo de acessos físico, os dispositivos de identificação/autenticação e os sensores/detectores de movimentos de entrada/saída dos espaços.

Destes actores, apenas o administrador e os gestores/auditores de espaços são considerados actores primários, atendendo a que a aplicação *WebGPACS* será exclusivamente criada para responder às suas necessidades.

Administrador

Por administrador entende-se um técnico, associado aos sistemas e tecnologias de informação, a quem foi atribuída a função de fazer a administração ou gestão da aplicação *WebGPACS*. Este actor executa as diferentes funções, referentes à *gestão do sistema de controlo de acessos físico*, que gerem os utilizadores, os espaços físicos controlados, os diferentes papéis a atribuir aos utilizadores e as permissões de acesso a espaços físicos. Executa também funções de auditoria ou rastreio, sobre os múltiplos acessos dos utilizadores (quando e quem acede aos diversos espaços físicos controlados), ...

Gestor/Auditor de Espaços

Por gestor/auditor de espaços entende-se qualquer funcionário, independentemente da sua área de especialidade, a quem foi atribuída a responsabilidade de gestão de determinados espaços físicos da organização (instituição). Depois de devidamente credenciado e autorizado poderá gerir e auditar os acessos aos espaços controlados, atribuídos à sua responsabilidade.

Utilizador

Por utilizador entende-se toda e qualquer pessoa registada, independentemente da sua função ou papel, para poder aceder a espaços físicos controlados pelo sistema de controlo de acessos físico da organização (instituição).

Aluno

Por aluno, entende-se todos os alunos da organização (instituição) registados na aplicação.

Funcionário

Por funcionário, entende-se todos os profissionais (professores/funcionários) da organização (instituição) registados na aplicação.

Colaborador/Visitante

Por colaborador/visitante, entende-se todas as pessoas que são utilizadores temporários de espaços físicos controlados pela organização, tais como, visitantes, profissionais ou colaboradores temporários, adjudicatários (pessoas doutras empresas contratadas para efectuarem serviços específicos), ... Estes utilizadores para acederem a determinados espaços físicos controlados, também, necessitam de estar registados.

Dispositivo de Identificação/Autenticação



Figura 5.5 – Reader de proximidade

Por dispositivo de identificação/autenticação entende-se todo e qualquer leitor (*reader*) ou dispositivo (*RFID*) destinado à identificação e autenticação automática dos utilizadores, que está situado no local de acesso ou à entrada de cada espaço físico controlado.

Leitor/Sensor/Detector (RFID) de Entrada/Saída



Figura 5.6 – Sensores

Por leitor/sensor/detector (*RFID*) entende-se todo e qualquer sensor ou detector de movimentos destinado à detecção da presença dum utilizador no seu processo de acesso (entrada) ou abandono (saída) dum determinado espaço físico controlado.

5.2.3 Subsistema “Gestão de Controlo de Acessos”

Após a identificação dos diversos actores apresentar-se-á, agora, uma visão global sobre a funcionalidade requerida pelo administrador e gestor/auditor de espaços na sua interacção com o *subsistema de gestão de controlo de acessos*. No sentido de tornar mais fácil a sua análise e compreensão, a funcionalidade foi expressa em termos de casos de uso e estes organizados em pacotes (ver *Figura 5.7* seguinte).

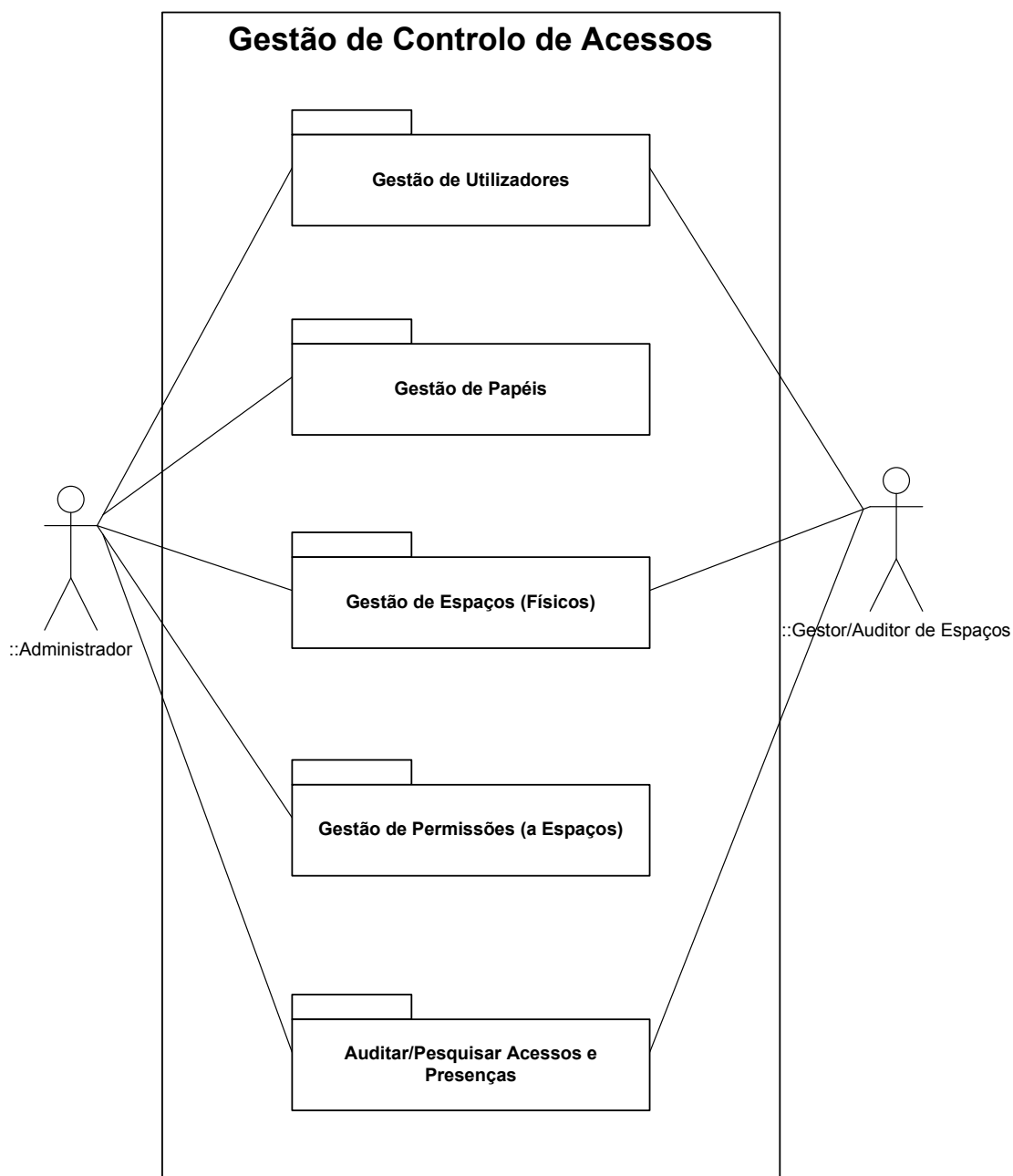


Figura 5.7 – Diagrama de pacotes de casos de utilização do subsistema “Gestão de Controlo de Acessos”

Os casos de uso deste subsistema encontram-se distribuídos por cinco pacotes: Gestão de Utilizadores, Gestão de Papéis, Gestão de Espaços, Gestão de Permissões (a Espaços) e Auditar/Pesquisar Acessos e Presenças. Nas secções seguintes far-se-á uma descrição de cada caso de utilização pertencente a cada um destes pacotes.

5.2.3.1 Gestão de Utilizadores

Os casos de uso agrupados neste pacote oferecem as funcionalidades necessárias para a *gestão de utilizadores*. Este pacote engloba os casos de utilização que permitem editar utilizadores (inserção, alteração e eliminação de utilizadores no sistema), editar papéis a utilizadores (atribuição e eliminação de papéis a utilizadores) e consultas sobre papéis e permissões (a espaços) de utilizadores [18].

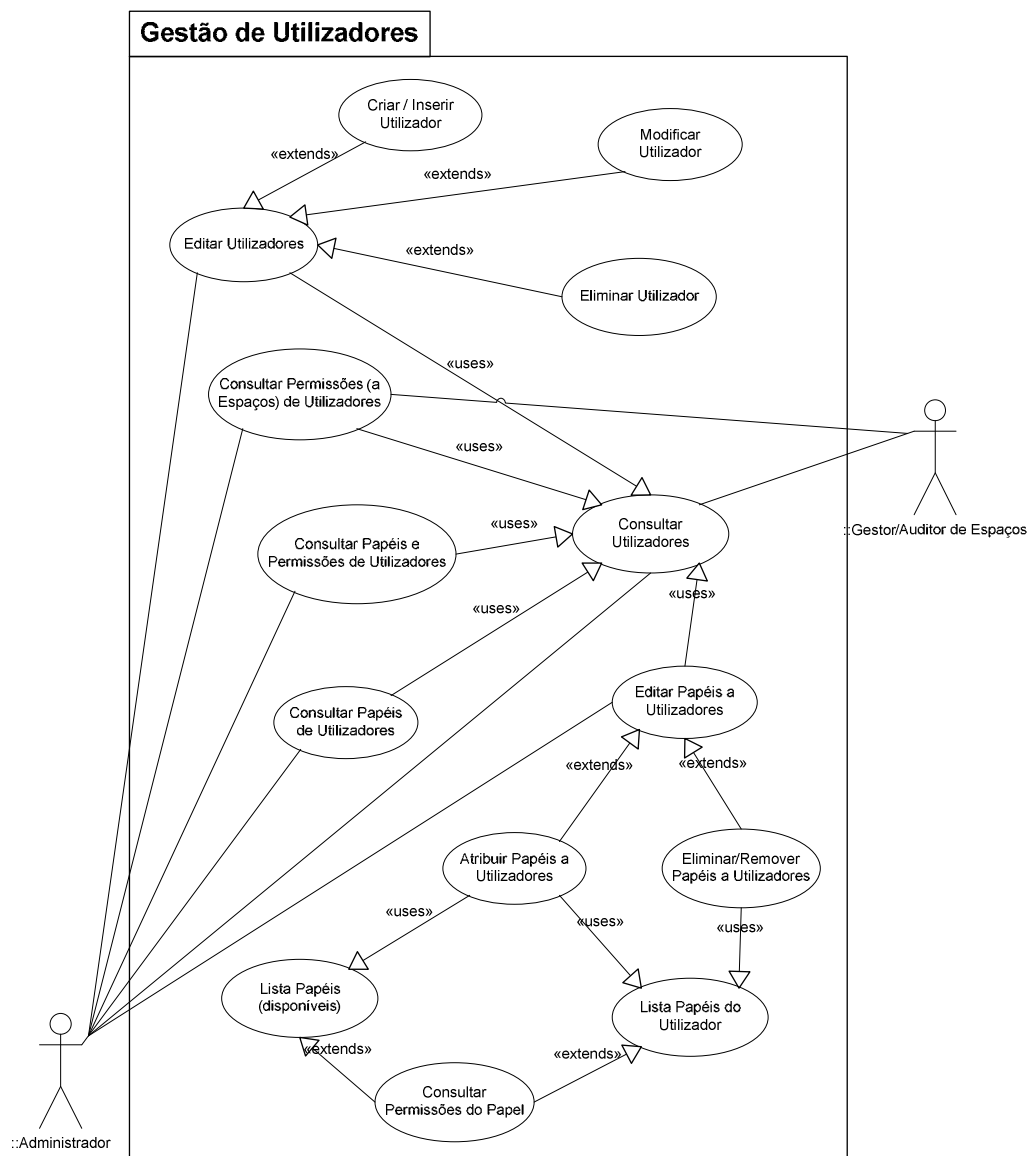


Figura 5.8 – Diagrama de casos de utilização de “Gestão de Utilizadores”

Pretende-se que a aplicação implemente as funcionalidades descritas pelos casos de utilização representados graficamente no diagrama anterior (ver *Figura 5.8*). A seguir, também são descritos textualmente, num formato alto-nível.

Caso de Uso: Editar Utilizadores

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de utilizadores, pretendendo inserir um novo utilizador, modificar ou eliminar um já existente. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...). O actor poderá depois pesquisar e seleccionar cada um desses utilizadores para o modificar ou eliminar.

Caso de Uso: Criar / Inserir Utilizador

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado o botão correspondente, solicita a inserção de um novo utilizador. O sistema solicita ao actor a introdução dos dados do utilizador. Cada utilizador deve ser definido por um número de identificação exclusivo. O sistema cria um novo utilizador com a informação indicada pelo actor, introduzindo-a na tabela correspondente da base de dados.

Caso de Uso: Modificar Utilizador

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um utilizador da listagem de utilizadores e, através da selecção do botão correspondente, solicita a sua modificação. O sistema mostra os dados actuais do utilizador e solicita ao actor a introdução dos dados a modificar. O sistema modifica os dados do utilizador com a informação indicada pelo actor. A nova informação é armazenada substituindo a anteriormente existente.

Caso de Uso: Eliminar Utilizador

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um utilizador da listagem de utilizadores e, através da selecção do botão correspondente, pretende eliminá-lo. Após confirmação do actor, o sistema elimina o utilizador da tabela correspondente da base de dados.

Caso de Uso: Editar Papéis a Utilizadores

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de papéis a utilizadores, pretendendo atribuir um novo papel a um utilizador ou eliminar um que já lhe tenha sido atribuído. O sistema invoca então a

consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...). O actor poderá depois pesquisar e seleccionar cada um desses utilizadores para lhes atribuir ou eliminar papéis.

Caso de Uso: Atribuir Papéis a Utilizadores

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um utilizador da listagem de utilizadores e, através da selecção do botão correspondente, solicita a atribuição de um novo papel ao utilizador. O sistema não só disponibiliza uma listagem dos papéis já atribuídos ao utilizador e outra correspondente aos papéis existentes no sistema que ainda não lhe foram atribuídos, como também a possibilidade de serem consultadas as permissões de cada papel listado. O actor deve seleccionar o novo papel a atribuir ao utilizador e, após confirmação, o sistema insere-o, de imediato, na lista de papéis atribuídos ao utilizador.

Caso de Uso: Eliminar/Remover Papéis a Utilizadores

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um utilizador da listagem de utilizadores e, através da selecção do botão correspondente, solicita a eliminação de um papel ao utilizador. O sistema disponibiliza uma listagem dos papéis já atribuídos ao utilizador e a possibilidade de serem consultadas as permissões de cada papel listado. O actor selecciona o papel a eliminar ao utilizador e, após confirmação, o sistema elimina-o, de imediato, da lista de papéis atribuídos ao utilizador.

Caso de Uso: Lista Papéis (Disponíveis)

Descrição: Este caso de uso inicia-se quando o actor solicita a atribuição de papéis a um utilizador seleccionado. O sistema disponibiliza uma listagem dos papéis do sistema ainda não atribuídos ao utilizador.

Caso de Uso: Lista Papéis do Utilizador

Descrição: Este caso de uso inicia-se quando o actor solicita a atribuição ou a remoção de papéis a um utilizador seleccionado. O sistema disponibiliza uma listagem dos papéis que já lhe foram atribuídos.

Caso de Uso: Consultar Permissões do Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel das listas de papéis já atribuídos ou por atribuir ao utilizador, solicita a consulta das permissões desse papel. O sistema disponibiliza ao actor uma listagem de permissões (a espaços físicos) do papel seleccionado.

Caso de Uso: Consultar Utilizadores

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar um utilizador ou solicita a edição de utilizadores ou de papéis a utilizadores, as consultas sobre papéis e permissões (a espaços) de utilizadores. O sistema possibilita que o actor pesquise e selecione um utilizador de uma lista de utilizadores que lhe é apresentada, podendo ser ordenada por vários atributos do utilizador (número de identificação, nome, ...).

Caso de Uso: Consultar Papéis de Utilizadores

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar os papéis atribuídos a um utilizador do sistema. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...), permitindo ao actor pesquisar e seleccionar cada um desses utilizadores. Para o utilizador seleccionado, o sistema disponibiliza ao actor uma listagem dos papéis que lhe estão atribuídos.

Caso de Uso: Consultar Permissões (a Espaços) de Utilizadores

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar as permissões (a espaços físicos) de um utilizador do sistema. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...), permitindo ao actor pesquisar e seleccionar cada um desses utilizadores. Para o utilizador seleccionado, o sistema disponibiliza ao actor uma listagem das permissões (a espaços físicos) do utilizador, em resultado das permissões dos papéis que lhe estão atribuídos.

Caso de Uso: Consultar Papéis e Permissões de Utilizadores

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar os papéis e as permissões (a espaços físicos) de um utilizador do sistema. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...), permitindo ao actor pesquisar e seleccionar cada um desses utilizadores. Para o utilizador seleccionado, o sistema disponibiliza ao actor uma listagem dos papéis que lhe estão atribuídos e das permissões (a espaços físicos) referentes a cada um desses papéis.

5.2.3.2 Gestão de Papéis

Os casos de uso agrupados neste pacote oferecem as funcionalidades necessárias para a *gestão de papéis* utilizados na aplicação e que serão atribuídos aos utilizadores do *sistema de controlo de acessos físico*. Este pacote engloba os casos de utilização que permitem editar papéis (inserção, modificação e eliminação de papéis no sistema), editar utilizadores a papéis (atribuição e eliminação de utilizadores a papéis) e consultas sobre utilizadores e permissões (a espaços) de papéis [18].



Figura 5.9 – Diagrama de casos de utilização de “Gestão de Papéis”

Pretende-se que a aplicação implemente as funcionalidades descritas pelos casos de utilização representados graficamente no diagrama anterior (ver *Figura 5.9*). Também são descritos textualmente, num formato alto-nível, em Anexos (ver Anexo B – Casos de Utilização, em B.1 – Gestão de Papéis, pág. 187).

5.2.3.3 Gestão de Espaços (Físicos)

Os casos de uso agrupados neste pacote oferecem as funcionalidades necessárias da aplicação para a *gestão de espaços físicos* utilizados e controlados pelo *sistema de controlo de acessos físico*. Este pacote engloba os casos de utilização que permitem editar *hierarquicamente* espaços físicos controlados (Listagem do código desta funcionalidade no Anexo C.1 – Código de “Editar Espaços (inserir, modificar, eliminar)”, pág. 197), editar tipos de espaços (inserção, modificação e eliminação de tipos de espaços físicos) e consultas sobre os espaços físicos, seus tipos e seus utilizadores (quais os utilizadores com permissão de acesso a cada um dos espaços físicos controlados).

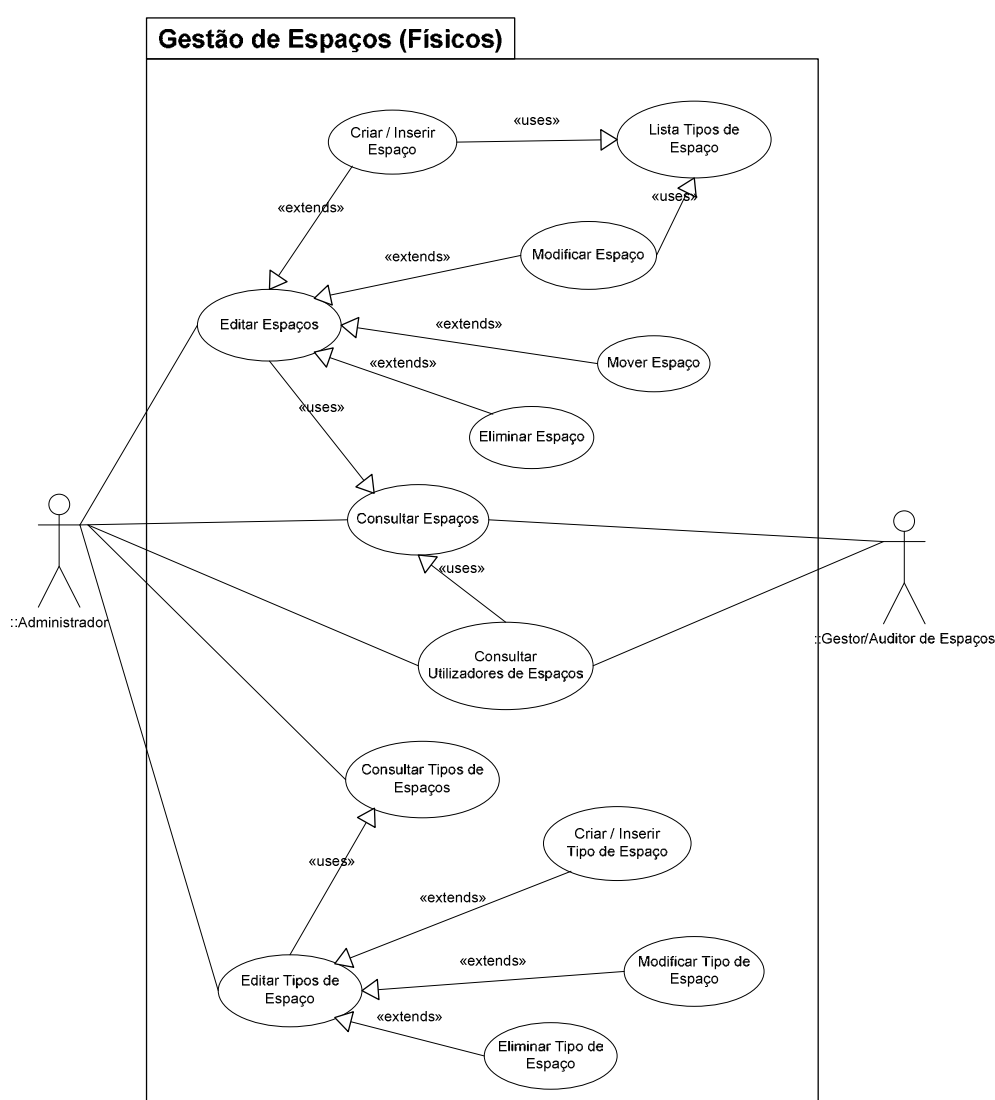


Figura 5.10 – Diagrama de casos de utilização de “Gestão de Espaços (Físicos)”

Pretende-se que a aplicação implemente as funcionalidades descritas pelos casos de utilização representados graficamente no diagrama anterior (ver *Figura 5.10*). Também

são descritos textualmente, num formato alto-nível, em Anexos (ver Anexo B – Casos de Utilização, em B.2 – Gestão de Espaços (Físicos), pág. 189), exceptuando os da *edição de espaços*, cuja caracterização está em formato detalhado, na secção seguinte.

5.2.3.3.1 Editar Espaços (formato detalhado)

A edição de espaços físicos controlados pelo sistema possibilita a consulta, criação, modificação, eliminação e movimentação de espaços físicos e seus descendentes hierárquicos (espaços contidos noutros espaços físicos). Os diferentes espaços físicos a serem controlados são identificados e inseridos hierarquicamente no sistema, devendo ser definidos por um simples endereço (por ex., *Edifício-I, I-104, ...*) exclusivo de cada espaço físico, em princípio, já definido na planta geográfica de localizações dos espaços físicos da organização. Também podem ser alterados, movidos e removidos do sistema. Os casos de uso que constituem esta funcionalidade são, a seguir, descritos e caracterizados em formato detalhado.

<i>Caso de Uso:</i>	Editar Espaços
---------------------	-----------------------

<i>Actores:</i>	Administrador da aplicação <i>WebGPACS</i> , sendo este o actor iniciador do caso de uso.
<i>Objectivo:</i>	Editar um espaço físico controlado e a informação relativa à sua hierarquia ou propriedades.
<i>Visão Global:</i>	O actor pretende editar um espaço físico controlado e o sistema possibilita a pesquisa, consulta e selecção dum espaço físico numa lista hierárquica de espaços físicos controlados pelo sistema (associados à estrutura física dos espaços ou localizações físicas da planta da Organização).
<i>Prioridade:</i>	Elevada.
<i>Estado:</i>	Implementado.
<i>Pré-Condições:</i>	O actor tem que estar registado no sistema com o perfil de Administrador.
<i>Descrição:</i>	Existência de planta dos espaços físicos da organização. Este caso de uso inicia-se quando o actor solicita a edição de espaços físicos no <i>menu</i> correspondente.

O sistema permite ao actor consultar a hierarquia de espaços físicos, pesquisar e seleccionar os espaços físicos que pretende editar, de uma listagem hierárquica de espaços físicos controlados pelo sistema que lhe é apresentada.

Após efectuar uma selecção do espaço físico, o actor poderá invocar várias operações.

No caso de o actor pretender criar um novo espaço físico descendente do que se encontra seleccionado, pode iniciar o caso de uso *Criar / Inserir Espaço* (ver caso de uso nesta

secção).

No caso de o actor pretender modificar o espaço físico seleccionado pode iniciar o caso de uso *Modificar Espaço* (ver caso de uso nesta secção).

No caso de o actor pretender eliminar o espaço físico seleccionado, pode iniciar o caso de uso *Eliminar Espaço* (ver caso de uso nesta secção).

No caso de o actor pretender alterar a posição hierárquica do espaço (físico) seleccionado, pode iniciar o caso de uso *Mover Espaço* (ver caso de uso nesta secção).

Pós-condições:

Seleccção do espaço físico.

Casos de Uso

Os casos de uso *Criar/Inserir Espaço*, *Modificar Espaço*, *Eliminar Espaço* e *Mover Espaço* constituem extensões opcionais a este, pelo que se relacionam através de uma associação do tipo *extends*.

Relacionados:

O caso de uso *Consultar Espaços* é usado por este, pelo que é representado por uma associação do tipo *uses*.

Caso de Uso:	Criar / Inserir Espaço
---------------------	-------------------------------

Actores:

Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Objectivo:

Criar um novo espaço físico que pertença a uma determinada hierarquia.

Visão Global:

O sistema cria/insere um espaço físico com a informação e posição hierárquica indicada pelo actor.

Prioridade:

Elevada.

Estado:

Implementado.

Pré-Condições:

O actor tem que estar registado no sistema com o perfil de Administrador.

Indicação do espaço físico ascendente.

Descrição:

Este caso de uso inicia-se quando o actor, após ter seleccionado um espaço físico (ver caso de uso *Editar Espaços* nesta secção), solicita a criação de um descendente.

O sistema cria um espaço físico como descendente do indicado e inicializa alguns dos seus atributos com os respectivos valores por defeito.

O sistema possibilita ao actor a inserção dos valores das propriedades do novo espaço físico.

A informação indicada pelo actor e relativa ao novo espaço físico é armazenada.

Pós-condições: Criação de um novo espaço físico controlado pelo sistema.
Casos de Uso Este caso de uso constitui uma das extensões opcionais ao
Relacionados: *Editar Espaços*, pelo que se relacionam através de uma associação do tipo *extends*.
 O caso de uso *Lista Tipos de Espaço* é usado por este, pelo que é representado por uma associação do tipo *uses*.

<i>Caso de Uso:</i>	Modificar Espaço
---------------------	-------------------------

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.
Objectivo: Modificar as propriedades de um espaço físico.
Visão Global: O sistema permite ao actor alterar os valores actuais das propriedades associadas a determinado espaço físico.
Prioridade: Elevada.
Estado: Implementado.
Pré-Condições: O actor tem que estar registado no sistema com o perfil de Administrador.
Descrição: Indicação do espaço físico a modificar.
 Este caso de uso inicia-se quando o actor, após ter seleccionado um espaço físico (ver caso de uso *Editar Espaços* nesta secção), solicita a modificação das suas propriedades.

O sistema possibilita ao actor a alteração dos valores actuais das propriedades do espaço físico seleccionado.

O actor após ter efectuado as alterações pretendidas pode cancelar a alteração ou confirmá-la.

Pós-condições: Caso opte pela confirmação, a informação alterada substitui a anteriormente armazenada. De outro modo, as alterações efectuadas são ignoradas e a informação anterior é reposta.
 Alteração eventual da informação relativa ao espaço físico seleccionado.
Casos de Uso Este caso de uso constitui uma das extensões opcionais ao
Relacionados: *Editar Espaços*, pelo que se relacionam através de uma associação do tipo *extends*.
 O caso de uso *Lista Tipos de Espaço* é usado por este, pelo que é representado por uma associação do tipo *uses*.

<i>Caso de Uso:</i>	Eliminar Espaço
---------------------	------------------------

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.
Objectivo: Eliminar um espaço físico, que pertença a determinada hierarquia.
Visão Global: O actor pretende eliminar um espaço físico, eliminando-o da

	hierarquia existente e desassociando-o como espaço físico controlado pelo sistema.
<i>Prioridade:</i>	Elevada
<i>Estado:</i>	Implementado.
<i>Pré-Condições:</i>	O actor tem que estar registado no sistema com o perfil de Administrador.
	Indicação do espaço físico a eliminar.
<i>Descrição:</i>	Este caso de uso inicia-se quando o actor, após ter seleccionado um espaço físico (ver caso de uso <i>Editar Espaços</i> nesta secção), solicita a sua eliminação.
	O sistema alerta o actor para o impacto da eliminação do espaço físico no sistema, entre outras, para a eliminação dos espaços físicos que sejam seus descendentes, possibilitando ao actor o cancelamento ou confirmação da eliminação.
	Caso o actor opte pela confirmação, o sistema elimina o espaço físico e seus descendentes, mostrando a identificação e outra informação relativa aos espaços físicos eliminados. De outro modo, a eliminação é ignorada e o espaço físico mantém-se no sistema.
<i>Pós-condições:</i>	Eliminação do espaço físico seleccionado da lista de espaços físicos controlados pelo sistema, associados à organização, e eventual eliminação dos seus descendentes. Eliminação das relações hierárquicas entre os espaços físicos eliminados e os seus ascendentes.
<i>Casos de Uso Relacionados:</i>	Este caso de uso constitui uma das extensões opcionais ao <i>Editar Espaços</i> , pelo que se relacionam através de uma associação do tipo <i>extends</i> .

Caso de Uso:	Mover Espaço
---------------------	---------------------

<i>Actores:</i>	Administrador da aplicação <i>WebGPACS</i> , sendo este o actor iniciador do caso de uso.
<i>Objectivo:</i>	Mover um espaço físico na estrutura hierárquica estabelecida.
<i>Visão Global:</i>	O sistema altera a posição hierárquica de um espaço físico de acordo com o indicado pelo actor, movendo-a na hierarquia.
<i>Prioridade:</i>	Baixa
<i>Estado:</i>	Não implementado.
<i>Pré-Condições:</i>	O actor tem que estar registado no sistema com o perfil de Administrador.
	Indicação do espaço físico a mover e da nova posição hierárquica.
<i>Descrição:</i>	Este caso de uso inicia-se quando o actor, após ter seleccionado um espaço físico (ver caso de uso <i>Editar Espaços</i> nesta secção), solicita a alteração da sua posição hierárquica.

O actor indica a posição hierárquica para a qual pretende mover o espaço físico seleccionado.

O sistema altera as relações hierárquicas do espaço físico de modo a efectivar a alteração indicada.

Pós-condições: A informação alterada substitui a anteriormente armazenada.
Alteração eventual das relações hierárquicas do espaço físico seleccionado.

Casos de Uso Relacionados: Este caso de uso constitui uma das extensões opcionais ao *Editar Espaços*, pelo que se relacionam através de uma associação do tipo *extends*.

<i>Caso de Uso:</i>	Lista Tipos de Espaço
---------------------	------------------------------

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Objectivo: Seleccionar um tipo de espaço físico.

Visão Global: O sistema permite consultar e seleccionar um tipo de espaço físico, a partir de um menu *drop-down*.

Prioridade: Média.

Estado: Implementado.

Pré-Condições: O actor tem que estar registado no sistema com o perfil de Administrador ou de Auditor/Gestor de Espaços.

Descrição: Este caso de uso inicia-se quando o actor solicita a criação ou a modificação de espaços (ver casos de uso *Criar/Inserir Espaço* e *Modificar Espaço* nesta secção).

O sistema permite ao actor seleccionar, a partir de um menu *drop-down*, o padrão ou tipo de espaço físico para inserção ou alteração duma propriedade do espaço físico

Pós-condições: O tipo de espaço físico foi seleccionado.

Casos de Uso Relacionados: Este caso de uso é usado pelos *Criar/Inserir Espaço* e *Modificar Espaço*, pelo que se relacionam através de uma associação do tipo *uses*.

5.2.3.4 Gestão de Permissões (a Espaços)

Os casos de uso agrupados neste pacote oferecem as funcionalidades da aplicação necessárias para *gestão das diferentes autorizações ou permissões de acesso* aos vários espaços físicos controlados, que são atribuídas aos diferentes papéis dos utilizadores do *sistema de controlo de acessos físico*. Este pacote engloba os casos de utilização que permitem editar permissões de papéis (inserção, modificação e eliminação de permissões, a espaços físicos, de papéis).

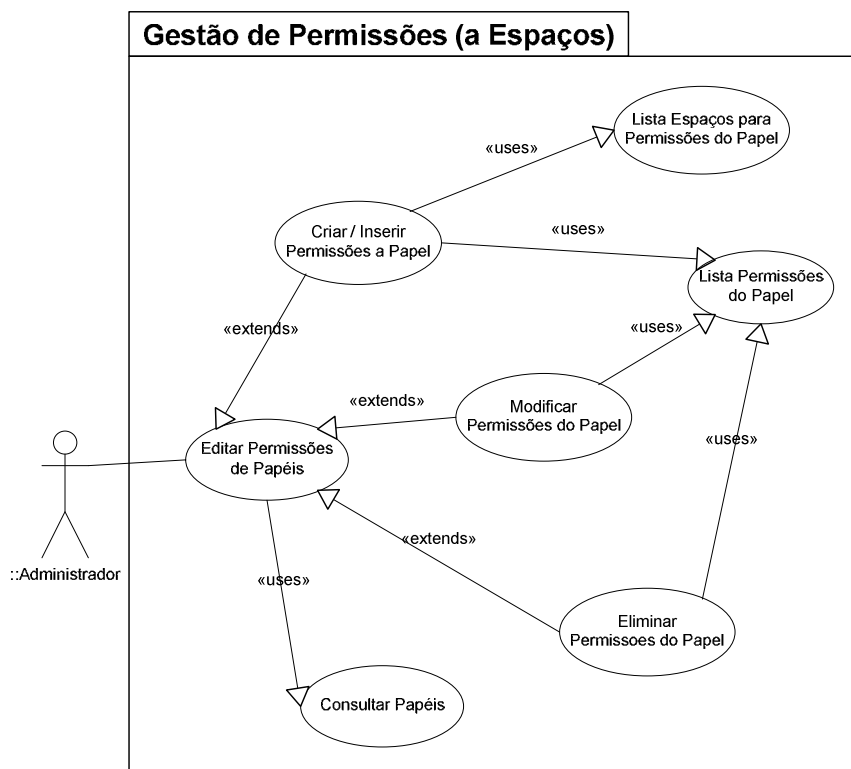


Figura 5.11 – Diagrama de casos de utilização de “Gestão de Permissões (a Espaços)”

Pretende-se que a aplicação implemente as funcionalidades descritas pelos casos de utilização representados graficamente no diagrama anterior (ver *Figura 5.11*). Também são descritos textualmente, num formato alto-nível, em Anexos (ver Anexo B – Casos de Utilização, em B.3 – Gestão de Permissões (a Espaços), pág. 191).

5.2.3.5 Auditar/Pesquisar Acessos e Presenças

Os casos de uso agrupados neste pacote oferecem as funcionalidades necessárias para auditar os acessos a espaços físicos efectuados por utilizadores, durante um determinado período de tempo, assim como, a pesquisa ou localização, em tempo real, de presenças de utilizadores em espaços físicos controlados. Com base num ficheiro de "log" que inclui informação de identificação dos utilizadores, do endereço dos espaços físicos, do tipo de acesso (entrada ou saída) e do tempo (data e hora de entrada ou saída), pode-se obter várias listagens de auditoria e administração de acessos. Os casos de utilização deste pacote permitem auditar os acessos de cada um dos utilizadores, os acessos a cada um dos espaços físicos controlados, os acessos a um espaço físico efectuados por um utilizador (Listagem do código desta funcionalidade no Anexo C.2 – Código de “Auditar Acessos a um Espaço por Utilizador”, pág. 215), pesquisar ou localizar, em tempo real, a presença dum determinado utilizador e consultar as presenças, em tempo real, de utilizadores num determinado espaço físico.

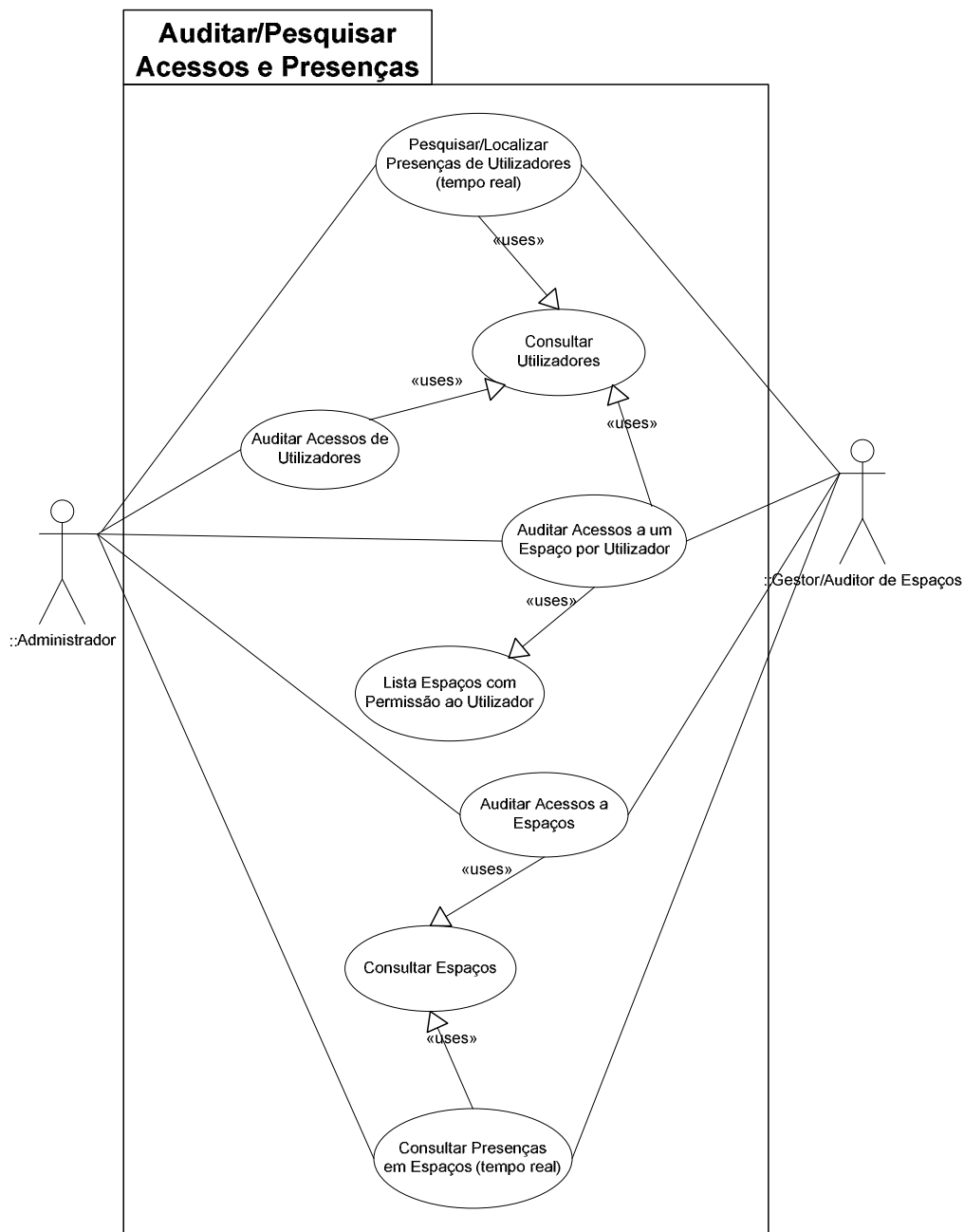


Figura 5.12 – Diagrama de casos de utilização de “Auditar/Pesquisar Acessos e Presenças”

Pretende-se que a aplicação implemente as funcionalidades descritas pelos casos de utilização representados graficamente no diagrama anterior (ver *Figura 5.12*). Também são descritos textualmente, num formato alto-nível, em Anexos (ver Anexo B – Casos de Utilização, em B.4 – Auditar/Pesquisar Acessos e Presenças, pág. 193).

5.2.4 Subsistema “Funcionamento do Controlo de Acessos Físico”

Os casos de uso do subsistema *funcionamento do controlo de acessos físico* oferecem as funcionalidades necessárias para as operações de funcionamento do sistema de controlo de acessos físico, relativas ao controlo de acessos (entradas e saídas) dos utilizadores aos espaços físicos controlados. Basicamente, este subsistema engloba dois casos de utilização principais: aceder a espaço e abandonar espaço.

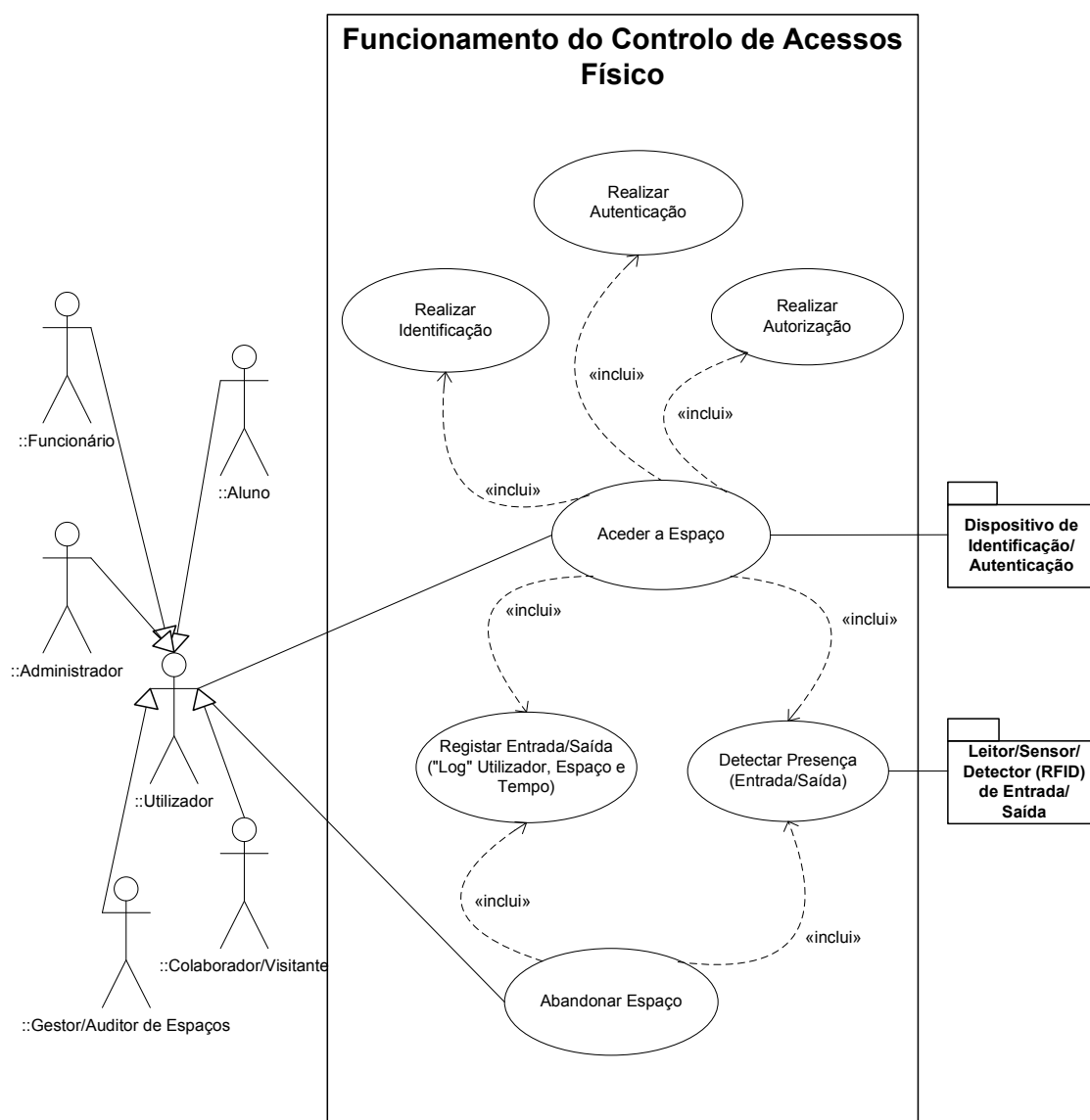


Figura 5.13 – Diagrama de casos de utilização do subsistema “Funcionamento do Controlo de Acessos Físico”

Pretende-se que a aplicação implemente as funcionalidades descritas pelos casos de utilização representados graficamente no diagrama anterior (ver Figura 5.13) e, na secção seguinte (ver secção §5.2.4.1 “Aceder e Abandonar Espaço”, pág. 107), descritos textualmente num formato alto-nível.

5.2.4.1 Aceder e Abandonar Espaço

Caso de Uso: Aceder a Espaço

Actores: Utilizador (do sistema de controlo de acessos físico), dispositivo de identificação/autenticação e sensor/detector de movimentos de entrada.

Descrição: Este caso de uso inicia-se quando o actor (utilizador) interagindo com o dispositivo de identificação ou autenticação, colocado no local de acesso, solicita o acesso a um espaço físico controlado. O sistema invoca, então, as operações de funcionamento do sistema de controlo de acessos físico, relativas ao controlo de acessos para *entradas*, efectuando a identificação, autenticação e autorização do utilizador, a detecção da sua presença (entrada) no espaço físico e o registo dessa entrada num ficheiro de *log*, em que regista a informação de identificação do utilizador, do espaço físico acedido, do tipo de acesso (entrada) e do tempo (data e hora de entrada) (ver casos de uso seguintes: “Realizar Identificação”, “Realizar Autenticação”, “Realizar Autorização”, “Detectar Presença (Entrada)”, “Registar Entrada”).

Caso de Uso: Realizar Identificação

Descrição: Este caso de uso inicia-se quando o utilizador interagindo com o dispositivo de identificação ou autenticação, solicita o acesso a um espaço físico controlado. Por sua vez, o sistema efectua os procedimentos de solicitação da identificação ou identidade do utilizador que pretende aceder ao espaço físico controlado. A identificação é o primeiro passo que um utilizador tem de efectuar para aceder a um determinado espaço físico controlado.

Caso de Uso: Realizar Autenticação

Descrição: Este caso de uso inicia-se após o processo de identificação do utilizador. O sistema realiza, então, o procedimento de autenticação, verificando se o utilizador, já identificado anteriormente, existe ou está registado no sistema e se, efectivamente, é quem reclamou ser na identificação. Na autenticação o sistema comprova a identidade do utilizador.

Caso de Uso: Realizar Autorização

Descrição: Este caso de uso inicia-se após o processo de autenticação do utilizador. O sistema realiza, então, o procedimento de autorização verificando ou validando se o utilizador, depois de identificado e autenticado, está efectivamente autorizado ou se tem permissão válida para aceder ao espaço físico controlado para o qual requer o acesso.

Caso de Uso: Detectar Presença (Entrada/Saída)

Descrição: Este caso de uso inicia-se com a entrada ou saída de um utilizador dum espaço físico controlado. O sistema detecta a presença do utilizador, confirmando a sua entrada ou saída do espaço físico controlado. Esta detecção poderá ser feita, através dum sensor, detector ou leitor *RFID* de movimentos, colocado no local de acesso, à entrada ou saída do espaço físico.

Caso de Uso: Registar Entrada/Saída

Descrição: Este caso de uso inicia-se após a tentativa ou confirmação de entrada ou saída de um utilizador dum espaço físico controlado. De cada vez que um utilizador tenta ou efectua a entrada ou saída dum determinado espaço físico controlado, é registado num ficheiro de *log* a informação de identificação do utilizador, do espaço físico, do tipo de acesso (entrada ou saída) e do tempo (data e hora de entrada ou saída).

Caso de Uso: Abandonar Espaço

Actores: Utilizador (do sistema de controlo de acessos físico) e sensor/detector de movimentos de saída.

Descrição: Este caso de uso inicia-se quando o actor (utilizador) interagindo com um sensor, detector de movimentos (ou leitor *RFID*), colocado no local de acesso (entrada ou saída), solicita a saída dum espaço físico controlado. O sistema invoca, então, as operações de funcionamento do sistema de controlo de acessos físico, relativas ao controlo de acessos para *saídas*, efectuando a detecção da presença do utilizador na saída do espaço físico e registo dessa saída num ficheiro de *log*, em que regista a informação de identificação do utilizador, do espaço físico abandonado, do tipo de acesso (saída) e do tempo (data e hora de saída) (ver casos de uso anteriores: “Detectar Presença (Saída)”, “Registar Saída”).

5.2.4.2 Diagramas de Sequência

A um caso de utilização podem corresponder vários diagramas de sequência para descrever sequências normais e excepcionais de funcionamento do sistema de controlo de acessos físico. Com base na estrutura interna do modelo de domínio (ver secção §5.3 “Modelo de Objectos do Domínio” seguinte, pág.111) apresentam-se, seguidamente, os diagramas de sequência para os casos de utilização *Aceder e Abandonar Espaço*, procurando-se, assim, mostrar a sequência de operações que ocorrem quando um utilizador acede e abandona um espaço físico controlado.

Para a sequência normal de funcionamento do *caso de utilização* “Aceder a Espaço”, tem-se o seguinte diagrama (ver *Figura 5.14* seguinte), que mostra a sequência de operações que ocorre quando um utilizador acede a um espaço físico controlado.

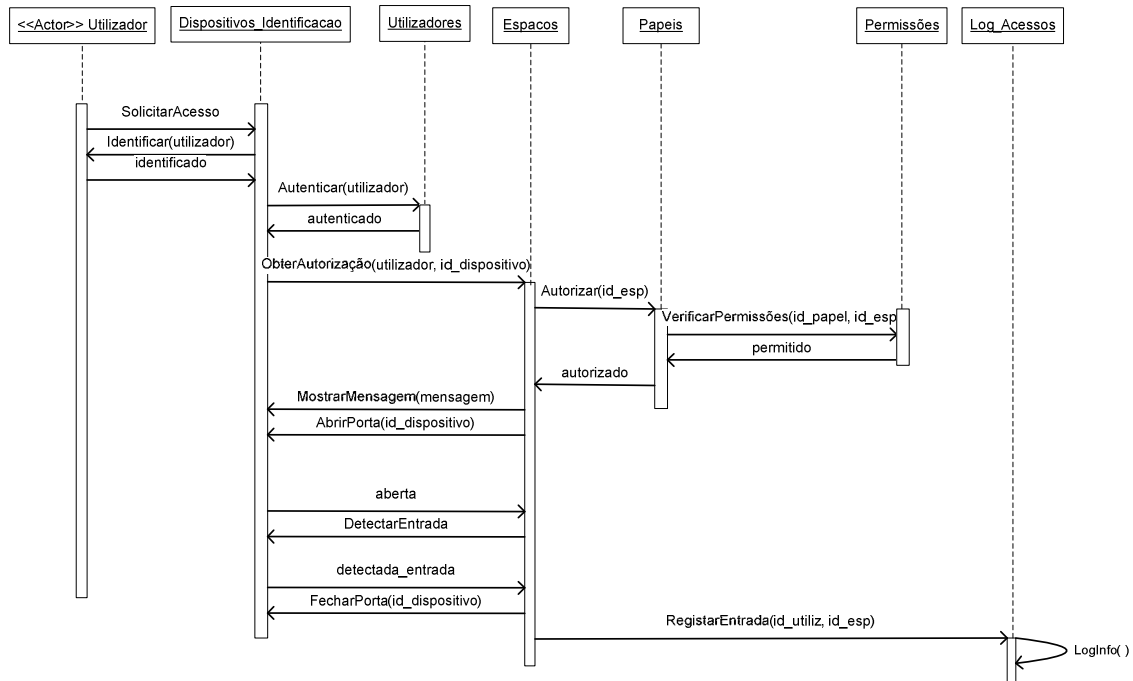


Figura 5.14 – Diagrama de sequência normal de funcionamento para aceder um espaço físico

O dispositivo de identificação ou autenticação, colocado no local de acesso, faz a aquisição ou leitura da informação do utilizador necessária à sua identificação e autenticação. De seguida, o sistema autentica e autoriza o utilizador, verificando se o mesmo tem permissão para aceder ao espaço físico. No caso do utilizador possuir permissão de acesso ao espaço requerido, é enviada uma mensagem “visual” para o dispositivo de identificação ou autenticação e abre-se a porta correspondente do local de acesso. Com a entrada do utilizador no espaço físico é detectada, através dum sensor/detector de movimentos, a sua presença no espaço físico, confirmando-se a sua entrada. O sistema ordena, então, o fecho da porta e efectua, num ficheiro de *log*, o registo do acesso do utilizador ao espaço físico.

No diagrama seguinte (ver *Figura 5.15*) é representada uma sequência excepcional de funcionamento para o mesmo caso de utilização mas, agora, na situação em que um utilizador, apesar de autenticado pelo sistema, solicita acesso a um espaço físico controlado para o qual não tem permissão ou autorização de acesso, permitindo-se que o sistema efectue o registo dessa “tentativa de acesso”.

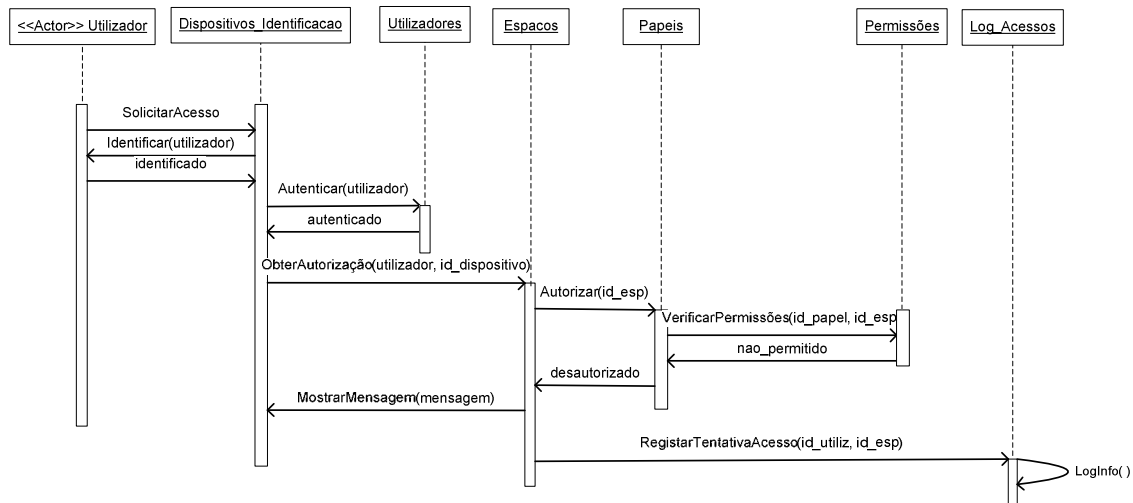


Figura 5.15 – Diagrama de sequência de funcionamento excepcional para aceder um espaço físico

Para a sequência normal de funcionamento do *caso de utilização* “Abandonar Espaço”, tem-se o seguinte diagrama (ver Figura 5.16), que mostra a sequência de operações que ocorre quando um utilizador sai ou abandona um espaço físico controlado.

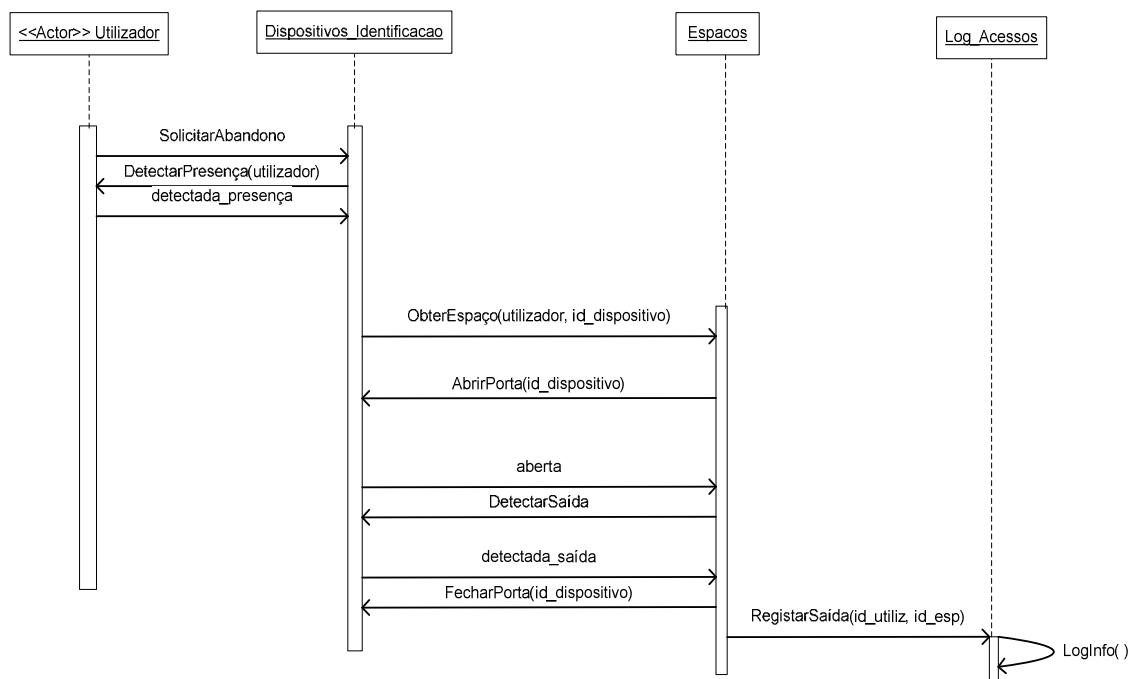


Figura 5.16 – Diagrama de sequência normal de funcionamento para abandonar um espaço físico

5.3 Modelo de Objectos do Domínio

Para se identificar as entidades correspondentes ao domínio do problema e seus relacionamentos, é apresentado em seguida (ver secção §5.3.1 “Diagrama do Modelo de Objectos do Domínio” seguinte, pág. 111), através dum diagrama de classes, o diagrama de objectos do domínio.

5.3.1 Diagrama do Modelo de Objectos do Domínio

O diagrama de classes da *Figura 5.17* seguinte representa as principais classes que constituem (no âmbito deste trabalho) o modelo de objectos do domínio da aplicação *WebGPACS* de gestão de sistemas de controlo de acessos físico.

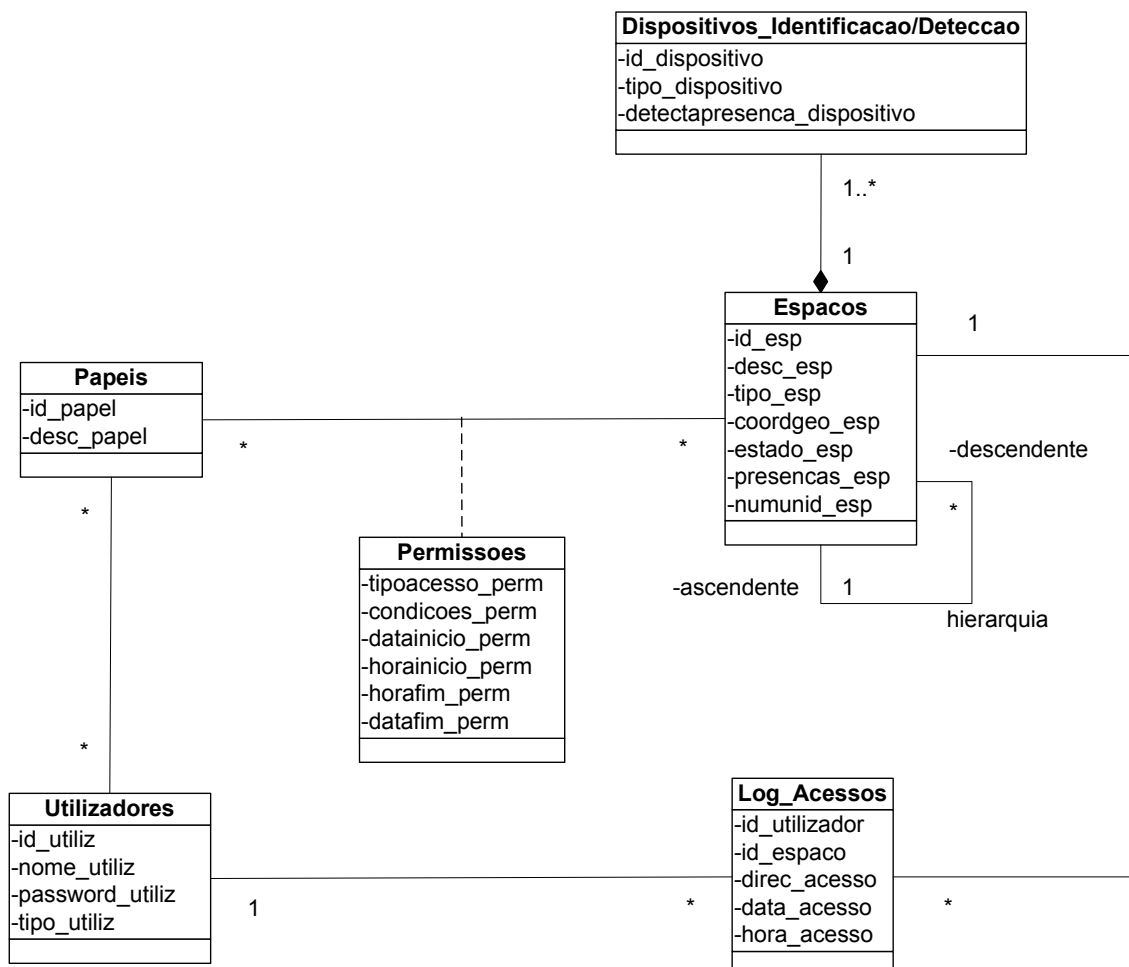


Figura 5.17 – Diagrama do modelo de objectos do domínio

5.3.2 Descrição do Modelo e Definições das Classes

O *diagrama* retrata um modelo de controlo de acessos baseado no papel cujos objectos de protecção são objectos físicos, representados pela classe *espacos* que contém os espaços físicos controlados. Um espaço físico (por ex., um edifício) pode ser composto sucessivamente por outros espaços mais pequenos (por ex., pisos, gabinetes, salas, laboratórios, armários,...) que se encaixam ou relacionam de modo hierárquico e sobre os quais o acesso é controlado. Um espaço físico controlado é um espaço fechado que requer uma *permissão* de acesso para ser acedido. Um objecto da classe *espacos* possui um ou vários objectos da classe *dispositivos_identificacao/deteccao*, não só responsáveis pela recepção do pedido de acesso e autenticação dos *utilizadores*, como também pela detecção da presença dos mesmos no espaço físico. Um *utilizador* pode ter vários *papéis* (por ex., um aluno de doutoramento em engenharia electrotécnica e computadores com o papel de “aluno de doutoramento do DEEC²⁶” pode também ter o papel específico de “aluno de doutoramento na área de informática e automação” (ver cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65 e secção §4.3.2.2 “Controlo de Acessos baseado nos Papéis de Utilizadores”, pág. 71) e a cada *papel* podem ser atribuídas várias *permissões* de acesso a espaços físicos. A classe *log_acessos* é utilizada para suportar o rastreio e controlo de quem acede (entrar/sair) a espaços físicos controlados. Para tal, utiliza-se auditorias de acessos, tanto para cada um dos utilizadores (onde tem estado, quais os espaços acedidos), como para cada um dos espaços físicos controlados (quem os acede, quais os utilizadores que o acederam).

Definições de Classes:

Utilizadores

Conjunto de dados relativos à identificação dos utilizadores do sistema de controlo de acessos.

Papéis

Conjunto de papéis utilizados na gestão do sistema de controlo de acessos físico que são atribuídos aos diferentes utilizadores do sistema.

Permissões

Conjunto de permissões de acesso aos diferentes espaços físicos que são atribuídas aos diferentes papéis utilizados na gestão do sistema de controlo de acessos físico.

Espacos

Entidade de espaços físicos controlados pelo sistema e que estão associados à estrutura física dos espaços ou localizações físicas da planta da organização (instituição). Encontra-se inter-relacionada de forma hierárquica com entidades do mesmo tipo.

²⁶ Sigla para designar “Departamento de Engenharia Electrotécnica e de Computadores”

Log_Acessos

Dados relativos a cada entrada ou saída dos utilizadores em espaços físicos controlados, com informação correspondente ao utilizador, ao espaço físico, ao tipo de acesso (entrada/saída) e tempo (data e hora).

Dispositivos_Identificacao/Deteccao

identificação dos dispositivos de identificação/autenticação e/ou detecção, utilizados em cada um dos locais de acesso dos espaços físicos controlados.

Capítulo 6

Arquitectura

6.1 Introdução

Arquitectura é, em geral, entendida como sinónimo de desenho de alto nível. No contexto dos sistemas de *software* e de informação entende-se por arquitectura, em sentido estrito, a estrutura de alto nível do sistema e, em sentido lato, todo o conjunto de decisões significativas acerca da organização do sistema [20]. Neste capítulo é apresentada a arquitectura suporte para a aplicação *WebGPACS*. Com esta apresentação pretende-se descrever a solução proposta, bem como as tecnologias que serão utilizadas para a implementação da aplicação desenvolvida. A *arquitectura lógica* da solução representar-se-á através de um *diagrama de pacotes de classes* em *UML* e, para a *arquitectura física*, utilizam-se dois diagramas, um informal e um *diagrama de distribuição* em *UML*, que permitem identificar a topologia do sistema, os nós de *hardware* e as suas ligações. Finalmente, explicita-se o *suporte tecnológico* que descreverá as tecnologias utilizadas e suas funções na arquitectura da solução *WebGPACS*.

6.2 Arquitectura Lógica

A *arquitectura lógica* preocupa-se com a decomposição do sistema em partes “lógicas”, sem preocupação de alocação dessas partes a componentes de *software*, máquinas (computadores) e processos (do sistema operativo) [20]. Nesta secção é apresentada a *arquitectura lógica* da solução proposta, através de um *diagrama de pacotes de classes*²⁷ em *UML* (ver *Figura 6.1* seguinte), decomposto em pacotes de classes para melhor organização e dividido em quatro camadas horizontais²⁸:

- *graphic user interface*
- páginas *web* dinâmicas
- lógica de negócio
- acesso a dados.

²⁷ Diagramas de pacotes lógicos utilizados para modelar a *arquitectura lógica* de um sistema de *software* (organização em módulos lógicos e especificação de *interfaces* e dependências entre módulos).

²⁸ Na caracterização da arquitectura lógica, a decomposição do sistema pode ser efectuada segundo duas perspectivas: decomposição *vertical* (por grupos de funcionalidades ou subsistemas) ou decomposição *horizontal* (por *camadas* da implementação). Normalmente, na decomposição *horizontal* são consideradas pelo menos três camadas: camada de *interface* com o utilizador (também chamada camada aplicacional, ou camada de apresentação e interacção com o utilizador); camada de lógica de negócio e acesso a dados (também chamada camada de domínio); camada de dados (a base de dados propriamente dita).

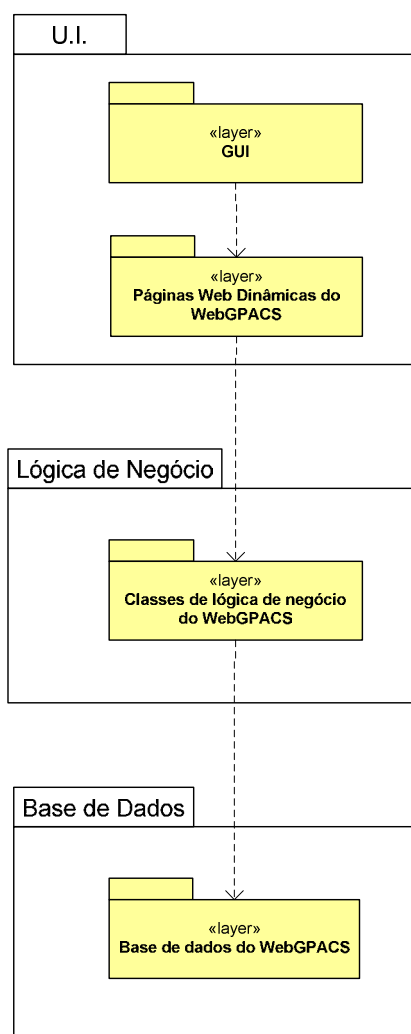


Figura 6.1 – Diagrama de pacotes de classes do WebGPACS

O *WebGPACS* sendo uma aplicação disponível na *Internet* e utilizada através dum navegador *web*, terá necessidade dum servidor *web* para responder aos pedidos *HTTP* dos seus utilizadores (Administrador e/ou Gestores/Auditores de Espaços).

O pacote de classes *GUI* (*Graphical User Interface*) englobará todas as classes e funções da *interface* gráfica do *browser* utilizado para aceder à aplicação. No pacote de classes das páginas *web* dinâmicas estarão as classes necessárias para os utilizadores poderem visualizar os dados e resultados da aplicação. Estas páginas são geradas dinamicamente pelo servidor *web* consoante as opções dos utilizadores da aplicação e dos resultados a apresentar. No pacote do servidor *web* existem diversos pacotes necessários para a aplicação correr num *browser* (entre os quais, o servidor *HTTP* que contém as classes necessárias para receber do *browser* os pedidos provenientes dos utilizadores) e também o pacote com a *Lógica de Negócio* do servidor, onde estão as classes que possibilitam a publicação do *WebGPACS* na *web* e o acesso a dados, a ligação ao pacote de classes da base de dados. O pacote de classes da Base de Dados permite guardar todos os dados necessários para posteriores análises, informações e resultados relacionados com o *WebGPACS*.

6.3 Arquitectura Física

A *arquitectura física* preocupa-se com a infra-estrutura de *hardware* (essencialmente computadores e redes) sobre a qual corre o sistema de *software*, com a decomposição do sistema de *software* em componentes e com a localização desses componentes nos computadores [20]. Nesta secção pretende-se, sobretudo, mostrar a conceptualização da estrutura física que poderá suportar a implementação da aplicação de *software* desenvolvida.

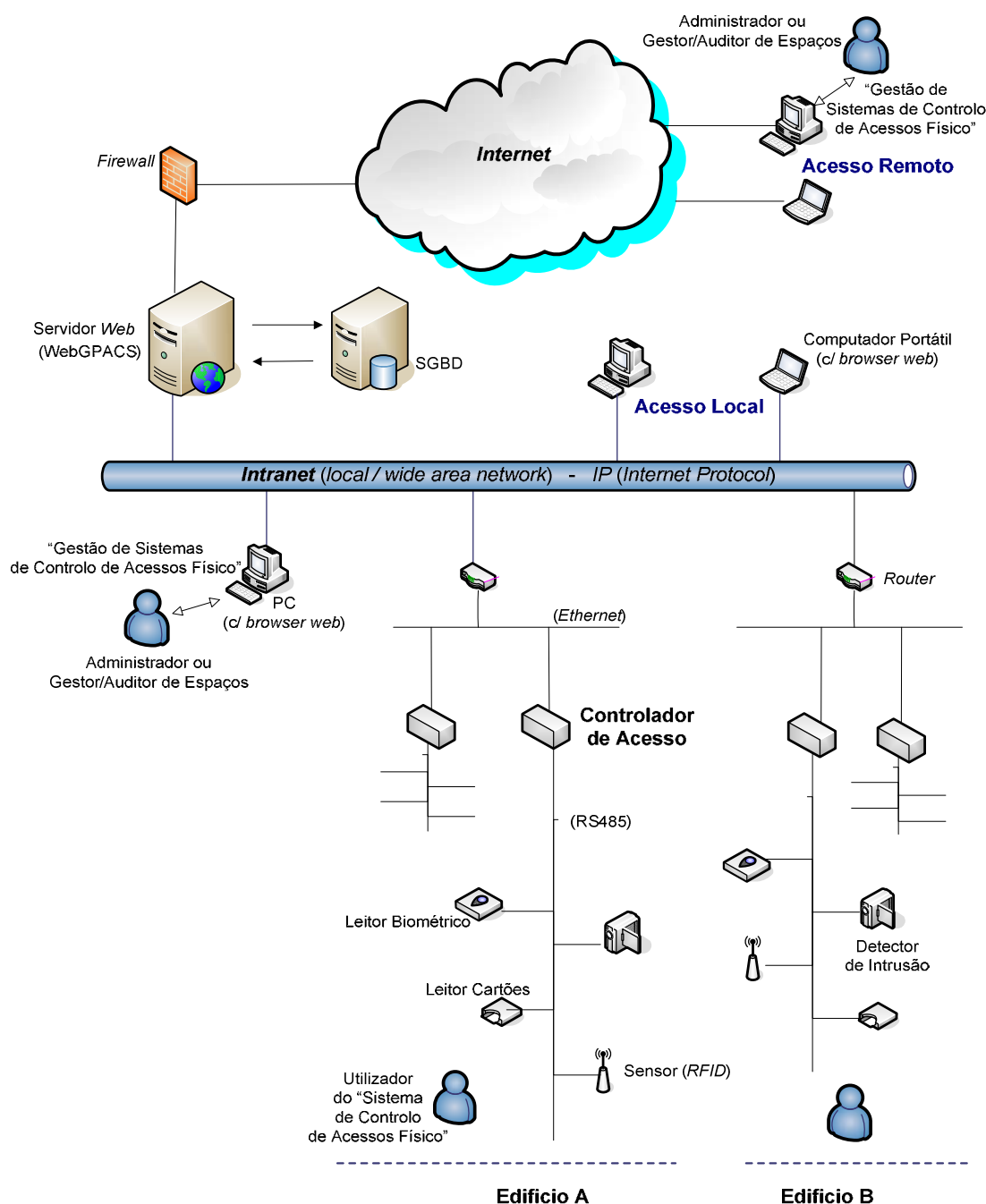


Figura 6.2 – Arquitectura física do WebGPACS, adaptada de [23]

A aplicação *WebGPACS* será utilizada através de um navegador *web* e deve funcionar em qualquer *máquina cliente* (*desktops, laptops,...*) que tenha instalado um *browser* no seu sistema operativo. Na *máquina servidora*, sistema central onde se processa a aplicação, ficará instalado um servidor *web* (*Apache*) com suporte *PHP* que comunica com um servidor²⁹ de base de dados (*MySQL*) para a gestão da informação e com os diversos controladores situados nos edifícios e espaços físicos controlados. O servidor *web* interpreta os pedidos *HTTP* do *browser* que provêm do utilizador e possibilita a ligação à componente lógica de negócio do *WebGPACS*. Esta componente efectua a leitura da informação residente na base de dados e gera as páginas dinâmicas correspondentes à aplicação, disponibilizando-as quer na rede privada (*intranet*) da organização, quer na *internet*, o que possibilita aos utilizadores (Administrador e/ou Gestores/Auditores de Espaços) aceder ao sistema por qualquer dos meios. Na *Figura 6.3* seguinte, mostra-se um *diagrama de distribuição* (*deployment*) em *UML* que retrata o ambiente de *hardware* em que se executa os componentes de *software* do *WebGPACS*.

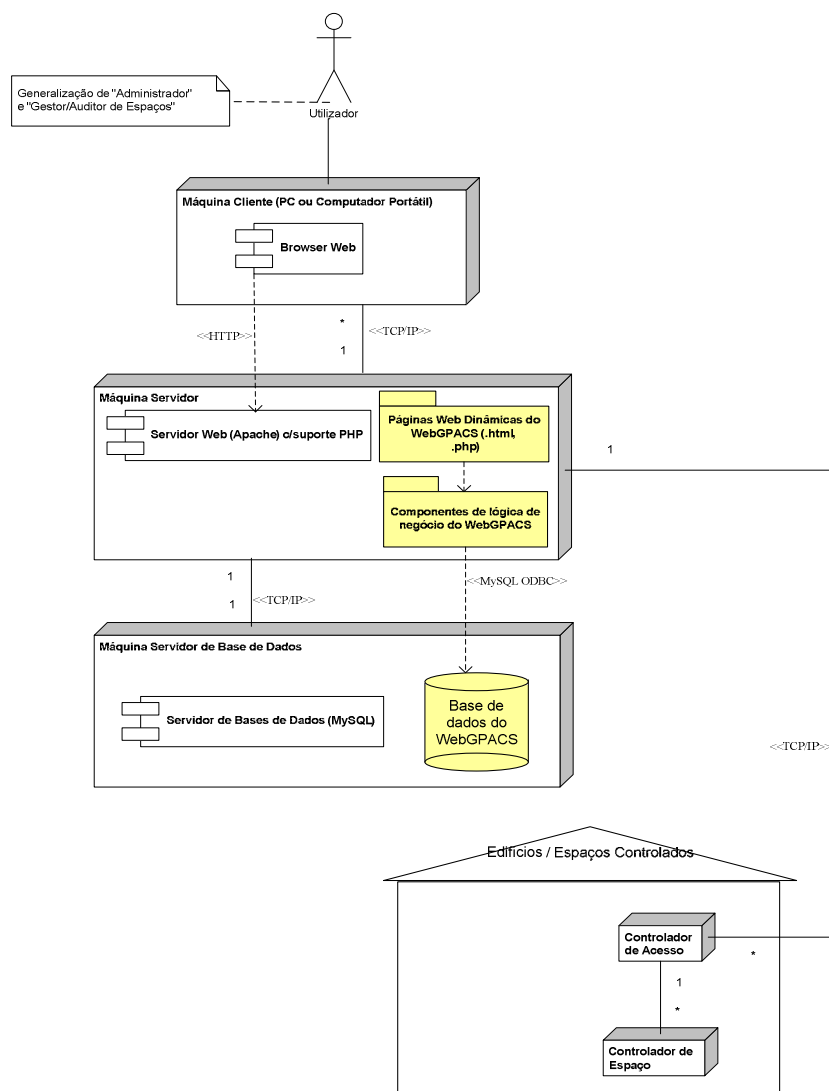


Figura 6.3 – Diagrama de distribuição do WebGPACS

²⁹ O servidor de base de dados poderá ficar na mesma máquina do servidor web ou num computador distinto, dependendo das condições de configuração da aplicação.

6.4 Tecnologias de Suporte

As tecnologias utilizadas no desenvolvimento do projecto são:

- um Servidor *Web* (*Apache*)
- um Sistema de Gestão de Base de Dados (*MySQL*)
- *DHTML*³⁰ (*HTML*, *CSS* e *JavaScript*)
- uma linguagem interpretada³¹ (*PHP*) para possibilitar a criação das lógicas de negócio e de apresentação da aplicação *WebGPACS*

6.4.1 Servidor *Web* (*Apache*)

O acesso a um recurso *web*³² faz-se a partir de um *software* cliente (navegador, *browser*) para um *software* servidor (servidor *web*). É através da *URL*³³ que um computador localiza o caminho dum servidor na *Internet*, o qual, por sua vez, devolve o recurso solicitado ao computador ou *software* cliente (ver *Figura 6.4* seguinte) [17].

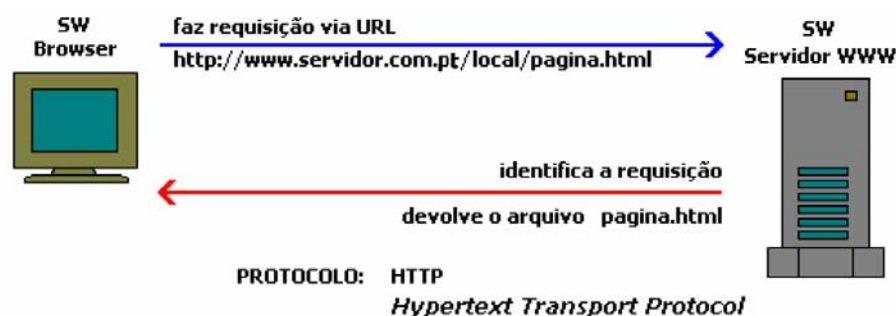


Figura 6.4 – Interação navegador (browser) e servidor Web

O servidor *web* utilizado no presente projecto é o *Apache Web Server*, um dos servidores *web* mais utilizados na *Internet*. O *Apache Server* é um *software* livre que executa código em diversas linguagens (tais como, *PHP*, *Perl*, *Shell Script*) e funciona como servidor *HTTP*³⁴, essencial para o funcionamento da aplicação *WebGPACS*.

³⁰ *HTML* Dinâmico (da expressão inglesa *Dynamic HTML*). Nome dado à utilização em conjunto de *HTML*, *CSS* e *JavaScript*.

³¹ Linguagem interpretada é uma linguagem cujo código fonte é traduzido e executado instrução a instrução, por um programa – interpretador, ao contrário das linguagens compiladas, em que todas as instruções do código fonte são traduzidas antes que se inicie a execução do programa. A linguagem *PHP* é uma linguagem interpretada, ou seja, de cada vez que se executa um código *PHP*, o código fonte é lido, interpretado e só depois executado, ao contrário das linguagens compiladas, onde o processo de leitura e interpretação do código fonte é feito numa única vez, na compilação do programa.

³² *Web* é a forma reduzida de *WWW* (*World Wide Web*).

³³ *URL* (*Uniform Resource Locator*), nome dado ao endereçamento de um recurso na *Web* e que define uma forma padrão de acesso: protocolo :// domínio / localização_do_recurso.

³⁴ Protocolo de comunicação *HTTP* (*Hypertext Transport Protocol*).

6.4.2 HTML

A aplicação será visualizada em navegadores *web*, devendo por essa razão gerar código padrão, de modo que os utilizadores (administrador e gestor/auditor de espaços) possam utilizar a aplicação *WebGPACS*. Para formatação e estruturação das páginas *web* foi adoptada a linguagem de formatação *HTML* (*Hypertext Markup Language*), que define a estrutura e o formato dos documentos *web*. As suas principais características traduzem-se por:

- produzir documentos (páginas *web*) compostos por textos e comandos especiais (*tags*) de *html*.
- possibilitar, através de *links* de hipertexto, a referência a outros documentos (documentos com ligações a outros documentos).
- permitir a inclusão de imagens, sons, vídeos, objectos.
- permitir a interacção do utilizador com vários sistemas, através da utilização de formulários, botões, *links*,...
- utilização do protocolo de comunicação *HTTP* (*Hypertext Transport Protocol*).
- associar-se a outras tecnologias, tais como:
 - *CSS* (*Cascading Style Sheet*), que engloba diversas melhorias aos níveis, visual e de interactividade.
 - *JavaScript*, que agrega programação, do lado do cliente (*browser*), para incremento de mais e melhor interactividade [17].

6.4.3 CSS

Para se definir o aspecto da aplicação utilizam-se folhas de estilo *CSS* (*Cascading Style Sheets*), uma tecnologia que se utiliza não só para suprir as insuficiências de apresentação gráfica e visual do *html*, como também para padronizar a apresentação das diversas páginas *web*. Uma folha de estilo *CSS* define um conjunto de regras que determinam a forma ou padrão do *browser* apresentar os documentos *html*, procurando-se, assim, melhorar a disposição da página (*layout*). O *CSS* faz parte dum padrão de utilização, chamado *DHTML*, que não é mais do que a utilização conjunta de *HTML*, *CSS* e *JavaScript*. Através das folhas de estilo *CSS* é possível separar-se o conteúdo do documento (*HTML*) do estilo da apresentação (*CSS*), em que as mesmas podem ser definidas numa das seguintes formas:

- no documento *html*, em que as folhas de estilo podem estar contidas nos cabeçalhos ou incluídas no corpo dos documentos *html* [19].
- externamente ao documento *html*, [17] em que as folhas de estilo podem estar definidas em ficheiros externos, deste modo, permitindo-se utilizar as mesmas definições de estilo em múltiplas páginas. Desta forma, é possível mudar completamente o estilo de uma aplicação, possivelmente com dezenas ou centenas de páginas, actuando sobre um único ficheiro.

6.4.4 JavaScript

Para executar algumas tarefas do lado do utilizador (*browser*) será utilizado *JavaScript*, uma linguagem que permite efectuar programação em documentos *HTML* na construção de páginas *web* interactivas. É uma linguagem (*script client-side*) em que o código fonte é executado pelo navegador (*web browser*), no “abrir” da página *HTML*. O *Javascript* tem alguma semelhança com *Java*, mas não deve ser confundida com esta. A codificação lógica do *Javascript* é independente da do *HTML*, o que permite maior dinamismo e interacção com os utilizadores das páginas *internet*. Algumas das vantagens desta linguagem são:

- reduzir o tempo de processamento do servidor, uma vez que é executada no lado do cliente.
- reduzir a quantidade de pedidos ou solicitações ao servidor, tornando a execução mais rápida.
- nas interacções dos utilizadores com a página, antes dos formulários serem enviados ao servidor, permitir efectuar validações nos próprios formulários.
- proporcionar maior e melhor interactividade com o documento *web* [17].

6.4.5 PHP

A linguagem interpretada³⁵ utilizada é o *PHP* (*Hypertext Preprocessor*), de ampla utilização e especialmente útil em desenvolvimento *web*. É uma das linguagens de programação suportadas directamente no servidor *Apache*, em que o código é executado por este servidor³⁶. A Figura 6.5 seguinte ilustra a interacção entre o *PHP*, o servidor *web* e o navegador *web* (*browser*) do utilizador.

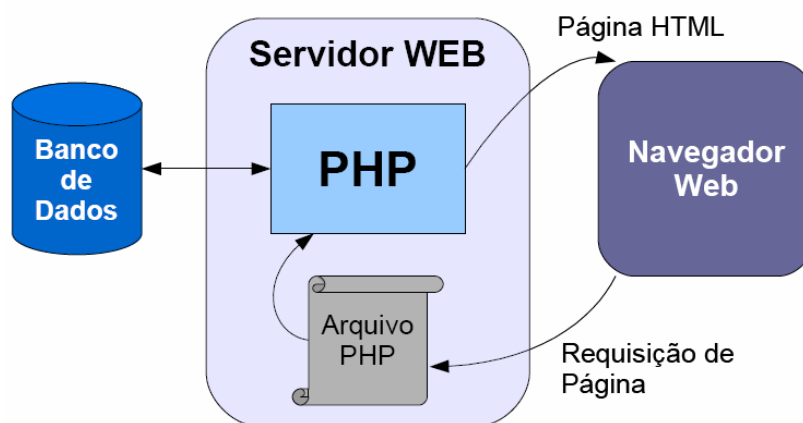


Figura 6.5 – Interacção entre PHP, o servidor Web e o browser do utilizador

³⁵ Linguagem interpretada é uma linguagem cujo código fonte é traduzido e executado instrução a instrução, por um programa – interpretador, ao contrário das linguagens compiladas, em que todas as instruções do código fonte são traduzidas antes que se inicie a execução do programa.

A linguagem *PHP* é uma linguagem interpretada, ou seja, de cada vez que se executa um código *PHP*, o código fonte é lido, interpretado e só depois executado, ao contrário das linguagens compiladas, onde o processo de leitura e interpretação do código fonte é feito numa única vez, na compilação do programa.

³⁶ De modo inverso, o código do *javascript* é executado no lado cliente.

É um *software* livre, à semelhança de todas as tecnologias utilizadas neste projecto, uma linguagem bastante poderosa, orientada a objectos e que pode ser executada em vários sistemas operativos (tais como, *Windows*, *Unix*, *Linux*, entre outros). Ao contrário das ferramentas que necessitam de *drivers ODBC* para se interligarem às bases de dados relacionais, esta linguagem permite uma interligação directa com estas (tais como, *Oracle*, *Sybase*, *Postgresql* e *MySQL* – o sistema de gestão de base de dados utilizado neste projecto). O *PHP* suporta também os principais protocolos de *Internet* (*IMAP*, *SNMP*, *NNTP*, *POP3*, *HTTP*, *LDAP*, *XML-RPC*, *SOAP*,...), sendo ainda possível abrir *sockets* para interagir com outros.

6.4.6 SGBD (*MySQL*)

O Sistema de Gestão de Base de Dados (*SGBD*) que será utilizado é o *MySQL*, um *SGBD* relacional livre, que utiliza o padrão *SQL* como linguagem de consulta e controlo de dados. Caracteriza-se pela sua simplicidade e eficiência, estando optimizado para aplicações baseadas na *web*. Também funciona com os principais sistemas operativos actuais, à semelhança do *PHP*, e devido à sua fácil e eficiente integração com este (*PHP*) (ver secção anterior §6.4.5 “*PHP*”, pág. 121), foi o servidor de base de dados escolhido para o desenvolvimento da aplicação *WebGPACS*.

Capítulo 7

Implementação

7.1 Introdução

Este capítulo descreve os aspectos mais relevantes relativos à implementação da aplicação *WebGPACS*. Começa por apresentar a estrutura e a configuração do sistema, utilizadas para a implementação. Em seguida, o desenho de dados da implementação, em que se apresenta o diagrama E-R e a descrição das entidades e atributos correspondentes da base de dados. De modo especial, é definido e caracterizado o *modelo de gestão de dados hierárquicos* utilizado para lidar, em concreto, com a tabela de *espaços físicos* (dados hierárquicos) da aplicação, em que são expostas e explicadas, em detalhe, as principais expressões *MySQL* do modelo. Por fim, são apresentadas todas as interrogações da aplicação *WebGPACS* que foram utilizadas no acesso à tabela de *espaços físicos* (dados hierárquicos) da base de dados da aplicação.

7.2 Instalação e Configuração do Sistema

A estrutura física do sistema desenvolvido possui um servidor *web*, onde se aloja o *sítio web* da aplicação *WebGPACS*, podendo ser acedido através dum *browser web*. O servidor *web* utilizado foi o *Apache* que, nesta implementação, é executado numa máquina *Windows*. Existe também um servidor de base de dados (*MySQL*) e um interpretador *PHP* utilizado para a lógica de negócio. Optou-se por numa mesma máquina, servidor da aplicação *WebGPACS*, alojarem-se os servidores de base de dados e *web*, bem como, o interpretador *PHP*.

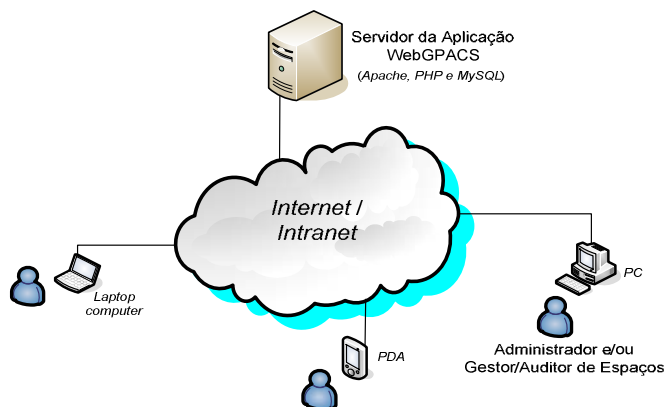


Figura 7.1 – Esquema da implementação da aplicação WebGPACS

O acesso à aplicação *WebGPACS*, quer pela *Internet*, quer pela *Intranet* da organização, é permitido, apenas, aos utilizadores que se identifiquem e autenticuem como administrador e/ou gestor/auditor de espaços. O sítio *web* da aplicação contém uma secção pública (página de entrada da aplicação) e uma secção privada acessível àqueles, depois de devidamente identificados e autenticados pelo sistema.



Figura 7.2 – Página inicial da aplicação WebGPACS

7.3 Modelo Relacional da Base de Dados da Aplicação

Nas subsecções desta secção, apresenta-se, através dum diagrama entidade-relação e da descrição das suas entidades e atributos, o modelo relacional da base de dados da aplicação.

7.3.1 Diagrama Entidade-Relação (*E-R*)

Para se poder armazenar a informação e os dados necessários à aplicação, criou-se uma base de dados *MySQL*, cuja estrutura é demonstrada pelo *diagrama de entidade-relação* da Figura 7.3 seguinte.

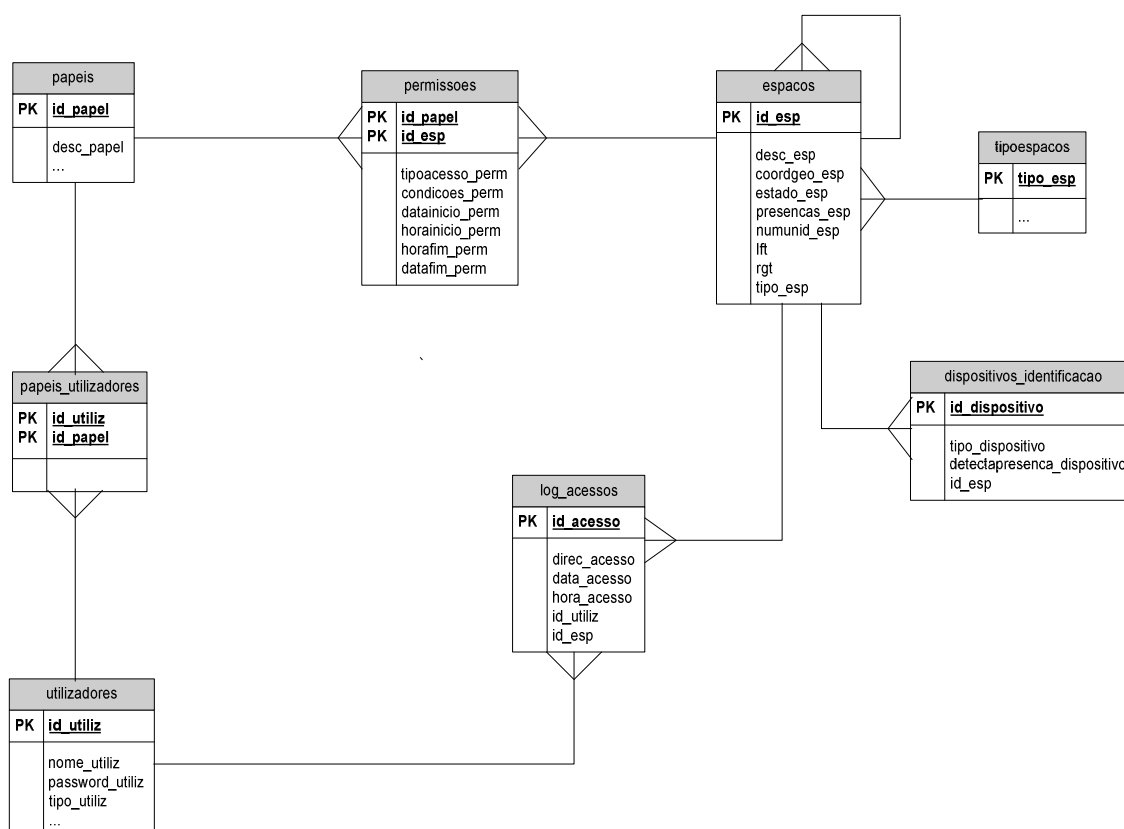


Figura 7.3 – Diagrama entidade-relação da base de dados da aplicação WebGPACS

7.3.2 Descrição das Tabelas e Atributos

Com base nas entidades ou estruturas do diagrama de entidade-relação da *Figura 7.3* anterior, segue-se uma breve descrição das entidades e seus atributos.

utilizadores

Tabela para armazenar os dados relativos à identificação dos utilizadores do sistema de controlo de acessos.

Principais Atributos:

id_utiliz

nome_utiliz

password_utiliz

tipo_utiliz

...

Descrição:

Identificação do utilizador

Nome do utilizador

Senha (*password*) do utilizador

Tipo de utilizador

papeis_utilizadores

Tabela constituída pela concatenação das chaves primárias das tabelas *utilizadores* e *papeis* envolvidas na associação de n para n.

Principais Atributos:

id_utiliz

id_papel

Descrição:

Identificação do utilizador

Identificação do papel

papeis

Tabela para armazenar os dados relativos aos papéis que são utilizados na gestão do sistema de controlo de acessos.

<i>Principais Atributos:</i>	<i>Descrição:</i>
<u>id_papel</u>	Identificação do papel
desc_papel	Descrição do papel
...	

permissoes

Tabela para armazenar os dados relativos a permissões (a espaços físicos) que são atribuídas aos papéis na gestão do sistema de controlo de acessos.

<i>Principais Atributos:</i>	<i>Descrição:</i>
<u>id_papel</u>	Identificação do papel
<u>id_esp</u>	Identificação do espaço
tipoacesso_perm	Tipo de acesso da permissão
condicoes_perm	Condições da permissão
datainicio_perm	Data início da permissão
horainicio_perm	Hora início da permissão
horafim_perm	Hora fim da permissão
datafim_perm	Data fim da permissão

espacos

Tabela para armazenar os dados relativos à identificação dos espaços físicos e sua hierarquia, controlados pelo sistema de controlo de acessos físico.

<i>Principais Atributos:</i>	<i>Descrição:</i>
<u>id_esp</u>	Identificação do espaço
desc_esp	Descrição do espaço
coordgeo_esp	Coordenadas do espaço (espaço "pai")
estado_esp	Estado do espaço
presencas_esp	Número de presenças/pessoas no espaço
numunid_esp	Número de unidades/espaços contidos nesse espaço
lft	Valor para representar a posição relativa do espaço físico na hierarquia
rgt	Valor para representar a posição relativa do espaço físico na hierarquia
tipo_esp	Tipo de espaço

tipoespacos

Tabela para armazenar dados de suporte à caracterização de espaços físicos, concretamente no que se refere a tipos de espaços.

<i>Principais Atributos:</i>	<i>Descrição:</i>
<u>tipo_esp</u>	Tipo de espaço
...	

log_acessos

Tabela para armazenar os dados referentes a acessos (entradas e saídas) de espaços físicos controlados pelo sistema, com informação relativa à identificação do utilizador, do espaço e do tempo de acesso.

<i>Principais Atributos:</i>	<i>Descrição:</i>
<u>id_acesso</u>	Identificação do acesso
direc_acesso	Direcção do acesso
data_acesso	Data do acesso
hora_acesso	Hora do acesso
id_utiliz	Identificação do utilizador
id_esp	Identificação do espaço

dispositivos_identificacao

Tabela para armazenar os dados relativos à identificação dos dispositivos de identificação/autenticação e/ou detecção utilizados no controlo de acessos aos espaços físicos.

Principais Atributos:

id_dispositivo

tipo_dispositivo

detectapresenca_dispositivo

id_esp

...

Descrição:

Identificação do dispositivo de identificação e/ou detecção

Tipo de dispositivo

Detecta presença do utilizador no espaço (valor de *entrada* / *saída*)

Identificação do espaço

7.4 Modelo de Gestão de Dados Hierárquicos da Tabela “Espaços”

As tabelas duma base de dados relacional não são hierárquicas mas, simplesmente, uma lista uniforme de dados. Os dados hierárquicos possuem uma relação de pai-filho que não é representada, de modo natural, numa tabela de base de dados relacional. Dados estruturados hierarquicamente podem ser necessários em várias aplicações, particularmente, neste projecto, em que será preciso não só representar-se edifícios no interior do *campus* universitário, como também, os espaços físicos (pisos, salas de aula, gabinetes,...) no interior dos mesmos edifícios ou doutros espaços físicos. Em seguida, apresenta-se um simples exemplo elucidativo desta necessidade, de representação hierárquica de dados, em que se supõem dois pisos, o *piso-0* e o *piso-1* do *edifício-I* do *DEEC* da *FEUP*. Cada um destes pisos contém múltiplos e variados espaços físicos: o *piso-0* composto pelos espaços físicos *I-006*, *I-010* e *I-014*; o *piso-1* pelos espaços físicos *I-104*, *I-109* e *I-119*. No interior do espaço *I-104* existe ainda uma parte reservada (por ex., um armário) que se vai designar por *I-104.1*. Todos estes espaços devem ser representados hierarquicamente, conforme ilustra a *Figura 7.4* seguinte.

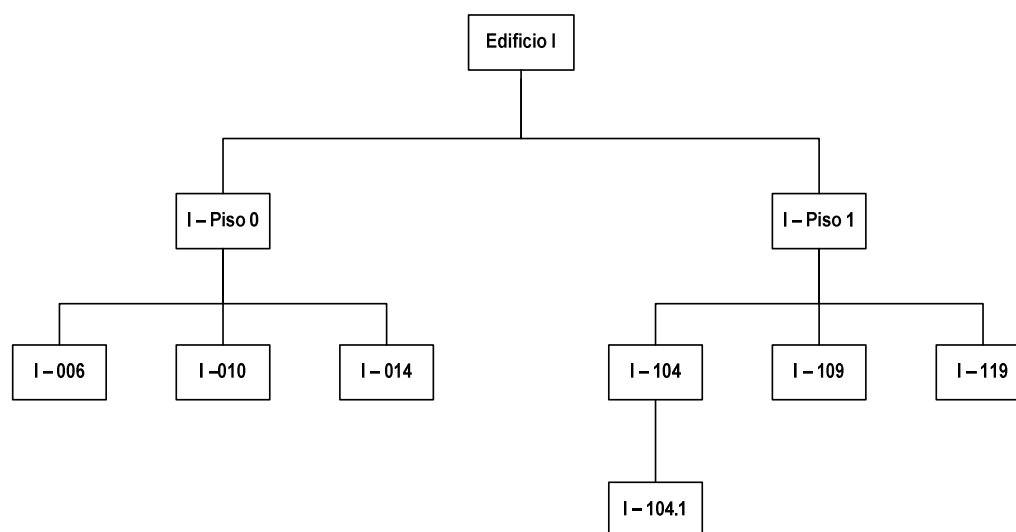


Figura 7.4 – Representação hierárquica dos espaços físicos em árvore (com nodos e linhas)

Na implementação da aplicação *WebGPACS*, o modelo de gestão utilizado para lidar com este tipo de representação hierárquica de dados, foi o *Modelo de Conjuntos Encaixados* (ou *Diagramas de Venn*) [15]. Neste modelo, pode-se observar que a hierarquia de dados é representada numa forma diferente, não com nodos e linhas como representado na *Figura 7.4* anterior, mas como conjuntos encaixados, conforme mostra a *Figura 7.5* seguinte.

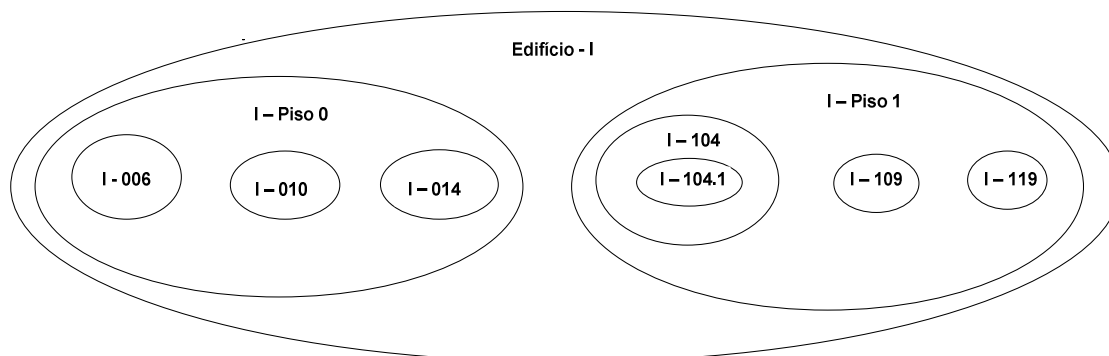


Figura 7.5 – Representação hierárquica dos espaços físicos em modelo de conjuntos encaixados

Note-se que neste modelo a hierarquia de dados mantém-se, com os espaços *pais* envolvendo os espaços *filho*. Esta hierarquia de dados pode também ser representada por meio duma tabela (ver *Tabela 5* seguinte), em que se utilizam os valores da esquerda e direita (*lft*, *rgt*)³⁷ para representarem o encaixamento dos espaços físicos.

Tabela 5 – Representação hierárquica dos espaços físicos, em modelo de conjuntos encaixados, numa tabela

id_registo	Espaços físicos	lft	rgt
1	Edifício – I	1	20
2	I – Piso 0	2	9
3	I – 006	3	4
4	I – 010	5	6
5	I – 014	7	8
6	I – Piso 1	10	19
7	I – 104	11	14
8	I – 104.1	12	13
9	I – 109	15	16
10	I – 119	17	18

Para determinar os valores de *lft* e *rgt* iniciou-se a numeração pelo lado esquerdo do nodo representado mais à esquerda, continuando-se, no sentido da direita, a ordem sucessiva de numeração, conforme representado no exemplo da *Figura 7.6* seguinte.

³⁷ Utiliza-se *lft* e *rgt* porque são palavras reservadas em *MySQL*, a base de dados utilizada na aplicação *WebGPACS*.

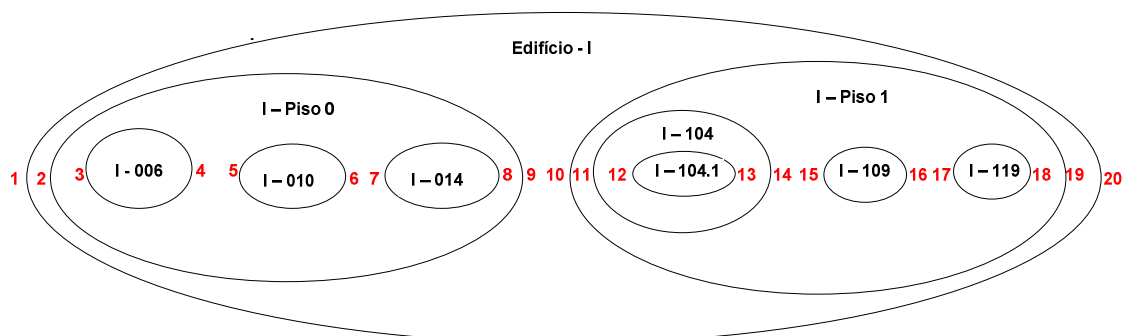


Figura 7.6 – Representação hierárquica dos espaços físicos no modelo de conjuntos encaixados, com discriminação dos valores lft e rgt de cada espaço físico (ou nodo hierárquico)

Este modelo pode, também, ser aplicado numa representação hierárquica de espaços físicos em árvore, conforme se observa na Figura 7.7 seguinte.

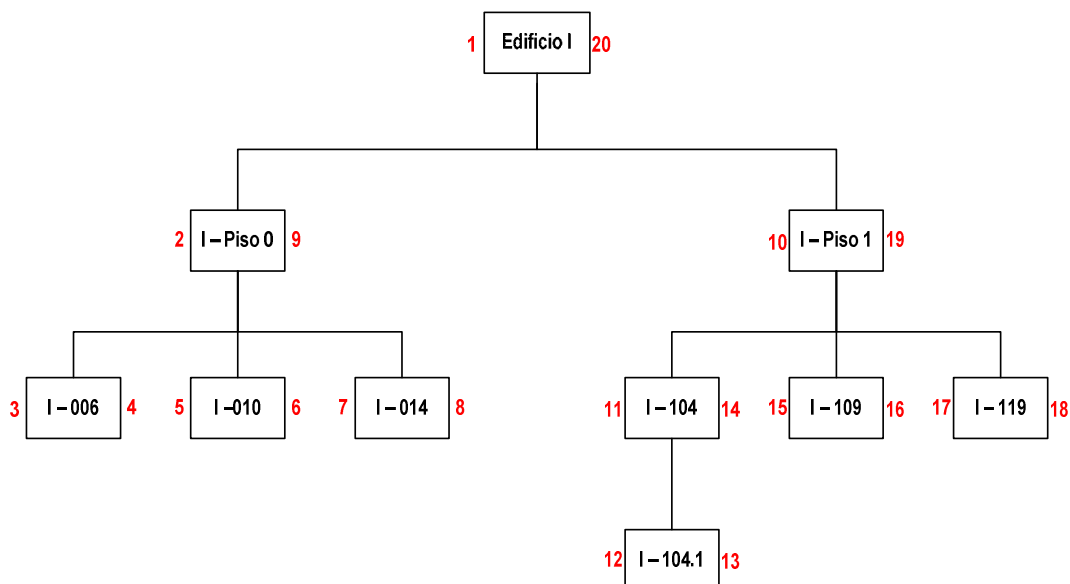


Figura 7.7 – Representação hierárquica dos espaços físicos em árvore (com nodos e linhas), com discriminação dos valores de lft e rgt de cada espaço físico (ou nodo da árvore)

Para se percorrer os diferentes nodos numa árvore hierárquica existem vários tipos de travessia. No caso concreto da elaboração da aplicação *WebGPACS*, o tipo utilizado foi a *Travessia (percurso) Pré-Ordem*, em que se percorre cada nodo da esquerda para a direita em cada nível, descendo-se de nível a cada nodo filho, começando-se por:

- 1º) Visitar o nó ou nodo raiz
- 2º) Percorrer a sub-árvore esquerda do nó visitado
- 3º) Percorrer a sub-árvore direita do nó visitado

7.4.1 Expressões MySQL para a Hierarquia de Espaços Físicos

Com base na tabela de *espacos* (dados hierárquicos) (ver secção §7.3.2 “Descrição das Tabelas e Atributos”, pág. 125) utilizada na aplicação *WebGPACS*, vai-se apresentar, nas secções subsequentes, algumas das *expressões MySQL* [15] que foram ou podem ser utilizadas para lidar com os dados relativos à hierarquia de espaços físicos do sistema.

7.4.1.1 Representação da Totalidade dos Espaços Físicos

Ao existir uma ligação entre os espaços físicos (nodos) pais e filhos, assumindo-se que o valor *lft* dum espaço físico filho aparecerá sempre entre os valores *lft* e *rgt* do espaço físico pai, pode-se representar a totalidade dos espaços físicos numa árvore. Para tal, utilizando o exemplo da tabela da secção anterior (ver *Tabela 5*, secção §7.4 “Modelo de Gestão de Dados Hierárquicos da Tabela “Espacos””, pág. 127) e a interrogação (*query*) que se segue, tem-se:

<i>Query</i>	<i>Saída (id_esp)</i>
	Edifício-I
	I – Piso 0
	I – 006
	I – 010
	I – 014
	I – Piso 1
	I – 104
	I – 104.1
	I – 109
	I – 119

A interrogação funciona independentemente da *profundidade da árvore*³⁸ (ver secção §7.4.1.4 “Profundidade (nível hierárquico) dos Espaços Físicos” pág. 131), não sendo necessário mencionar o valor de *node.rgt* porque este valor, tal como o valor de *lft*, estará sempre contido entre os valores de *lft* e *rgt* do espaço físico (nodo) pai.

7.4.1.2 Espaços Físicos (nodos) “Folha”

Ao analisar-se a tabela e a figura da representação hierárquica dos espaços físicos em modelo de conjuntos encaixados (ver *Tabela 5* ou *Figura 7.7* da secção §7.4 “Modelo de Gestão de Dados Hierárquicos da Tabela “Espacos””, pág. 127) pode-se observar que os valores *lft* e *rgt* dos espaços físicos (nodos) *folha* são números consecutivos. Para

³⁸ Profundidade (ou altura) de uma árvore é o número máximo dos níveis hierárquicos dos seus nodos (por ex., a profundidade de uma árvore com um só nodo – nodo raiz – é zero, a profundidade de uma árvore com um nodo raiz e um nível hierárquico de nodos filho é igual a um, e assim sucessivamente).

se encontrar os espaços físicos *folha*³⁹ da árvore basta procurar os nodos onde $rgt = lft + 1$. Com a interrogação (*query*) que se segue, tem-se:

<i>Query</i>	<i>Saída (id_esp)</i>
<pre>"SELECT node.id_esp FROM espacos AS node WHERE node.rgt = node.lft + 1";</pre>	I – 006
	I – 010
	I – 014
	I – 104.1
	I – 109
	I – 119

7.4.1.3 Caminho Mais Simples até um Espaço Físico

No *Modelo de Conjuntos Encaixados (ou Diagramas de Venn)* pode-se também encontrar o caminho mais simples (mais directo, curto) até um determinado espaço físico ou nodo.

<i>Query</i>	<i>Saída (id_esp)</i>
<pre>"SELECT parent.id_esp FROM espacos AS node, espacos AS parent WHERE node.lft BETWEEN parent.lft AND parent.rgt AND node.id_esp = 'I-104.1' ORDER BY parent.lft";</pre>	Edifício I
	I – Piso 1
	I – 104
	I – 104.1

7.4.1.4 Profundidade (nível hierárquico) dos Espaços Físicos

Para se mostrar a *profundidade de cada espaço físico (nodo) na árvore*⁴⁰ ou hierarquia de espaços físicos, basta adicionar a função *COUNT* e a cláusula *GROUP BY* à *query* que representa a árvore total (ver secção §7.4.1.1 “Representação da Totalidade dos Espaços Físicos”, pág. 130). Com a interrogação (*query*) que se segue e tomando como base a tabela (ver *Tabela 5* ou *Figura 7.7* da secção §7.4 “Modelo de Gestão de Dados Hierárquicos da Tabela “Espaços””, pág. 127) vai-se identificar o nível de cada nodo na hierarquia de espaços físicos:

³⁹ Espaços físicos (nodos) da árvore de espaços que não têm filhos (espaços físicos encaixados ou contidos).

⁴⁰ Profundidade (ou altura) de um nodo numa árvore corresponde ao nível hierárquico, em relação ao nodo raiz, da sua posição na árvore (por ex., a profundidade do nodo raiz é zero, a profundidade dos nodos filho do nodo raiz é igual a um e, assim, sucessivamente).

<i>Query</i>	<i>Saída</i>	
	<i>id_esp</i>	<i>profundidade</i>
<pre>"SELECT node.id_esp, (COUNT(parent.id_esp)- 1) AS profundidade FROM espacos AS node, espacos AS parent WHERE node.lft BETWEEN parent.lft AND parent.rgt GROUP BY node.id_esp ORDER BY node.lft";</pre>	Edifício I	0
	I – Piso 0	1
	I – 006	2
	I – 010	2
	I – 014	2
	I – Piso 1	1
	I – 104	2
	I – 104.1	3
	I – 109	2
	I – 119	2

7.4.1.5 Representação Hierárquica Indentada dos Espaços Físicos

Através das funções *string CONCAT*, *REPEAT* e do valor da profundidade dos nodos pode-se indentar (com *espaços em branco*) a identificação dos espaços físicos e, assim, visualizar-se a hierarquia.

<i>Query</i>	<i>Saída (id_esp)</i>
<pre>"SELECT CONCAT(REPEAT(' ',COUNT(parent.id_esp)- 1),node.id_esp) AS id_esp FROM espacos AS node, espacos AS parent WHERE node.lft BETWEEN parent.lft AND parent.rgt GROUP BY node.id_esp ORDER BY node.lft";</pre>	Edifício I
	I – Piso 0
	I – 006
	I – 010
	I – 014
	I – Piso 1
	I – 104
	I – 104.1
	I – 109
	I – 119

Como utilizado na edição de espaços físicos da aplicação *WebGPACS*, substituiu-se a indentação anterior pela colocação de pontos (.), através da interrogação (*query*) seguinte:

<i>Query</i>
<pre>"SELECT CONCAT(REPEAT('.',COUNT(parent.id_esp)-1),node.id_esp) AS id_esp, node.desc_esp, node.lft, node.rgt, node.tipo_esp, node.coordgeo_esp FROM espacos AS node, espacos AS parent WHERE node.lft BETWEEN parent.lft AND parent.rgt GROUP BY node.id_esp ORDER BY node.lft";</pre>

Saída



Figura 7.8 – Visualização da indentação da identificação dos espaços físicos na página de edição de espaços físicos da aplicação WebGPACS

Identificação	Descrição	Tipo	Localização
Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP
.I-Piso0	Piso 0 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia
..I-006	Laboratório - Controlo e Automação	Laboratório	Piso 0
..I-010	Laboratório - Electrónica e Instrumentação	Laboratório	Piso 0
..I-014	Gabinete - Director do MEEC	Gabinete	Piso 0
.I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia
..I-104	Laboratório - Automação e Informática Industrial	Laboratório	Piso 1
...I-104.1	Armário no Laboratório de Automação e Informática	Armário	Laboratório - Automação e Informática Industrial
..I-109	Gabinete do Prof. Adriano Carvalho	Gabinete	Piso 1
..I-119	Gabinete - Técnicos Automação e Energia	Gabinete	Piso 1

Figura 7.9 – Visualização mais aproximada da indentação da identificação dos espaços físicos de parte da página de edição de espaços físicos da aplicação WebGPACS

Identificação	Descrição	lft	rgt	Tipo
Edifício-I	Edifício de Electrotecnia	1	20	Edifício
.I-Piso0	Piso 0 - Edifício de Electrotecnia	2	9	Piso
..I-006	Laboratório - Controlo e Automação	3	4	Laboratório
..I-010	Laboratório - Electrónica e Instrumentação	5	6	Laboratório
..I-014	Gabinete - Director do MEEC	7	8	Gabinete
.I-Piso1	Piso 1 - Edifício de Electrotecnia	10	19	Piso
..I-104	Laboratório - Automação e Informática Industrial	11	14	Laboratório
...I-104.1	Armário no Laboratório de Automação e Informática	12	13	Armário
..I-109	Gabinete do Prof. Adriano Carvalho	15	16	Gabinete
..I-119	Gabinete - Técnicos Automação e Energia	17	18	Gabinete

Figura 7.10 – Visualização da indentação da identificação dos espaços físicos, com discriminação dos valores de “lft” e “rgt”, de parte duma página da aplicação WebGPACS

7.4.1.6 Adição Hierárquica de Espaços Físicos

Tomando como base a tabela e a figura de representação hierárquica dos espaços físicos (ver *Tabela 5* e *Figura 7.6* da secção §7.4 “Modelo de Gestão de Dados Hierárquicos da Tabela “Espaços””, pág. 127), ao adicionar-se um novo espaço físico, por exemplo, uma escadaria entre os espaços físicos *I – Piso 0* e *I – Piso 1*, esse novo nodo deve ficar com os valores de *lft* = 10 e de *rgt* = 11, assim como, todos os valores de *lft* e de *rgt* dos nodos à sua direita incrementados de 2, conforme exemplificado na *Figura 7.11* e interrogações (*queries*) que se seguem.

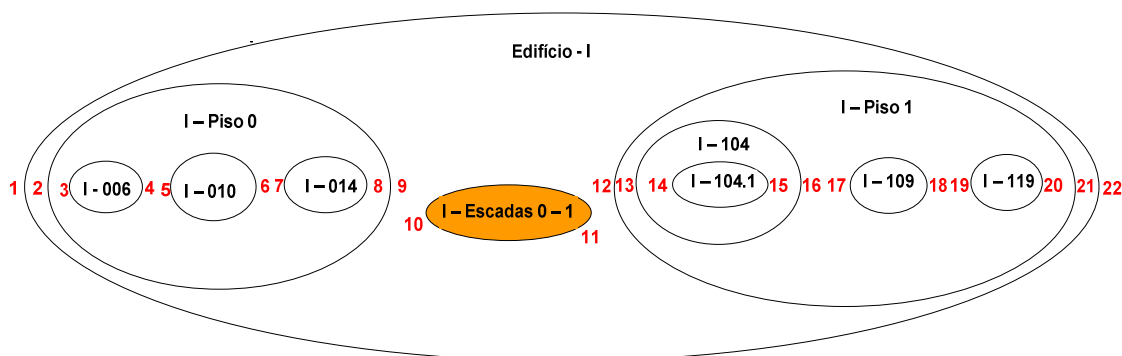


Figura 7.11 – Representação hierárquica dos espaços físicos no modelo de conjuntos encaixados depois de inserido o novo espaço *I – Escadas 0 – 1*, com discriminação dos valores *lft* e *rgt* de cada espaço físico (ou nodo hierárquico)

Queries

```
"SELECT @myRight := rgt FROM espacos
WHERE id_esp = 'I-Piso 0';

"UPDATE espacos SET rgt = rgt+2 WHERE rgt > @myRight;

"UPDATE espacos SET lft = lft+2 WHERE lft > @myRight;

"INSERT INTO espacos(id_esp, lft, rgt)
VALUES('I-Escadas 0-1', @myRight+1, @myRight+2);
```

Utilizando a interrogação (*query*) da representação da árvore indentada (da secção §7.4.1.5 “Representação Hierárquica Indentada dos Espaços Físicos”, pág. 132) seguinte, ter-se-ia:

Query

```
"SELECT CONCAT(REPEAT(' ', COUNT(parent.id_esp)-1), node.id_esp) AS id_esp
FROM espacos As node,
     espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

Saída

Antes (<i>id_esp</i>)		Depois (<i>id_esp</i>)
Edifício I		Edifício I
I – Piso 0		I – Piso 0
I – 006		I – 006
I – 010		I – 010
I – 014		I – 014
I – Piso 1	=>	I – Escadas 0 – 1
I – 104		I – Piso 1
I – 104.1		I – 104
I – 109		I – 104.1
I – 119		I – 109
		I – 119

Mas, opcionalmente, em substituição do exemplo anterior (adição do espaço *I – Escadas 0 – 1* entre os nodos *I – Piso 0* e *I – Piso 1*) vai-se adicionar um espaço físico, como filho de um que não tem filhos (nodo folha), por exemplo, um novo espaço físico *I – 119.1* ao espaço *I – 119*. Para esta operação de adição precisar-se-á de modificar ligeiramente as anteriores *queries* de adição, sendo substituídas pelas seguintes:

Queries

```
"SELECT @myLeft := lft FROM espacos
WHERE id_esp = 'I-119';";

"UPDATE espacos SET rgt = rgt+2 WHERE rgt > @myLeft;";

"UPDATE espacos SET lft = lft+2 WHERE lft > @myLeft;";

"INSERT INTO espacos(id_esp, lft, rgt)
VALUES('I-119.1', @myLeft+1, @myLeft+2);";
```

Neste exemplo, como se pode observar na *Figura 7.12* seguinte, vai-se expandir todos os valores à direita do valor do lado esquerdo (*lft*) do nodo pai, colocando-se de seguida o novo nodo filho à direita desse valor (do lado esquerdo (*lft*) do nodo pai).

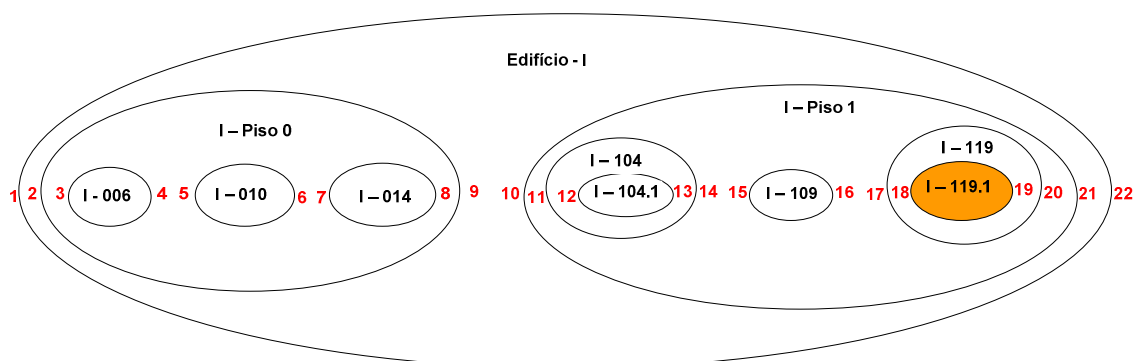


Figura 7.12 – Representação hierárquica dos espaços físicos no modelo de conjuntos encaixados depois de inserido o novo espaço físico I-119.1, com discriminação dos valores lft e rgt de cada espaço físico (ou nodo hierárquico)

Através da “query” da representação da árvore indentada seguinte, tem-se:

Query

```
"SELECT CONCAT(REPEAT(' ',COUNT(parent.id_esp)-1),node.id_esp) AS id_esp
FROM espacos AS node,
     espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

Saída

Antes (<i>id_esp</i>)		Depois (<i>id_esp</i>)
Edificio I		Edificio I
I – Piso 0		I – Piso 0
I – 006		I – 006
I – 010		I – 010
I – 014		I – 014
I – Piso 1	=>	I – Piso 1
I – 104		I – 104
I – 104.1		I – 104.1
I – 109		I – 109
I – 119		I – 119
		I – 119.1

Em substituição da indentação anterior, colocando-se pontos (.), como utilizado na edição de espaços físicos da aplicação *WebGPACS*, tem-se:

Query

```
"SELECT CONCAT(REPEAT('.',COUNT(parent.id_esp)-1),node.id_esp) AS id_esp,
              node.desc_esp, node.lft, node.rgt, node.tipo_esp, node.coordgeo_esp
FROM espacos AS node,
     espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

Saída

Figura 7.13 – Visualização da identificação dos espaços físicos, depois de inserido o novo espaço físico I-119.1

Identificação	Descrição	Tipo	Localização
Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP
.I-Piso0	Piso 0 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia
.I-006	Laboratório - Controlo e Automação	Laboratório	Piso 0
.I-010	Laboratório - Electrónica e Instrumentação	Laboratório	Piso 0
.I-014	Gabinete - Director do MEEC	Gabinete	Piso 0
.I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia
.I-104	Laboratório - Automação e Informática Industrial	Laboratório	Piso 1
.I-104.1	Armário no Laboratório de Automação e Informática	Armário	Laboratório - Automação e Informática Industrial
.I-109	Gabinete do Prof. Adriano Carvalho	Gabinete	Piso 1
.I-119	Gabinete - Técnicos Automação e Energia	Gabinete	Piso 1
.I-119.1	Armário (Gab. de Técnicos de Automação e Energia)	Armário	Gabinete - Técnicos de Automação e Energia

Figura 7.14 – Visualização mais aproximada da identificação dos espaços físicos, depois de inserido o novo espaço físico I-119.1

Identificação	Descrição	lft	rgt	Tipo
Edifício-I	Edifício de Electrotecnia	1	22	Edifício
.I-Piso0	Piso 0 - Edifício de Electrotecnia	2	9	Piso
.I-006	Laboratório - Controlo e Automação	3	4	Laboratório
.I-010	Laboratório - Electrónica e Instrumentação	5	6	Laboratório
.I-014	Gabinete - Director do MEEC	7	8	Gabinete
.I-Piso1	Piso 1 - Edifício de Electrotecnia	10	21	Piso
.I-104	Laboratório - Automação e Informática Industrial	11	14	Laboratório
.I-104.1	Armário no Laboratório de Automação e Informática	12	13	Armário
.I-109	Gabinete do Prof. Adriano Carvalho	15	16	Gabinete
.I-119	Gabinete - Técnicos Automação e Energia	17	20	Gabinete
.I-119.1	Armário (Gab. de Técnicos de Automação e Energia)	18	19	Armário

Figura 7.15 – Visualização da identificação dos espaços físicos depois de inserido o novo espaço físico I-119.1, com discriminação dos valores de “lft” e “rgt”

7.4.1.7 Eliminação Hierárquica de Espaços Físicos

A acção a empreender quando se pretende eliminar um espaço físico (nodo) depende da sua posição na hierarquia. A remoção de espaços físicos (nodos) folha é mais fácil do que a eliminação de espaços físicos pai (espaços físicos com filhos) porque, neste caso, poderá ser necessário “tratar” dos espaços físicos filho (“órfãos”) do espaço a ser removido [15].

Quando se pretende remover um espaço físico folha, por exemplo, a eliminação do espaço *I – 104.1*, o processo caracteriza-se por ser justamente o oposto da adição dum novo nodo, bastando eliminar o espaço físico em questão e efectuar o decremento de 2 a todos os valores de *lft* e de *rgt* dos espaços físicos (nodos) à sua direita, conforme as interrogações (*queries*) que se seguem:

Queries

```
"SELECT @myLeft := lft, @myRight := rgt, @myWidth := rgt-lft+1
FROM espacos
WHERE id_esp = 'I-104.1';";

"DELETE FROM espacos WHERE lft BETWEEN @myLeft AND @myRight;";

"UPDATE espacos SET rgt = rgt-@myWidth WHERE rgt > @myRight;";

"UPDATE espacos SET lft = lft-@myWidth WHERE lft > @myRight;";
```

Confirmando que o espaço físico foi removido sem corromper a hierarquia e utilizando-se a *query* da representação da árvore indentada, tem-se:

Query

```
"SELECT CONCAT(REPEAT(' ', COUNT(parent.id_esp)-1), node.id_esp) AS id_esp
FROM espacos AS node,
     espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

Saída

Antes (<i>id_esp</i>)		Depois (<i>id_esp</i>)
Edifício I		Edifício I
I – Piso 0		I – Piso 0
I – 006		I – 006
I – 010		I – 010
I – 014		I – 014
I – Piso 1		I – Piso 1
I – 104	=>	I – 104
I – 104.1		I – 109
I – 109		I – 119
I – 119		I – 119.1
I – 119.1		

A mesma expressão que serve para remover um espaço físico folha, funciona, igualmente bem, na remoção dum espaço físico e de todos os seus (nodos) filhos. Este tipo de remoção é o utilizado para os espaços físicos da aplicação *WebGPACS*, pois não faz sentido eliminar-se um determinado espaço físico controlado pelo sistema e permanecerem os espaços físicos que eram seus filhos. No exemplo subsequente, através das interrogações (*queries*) que se seguem, ver-se-á que ao eliminar-se o espaço físico *I – 119*, será correspondentemente eliminado o espaço físico seu filho *I – 119.1*.

Queries

```
"SELECT @myLeft := lft, @myRight := rgt, @myWidth := rgt-lft+1
FROM espacos
WHERE id_esp = 'I-119';";

"DELETE FROM espacos WHERE lft BETWEEN @myLeft AND @myRight;";

"UPDATE espacos SET rgt = rgt-@myWidth WHERE rgt > @myRight;";

"UPDATE espacos SET lft = lft-@myWidth WHERE lft > @myRight;";
```

Ao executar-se a interrogação (*query*) da representação da árvore indentada, abaixo, confirma-se que será removido o espaço físico (nodo) e a sua sub-árvore composta pelos espaços físicos (nodos) filho que, neste caso, em concreto, é constituída apenas por um único nodo, o espaço físico *I – 119.1*, mas poderiam ser múltiplos os espaços físicos filho a serem removidos.

Query

```
"SELECT CONCAT(REPEAT(' ', COUNT(parent.id_esp)-1), node.id_esp) AS id_esp
FROM espacos AS node,
     espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

Saída

Antes (<i>id_esp</i>)		Depois (<i>id_esp</i>)
Edifício I		Edifício I
I – Piso 0		I – Piso 0
I – 006		I – 006
I – 010		I – 010
I – 014		I – 014
I – Piso 1		I – Piso 1
I – 104		I – 104
I – 109		I – 109
I – 119	=>	
I – 119.1		

Em substituição da indentação anterior, colocando-se pontos (.), como utilizado na edição de espaços físicos da aplicação *WebGPACS*, tem-se:

Query

```
"SELECT CONCAT(REPEAT(' ',COUNT(parent.id_esp)-1),node.id_esp) AS id_esp,
      node.desc_esp, node.lft, node.rgt, node.tipo_esp, node.coordgeo_esp
FROM espacos AS node,
     espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

Saída



Figura 7.16 – Visualização da identificação dos espaços físicos, depois de eliminados o espaço físico I-119 e a sub-árvore de espaços físicos filho (neste caso, constituída apenas pelo espaço físico I-119.1)

Identificação	Descrição	Tipo	Localização
Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP
.I-Piso0	Piso 0 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia
..I-006	Laboratório - Controlo e Automação	Laboratório	Piso 0
..I-010	Laboratório - Electrónica e Instrumentação	Laboratório	Piso 0
..I-014	Gabinete - Director do MEEC	Gabinete	Piso 0
.I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia
..I-104	Laboratório - Automação e Informática Industrial	Laboratório	Piso 1
..I-109	Gabinete do Prof. Adriano Carvalho	Gabinete	Piso 1

Figura 7.17 – Visualização mais aproximada da identificação dos espaços físicos, depois de eliminados o espaço físico I-119 e a sub-árvore de espaços físicos filho (neste caso, constituída apenas pelo espaço físico I-119.1)

Identificação	Descrição	lft	rgt	Tipo
Edifício-I	Edifício de Electrotecnia	1	16	Edifício
.I-Piso0	Piso 0 - Edifício de Electrotecnia	2	9	Piso
..I-006	Laboratório - Controlo e Automação	3	4	Laboratório
..I-010	Laboratório - Electrónica e Instrumentação	5	6	Laboratório
..I-014	Gabinete - Director do MEEC	7	8	Gabinete
.I-Piso1	Piso 1 - Edifício de Electrotecnia	10	15	Piso
..I-104	Laboratório - Automação e Informática Industrial	11	12	Laboratório
..I-109	Gabinete do Prof. Adriano Carvalho	13	14	Gabinete

Figura 7.18 – Visualização da identificação dos espaços físicos, com discriminação dos valores de “lft” e “rgt”, depois de eliminados o espaço físico I-119 e a sub-árvore de espaços físicos filho (neste caso, constituída apenas pelo espaço físico I-119.1)

7.4.1.8 Outros

Existem muitas outras *expressões em SQL avançado*, para além das anteriormente apresentadas, que poderão ser utilizadas para gerir e lidar com a hierarquia de dados no *Modelo de Conjuntos Encaixados (ou Diagramas de Venn)*, entre outras, “*determinar a profundidade dos espaços físicos filho da sub-árvore dum determinado espaço físico*”, “*encontrar os espaços físicos filho imediatos dum determinado espaço físico*”, “*agregar funções em conjuntos de espaços físicos encaixados*”,... [15] Todas estas expressões, poder-se-ão justificar em desenvolvimentos posteriores e mais avançados deste projecto, não se inserindo, por agora, no âmbito da presente aplicação.

7.4.2 Interrogações da Aplicação sobre a Tabela “Espaços”

Apresentam-se, nesta secção, as interrogações da aplicação *WebGPACS* que lidam, apenas, com a tabela de *espaços* (dados hierárquicos) da base de dados (podem ser consultadas no “Anexo D – Interrogações à Base de Dados”, pág. 231, as restantes interrogações à base de dados da aplicação) (ver também “Anexo C – Listagem Parcial do Código da Aplicação”⁴¹, pág. 197).

7.4.2.1 Editar Espaços

Criar / Inserir Espaço

1ª FORMA:

```
$lft = '1';
$rgt = '2';
"INSERT INTO espacos(id_esp, desc_esp, lft, rgt, tipo_esp, coordgeo_esp,
                    estado_esp, presencas_esp, numunid_esp)
VALUES('$Identificacao','$Descricao','$lft','$rgt','$Tipo','$Coordenadas_geo',
      '$Estado','$Presencas','$Num_unidades');" ;
```

2ª FORMA:

```
"SELECT @myLeft := lft
FROM espacos
WHERE id_esp = '$Identificacao_espaco_referencia'";

"UPDATE espacos SET rgt = rgt+2
WHERE rgt > @myLeft;";

"UPDATE espacos SET lft = lft+2
WHERE lft > @myLeft;";

"INSERT INTO espacos(id_esp, desc_esp, lft, rgt, tipo_esp, coordgeo_esp,
                    estado_esp, presencas_esp, numunid_esp)
VALUES('$Identificacao','$Descricao',@myLeft+1,@myLeft+2,'$Tipo',
      '$Coordenadas_geo','$Estado','$Presencas','$Num_unidades');" ;
```

⁴¹ Listagem do código correspondente às funcionalidades de *Edição (hierárquica) de Espaços (inserção, modificação e remoção de espaços físicos)* e de *Auditar Acessos a um Espaço por Utilizador*.

Modificar Espaço

```
"UPDATE espacos SET id_esp = '$identificacao', desc_esp = '$descricao',
    tipo_esp = '$tipo', coordgeo_esp = '$coordenadas_geo',
    estado_esp = '$estado', presencas_esp = '$presencas',
    numunid_esp = '$num_unidades'
WHERE id_esp = '$identificacao_original';";
```

Eliminar Espaço e todos os seus Descendentes

```
"SELECT @myLeft := lft, @myRight := rgt, @myWidth := rgt-lft+1
FROM espacos
WHERE id_esp = '$Identificacao_espaco';";

/* Nota: Gera o espaço a eliminar e todos os seus descendentes (espaços
filho)*/
"SELECT * FROM espacos
WHERE lft BETWEEN @myLeft AND @myRight
ORDER BY espacos.lft;";

"DELETE FROM espacos WHERE lft BETWEEN @myLeft AND @myRight;";

"UPDATE espacos SET rgt = rgt-@myWidth WHERE rgt > @myRight;";

"UPDATE espacos SET lft = lft-@myWidth WHERE lft > @myRight;";
```

7.4.2.2 Consultar Espaços

Consultar / Pesquisar Espaço

1ª FORMA:

```
"SELECT * FROM espacos WHERE id_esp = '$Identificacao_espaco';";
```

2ª FORMA:

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
    espacos.coordgeo_esp, espacos.lft
FROM espacos
WHERE id_esp = '$Identificacao_espaco';";
```

Consultar Espaços

```
"SELECT node.id_esp, CONCAT(REPEAT('.', COUNT(parent.id_esp)-1), node.id_esp) AS
    id_esp, node.desc_esp, node.lft, node.rgt, node.tipo_esp,
    node.coordgeo_esp
FROM espacos AS node,
    espacos AS parent
WHERE node.lft BETWEEN parent.lft AND parent.rgt
GROUP BY node.id_esp
ORDER BY node.lft";
```

7.4.2.3 Consultar Caminho mais simples até um Espaço

Consultar Caminho mais simples até um Espaço

```
"SELECT parent.id_esp
FROM espacos AS node,
    espacos AS parent
```

```
WHERE node.lft BETWEEN parent.lft AND parent.rgt
      AND node.id_esp = '$Identificacao_espaco'
ORDER BY parent.lft;";
      AND id_papel = '$Identificacao_papel';";
```

7.4.2.4 Consultar Permissões (a Espaços) do Papel

Consultar Permissões (a Espaços) do Papel

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
      espacos.coordgeo_esp, espacos.lft, permissoes.tipoacesso_perm,
      permissoes.datainicio_perm, permissoes.horainicio_perm,
      permissoes.horafim_perm, permissoes.datafim_perm
FROM espacos, permissoes
WHERE permissoes.id_papel = '$Identificacao_papel'
      AND permissoes.id_esp = espacos.id_esp
ORDER BY espacos.lft;";
```

7.4.2.5 Consultar Espaços (disponíveis) para Permissões do Papel

Consultar Espaços (disponíveis) para Permissões do Papel

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
      espacos.coordgeo_esp, espacos.lft
FROM espacos
WHERE espacos.id_esp NOT IN (SELECT espacos.id_esp
      FROM espacos, permissoes
      WHERE permissoes.id_papel = '$Identificacao_papel'
            AND permissoes.id_esp = espacos.id_esp)
ORDER BY espacos.lft;";
```

7.4.2.6 Consultar Permissões (a Espaços) de Utilizadores

Ordenar pela Hierarquia de Espaços

```
"SELECT DISTINCT espacos.id_esp, espacos.desc_esp, espacos.lft, espacos.rgt,
      espacos.tipo_esp, espacos.coordgeo_esp
FROM papeis_utilizadores, papeis, permissoes, espacos
WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
      AND papeis_utilizadores.id_papel = papeis.id_papel
      AND papeis.id_papel = permissoes.id_papel
      AND permissoes.id_esp = espacos.id_esp
ORDER BY espacos.lft;";
```

Ordenar por Descrição do Espaço

```
"SELECT DISTINCT espacos.id_esp, espacos.desc_esp, espacos.lft, espacos.rgt,
      espacos.tipo_esp, espacos.coordgeo_esp
FROM papeis_utilizadores, papeis, permissoes, espacos
WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
      AND papeis_utilizadores.id_papel = papeis.id_papel
      AND papeis.id_papel = permissoes.id_papel
      AND permissoes.id_esp = espacos.id_esp
ORDER BY espacos.desc_esp;";
```

Ordenar por Tipo de Espaço

```
"SELECT DISTINCT espacos.id_esp, espacos.desc_esp, espacos.lft, espacos.rgt,
                  espacos.tipo_esp, espacos.coordgeo_esp
FROM papeis_utilizadores, papeis, permissoes, espacos
WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
      AND papeis_utilizadores.id_papel = papeis.id_papel
      AND papeis.id_papel = permissoes.id_papel
      AND permissoes.id_esp = espacos.id_esp
ORDER BY espacos.tipo_esp;"
```

Ordenar por Localização do Espaço

```
"SELECT DISTINCT espacos.id_esp, espacos.desc_esp, espacos.lft, espacos.rgt,
                  espacos.tipo_esp, espacos.coordgeo_esp
FROM papeis_utilizadores, papeis, permissoes, espacos
WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
      AND papeis_utilizadores.id_papel = papeis.id_papel
      AND papeis.id_papel = permissoes.id_papel
      AND permissoes.id_esp = espacos.id_esp
ORDER BY espacos.coordgeo_esp;"
```

7.4.2.7 Auditar Acessos de Utilizadores

Ordenar por Identificação do Espaço e Data/Hora do Acesso

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.coordgeo_esp,
        espacos.tipo_esp, log_acessos.direc_acesso, log_acessos.data_acesso,
        log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY espacos.id_esp, log_acessos.data_acesso, log_acessos.hora_acesso;"
```

Ordenar por Descrição do Espaço e Data/Hora do Acesso

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.coordgeo_esp,
        espacos.tipo_esp, log_acessos.direc_acesso, log_acessos.data_acesso,
        log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY espacos.desc_esp, log_acessos.data_acesso,
        log_acessos.hora_acesso;"
```

Ordenar por Data/Hora do Acesso

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.coordgeo_esp,
        espacos.tipo_esp, log_acessos.direc_acesso, log_acessos.data_acesso,
        log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'";
```

7.4.2.8 Auditar Acessos por Utilizador a um Espaço

Ordenar por Identificação do Espaço e Data/Hora do Acesso

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
        espacos.coordgeo_esp, log_acessos.direc_acesso,
        log_acessos.data_acesso, log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY espacos.id_esp, log_acessos.data_acesso, log_acessos.hora_acesso;"
```

Ordenar por Descrição do Espaço e Data/Hora do Acesso

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
        espacos.coordgeo_esp, log_acessos.direc_acesso,
        log_acessos.data_acesso, log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY espacos.desc_esp, log_acessos.data_acesso,
        log_acessos.hora_acesso;"
```

Ordenar por Data/Hora do Acesso

```
"SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
        espacos.coordgeo_esp, log_acessos.direc_acesso,
        log_acessos.data_acesso, log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'";
```


Capítulo 8

Caso de Estudo

8.1 Introdução

Neste capítulo é apresentado um caso de estudo, com base num cenário de gestão de controlo de acessos num *campus* universitário, para validação de resultados de utilização da aplicação *WebGPACS*, desenvolvida neste projecto. São descritas e exemplificadas algumas das suas principais formas de utilização, testadas e validadas funcionalidades de vários casos de utilização, demonstrados resultados e *interfaces* da aplicação.

8.2 Apresentação do Caso de Estudo e Pressupostos

O caso de estudo baseia-se no cenário retratado numa secção anterior (ver cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65), em que se assume que o espaço físico *I-104* (laboratório de automação e informática industrial) é um laboratório fechado, no qual, apenas, professores da área de “informática e automação” e alunos de mestrado e doutoramento a realizar trabalhos ou projectos nessa área de conhecimento, o podem aceder. Para tal, começa-se por criar um novo aluno na aplicação, para depois lhe ser atribuído o papel correspondente – “aluno de doutoramento em informática e automação” – já existente no sistema mas, ainda, sem permissões (a espaços físicos) atribuídas. Antes de ser atribuído o papel ao utilizador, será atribuída, ao papel referido, uma permissão de acesso para o *laboratório I-104* (laboratório de automação e informática industrial) para que, assim (em conformidade com o cenário 2 da secção §4.2 “A Gestão de Acessos (Físico) em Universidades”, pág. 65), seja permitido ao aluno aceder ao *laboratório I-104* e, aí, o aluno possa desenvolver os seus trabalhos de investigação. De seguida, exemplifica-se a modificação ou alteração dos dados dessa permissão de acesso, agora, já atribuída ao papel e, só depois, será atribuído este papel ao utilizador. Conclui-se, com a efectuação de um conjunto de casos simulados, referente a funcionalidades de auditoria de acessos (entre duas datas): um, para auditar os acessos do aluno referido, a espaços físicos controlados pelo sistema; outro, sobre acessos efectuados ao *laboratório I-104* por quaisquer utilizadores; um último, relativo a auditoria de acessos efectuados ao mesmo laboratório mas, somente, pelo aluno em questão.

Em resumo, o caso de estudo apresentado irá testar e validar as funcionalidades de alguns casos de utilização da aplicação, referentes ao Subsistema “Gestão de Controlo de Acessos” (incluídos nas várias subsecções da secção §5.2.3, pág. 92). Esses casos de uso são os seguintes:

- Criar ou Inserir Utilizador
- Criar ou Inserir Permissões a Papel
- Modificar Permissões do Papel
- Atribuir Papéis a Utilizadores
- Auditar Acessos de Utilizadores
- Auditar Acessos a Espaços
- Auditar Acessos a um Espaço por Utilizador

Pressupostos (do sistema)

Antes de executar o caso de estudo, devem-se verificar os seguintes pressupostos relativos ao sistema:

- O sistema deve estar instalado e configurado (ver secção §7.2 “Instalação e Configuração do Sistema”, pág. 123, para mais detalhes)
- Os serviços dos servidores *web* (*Apache*) e de base de dados (*MySQL*) devem ser iniciados e ficar *online* durante o tempo de execução
- O utilizador tem que se autenticar com o perfil de “Administrador” para entrar na secção privada da aplicação *WebGPACS* e poder utilizá-la.

8.3 Validação de Funcionalidades da Aplicação

Esta secção, com base no caso de estudo anteriormente apresentado, irá validar as funcionalidades de alguns casos de utilização (mencionados na secção anterior) da aplicação. Contudo, refere-se que, somente, serão testados os caminhos ou os passos das funcionalidades necessários ao caso de estudo referido [21].

8.3.1 Criar ou Inserir um Utilizador

Para inserção de um novo utilizador na aplicação, o administrador solicita, através do menu *Editar Utilizadores*, a funcionalidade de edição de utilizadores que permitirá inserir um novo utilizador, modificar ou eliminar um já existente. Após selecção do botão referente à inserção de um novo utilizador e a introdução dos seus dados, o sistema cria, na tabela correspondente da base de dados, um novo utilizador com a informação indicada pelo administrador (ver secção §5.2.3.1 “Gestão de Utilizadores”, pág. 93).

Na inserção de um novo utilizador são executados os seguintes passos:

1. O administrador clica no *Menu Utilizadores* → *Editar Utilizadores*
2. A aplicação disponibiliza uma página *Editar Utilizadores* com uma lista de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...).
3. O administrador solicita a inserção de novos utilizadores, clicando no botão *Inserir*.
4. Uma nova página é mostrada para preenchimento dos atributos do novo utilizador.
5. O administrador insere os seguintes dados relativos ao novo utilizador:
 - Identificação: 3250wy46
 - Nome: Ricardo Nuno Moreira Freitas
 - Senha (password): hfdfdf4

Poderá apagar duma vez, através do botão *Cancelar*, todos os campos relativos aos dados do utilizador ou, clicando no botão *Submeter*, proceder à sua inserção.

Figura 8.1 – Página para inserção de dados do novo utilizador

6. O sistema valida o preenchimento de todos os campos relativos aos dados do utilizador e emite mensagens correspondentes a campos não completos.

Criar / Inserir Utilizador

Atributos	Dados do Utilizador
Identifi	Windows Internet Explorer
Nome	
Passw	

Deve preencher o campo Identificação !!!

Figura 8.2 – Mensagem relativa ao preenchimento dos campos de inserção

O sistema também efectua a validação da identificação do novo utilizador e, caso exista um com a mesma identificação no sistema, emite uma mensagem alertando da existência de um utilizador com essa identificação, não inserindo os dados.

Inserção de Utilizador

O Utilizador com a identificação **001623w** não pode ser inserido !!!

Identificação JÁ EXISTENTE

Figura 8.3 – Não inserção do utilizador, já existência da identificação do utilizador

Na inserção bem sucedida emite mensagem correspondente, com revelação dos dados do novo utilizador inserido.

Inserção de Utilizador

Utilizador inserido com Sucesso !!!

Identificação	Nome	Password
3250wy46	Ricardo Nuno Moreira Freitas	hfdfdf4

Figura 8.4 – Inserção bem sucedida, com revelação dos dados inseridos

8.3.2 Criar ou Inserir Permissões a Papel

Para inserção de uma permissão a um papel, o administrador solicita, através do menu *Editar Permissões de Papéis*, a edição de permissões (a espaços físicos) de papéis que permitirá inserir uma nova permissão, modificar ou eliminar uma já existente. O sistema possibilita que o actor pesquise e selecione um papel de uma lista de papéis, que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...). Para o papel seleccionado e a partir duma lista de espaços físicos apresentada, a que o papel não dá acesso, o actor selecciona o espaço físico pretendido e insere a informação (data e hora início/fim, condições,...) referente à nova permissão, atribuindo-a, de seguida, ao papel (ver secção §5.2.3.4 “Gestão de Permissões (a Espaços)”, pág. 103).

Na inserção de uma permissão a um papel são executados os seguintes passos:

1. O administrador clica no *Menu Permissões* → *Editar Permissões de Papéis*
2. A aplicação disponibiliza uma página *Editar Permissões de Papéis* com uma lista de papéis que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...).
3. O administrador selecciona o papel *AlunoDocDEEC_IA* (*alunos de doutoramento em informática e automação*), ao qual pretende atribuir a permissão, clicando no botão *Inserir* respectivo.
4. A aplicação disponibiliza uma página *Inserir Permissões a Papel* que contém a enumeração dos principais atributos do papel (identificação, descrição), uma lista das permissões a espaços físicos controlados e já atribuídas ao papel, outra correspondente aos espaços físicos existentes no sistema, mas sem permissão através do papel, e os campos necessários à inserção da informação (data e hora início/fim, condições,...) referente à nova permissão a atribuir.

Inserir Permissões a Papel

Identificação do Papel: **AlunoDocDEEC_IA**

Atributos do Papel: **AlunoDocDEEC_IA**
 Descrição: **Alunos de Doutoramento em Informática e Automação**

Permissões do Papel: **AlunoDocDEEC_IA**

NÃO EXISTEM

Permissões Disponíveis para o Papel: **AlunoDocDEEC_IA**

Opção	Identificação	Descrição	Tipo	Localização	
☐	Edificio-I	Edifício de Electrotecnia	Edificio	Campus da FEUP	Consultar
☐	I-Piso0	Piso 0 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	Consultar
☐	I-006	Laboratório - Controlo e automação	Laboratório	Piso 0	Consultar
☐	I-010	Laboratório - Electrónica e Instrumentação	Laboratório	Piso 0	Consultar
☐	I-014	Gabinete - Director do MEEC	Gabinete	Piso 0	Consultar
☐	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	Consultar
☐	I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	Consultar
☐	I-104.1	Armário no Laboratório de Automação e informática	Armário	Laboratório - Automação e informática industrial	Consultar
☐	I-109	Gabinete do Prof. Adriano Carvalho	Gabinete	Piso 1	Consultar
☐	I-119	Gabinete - Técnicos Automação e Energia	Gabinete	Piso 1	Consultar

Data e Hora Iniciais: Tipo e Condições do Acesso: Data e Hora Finais:

Figura 8.5 – Visualização parcial da página de inserção de permissões de acesso a um papel

5. O administrador ao pretender atribuir uma permissão de acesso para o espaço físico *I-104 (laboratório – automação e informática industrial)*, selecciona o botão correspondente a esse espaço físico, preenche alguns campos (entre os quais, datas de início e fim da permissão) relativos à informação da nova permissão e, de seguida, clica no botão *Inserir*.

Nota: a introdução das respectivas datas está facilitada por um calendário que pode ser despoletado pelo clicar dum simples botão, ao lado dos referentes campos de inserção.

6. Na inserção bem sucedida, o sistema não só emite uma mensagem que revela a identificação do papel, os dados da nova permissão ao espaço físico, como também, de imediato, mostra a nova permissão atribuída na lista de permissões do papel.

Nota importante: Se necessário, o sistema atribui automaticamente permissões de acesso a espaços físicos, hierarquicamente ascendentes, que conduzem ao espaço físico da nova permissão, mostrando-as também na lista de permissões do papel.

O sistema fica disponível para continuar com a inserção de novas permissões (a espaços físicos) ao papel.

Identificação do Papel: AlunoDocDEEC_IA

Atributos: AlunoDocDEEC_IA
Dados do Papel: Alunos de Doutoramento em Informática e Automação

Permissões do Papel: AlunoDocDEEC_IA

Identificação	Descrição	Tipo	Localização	Tipo de Acesso	Data Início	Hora Início	Hora Fim	Data Fim	
Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP						Consultar
I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia						Consultar
I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	Normal	01-07-2008	00:00:00	00:00:00	01-01-2009	Consultar

Permissões Disponíveis para o Papel: AlunoDocDEEC_IA

Opção	Identificação	Descrição	Tipo	Localização	
☐	I-Piso0	Piso 0 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	Consultar
☐	I-006	Laboratório - Controlo e automação	Laboratório	Piso 0	Consultar
☐	I-010	Laboratório - Electrónica e Instrumentação	Laboratório	Piso 0	Consultar
☐	I-014	Gabinete - Director do MEEC	Gabinete	Piso 0	Consultar
☐	I-104.1	Armário no Laboratório de Automação e informática	Armário	Laboratório - Automação e informática industrial	Consultar
☐	I-109	Gabinete do Prof. Adriano Carvalho	Gabinete	Piso 1	Consultar
☐	I-119	Gabinete - Técnicos Automação e Energia	Gabinete	Piso 1	Consultar

Data e Hora Iniciais: Data Início: Hora Início: Tipo e Condições do Acesso: Tipo de Acesso: Condições de Acesso: Data e Hora Finais: Data Fim: Hora Fim:

Figura 8.6 – Lista das permissões do papel, depois de atribuição automática de permissões de acesso a espaços físicos, hierarquicamente ascendentes, que conduzem ao espaço físico da nova permissão. Disponibilidade para continuação da inserção de novas permissões ao papel.

8.3.3 Modificar Permissões do Papel

Para alteração de uma permissão a um papel, o administrador, através do menu *Editar Permissões de Papéis*, solicita a edição de permissões (a espaços físicos) de papéis que permitirá inserir, modificar ou eliminar uma permissão já existente. O sistema

possibilita que o actor pesquise e selecione um papel de uma lista de papéis, que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...). Para o papel seleccionado e a partir duma lista de permissões (a espaços físicos) apresentada, cujo papel dá acesso, o actor selecciona a permissão a alterar e, de seguida, modifica a informação (data e hora início/fim, condições,...) referente à permissão que pretende alterar. Após confirmação, o sistema modifica os dados da permissão com a informação indicada pelo actor e mostra-a, de imediato, na lista de permissões de acesso (a espaços físicos) do papel em questão (ver secção §5.2.3.4 “Gestão de Permissões (a Espaços)”, pág. 103).

Para modificação duma permissão dum papel são executados os seguintes passos:

1. O administrador clica no *Menu Permissões → Editar Permissões de Papéis*
2. A aplicação disponibiliza uma página *Editar Permissões de Papéis* com uma lista de papéis, que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...).
3. O administrador selecciona o papel *AlunoDocDEEC_IA* (*alunos de doutoramento em informática e automação*), ao qual pretende modificar a permissão, clicando no botão *Alterar* respectivo.
4. A aplicação disponibiliza uma página *Modificar Permissões do Papel* que contém a enumeração dos principais atributos do papel (identificação, descrição) e uma lista das permissões a espaços físicos controlados já atribuídas ao papel.
5. O administrador selecciona a permissão ao espaço físico *I-104* (*laboratório – automação e informática industrial*) que pretende modificar, clicando no botão *Alterar* respectivo.



Figura 8.7 – Lista das permissões a espaços físicos já atribuídas ao papel *AlunoDocDEEC_IA* e selecção da permissão ao espaço físico *I-104* para alteração

6. A aplicação disponibiliza uma página *Modificar Permissão do Papel* que contém a enumeração dos principais atributos do papel (identificação, descrição), uma lista das permissões a espaços físicos controlados já atribuídas ao papel e destaca a permissão seleccionada a alterar, em que são mostrados os campos com os dados actuais dos atributos da permissão e que vão servir também para a introdução da informação ou dos novos dados da permissão.
7. O administrador preenche os campos a alterar relativos à informação da nova permissão, inclusive, podendo modificar as datas de início e fim da permissão, através dum calendário que é despoletado pelo clicar dum botão específico, ao lado dos correspondentes campos de inserção. De seguida, clica no botão *Submeter*.
- Neste caso, apenas, altera a *data fim da permissão para 31-07-2009*

WebGPACS - Aplicação Web de Gestão de Sistemas de Controlo de Acesso Físico - Windows Internet Explorer

http://localhost/Web_Tesev2/novo/permissoes_papeis/alterar/a_permissoes_papeis3.php?Identificacao1=I-104&Identificacao2=AlunoDocDEEC_IA

Utilizadores
Papeis
Espaços
Permissões
Acessos
Contactos
Logout

Identificação do Papel: AlunoDocDEEC_IA

Atributos
Identificação: AlunoDocDEEC_IA
Descrição: Alunos de Doutoramento em Informática e Automação

Dados do Papel

Permissões do Papel: AlunoDocDEEC_IA

Identificação	Descrição	Tipo	Localização	Tipo de Acesso	Data Início	Hora Início	Hora Fim	Data Fim	
Edificio-I	Edifício de Electrotecnia	Edifício	Campus da FEUP						Consultar
I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia						Consultar
I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	Normal	01-07-2008	00:00:00	00:00:00	01-01-2009	Consultar

ADMINISTRADOR

Alterar a Permissão ao Espaço com Identificação: I-104

Identificação	Descrição	Tipo	Localização
I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1

Consultar

Atributos	Dados actuais	Novos Dados
Data Início	01/07/2008	01/07/2008
Hora Início	00:00:00	00:00:00
Tipo de Acesso	Normal	Normal
Condições de Acesso	Normal	Normal
Hora Fim	00:00:00	00:00:00
Data Fim	01/01/2009	31/07/2009

Submeter

July, 2009

Today

Mon Tue Wed Thu Fri Sat Sun

27 1 2 3 4 5

28 6 7 8 9 10 11 12

29 13 14 15 16 17 18 19

30 20 21 22 23 24 25 26

31 27 28 29 30 31

Select date

Figura 8.8 – Visualização parcial da modificação da permissão de acesso ao espaço físico I-104 do papel AlunoDocDEEC_IA

8. O sistema efectua a validação do preenchimento dos diferentes campos da permissão, altera os dados na tabela correspondente da base de dados e avisa da alteração bem sucedida, com revelação dos dados da permissão alterada.

Modificação da Permissão do Papel

Permissão ao espaço físico I-104 do papel AlunoDocDEEC_IA

alterada com Sucesso !!!

Atributos	Novos Dados
Data Início	01/07/2008
Hora Início	00:00:00
Tipo de Acesso	Normal
Condições de Acesso	Normal
Hora Fim	00:00:00
Data Fim	31/07/2009

Voltar (Menu Anterior)

Figura 8.9 – Alteração bem sucedida, com revelação dos dados da permissão de acesso

O sistema volta à página *Modificar Permissões do Papel* onde, de imediato, inclui a permissão alterada na lista das permissões a espaços físicos controlados, já atribuídas ao papel, ficando disponível para continuar com a alteração de outras permissões do papel.

8.3.4 Atribuir Papéis a Utilizadores

Para atribuir um novo papel a um utilizador ou eliminar um que já lhe tenha sido atribuído, o administrador solicita a edição de papéis a utilizadores, através do menu *Editar Papéis a Utilizadores*. O sistema vai possibilitar que o administrador pesquise e selecione um utilizador de uma lista de utilizadores que lhe é apresentada, podendo ser ordenada por vários atributos do utilizador (número de identificação, nome,...). Para o utilizador seleccionado e a partir duma lista de papéis que não lhe estão atribuídos, o actor selecciona o novo papel pretendido e atribui-o, de seguida, ao utilizador (ver secção §5.2.3.1 “Gestão de Utilizadores”, pág. 93).

Na atribuição de um papel a um utilizador são executados os seguintes passos:

1. O administrador clica no *Menu Utilizadores* → *Editar Papéis a Utilizadores*
2. A aplicação disponibiliza uma página *Editar Papéis a Utilizadores* com uma lista de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...).
3. O administrador selecciona o utilizador (aluno com identificação: 3250wy46), ao qual pretende atribuir o papel, clicando no botão *Inserir* respectivo.
4. A aplicação disponibiliza uma página *Atribuir Papéis ao Utilizador* que contém a enumeração dos principais atributos do utilizador (identificação, nome, senha – *password*), uma lista de papéis já atribuídos ao utilizador e outra, correspondente a papéis existentes no sistema, mas que ainda não lhe foram atribuídos. Também é possível a consulta das permissões de cada papel listado, bastando para tal, clicar no botão *Consultar* respectivo.
5. O administrador pretende consultar as permissões relativas ao papel com a identificação *AlunoDocDEEC_IA* (*alunos de doutoramento em informática e automação*) e clica no botão *Consultar* referente a esse papel.

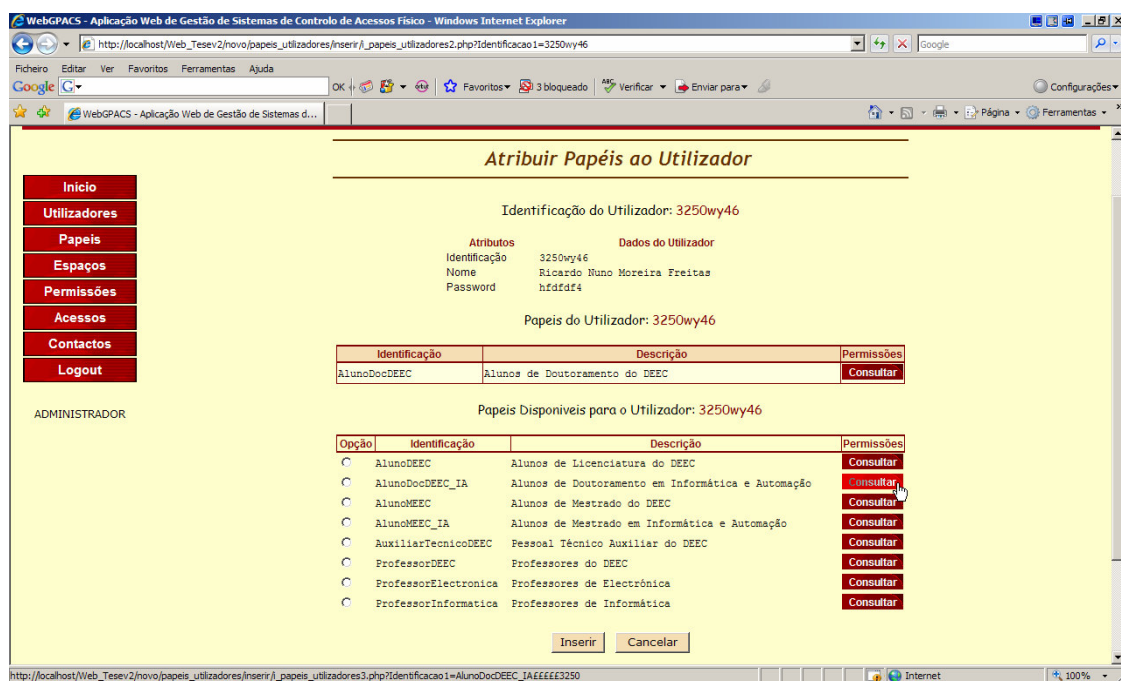


Figura 8.10 – Listas dos papéis já atribuídos ao utilizador e dos, existentes no sistema, que não lhe estão atribuídos, com selecção do papel AlunoDocDEEC_IA para consulta das suas permissões de acesso

- Uma nova página é mostrada com a enumeração dos atributos do papel (identificação, descrição) e uma lista discriminada das permissões a espaços físicos controlados, cujo papel dá acesso.



Figura 8.11 – Visualização das permissões de acesso (a espaços físicos) correspondentes ao papel

- O administrador volta à página anterior, *Atribuir Papéis ao Utilizador*, clicando no botão *Voltar (Menu Anterior)*.

8. O administrador selecciona o botão correspondente ao papel com a identificação *AlunoDocDEEC_IA* (alunos de doutoramento em informática e automação) e para o atribuir ao utilizador clica no botão *Inserir*.
9. O sistema avisa da inserção bem sucedida, emitindo uma mensagem que revela as identificações do utilizador e do papel atribuído. Também mostra, de imediato, o papel atribuído na lista de papéis do utilizador, ao mesmo tempo, ficando disponível para continuar com a atribuição de outros papéis ao utilizador.

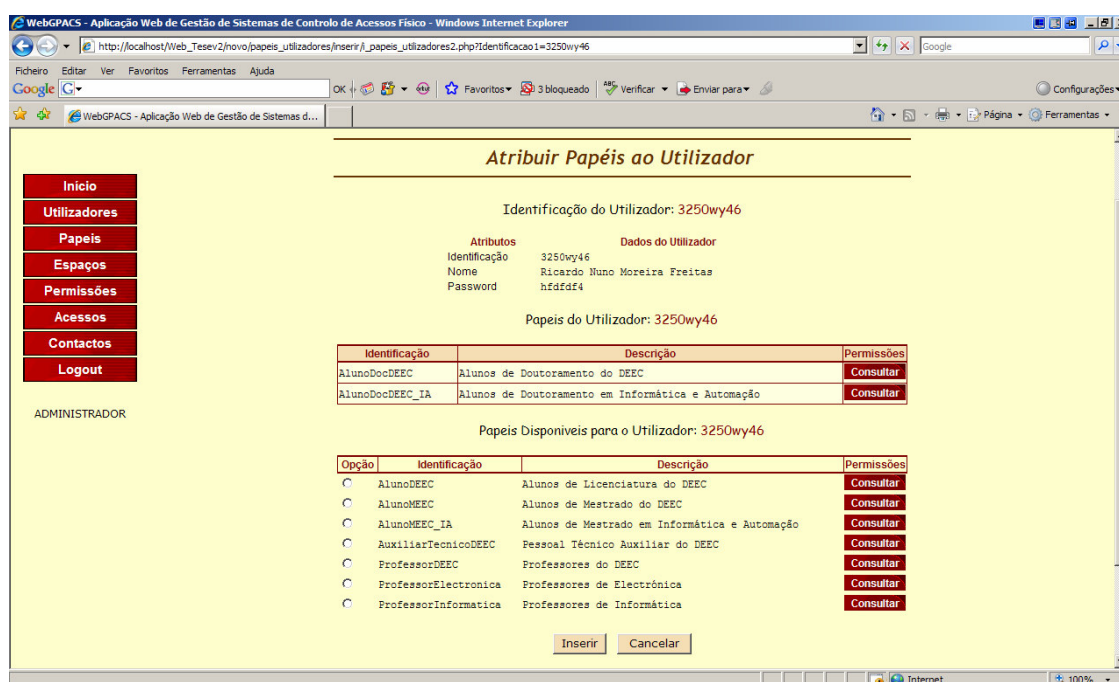


Figura 8.12 – O sistema mostra de imediato o novo papel atribuído ao utilizador na lista de papéis do utilizador e lista os papéis disponíveis, existentes no sistema

8.3.5 Auditar Acessos de Utilizadores

O actor, através do menu *Auditar Acessos de Utilizadores*, solicita a auditoria de acessos de utilizadores. O sistema possibilita que o actor pesquise e selecciona um utilizador de uma lista de utilizadores que lhe é apresentada, podendo ser ordenada por vários atributos do utilizador (número de identificação, nome,...). Para o utilizador seleccionado e depois de assinaladas duas datas (início e fim) de pesquisa, o sistema vai disponibilizar ao actor uma listagem dos acessos aos espaços físicos (com direcção do acesso – entrada ou saída, vários elementos de identificação do espaço físico, data e hora do acesso,...) efectuados pelo utilizador, entre as datas assinaladas (ver secção §5.2.3.5 “Auditar/Pesquisar Acessos e Presenças”, pág. 104 e Anexo “B.4 – Auditar/Pesquisar Acessos e Presenças”, pág. 193).

Para auditar os acessos dum utilizador são executados os seguintes passos:

1. O administrador clica no *Menu Acessos* → *Auditar Acessos de Utilizadores*



Figura 8.13 –Menu da aplicação WebGPACS, *Acessos* → *Auditar Acessos de Utilizadores*

2. A aplicação disponibiliza uma página *Auditar Acessos de Utilizadores* com uma lista de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...).
 3. O administrador selecciona o utilizador pretendido, a ser auditado, clicando no botão *Consultar* respectivo.
- Consultar acessos do utilizador (aluno): *Ricardo Nuno Moreira Freitas*



Figura 8.14 – Página *Auditar Acessos de Utilizadores* com selecção do utilizador a auditar

4. Uma nova página é mostrada, contendo a enumeração dos principais atributos do utilizador (identificação, nome) e dois campos para inserção de duas datas (início e fim) de parametrização de pesquisa dos acessos do utilizador.



Figura 8.15 – Página de inserção das datas de início e fim, para parametrização da pesquisa de acessos

5. O administrador, através dum calendário que é despoletado pelo clicar dum botão específico, ao lado de cada campo de inserção, facilmente insere as datas de parametrização de pesquisa dos acessos e, em seguida, clica no botão *Submeter*.
- Data Início: 10/07/2008 e Data Fim: 11/07/2008



Figura 8.16 – Inserção de datas, pelo despoletar dum calendário ao lado de cada campo de inserção

Acessos do Utilizador 3250wy46 entre duas Datas (Assinale as Datas !)

... ...

Aplicação realizada por Pedro Moreira no âmbito do:

Figura 8.17 – Visualização parcial e aproximada da inserção de datas

6. A aplicação disponibiliza uma nova página com a listagem dos acessos do utilizador, entre as datas assinaladas. Na listagem são mencionados: a direcção dos acessos (entrada ou saída); a identificação, a descrição, o tipo e a localização do espaço acedido; a data e hora do acesso.

A listagem dos acessos do utilizador pode ser ordenada ascendentemente por:

- data/hora dos acessos (ordenação por defeito)
- identificação do espaço e data/hora do acesso
- descrição do espaço e data/hora do acesso

WebGPACS - Aplicação Web de Gestão de Sistemas de Controlo de Acessos Físico - Windows Internet Explorer

http://localhost/Web_Tesev2/novo/acessos_utilizadores/listar/c_acessos_utilizadores2.php

WebGPACS (Aplicação Web de Gestão de Sistemas de Controlo de Acessos Físico)

Universidade do Porto
FEUP Faculdade de Engenharia

Acessos do Utilizador

Identificação do Utilizador: 3250wy46

Atributos: 3250wy46
Dados do Utilizador: Ricardo Nuno Moreira Freitas

Acessos do Utilizador 3250wy46 entre as Datas: 10/07/2008 e 11/07/2008

Direcção	Id. do Espaço	Descrição de Espaço	Tipo	Localização	Data do Acesso	Hora do Acesso
in	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	10-07-2008	14:20:02
out	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	10-07-2008	17:30:22
in	Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP	11-07-2008	08:08:10
in	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	11-07-2008	08:10:04
in	I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	11-07-2008	08:11:04
out	I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	11-07-2008	09:34:00
out	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	11-07-2008	09:35:40
out	Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP	11-07-2008	09:37:55

Aplicação realizada por Pedro Moreira no âmbito do:

Mestrado em Engenharia Electrotécnica e de Computadores // Especialização em Tecnologias de Informação para Gestão Empresarial

Figura 8.18 – Listagem dos acessos (a espaços físicos) do utilizador, entre as datas assinaladas

Acessos do Utilizador

Identificação do Utilizador: 3250wy46

Atributos

Dados do Utilizador

Identificação3250wy46

NomeRicardo Nuno Moreira Freitas

Acessos do Utilizador 3250wy46 entre as Datas: 10/07/2008 e 11/07/2008

Direcção	Id. do Espaço	Descrição de Espaço	Tipo	Localização	Data do Acesso	Hora do Acesso
in	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	10-07-2008	14:20:02
out	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	10-07-2008	17:30:22
in	Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP	11-07-2008	08:08:10
in	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	11-07-2008	08:10:04
in	I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	11-07-2008	08:11:04
out	I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	11-07-2008	09:34:00
out	I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	11-07-2008	09:35:40
out	Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP	11-07-2008	09:37:55

Voltar (Menu Anterior)

Figura 8.19 – Visualização parcial da listagem de acessos (direcção dos acessos; identificação, descrição, tipo e localização dos espaços acedidos, data e hora dos acessos)

8.3.6 Auditar Acessos a Espaços

O actor, através do menu *Auditar Acessos a Espaços*, solicita a auditoria de acessos a espaços físicos controlados. O sistema possibilita que o actor pesquise e selecione um espaço físico de uma listagem de espaços físicos controlados, listados hierarquicamente, que lhe é apresentada. Para o espaço físico seleccionado e depois de assinaladas duas datas (início e fim) de pesquisa, o sistema vai disponibilizar ao actor uma listagem dos acessos dos utilizadores (com direcção do acesso – entrada ou saída, identificação e nome do utilizador, data e hora do acesso,...) efectuados ao espaço físico, entre as datas assinaladas (ver secção §5.2.3.5 “Auditar/Pesquisar Acessos e Presenças”, pág. 104 e Anexo “B.4 – Auditar/Pesquisar Acessos e Presenças”, pág. 193).

Para auditar os acessos a um espaço controlado são executados os seguintes passos:

1. O administrador clica no *Menu Acessos → Auditar Acessos a Espaços*
2. A aplicação disponibiliza uma página *Auditar Acessos a Espaços* com uma listagem da hierarquia de espaços físicos controlados pelo sistema.
3. O administrador selecciona o espaço físico controlado que pretende auditar, clicando no botão *Consultar* respectivo.
- Consultar acessos ao espaço físico *I-104 (laboratório – automação e informática industrial)*



Figura 8.20 – Página Auditar Acessos a Espaços com selecção do espaço físico a auditar

4. Uma nova página é mostrada, contendo a enumeração dos principais atributos do espaço físico controlado (identificação, descrição, tipo, localização) e dois campos para inserção de duas datas (início e fim) de parametrização de pesquisa dos acessos ao espaço físico.
5. O administrador, através dum calendário que é despoletado pelo clicar dum botão específico, ao lado de cada campo de inserção, facilmente insere as datas de parametrização de pesquisa dos acessos e, em seguida, clica no botão *Submeter*.
- Data Início: 10/07/2008 e Data Fim: 11/07/2008

Figura 8.21 – Visualização parcial com os dados do espaço físico a auditar entre duas datas

6. A aplicação disponibiliza uma nova página com a listagem dos acessos ao espaço físico, entre as datas assinaladas. Na listagem são mencionados: a direcção dos acessos (entrada ou saída); a identificação e o nome do utilizador; a data e hora do acesso.

A listagem dos acessos ao espaço físico pode ser ordenada ascendentemente por:

- identificação do utilizador e data/hora do acesso (ordenação por defeito)
- nome do utilizador e data/hora do acesso
- data/hora dos acessos e identificação do utilizador

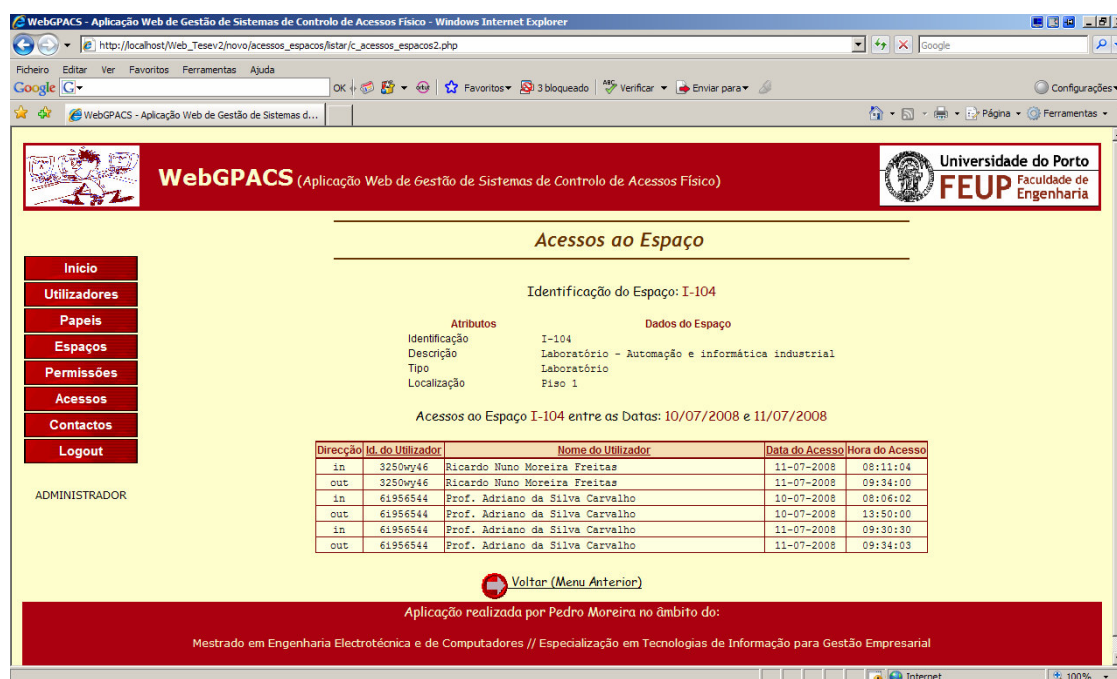


Figura 8.22 – Listagem dos acessos de utilizadores efectuados ao espaço físico, entre as datas assinaladas (ordenada por identificação do utilizador e data/hora do acesso)

8.3.7 Auditar Acessos a um Espaço por Utilizador

O actor, através do menu *Auditar Acessos a Espaço por Utilizador*, solicita a auditoria de acessos dum utilizador a um espaço. O sistema possibilita que o actor pesquise e selecione um utilizador de uma lista de utilizadores que lhe é apresentada, podendo ser ordenada por vários atributos do utilizador (número de identificação, nome,...). Para o utilizador seleccionado, o sistema disponibiliza uma listagem da hierarquia de espaços físicos controlados, sobre os quais o utilizador tem permissão de acesso, permitindo ao actor pesquisar e seleccionar cada um desses espaços físicos. Para o utilizador e espaço físico seleccionados, assim como, depois de assinaladas duas datas (início e fim) para parametrização de pesquisa, o sistema vai disponibilizar ao actor uma listagem dos acessos do utilizador (com direcção do acesso – entrada/saída, data e hora do acesso,...) efectuados ao espaço físico, entre as datas assinaladas (ver secção §5.2.3.5 “Auditar/Pesquisar Acessos e Presenças”, pág. 104 e Anexo “B.4 – Auditar/Pesquisar Acessos e Presenças”, pág. 193).

Para auditar os acessos dum utilizador a um espaço físico controlado são executados os seguintes passos:

1. O administrador clica no *Menu Acessos* → *Auditar Acessos a Espaço por Utilizador*
2. A aplicação disponibiliza uma página *Auditar Acessos dum Utilizador a um Espaço* com uma lista de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...).
3. O administrador selecciona o utilizador a ser auditado, clicando no botão *Consultar* respectivo.
- Consultar acessos do utilizador *Ricardo Nuno Moreira Freitas*
4. Uma nova página é mostrada, que contém a enumeração dos principais atributos do utilizador (identificação, nome), uma listagem de espaços físicos controlados, listados hierarquicamente e sobre os quais o utilizador tem permissão de acesso.
5. O administrador selecciona o espaço físico controlado, a ser auditado em relação aos acessos do utilizador já assinalado, clicando no botão *Consultar* respectivo.
- Consultar acessos do utilizador (assinalado) ao espaço físico *I-104 (laboratório – automação e informática industrial)*

Auditar Acessos do Utilizador a um Espaço

Identificação do Utilizador: 3250wy46

Atributos	Dados do Utilizador
Identificação	3250wy46
Nome	Ricardo Nuno Moreira Freitas

Espaços a que o Utilizador 3250wy46 tem acesso (ou permissão)

Identificação	Descrição	Tipo	Localização	Acessos
Edifício-I	Edifício de Electrotecnia	Edifício	Campus da FEUP	Consultar
I-Piso0	Piso 0 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	Consultar
I-Piso1	Piso 1 - Edifício de Electrotecnia	Piso	Edifício de Electrotecnia	Consultar
I-104	Laboratório - Automação e informática industrial	Laboratório	Piso 1	Consultar

[Voltar \(Menu Anterior\)](#)

Figura 8.23 – Visualização parcial, com os dados do utilizador, listagem dos espaços físicos cujo utilizador tem permissão de acesso e selecção do espaço físico

6. Uma nova página é mostrada, não só contendo a enumeração dos principais atributos do utilizador (identificação, nome) e da identificação do espaço físico, como também dois campos para inserção de duas datas (início e fim) de parametrização de pesquisa dos acessos.
7. O administrador, através dum calendário que é despoletado pelo clicar dum botão específico, ao lado de cada campo de inserção, facilmente insere as datas de parametrização de pesquisa dos acessos e, em seguida, clica no botão *Submeter*.
- Data Início: 10/07/2008 e Data Fim: 11/07/2008

8. A aplicação disponibiliza uma nova página que contém a enumeração dos principais atributos do utilizador (identificação, nome), do espaço físico controlado (identificação, descrição, tipo, localização) e a listagem dos acessos do utilizador ao espaço físico mencionado, entre as datas assinaladas e ordenados ascendentemente por data/hora. Na listagem são mencionados a direcção dos acessos (entrada ou saída) e a data e hora do acesso.



Figura 8.24 – Página dos acessos do utilizador a um determinado espaço físico

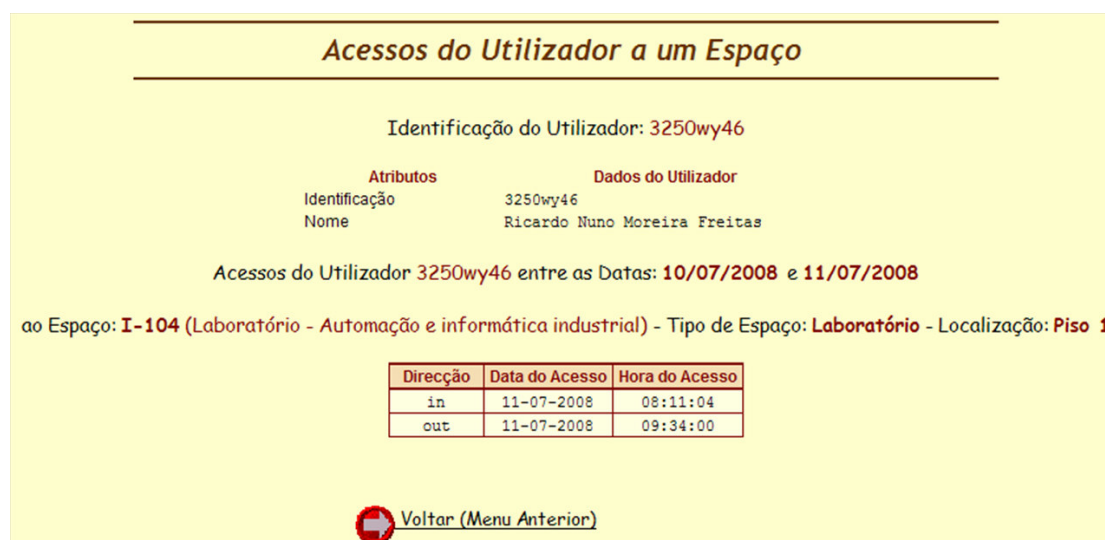


Figura 8.25 – Visualização parcial, com enumeração dos principais atributos do utilizador e do espaço físico, datas de parametrização de pesquisa e lista dos acessos do utilizador efectuados ao espaço físico, entre as datas mencionadas

Capítulo 9

Conclusões

Foi a partir da constatação da utilidade que os sistemas de *software* de gestão de controlo de acessos físico proporcionam na eficácia da administração dos acessos a recursos tangíveis das organizações e da crescente necessidade de desenvolvimento e implementação destes sistemas, que o presente trabalho se desenvolveu. Nesse sentido, o seu objectivo principal centrou-se na concepção, desenvolvimento e implementação de uma aplicação *web* de gestão de sistemas de controlo de acessos físico, mais propriamente, adequada a um *campus* universitário.

Neste contexto, numa etapa inicial, o trabalho incidiu, sobretudo, em actividades de pesquisa, selecção e síntese de documentação disponível sobre os vários temas abrangidos pela problemática dos sistemas de controlo de acessos físico e sua gestão. Deste modo, procuraram-se obter os conhecimentos específicos que permitissem efectuar a caracterização dos principais conceitos e mecanismos relacionados com o processo de controlo de acessos físico, tecnologias utilizadas e sistemas correspondentes.

Em etapas subsequentes, já dedicadas à concepção, desenvolvimento e implementação da aplicação *web* de gestão de sistemas de controlo de acessos físico (*WebGPACS*), o trabalho dirigiu-se à compreensão do domínio do problema, à identificação dos requisitos gerais da aplicação e à concepção da arquitectura do sistema. Por fim, foram mencionados os aspectos mais relevantes da implementação, em especial, o modelo de gestão de dados hierárquicos utilizado, efectuado o desenvolvimento da codificação da aplicação e, com base num caso de estudo, a correspondente validação de resultados e requisitos funcionais.

9.1 Funcionalidades da Aplicação (Implementadas)

O desenvolvimento e programação da aplicação *WebGPACS* suportou, numa primeira fase (âmbito deste trabalho), as principais *funcionalidades standard e essenciais de administração ou de gestão de controlo de acessos* (ver secção §5.1.6 “Funcionalidades Essenciais de Gestão / Administração”, pág. 81) e que estão directamente relacionadas com a *Gestão de*:

- *Utilizadores* – funcionalidades referentes à *gestão de utilizadores* do sistema de controlo de acessos físico:
 - *Inserção, Modificação e Remoção de Utilizadores*
 - *Atribuição e Eliminação de Papéis a Utilizadores*
 - *Listagem de Utilizadores*

- *Consultar Papéis de Utilizadores*
 - *Consultar Permissões de Utilizadores*
 - *Consultar Papéis e Permissões de Utilizadores*
- *Papéis* – funcionalidades referentes à *gestão de papéis* utilizados na gestão do sistema de controlo de acessos:
 - *Inserção, Modificação e Remoção de Papéis*
 - *Atribuição e Eliminação de Utilizadores a Papéis*
 - *Listagem de Papéis*
 - *Consultar Utilizadores de Papéis*
 - *Consultar Permissões de Papéis*
- *Espaços Físicos (controlados)* – funcionalidades que se prendem com a *gestão dos espaços físicos (controlados)*, os espaços físicos *hierárquicos* utilizados e controlados pelo sistema de controlo de acessos físico:
 - *Inserção, Modificação e Remoção de Espaços (físicos)* (ver código no Anexo C.1 – Código de “Editar Espaços (inserir, modificar, eliminar)”, pág. 197)
 - *Listagem de Espaços (físicos)*
 - *Consultar Utilizadores de Espaços (físicos)*

Nota: Refere-se que a implementação desta funcionalidade lidou convenientemente com a *estrutura física dos espaços físicos* das organizações (ver secção §4.3.1 “A Estrutura dos Espaços Físicos”, pág. 69), em conformidade com o *conceito dos espaços físicos encaixados*, isto é, com o facto de os espaços físicos possuírem ou conterem outros espaços físicos no seu interior. A *implementação* desta funcionalidade obrigou à utilização de um *modelo de gestão de dados hierárquicos* (ver secção §7.4 “Modelo de Gestão de Dados Hierárquicos da Tabela “Espaços””, pág. 127) para que, através deste, a aplicação pudesse não só lidar com estes dados, concretamente, os espaços físicos, como também, representá-los *hierarquicamente*.

- *Gestão de Permissões (a espaços físicos)* – funcionalidades que respeitam à *gestão de permissões* (a espaços físicos) dos diferentes papéis de utilizadores do sistema de controlo de acessos físico.
 - *Inserção, Modificação e Remoção de Permissões, a Espaços (físicos), de Papeis (de Utilizadores)*

Nota: Salienta-se que a implementação desta funcionalidade está em conformidade com o *conceito ou regra da herança reversa* (ver secção §4.3.3.2 “Autorização Implícita e Herança Reversa”, pág. 72), implicando que na atribuição de uma permissão de acesso a um espaço físico, são também atribuídas ao papel, caso necessário e de modo automático, permissões de acesso a espaços físicos que conduzem ao primeiro. Inversamente, na remoção de uma permissão

de acesso, a um espaço físico, de um determinado papel, são automaticamente removidas deste, as permissões de acesso a espaços físicos hierarquicamente descendentes do espaço físico, ao qual se removeu a permissão.

A aplicação tratou, ainda, da implementação de um último conjunto de *funcionalidades standard e essenciais de administração ou de gestão de controlo de acessos*, referentes à efectuação de *Consultas e Produção de “Reports”* (apenas, em páginas da aplicação) *de Auditoria*:

- *Auditar/Consultar Acessos (de Utilizadores e a Espaços)* – funcionalidades de *auditorias sobre acessos* dos utilizadores aos espaços físicos controlados, nomeadamente:
 - *Auditar Acessos de Utilizadores*
 - *Auditar Acessos a um Espaço por Utilizador* (ver código no Anexo C.2 – Código de “Auditar Acessos a um Espaço por Utilizador”, pág. 215).
 - *Auditar Acessos a Espaços (físicos)*

9.2 Perspectivas de Trabalho Futuro

Seguidamente, serão mencionadas as funcionalidades que, futuramente, poderão vir a ser implementadas para uma aplicação completa de gestão de controlo de acessos físico, de âmbito alargado, bem como, em traços gerais, uma ideia para a viabilização de oferta de serviços nesta área, de “gestão de controlo de acessos”.

9.2.1 Funcionalidades da Aplicação (a Implementar)

Para uma *aplicação de gestão de sistemas de controlo de acessos físico*, de âmbito alargado, seria necessário desenvolver e implementar, em fases posteriores, as restantes *funcionalidades* (ver secção §5.1 “Requisitos Gerais”, pág.77), fora do âmbito deste trabalho, que, obviamente, não puderam ser implementadas.

Nesse sentido, o desenvolvimento e programação da aplicação *WebGPACS* deverá, futuramente, vir a suportar as *funcionalidades que respeitam a registos da Base de Dados*, nomeadamente de:

- *Eventos de Acessos* – em que cada evento de acessos ou verificado nos locais de acesso deverá ser registado na base de dados da aplicação, como o registo automático de todos os acessos (*logs*) de utilizadores aos espaços físicos controlados pelo sistema de controlo de acessos.
- *Eventos de Sistema ou Rede* – em que cada evento referente ao sistema ou rede poderá ser registado na base de dados da aplicação, nomeadamente:

- perdas de energia ou de ligação dum local de acesso
 - falhas de comunicação
 - e outros eventos específicos do funcionamento do próprio sistema.
- *Eventos (Actividades ou Operações) de Administração do Sistema* – em que todas os eventos relacionados com a administração ou gestão do sistema, seriam gravados e registados na base de dados da aplicação (por ex., o facto dum administrador criar um novo utilizador ou modificar as suas permissões de acesso, é uma acção que deve ser registada na base de dados, possibilitando que, futuramente, possam ser efectuadas auditorias de rastreio dirigidas à administração do sistema).

A aplicação poderá, também, ser complementada com *funcionalidades que se relacionam com o funcionamento, monitorização e notificações do sistema em tempo real*:

- *Funcionamento (em Tempo Real)* – cada evento de acessos, ocorrido num determinado local de acesso, tais como, entradas e saídas de utilizadores a espaços físicos controlados, deve ser comunicado, em tempo real, ao servidor central, bem como, todas as operações de funcionamento do sistema de controlo de acessos físico, relativas ao controlo de acessos (entradas e saídas). De cada vez que um evento de acessos ocorre (entrada ou saída), deverá ser comunicado ao servidor central e registado na base de dados. (*Nota*: esta funcionalidade está directamente relacionada com o *registo na base de dados de eventos de acessos*, mencionada anteriormente).
- *Monitorização (em Tempo Real)* – monitorização e controlo do sistema, proporcionando que, a partir dum local remoto, qualquer local de acesso a um espaço físico possa ser gerido em tempo real. Esta funcionalidade exigirá que a aplicação possa dispor de:
 - *Integração com Sistemas de Software de Automação* – a aplicação poderá vir a ser integrada com sistemas de *software* de automação para que alguns dos acessos possam ser monitorizados, em tempo real, em conjunto com sistemas de alarme e/ou de videovigilância – CCTV (por ex., uma determinada porta de um local de acesso a um espaço físico poderá ser aberta remotamente, a partir da confirmação visual dum determinado utilizador).
 - *Customização do Sistema de Controlo de Acessos* – a aplicação deverá permitir que seja efectuada a devida configuração do sistema, para que possam ser designados e atribuídos os *eventos de acessos* (por ex., porta deixada aberta, porta forçada, tentativa de utilização de um cartão furtado ou perdido,...) ou *de sistema* (por ex., leitor com bateria fraca, falha de energia ou das comunicações,...) a serem monitorizados.

- *Notificações (em Tempo Real)* – conjunto de notificações, por comunicação electrónica, que poderão ser dirigidas a determinados responsáveis ou administradores,..., interessados em resultados específicos da aplicação. Estas notificações, depois de customizadas, serão despoletadas em função da ocorrência de determinados eventos (quer de *acessos*, quer de *sistema* ou, mesmo, de *administração do sistema*):
 - *Notificações de Eventos de Acessos* – envio de notificações de aviso sobre ocorrências de determinados acessos (por ex., notificação dirigida a um qualquer director da instituição ou departamento, relativamente ao acesso, hora de entrada, de determinada pessoa ou colaborador numa determinada instalação da organização).
 - *Notificações de Eventos de Sistema* – envio de notificações de aviso, em casos de falha do sistema (por ex., uma notificação, via *e-mail*, para o administrador de rede, avisando-o de uma falha nas comunicações de rede e das portas ou locais de acesso afectados; envio de alertas para funcionários / directores de segurança, em casos de portas deixadas abertas ou falhas de corrente eléctrica,...).
 - *Notificações de Eventos (Actividades ou Operações) de Administração do Sistema* – acções de notificação do sistema, em casos de ocorrência de certos eventos administrativos (por ex., de cada vez que um administrador regista um novo utilizador, os departamentos de *RH* ou de Segurança recebem um *e-mail* a indicar as permissões do novo utilizador,...)

A aplicação poderá também vir a permitir que possam ser atribuídas ou concedidas permissões de gestão do sistema a outros utilizadores (além de administradores) ou grupos de utilizadores da aplicação, concretamente, para certos conjuntos de funcionalidades de administração ou gestão. Em futuros desenvolvimentos, a aplicação poderá suportar esta funcionalidade, de *atribuição de*:

- *Privilégios Especiais de Operação/Gestão* – um administrador do sistema poderá conceder, a determinados utilizadores ou grupos específicos de utilizadores, privilégios especiais de operacionalidade de gestão do sistema, particularmente de:
 - *Acesso a Áreas Específicas* – acesso a áreas de gestão do sistema que possam directamente relacionar-se com determinados utilizadores ou grupos de utilizadores (por ex., o pessoal das *TI* acede, somente, a páginas relacionadas com a gestão de rede e comunicações *IP*; o de *RH* pode ter permissão, apenas, para registar utilizadores e não, a quaisquer outras funcionalidades – “muito menos sobre auditorias de acessos”,...)

Por último, a aplicação poderá, ainda, ser complementada com o acrescento de funcionalidades de *Consultas e Produção de “Reports”* (*standard* ou customizados)

sobre ocorrências, quer ao nível da *gestão*, quer ao nível dos *acessos* (utilização do sistema de controlo de acessos físico), nomeadamente:

- *Pesquisar/Localizar Presenças de Utilizadores em Espaços* – funcionalidades que permitem efectuar várias consultas e listagens sobre a localização, em tempo real, de utilizadores em quaisquer dos espaços físicos controlados, como:
 - *Pesquisar/Localizar Presenças de Utilizadores* – pesquisar ou localizar, em tempo real, a presença dum determinado utilizador em qualquer um dos espaços físicos controlados pelo sistema de controlo de acessos.
 - *Consultar Presenças em Espaços* – consultar ou listar todas as presenças de utilizadores, em tempo real, num determinado espaço físico controlado pelo sistema de controlo de acessos.
- *Auditorias sobre a Administração e a Segurança do Sistema* – auditorias sobre eventos ocorridos, tanto ao nível da gestão/administração, como da utilização do sistema de controlo de acessos físico, particularmente:
 - *Auditorias sobre Administração ou Gestão do Sistema* – emissão de “reports” em que podem ser mostradas, com algum detalhe, as *actividades ou operações* efectuadas pelos “administradores” (por ex., os utilizadores que registaram no sistema, as permissões de acesso atribuídas ou removidas,...) em cada uma das suas sessões (tempo de autenticação na aplicação) e, obviamente, o *tempo de utilização*.
 - *Auditorias sobre Segurança do Sistema* – produção de “reports” dirigidos à *segurança* do sistema de controlo de acessos, quer ao nível da sua utilização indevida (por ex., as tentativas de intrusão – tentativas de acesso, a espaços físicos, efectuadas por utilizadores não autorizados ou sem permissão, com senhas – *passwords* – inválidas,...), quer, mesmo, à eficiência do seu funcionamento (por ex., as falhas do sistema ou das comunicações, ocorridas em cada local de acesso,...).
- *Consultas Gerais à Base de Dados* – outras possibilidades de se efectuar vários tipos de consultas e listagens, definidas pelo utilizador, de suporte à gestão de controlo de acessos, a partir dos múltiplos dados armazenados na base de dados e da informação que podem proporcionar.

9.2.1.1 Outras Funcionalidades (Relacionadas)

Durante o desenvolvimento da aplicação de gestão de sistemas de controlo de acessos físico, desde logo, foram surgindo diversas ideias para novas funcionalidades relacionadas, não em específico, com a gestão de sistemas de controlo de acessos físico, mas que, directamente ou indirectamente, se dirigem a ambientes próprios de instituições de ensino ou de *campus* universitários. Assim, em futuros desenvolvimentos

do projecto, de âmbito mais alargado, a aplicação poderia ser complementada com a integração das seguintes funcionalidades:

- *Controlo de presenças ou de ponto (para alunos e funcionários)* – numa perspectiva mais abrangente, o controlo de alunos poderia integrar os seus horários de aulas das diferentes disciplinas. Também, agora dirigido mais a escolas de ensino de escalões inferiores, conferir a possibilidade dos pais consultarem e auditarem, via *Internet*, a assiduidade e frequência dos seus filhos às aulas, em tempo real.
- *Parqueamento automóvel* – funcionalidades específicas de contador, reserva e pagamento de parqueamento automóvel.
- *Utilização de porta-moedas electrónico* – funcionalidades referentes à gestão de transacções comerciais, através do sistema de pagamento de porta-moedas electrónico por cartão (*e-cash*), no interior das instituições de ensino, que poderiam abranger, desde o carregamento de cartões, até ao pagamento ou crédito de serviços (por ex., de papelaria – fotocópias/impressões de documentos ou serviço de impressoras, de bar/cafetaria, cantinas, máquinas de venda “*self service*”, livraria e biblioteca, outros possíveis quiosques internos e, mesmo, serviços específicos de residências universitárias, ...)

9.2.2 Serviços de “Gestão de Controlo de Acessos”

Uma vez que as organizações estão, cada vez mais, não só a ter preocupações relativas à segurança das suas instalações, como também, mais e melhores infra-estruturas de comunicações *IP*, poder-se-á avançar com a ideia da viabilidade de desenvolvimento de uma empresa que pudesse actuar na área de “Gestão de Controlo de Acessos (Físico)”, objecto de estudo desta dissertação. Em linhas gerais, uma empresa que pudesse, futuramente, vir a funcionar como uma estação central de alojamento (*hosting*) de uma *Plataforma Web de Software de Gestão de Controlo de Acessos (Físico)* e cuja oferta de serviços seria, por meio dessa aplicação, efectuar e proporcionar a *gestão remota dos sistemas de controlo de acessos físico* das organizações clientes. (instituições, empresas, condomínios residenciais,...). Estas, a partir de qualquer *PC* com ligação à *internet*, poderiam ter acesso, tanto a resultados da gestão dos seus sistemas, como mesmo, a funcionalidades específicas para administração própria. Outro benefício complementar neste tipo de oferta, seria dispensar, as organizações clientes, da utilização dos tradicionais “*host systems*” (servidor *web* e *software* instalados localmente – ver secção §3.4.2.2 “Os Sistemas Analíticos (do *Host System*)”, pág. 52) e outros serviços afins, exigidos nas implementações locais de sistemas de controlo de acessos físico. Muitas organizações aceitariam, certamente, a transferência da gestão dos seus sistemas de controlo de acessos físico (ou, doutros sistemas de segurança) para um serviço deste tipo, em particular, as pequenas/médias empresas que, em princípio, não terão pessoal dedicado, em exclusivo, a estas actividades (serviços informáticos, gestão de sistemas de controlo de acessos,...). A oferta destes serviços de gestão de acessos poderia, mesmo, contribuir para o fomento dos próprios sistemas de controlo de acessos (físico) em organizações que, até ao presente, apenas, têm confiado a segurança das suas

instalações às simples fechaduras convencionais (...) (aditamento no Anexo E – Serviços de “Gestão de Controlo de Acessos”, pág. 239).

Bibliografia

- [1] *Access Control in Support of Information Systems - STIG*. Version 2, Release 1. Defense Information Systems Agency (DISA) for the Department of Defense (DoD), 2007.
- [2] *Access Control Systems*. Product Catalogue 2006. Honeywell Security Deutschland, 2006.
- [3] *Annual Report*. Institute of Control and Computation Engineering. Faculty of Electronics and Information Technology, Warsaw University of Technology, 2005.
- [4] *Biometrics Tutorial*. ISO/IEC JTC 1/SC 37 Biometrics. American National Standards Institute (ANSI), 2005.
- [5] *Forensic Implications of Identity Management Systems*. FIDIS Consortium, 2006.
- [6] *German Biometric Strategy Platform - Biometrics State of the Art, Industry Strategy Development, and Platform Conception*. Study. BITKOM, 2005.
- [7] *Government Smart Card Handbook*. GSA - U.S. General Service Administration, 2004.
- [8] *Honeywell Physical Access Control Systems, HSPD-12 / FIPS 201 Compliance*. White Paper. Honeywell, 2006.
- [9] *OSE Best Practices - Guidelines for Selection and Issuance of Identification Tokens For Logical and Physical Systems*. Open Security Exchange (OSE), 2004.
- [10] *Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials*. PAC-07002. Smart Card Alliance Physical Access Council in collaboration with Open Security Exchange, Security Industry Association, and International Biometric Industry Association, 2007.
- [11] *Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems*. Smart Card Alliance, 2002.
- [12] *Smart Cards and Parking*. Smart Card Alliance, 2006.
- [13] *Using Smart Cards for Secure Physical Access*. Smart Card Alliance, 2003.

- [14] Brooks, C., Dieter, L., Edwards, D., Garcia, H., Hahn, C., and Lee, M. *IBM Tivoli Storage Manager Building a Secure Environment*. Redbooks. IBM, 2007.
- [15] Celko, J. *Joe Celko's Trees and Hierarchies in SQL for Smarties*. Elsevier, 2004.
- [16] Costa, L. R., Obelheiro, R. R., and Fraga, J. S. *Introdução à Biometria*. Departamento de Automação e Sistemas, Universidade Federal de Santa Catarina, 2007?
- [17] Dias, R. P. *Apostila Web - Curso Básico de Web - DHTML (HTML - CSS - JavaScript), Apache, MySQL, PHP*, 2007?
- [18] Faltin, U., Kohler, M., Kowski, S., and Wolf, R. *Requirements Analysis - Requirements for Specification of Security Policies*. Deliverable AP 5.1. Organizational Control Architecture (ORKA Consortium), 2007.
- [19] Faria, J. A. *Introdução à linguagem HTML*. FEUP, 2005.
- [20] Faria, J. P. and Aguiar, A. *Análise e Desenho Orientado por Objectos de um Sistema de Gestão de Espectáculos e Bilheteira*, 2004.
- [21] Ganci, J., Cherukuwada, S., McGoogan, B., Olivera, L., Thorwart, J., and Wardell, W. *Identity and Access Management Solutions*. Redbooks. IBM, 2005.
- [22] Grance, T., Stevens, M., and Myers, M. *Guide to Selecting Information Technology Security Products*. Special Publication 800-36. National Institute of Standards and Technology (NIST), 2003.
- [23] Grieken, I. K. v. *Applying Internet Technology and BACnet to Building Automation*. White Paper. Priva Building Intelligence, 2007.
- [24] Hu, V. C., Ferraiolo, D. F., and Kuhn, D. R. *Assessment of Access Control Systems*. Interagency Report 7316. National Institute of Standards and Technology (NIST), 2006.
- [25] Karygiannis, T., Eydt, B., Barber, G., Bunn, L., and Phillips, T. *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. Special Publication 800-98. National Institute of Standards and Technology (NIST), 2007.
- [26] Kuhn, M. *Security - Biometric identification*. Michaelmas 2003 - Part II. University of Cambridge, 2003.
- [27] Luis-Garcia, R. d., Alberola-López, C., Aghzout, O., and Ruiz-Alzola, J. *Biometric identification systems*. Elsevier, 2003.
- [28] MacGregor, W., Mehta, K., Cooper, D., and Scarfone, K. *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*. Special Publication 800-116. National Institute of Standards and Technology (NIST), 2008.

- [29] Merkert, R. J. *Smart Cards and Biometrics in Physical Access Control Systems*. Biometric Consortium 2005 Conference. SCM Microsystems, 2005.
- [30] Podio, F. L. and Dunn, J. S. *Biometric Authentication Technology: From the Movies to Your Desktop*. Biometric Consortium, 200?
- [31] Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., and Rogers, G. *Recommended Security Controls for Federal Information Systems - Information Security*. NIST Special Publication 800-53 Revision 2. National Institute of Standards and Technology (NIST), 2007.
- [32] Souffer, K., Falco, J., and Scarfone, K. *Guide to Industrial Control Systems (ICS) Security*. Special Publication 800-82. National Institute of Standards and Technology (NIST), 2007.
- [33] Sukhai, N. B. *Access Control & Biometrics*. InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA. ACM, 2004.
- [34] www.acura.com.br/acurasecurity/comparar.php, 2008.
- [35] www.ibia.org/biometrics/, 2008.
- [36] www.rfidsystems.com.br/, 2008.
- [37] www.usb.org/home, 2008.

ANEXOS

Anexo A – Sistema Biométrico (pág. 181)

- A.1 – Modelo Conceptual dum Sistema Genérico
- A.2 – Funcionamento: Processos Característicos
- A.3 – Erros
- A.4 – Critérios Base

Anexo B – Casos de Utilização (Descrição) (pág. 187)

- B.1 – Gestão de Papéis
- B.2 – Gestão de Espaços (Físicos)
- B.3 – Gestão de Permissões (a Espaços)
- B.4 – Auditar/Pesquisar Acessos e Presenças

Anexo C – Listagem Parcial do Código da Aplicação (pág. 197)

- C.1 – Código de “Editar Espaços (inserir, modificar, eliminar)”
- C.2 – Código de “Auditar Acessos a um Espaço por Utilizador”

Anexo D – Interrogações à Base de Dados (pág. 231)

- D.1 – Utilizadores
- D.2 – Papéis
- D.3 – Espaços
- D.4 – Permissões (a Espaços)
- D.5 – Acessos e Presenças

Anexo E – Serviços de “Gestão de Controlo de Acessos” (pág. 239)

Anexo A – Sistema Biométrico

Este Anexo, tomando por base a apresentação dum Sistema Biométrico (genérico), procura apresentar, em traços gerais, uma visão geral sobre os sistemas biométricos e suas principais características.

A.1 – Modelo Conceptual dum Sistema Genérico

À partida, dada a multiplicidade de aplicações e de tecnologias biométricas, pode parecer difícil generalizar sobre sistemas biométricos. No entanto, verifica-se que todos estes sistemas têm muitos elementos em comum, o que leva à concepção dum *modelo de sistema biométrico genérico*.

Nesse modelo, as amostras biométricas são *adquiridas* por um sensor e depois enviadas a um processador. Este retira o essencial da amostra (características), eliminando todos os outros componentes. Estas características não só podem ser armazenadas numa base de dados (como *template*), como também, comparadas a um, a vários ou a todos os *templates*, já existentes na base de dados, no sentido de se averiguar acerca duma possível *correspondência*. Essa *decisão* é feita com base na semelhança entre as características da amostra e as do *template* ou as dos vários comparados.

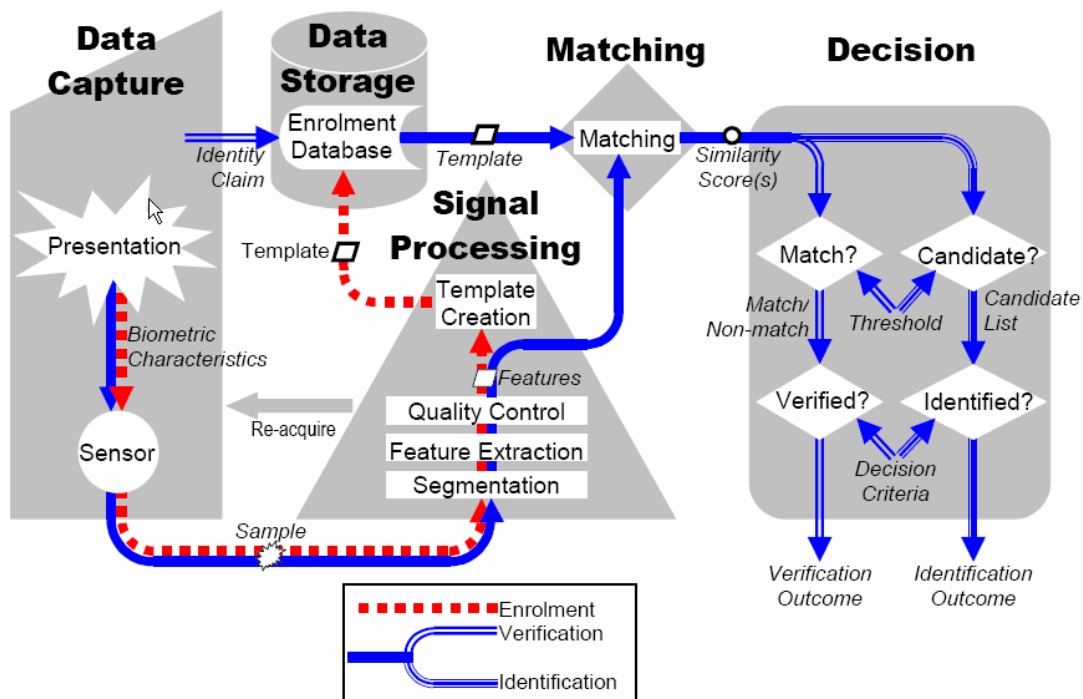


Figura 0.1 – Modelo conceptual dum sistema biométrico genérico e seus subsistemas [4]

A *Figura 0.1* ilustra o modelo e o fluxo de informação num *sistema biométrico genérico*, mostrando que o mesmo é constituído pelos seguintes *subsistemas*:

- *Aquisição de Dados (Data Capture)*
- *Processamento de Sinal (Signal Processing)*
- *Armazenamento de Dados (Data Storage)*
- *Correspondência (Matching)*
- *Decisão (Decision)*

O diagrama mostra também os *processos* de:

- *Registo (Enrollment)*
- *Verificação (Verification)*
- *Identificação (Identification)*

Refere-se que num *sistema biométrico* real, pode não existir qualquer um dos componentes conceptuais apresentados no diagrama ou, mesmo, não corresponderem directamente com os componentes físicos do sistema.

Componentes Físicos

Um *sistema biométrico* para funcionar necessita basicamente de:

- Dispositivo de aquisição (sensor)
 - digitalizador (*scanner*), microfone, câmara de vídeo,...
- Programas informáticos para:
 - aquisição (da característica biométrica)
 - correspondência (comparações 1:1 ou 1:N)
- Repositório dos registos biométricos (para comparação posterior)
 - base de dados com protecção (área segura, dados encriptados,...)

Arquitecturas de Localização

Um *sistema biométrico* pode efectuar em diferentes *localizações*:

- o *armazenamento* de dados biométricos:
 - base de dados central
 - estação de trabalho (*workstation*)
 - dispositivo biométrico
 - cartão *smart card*

- o processo de *correspondência*:
 - servidor central
 - estação de trabalho (*workstation*) local
 - interior do dispositivo biométrico
 - cartão *smart card*

A.2 – Funcionamento: Processos Característicos

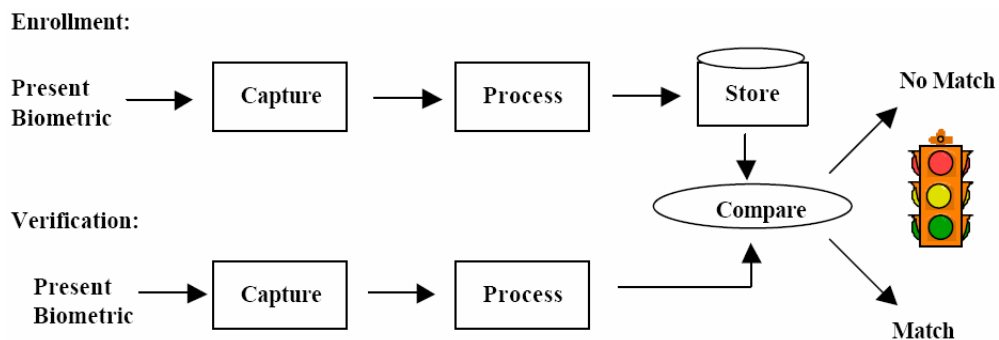


Figura 0.2 – A lógica dos passos dum sistema biométrico [30]

No funcionamento dum *sistema biométrico* existem três processos ou funções básicas:

- *Registo (Enrollment)*
- *Verificação (Verification)*
- *Identificação (Identification)*

Registo

O *Registo (Enrollment)* é o processo efectuado pelo sistema com o objectivo de obter, previamente, os dados biométricos do utilizador e os poder armazenar como um *template* biométrico. Embora realizado raramente, este processo é necessário para se obter um registo do perfil biométrico (*template*) do utilizador, que, posteriormente, servirá de base para futuras comparações.

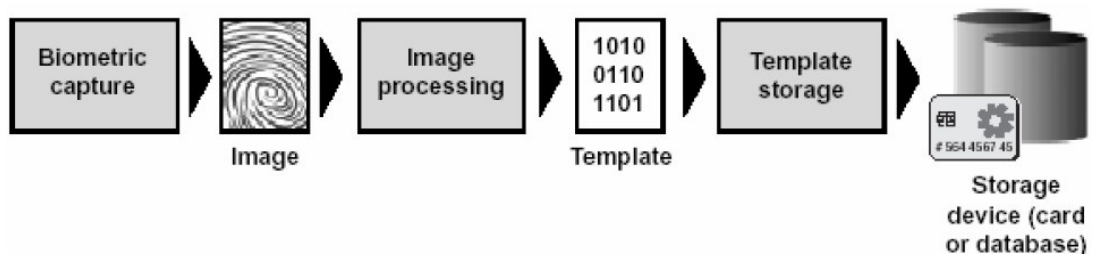
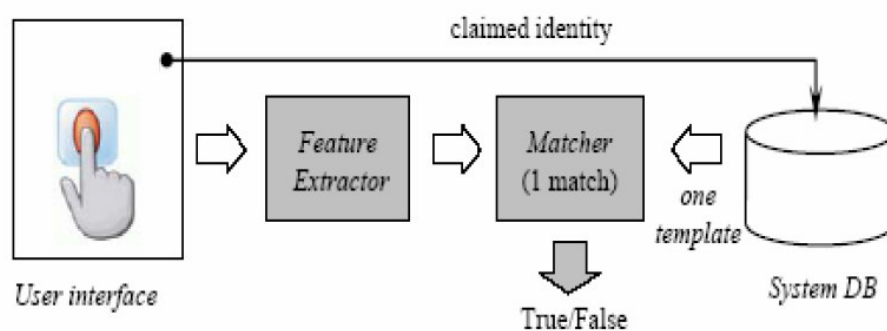


Figura 0.3 – Exemplo do processo de registo (enrollment) [11]

Verificação

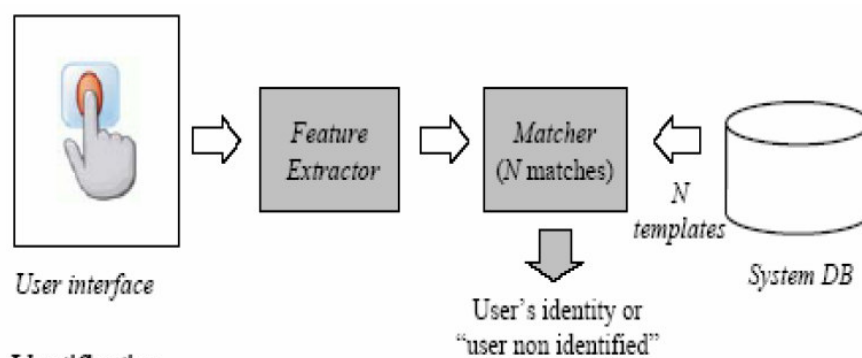


Verification

Figura 0.4 – Exemplo do Processo de Verificação [6]

A *Verificação* (*Verification*) é um modo de autenticação em que uma característica biométrica é apresentada ao sistema, juntamente com uma identidade do utilizador (por ex., código de identificação). Este tipo de autenticação é chamado de pesquisa ou *processo de correspondência de 1:1*, em que o sistema, através duma base de dados de perfis biométricos (*templates*), vai *verificar* ou provar a identidade do utilizador, isto é, “se o utilizador é, efectivamente, quem reivindica ser” [16].

Identificação



Identification

Figura 0.5 – Exemplo do Processo de Identificação [6]

A *Identificação* (*Identification*) é um modo de autenticação em que o utilizador fornece, apenas, a característica biométrica ao sistema, competindo a este (sistema) “*identificar*” o utilizador. Este tipo de autenticação, é chamado de pesquisa ou *processo de correspondência de 1:N*, em que o sistema, através duma base de dados de perfis biométricos (*templates*), pesquisa todos os seus registos (da base de dados) com o objectivo de *identificar* ou encontrar, a um nível suficientemente coincidente, a identidade do utilizador, isto é, “saber qual é o utilizador”. [16]

A.3 – Erros

Um *sistema biométrico* comete *erros*, pois uma determinada *verificação* pode ser, efectivamente, rejeitada quando deveria ter sido aceite ou, mesmo o contrário, ser aceite quando deveria ter sido rejeitada. O valor correcto associado às diversas *taxas de erro* não pode ser estabelecido teoricamente mas, somente, por cálculo de estimativas ou estatísticas dos erros. As taxas desenvolvidas para avaliar essas probabilidades são denominadas *FRR* (taxa de falsa rejeição) e *FAR* (taxa de falsa aceitação).

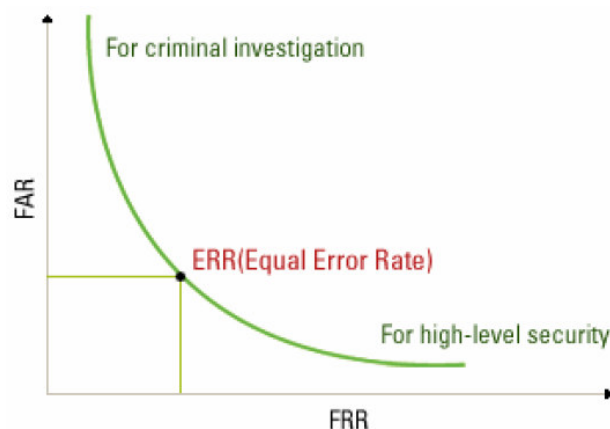


Figura 0.6 – Gráfico representativo das alterações das taxas *FRR* e *FAR* consoante o valor crítico *ERR*

A *Figura 0.6* retrata as diferenças nas taxas de *FRR* e *FAR*, consoante as mudanças do seu valor crítico *ERR* (*equal error rate*), o ponto onde as taxas coincidem e que deve ser utilizado para avaliação do desempenho do sistema. De acordo com a utilização dada ao sistema, poderá ter interesse que uma ou outra taxa seja menor. Por exemplo, no caso de espaços físicos com um alto nível de segurança, pode-se reduzir o risco de um utilizador poder aceder às mesmas, diminuindo a *FAR* (taxa de falsa aceitação), em detrimento da *FRR* (taxa de falsa rejeição) que aumenta. Ao contrário, em aplicações para detecção de “pessoas inconvenientes” convém aumentar a *FAR*, ficando o sistema mais permissivo e, assim, se poder detectar e identificar potenciais suspeitos.

A.4 – Critérios Base

Um *sistema biométrico* deve fundamentar-se nos seguintes critérios base:

- *Universalidade* – todas as pessoas devem poder utilizar o sistema biométrico em questão.
- *Unicidade ou Singularidade* – os dados biométricos de cada pessoa devem ser únicos. Deve ser nula a possibilidade de duas pessoas diferentes possuírem os mesmos dados ou características biométricas.
- *Permanência* – os dados biométricos não se modificam e não podem ser modificados, isto é, as características biométricas devem ser imutáveis. Na

prática, existem alterações que podem ser provocadas pelo envelhecimento, alteração das condições de saúde ou, mesmo, emocionais das pessoas, assim como, por alterações do meio ambiente de aquisição dos dados.

- *Colectável* – as características biométricas têm de ser fáceis de adquirir e quantificar (mensuráveis).

O desenvolvimento dum *sistema biométrico* deve atender a características, como:

- *Desempenho* – precisão, fiabilidade, velocidade de processamento, robustez, requisitos materiais e de condições ambientais.
- *Aceitabilidade* – grau de aceitação dos utilizadores em relação ao sistema. O processo de aquisição das características biométricas deverá ser aceite ou tolerado pelos utilizadores e, na realidade, existem preocupações relacionadas com as condições de higiene, privacidade e aspectos culturais que poderão diminuir a sua aceitação.
- *Protecção* – resistência à fraude, grau de facilidade para corromper o sistema.

Anexo B – Casos de Utilização (Descrição)

Este Anexo, apresenta as descrições textuais, em formato alto-nível, dos casos de utilização dos diagramas do Modelo de Casos de Utilização (ver secção §5.2 “Modelo de Casos de Utilização”, pág. 86) da aplicação *WebGPACS*, desenvolvida neste trabalho. Concretamente, sobre os diagramas de casos de utilização referentes a:

- B.1 – “Gestão de Papéis”
- B.2 – “Gestão de Espaços (Físicos)” (descrição parcial)
- B.3 – “Gestão de Permissões (a Espaços)”
- B.4 – “Auditar/Pesquisar Acessos e Presenças”

B.1 – Gestão de Papéis

Caso de Uso: Editar Papéis

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de papéis, pretendendo inserir um novo papel, modificar ou eliminar um já existente. O sistema invoca então a consulta de papéis, produzindo uma listagem de papéis que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...). O actor poderá depois pesquisar e seleccionar cada um desses papéis para o modificar ou eliminar.

Caso de Uso: Criar / Inserir Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado o botão correspondente, solicita a inserção de um novo papel. O sistema solicita ao actor a introdução dos dados do papel. Cada papel deve ser definido por uma identificação exclusiva. O sistema cria um novo papel com a informação indicada pelo actor, introduzindo-a na tabela correspondente da base de dados.

Caso de Uso: Modificar Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, solicita a sua modificação. O sistema mostra os dados actuais do papel e solicita ao actor a introdução dos dados a modificar. O sistema modifica os dados do papel com a informação indicada pelo actor. A nova informação é armazenada substituindo a anteriormente existente.

Caso de Uso: Eliminar Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, pretende eliminá-lo. Após confirmação do actor, o sistema elimina o papel da tabela correspondente da base de dados.

Caso de Uso: Editar Utilizadores a Papéis

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de utilizadores a papéis, pretendendo atribuir um novo utilizador a um papel ou eliminar um que já lhe tenha sido atribuído. O sistema invoca então a consulta de papéis, produzindo uma listagem de papéis que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...). O actor poderá depois pesquisar e seleccionar cada um desses papéis para lhes atribuir ou eliminar utilizadores.

Caso de Uso: Atribuir Utilizadores a Papéis

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, solicita a atribuição de um novo utilizador ao papel. O sistema disponibiliza uma listagem dos utilizadores já detentores do papel seleccionado e outra correspondente aos utilizadores que não têm esse papel. O actor deve seleccionar o novo utilizador a atribuir ao papel e, após confirmação, o sistema insere-o, de imediato, na lista de utilizadores do papel.

Caso de Uso: Eliminar/Remover Utilizadores a Papéis

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, solicita a eliminação de um utilizador ao papel. O sistema disponibiliza uma listagem dos utilizadores detentores do papel seleccionado. O actor selecciona o utilizador a remover do papel e, após confirmação, o sistema elimina-o, de imediato, da lista de utilizadores do papel.

Caso de Uso: Lista Utilizadores (Disponíveis)

Descrição: Este caso de uso inicia-se quando o actor solicita a atribuição de utilizadores a um papel seleccionado. O sistema disponibiliza uma listagem dos utilizadores registados no sistema que não têm esse papel.

Caso de Uso: Lista Utilizadores do Papel

Descrição: Este caso de uso inicia-se quando o actor solicita a atribuição ou a remoção de utilizadores a um papel seleccionado. O sistema disponibiliza uma listagem dos utilizadores que possuem esse papel.

Caso de Uso: Consultar Papéis

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar um papel ou solicita a edição de papéis ou de utilizadores a papéis, as consultas sobre utilizadores e permissões (a espaços) de papéis. O sistema possibilita que o actor pesquise e selecione um papel de uma lista de papéis que lhe é apresentada, podendo ser ordenada por vários atributos do papel (identificação, descrição,...).

Caso de Uso: Consultar Utilizadores de Papéis

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar os utilizadores que possuem um papel do sistema. O sistema invoca então a consulta de papéis, produzindo uma listagem de papéis que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...), permitindo ao actor pesquisar e seleccionar cada um desses papéis. Para o papel seleccionado, o sistema disponibiliza ao actor uma listagem dos utilizadores com esse papel.

Caso de Uso: Consultar Permissões (a Espaços) de Papéis

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar as permissões (a espaços físicos) atribuídas a um papel do sistema. O sistema invoca então a consulta de papéis, produzindo uma listagem de papéis que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...), permitindo ao actor pesquisar e seleccionar cada um desses papéis. Para o papel seleccionado, o sistema disponibiliza ao actor uma listagem das permissões (a espaços físicos) atribuídas ao papel.

B.2 – Gestão de Espaços (Físicos)

Caso de Uso: Consultar Espaços

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar um espaço físico controlado pelo sistema ou solicita a edição de espaços físicos ou a consulta de utilizadores de espaços. O sistema possibilita que o actor pesquise e selecione um espaço físico de uma listagem hierárquica de espaços físicos controlados que lhe é apresentada.

Caso de Uso: Consultar Utilizadores de Espaços

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar os utilizadores com permissão de acesso a um espaço físico controlado pelo sistema. O sistema invoca então a consulta de espaços, produzindo uma listagem da hierarquia de espaços físicos controlados pelo sistema, permitindo ao actor pesquisar e seleccionar cada um desses espaços físicos. Para o espaço físico seleccionado, o sistema disponibiliza ao actor uma listagem dos utilizadores desse espaço, ou seja, dos utilizadores com permissão de acesso a esse espaço.

Caso de Uso: Editar Tipos de Espaço

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de tipos de espaços, pretendendo inserir um novo tipo de espaço, modificar ou eliminar um já existente. O sistema invoca então a consulta de tipos de espaços, produzindo uma listagem de tipos de espaços que pode ser ordenada ascendente ou descendentemente por identificação do tipo de espaço. O actor poderá depois pesquisar e seleccionar cada um desses tipos de espaços para o modificar ou eliminar.

Caso de Uso: Criar / Inserir Tipo de Espaço

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado o botão correspondente, solicita a inserção de um novo tipo de espaço. O sistema solicita ao actor a introdução dos dados do tipo de espaço. Cada tipo de espaço deve ser definido por uma identificação exclusiva. O sistema cria um novo tipo de espaço com a informação indicada pelo actor, introduzindo-a na tabela correspondente da base de dados.

Caso de Uso: Modificar Tipo de Espaço

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um tipo de espaço da listagem de tipos de espaços e, através da selecção do botão correspondente, solicita a sua modificação. O sistema mostra os dados actuais do tipo de espaço e solicita ao actor a introdução dos dados a alterar. O sistema modifica os dados do tipo de espaço com a informação

indicada pelo actor. A nova informação é armazenada substituindo a anteriormente existente.

Caso de Uso: Eliminar Tipo de Espaço

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um tipo de espaço da listagem de tipos de espaço e, através da selecção do botão correspondente, pretende eliminá-lo. Após confirmação do actor, o sistema elimina o tipo de espaço da tabela correspondente da base de dados.

Caso de Uso: Consultar Tipos de Espaços

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende consultar um tipo de espaço ou solicita a edição de tipos de espaços. O sistema possibilita que o actor pesquise e selecione um tipo de espaço de uma lista de tipos de espaços que lhe é apresentada, podendo ser ordenada ascendente ou descendentemente por identificação do tipo de espaço.

B.3 – Gestão de Permissões (a Espaços)

Caso de Uso: Editar Permissões de Papéis

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de permissões (a espaços físicos) de papéis, pretendendo inserir uma nova permissão, modificar ou eliminar uma já existente. O sistema invoca então a consulta de papéis, produzindo uma listagem de papéis que pode ser ordenada por diferentes atributos do papel (identificação, descrição,...). O actor poderá depois pesquisar e seleccionar cada um desses papéis para lhes atribuir, modificar ou eliminar permissões (a espaços físicos).

Caso de Uso: Criar / Inserir Permissões a Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, solicita a inserção de novas permissões (a espaços físicos) do papel. O sistema disponibiliza uma listagem das permissões de acesso (a espaços físicos) do papel seleccionado e outra correspondente aos espaços físicos cujo papel não dá acesso. O actor deve seleccionar um espaço físico sem permissão e introduzir a informação (data e hora início/fim, condições,...) referente à nova permissão do papel. Após confirmação, o sistema insere, de imediato, a nova permissão na lista de permissões de acesso (a espaços

físicos) do papel e, se necessário, permite automaticamente acesso a espaços físicos ascendentes da hierarquia de espaços que conduzem ao da nova permissão.

Caso de Uso: Modificar Permissões do Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, solicita a modificação de permissões (a espaços físicos) do papel. O sistema disponibiliza uma listagem das permissões de acesso (a espaços físicos) do papel seleccionado. O actor deve seleccionar, através do botão correspondente, a permissão a modificar. Após essa selecção, o sistema mostra os dados actuais da permissão e solicita ao actor a introdução dos dados a alterar. Após confirmação, o sistema modifica os dados da permissão com a informação indicada pelo actor, mostrando-a, de imediato, na lista de permissões de acesso (a espaços físicos) do papel.

Caso de Uso: Eliminar Permissões do Papel

Descrição: Este caso de uso inicia-se quando o actor, após ter seleccionado um papel da listagem de papéis e, através da selecção do botão correspondente, solicita a eliminação de permissões (a espaços físicos) do papel. O sistema disponibiliza uma listagem das permissões de acesso (a espaços físicos) do papel seleccionado. O actor deve seleccionar, através do botão correspondente, a permissão a eliminar. Após confirmação, o sistema elimina, de imediato, a permissão (ao espaço físico e seus descendentes hierárquicos) da lista de permissões (a espaços físicos) do papel.

Caso de Uso: Lista Espaços para Permissões do Papel

Descrição: Este caso de uso inicia-se quando o actor solicita a inserção de permissões (a espaços físicos) a um papel seleccionado. O sistema disponibiliza uma listagem dos espaços físicos cujo papel não confere ou dá permissão de acesso.

Caso de Uso: Lista Permissões do Papel

Descrição: Este caso de uso inicia-se quando o actor solicita a inserção, a modificação ou a remoção de permissões (a espaços físicos) dum papel seleccionado. O sistema disponibiliza uma listagem das permissões de acesso (a espaços físicos) desse papel.

Caso de Uso: Consultar Papéis

Descrição: Este caso de uso inicia-se quando o actor solicita a edição de permissões (a espaços físicos) de papéis. O sistema possibilita que o actor pesquise e selecione um papel de uma lista de papéis que lhe é apresentada, podendo ser ordenada por vários atributos do papel (identificação, descrição,...).

B.4 – Auditar/Pesquisar Acessos e Presenças

Caso de Uso: Auditar Acessos de Utilizadores

Actores: Administrador da aplicação *WebGPACS*, sendo este o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende auditar os acessos (fluxos de entrada/saída) a espaços físicos controlados efectuados por um utilizador. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...), permitindo ao actor pesquisar e seleccionar cada um desses utilizadores. Para o utilizador seleccionado e depois de assinaladas duas datas (início e fim), o sistema disponibiliza ao actor uma listagem dos acessos aos espaços físicos (com a identificação, do espaço físico, do tipo de acesso – entrada/saída, da data e hora de entrada ou saída,...) efectuados pelo utilizador entre as datas assinaladas.

Caso de Uso: Consultar Utilizadores

Descrição: Este caso de uso inicia-se quando o actor solicita a auditoria de acessos de utilizadores ou a pesquisa/localização, em tempo real, de presenças de utilizadores. O sistema possibilita que o actor pesquise e seleccione um utilizador de uma lista de utilizadores que lhe é apresentada, podendo ser ordenada por vários atributos do utilizador (número de identificação, nome,...).

Caso de Uso: Auditar Acessos a Espaços

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende auditar os acessos (fluxos de entrada/saída) de utilizadores efectuados a um espaço físico controlado. O sistema invoca então a consulta de espaços, produzindo uma listagem da hierarquia de espaços físicos controlados pelo sistema, permitindo ao actor pesquisar e seleccionar cada um desses espaços físicos. Para o espaço físico seleccionado e depois de assinaladas duas datas (início e fim), o sistema disponibiliza ao actor uma listagem dos acessos dos utilizadores (com a identificação do utilizador, do tipo de acesso – entrada/saída, da data e hora de entrada ou saída,...) efectuados ao espaço entre as datas assinaladas.

Caso de Uso: Consultar Espaços

Descrição: Este caso de uso inicia-se quando o actor solicita a auditoria de acessos a espaços ou a pesquisa de presenças de utilizadores, em tempo real, em espaços físicos controlados. O sistema possibilita que o actor pesquise e selecione um espaço físico de uma listagem da hierarquia de espaços físicos controlados que lhe é apresentada.

Caso de Uso: Auditar Acessos a um Espaço por Utilizador

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor pretende auditar os acessos (fluxos de entrada/saída) a um espaço físico controlado efectuados por um utilizador. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...), permitindo ao actor pesquisar e seleccionar cada um desses utilizadores. Para o utilizador seleccionado, o sistema disponibiliza uma listagem da hierarquia de espaços físicos controlados sobre os quais o utilizador tem permissão de acesso, permitindo ao actor pesquisar e seleccionar cada um desses espaços físicos. Para o utilizador e espaço físico seleccionados e depois de assinaladas duas datas (início e fim), o sistema disponibiliza ao actor uma listagem dos acessos (com discriminação do tipo de acesso – entrada/saída, data e hora de entrada ou saída,...) efectuados ao espaço físico pelo utilizador entre as datas assinaladas.

Caso de Uso: Lista Espaços com Permissão ao Utilizador

Descrição: Este caso de uso inicia-se quando o actor solicita a auditoria dos acessos a um espaço físico controlado efectuados por um utilizador seleccionado. O sistema possibilita que o actor pesquise e selecione um espaço físico controlado de uma lista hierárquica de espaços físicos controlados sobre os quais o utilizador tem permissão de acesso.

Caso de Uso: Pesquisar / Localizar Presenças de Utilizadores (tempo real)

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a pesquisa ou a localização, em tempo real, da presença de um utilizador em espaços físicos controlados. O sistema invoca então a consulta de utilizadores, produzindo uma listagem de utilizadores que pode ser ordenada por diferentes atributos do utilizador (número de identificação, nome,...), permitindo ao actor pesquisar e seleccionar cada um desses utilizadores. Para o utilizador seleccionado, o sistema fornece ao actor a identificação do espaço físico em que se verifique a presença do utilizador, com a correspondente data e hora de entrada.

Caso de Uso: Consultar Presenças em Espaços (tempo real)

Actores: Administrador da aplicação *WebGPACS* e Gestor/Auditor de Espaços, sendo qualquer destes o actor iniciador do caso de uso.

Descrição: Este caso de uso inicia-se quando o actor solicita a consulta das presenças de utilizadores, em tempo real, num espaço físico controlado. O sistema invoca então a consulta de espaços, produzindo uma listagem da hierarquia de espaços físicos controlados pelo sistema, permitindo ao actor pesquisar e seleccionar cada um desses espaços físicos. Para o espaço físico seleccionado, o sistema disponibiliza ao actor uma listagem das presenças, em tempo real, dos utilizadores (com a identificação do utilizador, da data e hora de entrada,...).

Anexo C – Listagem Parcial do Código da Aplicação

Neste Anexo, é apresentada uma listagem parcial do código da aplicação *WebGPACS*, que contempla, apenas, a demonstração do código de duas funcionalidades:

- C.1 – “Editar Espaços (criar/insserir, modificar e eliminar)”
- C.2 – “Auditar Acessos a Espaço por Utilizador”

das várias desenvolvidas (ver secção §9.1 “Funcionalidades da Aplicação (Implementadas)”, pág.167).

C.1 – Código de “Editar Espaços (inserir, modificar, eliminar)”

iae_espacos.php

```
<?php

include("gera_pagina_ate_meio.php");

switch ($_SESSION['permit'])
{

    case (null || ($_SESSION['permit'] == "2")):
        echo "<p><br><br><br><br><br><br><br><br><center>
        <FONT class='h2' COLOR='#663300'>Não tem permissões para aceder a estes
        recursos<p>";
        break;

    case ($_SESSION['permit'] == "1"):
        include("espacos/iae_espacos1.php");
        break;

}

include("gera_fim.php");

?>
```

iae_espacos1.php

```
<SCRIPT language=Javascript>

function MouseSobre(numero,tip0,num_linhas) //
{
    if((tip0==1) && (num_linhas==0) && (numero==0)){
        indice=numero;
        document.images[indice+9].src = "espacos/inseriron.gif";
        document.images[indice+9].border = "0";
    }
    if((tip0==1) && (num_linhas>numero)){
        indice=numero+numero+numero;
        document.images[indice+9].src = "espacos/inseriron.gif";
    }
}
```

```

        document.images[indice+9].border = "0";
    }
    if((tipo==1) && (numero>=num_linhas) && ((2*num_linhas)>numero)){
        indice=(numero-num_linhas)*3+1;
        document.images[indice+9].src = "espacos/alteraron.gif";
        document.images[indice+9].border = "0";
    }
    if((tipo==1) && (numero>=(2*num_linhas))){
        indice=(numero-(2*num_linhas))*3+2;
        document.images[indice+9].src = "espacos/eliminaron.gif";
        document.images[indice+9].border = "0";
    }
}

function MouseFora(numero,tipo,num_linhas)
{
    if((tipo==1) && (num_linhas==0) && (numero==0)){
        indice=numero;
        document.images[indice+9].src = "espacos/inserirout.gif";
        document.images[indice+9].border = "0";
    }
    if((tipo==1) && (num_linhas>numero)){
        indice=numero+numero+numero;
        document.images[indice+9].src = "espacos/inserirout.gif";
        document.images[indice+9].border = "0";
    }
    if((tipo==1) && (numero>=num_linhas) && ((2*num_linhas)>numero)){
        indice=(numero-num_linhas)*3+1;
        document.images[indice+9].src = "espacos/alterarout.gif";
        document.images[indice+9].border = "0";
    }
    if((tipo==1) && (numero>=(2*num_linhas))){
        indice=(numero-(2*num_linhas))*3+2;
        document.images[indice+9].src = "espacos/eliminarout.gif";
        document.images[indice+9].border = "0";
    }
}

function validar(nodo,Identificacao_espaco,Flag)
{
    if (Flag == 'inserir')
    {
        var conf=confirm("Deseja mesmo Inserir um novo Espaço contido em "+nodo+" ?");
        if (conf)
        {
            alert("Preencha seguidamente os dados do novo Espaço a inserir em "+nodo+" ");
            submitOK="True"
        }
        else
        {
            alert("A Inserção do novo Espaço contido em "+nodo+" será Anulada !");
            submitOK="False"
        }
        if (submitOK=="False")
        {
            return false
        }
    }
    else
    {
        if (Flag == 'alterar')
        {
            var conf=confirm("Deseja mesmo Alterar o Espaço "+nodo+" ?");
            if (conf)
            {
                alert("Preencha seguidamente os novos dados do Espaço "+nodo+" ");
                submitOK="True"
            }
            else
            {

```

```

        alert("A Alteração do Espaço "+nodo+" será Anulada !");
        submitOK="False"
    }
    if (submitOK=="False")
    {
        return false
    }
}
else
{
    if (Flag == 'eliminar')
    {
        var conf=confirm("Deseja mesmo Eliminar o Espaço "+nodo+" ? \n\nNOTA:
            Ao eliminá-lo também eliminará todos os Espaços
            nele contidos, \ntodas as Permissões e Acessos
            respectivos !");

        if (conf)
        {
            alert("O Espaço "+nodo+" vai ser Eliminado, \nassim como todos
                os Espaços nele contidos, \ntodas as Permissões e Acessos
                respectivos");
            submitOK="True"
        }
        else
        {
            alert("A Eliminação do Espaço "+nodo+" será Anulada !");
            submitOK="False"
        }
        if (submitOK=="False")
        {
            return false
        }
    }
}
}

function validar_raiz(nodo)  <!-- Nota: Para o caso de tabela vazia (nodo raiz)-->
{
    var conf=confirm("Deseja mesmo Inserir um novo Espaço que será o nodo "+nodo+" ?");
    if (conf)
    {
        alert("Preencha seguidamente os dados do novo Espaço a inserir como nodo
            "+nodo+" ");
        submitOK="True"
    }
    else
    {
        alert("A Inserção do Espaço "+nodo+" será Anulada !");
        submitOK="False"
    }
    if (submitOK=="False")
    {
        return false
    }
}

</SCRIPT>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Gestão de Espaços (Inserir/Alterar/Eliminar)
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

include("ligabd_pedro.php");

```

```
$query = "SELECT node.esp_id, CONCAT(REPEAT('.',COUNT(parent.id_esp)-1),node.id_esp) AS
        id_esp, node.desc_esp, node.lft, node.rgt, node.tipo_esp, node.coordgeo_esp
        FROM espacos AS node, espacos AS parent
        WHERE node.lft BETWEEN parent.lft AND parent.rgt
        GROUP BY node.id_esp
        ORDER BY node.lft";

$result = mysql_db_query("dbname",$query);

$num_linhas = mysql_numrows($result);

if ($num_linhas > 0)
{
    /* Escrita do cabeçalho da tabela */
    echo "<CENTER>";

    echo "<TABLE class=\"comBordaSimples3\" width=1100><p>";
    echo "<TR>";
    <TH width=130><FONT class=\"h4_2\" color=\"Maroon\">Identificaç&#227o</FONT></TH>
    <TH><FONT class=\"h4_2\" color=\"Maroon\">Descr&#231&#227o</FONT></TH>
    <TH><FONT class=\"h4_2\" color=\"Maroon\">Tipo</FONT></TH>
    <TH><FONT class=\"h4_2\" color=\"Maroon\">Localização</FONT></TH>";
    echo "</TR>";

    $i = 0;
    $ii = $num_linhas;
    $iii = ($num_linhas+$num_linhas);
    while ($i < $num_linhas)
    {
        $linha = mysql_fetch_row($result);
        $nodo = ltrim($linha[1],"."); /* Nota: Para dar o argumento da função
                                     validar($nodo) em JavaScript */

        echo "<TR>";
        echo "<TD class=\"t_left\">".$linha[1].</TD>
        <TD class=\"t_left\">".$linha[2].</TD>
        <TD class=\"t_left\">".$linha[5].</TD>
        <TD class=\"t_left\">".$linha[6].</TD>

        <TD width=70 class=\"t_left\"><A
href=\"espacos/inserir/inserir_espacos2.php?Identificacao1=$linha[1]\" onclick=\"return
validar('$nodo','$linha[1]','inserir')\" onmouseover=\"MouseSobre($i,1,$num_linhas);\"
onmouseout=\"MouseFora($i,1,$num_linhas);\"><img src=\"espacos/inserirout.gif\" name
=\"$i\" border = \"none\"></TD>";

        echo "<TD width=70 class=\"t_left\"><A
href=\"espacos/alterar/modificar_espacos2.php?Identificacao1=$linha[1]\" onclick=\"return
validar('$nodo','$linha[1]','alterar')\" onmouseover=\"MouseSobre($ii,1,$num_linhas);\"
onmouseout=\"MouseFora($ii,1,$num_linhas);\"><img src=\"espacos/alterarout.gif\" name
=\"$i\" border = \"none\"></TD>";

        echo "<TD width=70 class=\"t_left\"><A
href=\"espacos/eliminar/eliminar_espacos2.php?Identificacao1=$linha[1]\" onclick=\"return
validar('$nodo','$linha[1]','eliminar')\" onmouseover=\"MouseSobre($iii,1,$num_linhas);\"
onmouseout=\"MouseFora($iii,1,$num_linhas);\"><img src=\"espacos/eliminarout.gif\" name
=\"$iii\" border = \"none\"></TD>";

        echo "</TR>";
        $i++;
        $ii++;
        $iii++;
    }
    echo "</TABLE>";

    echo "</Select><p>";
}
else
{
    echo"<FONT class=\"h3\">A TABELA DOS ESPAÇOS ESTÁ VAZIA !!!</FONT>";
    echo"<br><p>";
    echo"<FONT class=\"h3\">VAI TER QUE INSERIR UM 1º ESPAÇO QUE SERÁ O NODO
        RAÍZ</FONT>";
}
```

```

echo"<br><p>";
echo"<FONT class=\"h3\"> DE TODOS OS ESPAÇOS SUBSEQUENTES </FONT>";

$i = 0;
$num_linhas = 0;
$node = "Raiz";
$nodoraiz = "Nodo Raiz";
echo "<A href=\"espacos/inserir/inserir_espacos2.php?Identificacao1=$nodoraiz\"
      onclick=\"return validar_raiz('$node')\"
      onMouseOver=\"MouseSobre($i,1,$num_linhas);\"
      onMouseOut=\"MouseFora($i,1,$num_linhas);\">
      <img src=\"espacos/inserirout.gif\" name =\"$i\" border = \"none\">";

}

mysql_close();

?>

</form>

```

inserir_espacos2.php

```

<?php

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio.php");

?>

<script type="text/javascript">

function validar()
{
    var formulario = document.formulario

    var Identificacao = formulario.Identificacao.value

    var Descricao = formulario.Descricao.value

    var Tipo = formulario.Tipo.value

    var Coordenadas_geo = formulario.Coordenadas_geo.value

    var Estado = formulario.Estado.value

    var Presencas = formulario.Presencas.value

    var Num_unidades = formulario.Num_unidades.value

    var submitOK="True"

    if (!Identificacao)
    {
        alert("Deve preencher o campo Identificação !")
        submitOK="False"
    }
    if (!Descricao)
    {
        alert("Deve preencher o campo Descrição !")
        submitOK="False"
    }

    if (!Tipo)
    {
        alert("Deve preencher o campo Tipo !")
        submitOK="False"
    }

    if (!Coordenadas_geo)
    {

```

```

        alert("Deve preencher o campo Coordenadas Geo !")
        submitOK="False"
    }

    if (!Estado)
    {
        alert("Deve preencher o campo Estado !")
        submitOK="False"
    }

    if (!Presencas)
    {
        alert("Deve preencher o campo Presenças !")
        submitOK="False"
    }

    if (!Num_unidades)
    {
        alert("Deve preencher o campo N° de Unidades !")
        submitOK="False"
    }

    if (submitOK=="False")
    {
        return false
    }
}

</script>

<CENTER>

<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Inserir Espa&#231o
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

$Identificacao_espaco_referencia = ltrim($_GET['Identificacao1'], ".");

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

if ($Identificacao_espaco_referencia != 'Nodo Raiz')
{
    echo"<FONT class=\"h7\">O Novo Espa&#231o será incluído no Espa&#231o c/
        Identifica&#231&#227o: </FONT>
        <FONT color=\"Maroon\" class=\"h7\"> $Identificacao_espaco_referencia</FONT><p>";
}
else
{
    echo"<FONT class=\"h7\">O Novo Espa&#231o será o </FONT>
        <FONT color=\"Maroon\" class=\"h7\"> $Identificacao_espaco_referencia</FONT>
        <FONT class=\"h7\"> de todos os Espa&#231os</FONT><p>";
}

echo "<CENTER>";
echo "<TABLE class=\"comBordaSimples1\" width=330<p>";

    echo "<TR>";
        echo "<TH><FONT class=\"h4_2\" color=\"Maroon\">Atributos</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Dados do Espa&#231o</FONT></TH>";
    echo "</TR>";

    echo "<TR>";
        echo"<TD class=\"h4_2\">Identifica&#227o</TD>
        <TD><form method=post name =\"formulario\"action=\"inserir_espacos3.php\"
            onsubmit=\"return validar()\">
            <input type=text class=\"caixatexto\" length=\"10\" size=\"40\"

```

```

        name=\"Identificacao\" value = $Identificacao></input></TD>";
echo "</TR>";

echo "<TR>";
echo "<TD class=\"h4_2\">Descrição</TD>";
echo "<TD><form method=post name =\"formulario\"";
echo "    action=\"inserir_espacos3.php\" onsubmit=\"return validar()\">";
echo "    <input type=text class=\"caixatexto\" length=\"10\" size=\"40\"";
echo "    name=\"Descricao\" value = $Descricao></input></TD>";
echo "</TR>";

echo "<TR>";
echo "<TD class=\"h4_2\">Tipo</TD>";
echo "<TD><form method=post name =\"formulario\"";
echo "    action=\"inserir_espacos3.php\" onsubmit=\"return validar()\">";
echo "    <Select class=\"caixatexto\" name=\"Tipo\">";
echo "        <Option value = '\"'></Option>";
echo "$query = \"select * from tiposespacos ORDER BY tipo_esp\";";
echo "$result = mysql_db_query(\"dbname\", $query);";
echo "$num_linhas = mysql_numrows($result);";
echo "$i = 0;";
echo "while ($i < $num_linhas)";
echo "{";
echo "    $linha = mysql_fetch_row($result);";
echo "    echo \"<Option value='\"$linha[0]\">\".\"$linha[0].\"</Option><p>\";";
echo "    $i++;";
echo "    }";
echo "echo \"</Select>\"";
echo "</TD>\";";
echo "</TR>\";";

echo "<TR>\";";
echo "<TD class=\"h4_2\">Localização</TD>";
echo "<TD><form method=post name =\"formulario\" action=\"inserir_espacos3.php\"";
echo "    onsubmit=\"return validar()\">";
echo "    <input type=text class=\"caixatexto\" length=\"10\" size=\"40\"";
echo "    name=\"Coordenadas_geo\" value = $Coordenadas_geo></TD>\";";
echo "</TR>\";";

echo "<TR>\";";
echo "<TD class=\"h4_2\">Estado</TD>";
echo "<TD><form method=post name =\"formulario\" action=\"inserir_espacos3.php\"";
echo "    onsubmit=\"return validar()\">";
echo "    <Select class=\"caixatexto\" name=\"Estado\">";
echo "        <Option value = '\"'></Option>";
echo "        <option value=Aberto>Aberto</option>";
echo "        <option value=Fechado>Fechado</option>";
echo "    </Select>";
echo "</TD>\";";
echo "</TR>\";";

echo "<TR>\";";
echo "<TD class=\"h4_2\">Presenças</TD>";
echo "<TD><form method=post name =\"formulario\"";
echo "    action=\"inserir_espacos3.php\" onsubmit=\"return validar()\">";
echo "    <input type=text class=\"caixatexto\" length=\"10\" size=\"40\"";
echo "    name=\"Presencas\" value = $Presencas></TD>\";";
echo "</TR>\";";

echo "<TR>\";";
echo "<TD class=\"h4_2\">Nº de Unidades</TD>";
echo "<TD><form method=post name =\"formulario\" action=\"inserir_espacos3.php\"";
echo "    onsubmit=\"return validar()\">";
echo "    <input type=text class=\"caixatexto\" length=\"10\" size=\"40\"";
echo "    name=\"Num_unidades\" value = $Num_unidades></TD>\";";
echo "</TR>\";";

echo "</TABLE><p>\";

echo "<TABLE>\";
echo "<input type=\"hidden\" name=\"Identificacao_espaco_referencia\"";
echo "    value=\"\"$Identificacao_espaco_referencia\">\";";

```

```

echo"<td><input type = \"submit\" name=\"cmdsubmit\" class=\"buttons\"
    value=\"Submeter\"></input></td>";
echo"<td></td>";
echo "<td><input type=\"reset\" name=\"cmdcancelar\" class=\"buttons\"
    value=\"Cancelar\" ></input></td>";
echo "</TABLE><p>";

echo "</CENTER>";

echo "</Select><p></form>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'><a href=\"../../iae_espacos.php\">
<img src='botao_b.gif' name='botaol' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

?>

```

inserir_espacos3.php

```

<?php

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio.php");

?>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
<!-- Confirma&#231&#227o dos Valores Inseridos na Tabela Espa&#231os -->
Inserção de Espa&#231o
</b></FONT>
<!-- <HR size="5" width="80%" color="#663300"><p><br> -->
<HR size="2" width="60%" color="#663300">
<p>

<?php
echo"<CENTER>";

$Identificacao_espaco_referencia = $_POST['Identificacao_espaco_referencia']; /* Nota:
    Identificação do nodo pai (onde vai ser inserido o novo nodo) */
$Identificacao = $_POST['Identificacao'];
$Descricao = $_POST['Descricao'];
$Tipo = $_POST['Tipo'];
$Coordenadas_geo = $_POST['Coordenadas_geo'];
$Estado = $_POST['Estado'];
$Presencas = $_POST['Presencas'];
$Num_unidades = $_POST['Num_unidades'];

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

$i=0;
$query = "select * from espacos;";
$result = mysql_db_query("dbname",$query);
$num_linhas = mysql_numrows($result);

while ($i < $num_linhas)
{
    $linha = mysql_fetch_row($result);
    $resultado = $linha[1];
    if ($resultado == $Identificacao)
    {
        echo "<br><br><FONT class=\"h3\">A Identificaç&#227o <FONT class=\"h3\">
        <FONT color=\"Maroon\" class=\"h3\"> $Identificacao</FONT>
        <FONT class=\"h3\">do Espaço n&#227o pode ser inserida</FONT><p>
        <FONT color=\"Maroon\" class=\"h3\"><b>JÁ EXISTE !</b></FONT>";
    }
}

```

```

/* Introdução do botão "Voltar (Menu Anterior) */
echo"<tr><td width='100%' colspan='2' height='3'
    bgcolor='#ffffcc'><center><FONT class='h8' color='#aa0010'>
    <a href=\"../../iae_espacos.php\"> <img src='botao_b.gif'
    name='botaol' border='none' height=30 width=30 align='middle'>
    Voltar (Menu Anterior)</a></td></tr>";
include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");
echo"<meta http-equiv=\"refresh\" content=\"3;URL=../../iae_espacos.php\">";
exit();
}
$i++;
}

if ($Identificacao_espaco_referencia != 'Nodo Raiz')
{
    /**** 2ª FORMA ****/
    $query = "SELECT @myLeft := lft FROM espacos WHERE id_esp =
        '$Identificacao_espaco_referencia'";
    $result = mysql_db_query("dbname", $query);

    $query = "UPDATE espacos SET rgt = rgt+2 WHERE rgt > @myLeft;";
    $result = mysql_db_query("dbname", $query);

    $query = "UPDATE espacos SET lft = lft+2 WHERE lft > @myLeft;";
    $result = mysql_db_query("dbname", $query);

    $query = "INSERT INTO espacos(id_esp, desc_esp, lft, rgt, tipo_esp, coordgeo_esp,
        estado_esp, presencas_esp, numunid_esp)
        VALUES('$Identificacao', '$Descricao', @myLeft+1, @myLeft+2, '$Tipo',
        '$Coordenadas_geo', '$Estado', '$Presencas', '$Num_unidades')";
}
else
{
    $lft = '1';
    $rgt = '2';
    $query = "INSERT INTO espacos(id_esp, desc_esp, lft, rgt, tipo_esp, coordgeo_esp,
        estado_esp, presencas_esp, numunid_esp)
        VALUES('$Identificacao', '$Descricao', '$lft', '$rgt', '$Tipo',
        '$Coordenadas_geo', '$Estado', '$Presencas', '$Num_unidades')";
}

$result = mysql_db_query("dbname", $query);

if ($result)
{
    echo "<br><FONT class=\"h3\">Os valores foram inseridos com Sucesso !</FONT><p>";

    echo "<TABLE class=\"comBordaSimples\" width=1100><p>";
    echo "<TR>";
    echo "<TH width=5%><FONT class=\"h4_2\"
        color=\"Maroon\">Identificaç&#227o</FONT></TH>
        <TH width=30%><FONT class=\"h4_2\"
        color=\"Maroon\">Descri&#231&#227o</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Tipo</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Localização</FONT></TH>
        <TH width=5%><FONT class=\"h4_2\" color=\"Maroon\">Estado</FONT></TH>
        <TH width=5%><FONT class=\"h4_2\"
        color=\"Maroon\">Presen&#231as</FONT></TH>
        <TH width=9%><FONT class=\"h4_2\" color=\"Maroon\">Nº de
        Unidades</FONT></TH>";
    echo "</TR>";

    echo "<TR>";
    echo "<TD><FONT class=\"t_left\">$Identificacao</FONT></TD>
        <TD><FONT class=\"t_left\">$Descricao</FONT></TD>
        <TD><FONT class=\"t_left\">$Tipo</FONT></TD>
        <TD><FONT class=\"t_left\">$Coordenadas_geo</FONT></TD>
        <TD><FONT class=\"t_left\">$Estado</FONT></TD>
        <TD><FONT class=\"t_center\">$Presencas</FONT></TD>
        <TD><FONT class=\"t_center\">$Num_unidades</FONT></TD>";
    echo "</TR>";
}

```

```

echo"</TABLE><p>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
    <FONT class='h8' color='#aa0010'><a href=\"../../iae_espacos.php\">
    <img src='botao_b.gif' name='botaol' border='none' height=30 width=30
    align='middle'> Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

echo"<meta http-equiv=\"refresh\" content=\"3;URL=../../iae_espacos.php\">";

exit();
}

echo "<FONT class=\"h3\">Erro na Inser&#231&#227o</FONT><p><br>";

echo "</Select><br></form>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'><a href=\"../../iae_espacos.php\">
<img src='botao_b.gif' name='botaol' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

echo"<meta http-equiv=\"refresh\" content=\"3;URL=../../iae_espacos.php\">";

?>

</form>

```

modificar_espacos2.php

```

<?php

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio.php");

?>

<script type="text/javascript">

    function validar()
    {
        var formulario = document.formulario

        var identificacao = formulario.identificacao.value

        var descricao = formulario.descricao.value

        var tipo = formulario.tipo.value

        var coordenadas_geo = formulario.coordenadas_geo.value

        var estado = formulario.estado.value

        var presencas = formulario.presencas.value

        var num_unidades = formulario.num_unidades.value

        var submitOK="True"

        if (!identificacao)
        {

```

```

        alert("Deve preencher o campo Identificação!!")
        submitOK="False"
    }
    if (!descricao)
    {
        alert("Deve preencher o campo Descrição!!")
        submitOK="False"
    }

    if (!tipo)
    {
        alert("Deve preencher o campo Tipo!!")
        submitOK="False"
    }

    if (!coordenadas_geo)
    {
        alert("Deve preencher o campo Coordenadas Geo!!")
        submitOK="False"
    }

    if (!estado)
    {
        alert("Deve preencher o campo Estado!!")
        submitOK="False"
    }

    if (!presencas)
    {
        alert("Deve preencher o campo Presenças!!")
        submitOK="False"
    }

    if (!num_unidades)
    {
        alert("Deve preencher o campo N° de Unidades!!")
        submitOK="False"
    }

    if (submitOK=="False")
    {
        return false
    }
}

</script>

<CENTER>

<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Alterar Espa&#231o
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

$Identificacao_espaco = ltrim($_GET['Identificacao1'],".");

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<FONT class=\"h7\">Identifica&#231&#227o do Espa&#231o a Alterar: </FONT>
<FONT color=\"Maroon\" class=\"h7\"> $Identificacao_espaco</FONT><p>";

echo"<CENTER>";

echo "<TABLE class=\"comBordaSimples1\" width=600<p>

<TR>
<TH><FONT class=\"h4_2\" color=\"Maroon\">Atributos</FONT></TH>

```

```

        <TH width=40%><FONT class=\"h4_2\" color=\"Maroon\">Dados actuais</FONT></TH>
        <TH width=40%><FONT class=\"h4_2\" color=\"Maroon\">Novos Dados</FONT></TH>
    </TR>

    <TR>
        <TD class=\"h4_2\">Identifica&#231&#227o</TD>
        <TD class=\"t_left\">{$Identificacao_espaco}</TD>
        <TD>
            <form name =\"formulario\" method=post action=\"modificarespacos3.php\"
                onsubmit=\"return validar()\">
                <input type=text class=\"caixatexto\" length=\"10\" size=\"35\"
                    name=\"identificacao\" value = '{$Identificacao_espaco}'>
            </TD>
        </TR>;

    $query = "SELECT * FROM espacos WHERE id_esp = '{$Identificacao_espaco}';";
    $result = mysql_db_query("dbname", $query);
    $row = mysql_fetch_row($result);

    echo"<TR>
        <TD class=\"h4_2\">Descri&#231&#227o</TD>
        <TD class=\"t_left\">".$row[2]."</TD>";
        $resultado = $row[2];
        echo"<TD>
            <form method=post action=\"modificarespacos3.php\"
                <input type=text class=\"caixatexto\" length=\"10\" size=\"35\"
                    name=\"descricao\"value = '{$resultado}'>
            </TD>
        </TR>";

    echo"<TR>
        <TD class=\"h4_2\">Tipo</TD>
        <TD class=\"t_left\">".$row[5]."</TD>";
        $resultado = $row[5];
        echo"<TD>
            <form name =\"formulario\" method=post action=\"modificarespacos3.php\"
                onsubmit=\"return validar()\">
                <Select class=\"caixatexto\" name=\"tipo\">;
                echo"<Option value='{$resultado}'>".$resultado."</Option>";
                /* Nota: Instrução Select que selecciona ordenadamente os diferentes
                Tipos de Espaços, excepto o seleccionado por $resultado (o visível, o 1º
                do menu dropdown) */
                $query1 = "SELECT * FROM tiposespacos
                    WHERE tipo_esp != '{$resultado}'
                    ORDER BY tipo_espt";
                $result1 = mysql_db_query("dbname", $query1);
                $num_linhas1 = mysql_numrows($result1);
                $ii = 0;
                while ($ii < $num_linhas1)
                {
                    $linha1 = mysql_fetch_row($result1);
                    echo "<Option value='{$linha1[0]}'>".$linha1[0]."</Option><p>";
                    $ii++;
                }
                echo "</Select>
            </TD>
        </TR>";

    echo"<TR>
        <TD class=\"h4_2\">Localização</TD>
        <TD class=\"t_left\">".$row[6]."</TD>";
        $resultado = $row[6];
        echo"<TD>
            <form name =\"formulario\" method=post action=\"modificarespacos3.php\"
                onsubmit=\"return validar()\">
                <input type=text class=\"caixatexto\" length=\"10\" size=\"35\"
                    name=\"coordenadas_geo\" value = '{$resultado}'>
            </TD>
        </TR>";

    echo"<TR>
        <TD class=\"h4_2\">Estado</TD>

```

```

<TD class="t_left">".$row[7]."</TD>";
$resultado = $row[7];
echo"<TD>
    <form name =\"formulario\" method=post action= \"modificarespacos3.php\"
        onsubmit= \"return validar()\">
    <Select class= \"caixatexto\" name= \"estado\">";
    echo"<Option value= '$resultado'>".$resultado."</Option>";
    if (" $resultado"=="Aberto")
    {
        echo"<option value=Fechado>Fechado</option>";
    }
    else
    {
        echo"<option value=Aberto>Aberto</option>";
    }
    echo"</Select>
</TD>
</TR>";

echo"<TR>
<TD class= \"h4_2\">Presen&#231as</TD>
<TD class= \"t_left\">".$row[8]."</TD>";
$resultado = $row[8];
echo"<TD>
    <form name =\"formulario\" method=post action= \"modificarespacos3.php\"
        onsubmit= \"return validar()\">
    <input type=text class= \"caixatexto\" length= \"10\" size= \"35\"
        name= \"presencas\" value = '$resultado'>
</TD>
</TR>";

echo"<TR>
<TD class= \"h4_2\">N° de Unidades</TD>
<TD class= \"t_left\">".$row[9]."</TD>";
$resultado = $row[9];
echo"<TD>
    <form name =\"formulario\" method=post action= \"modificarespacos3.php\"
        onsubmit= \"return validar()\">
    <input type=text class= \"caixatexto\" length= \"10\" size= \"35\"
        name= \"num_unidades\" value = '$resultado'>
</TD>
</TR>";

echo"</TABLE><p>
    <form method=post action= \"modificarespacos3.php\">
    <input type= \"hidden\" name= \"identificacao_original\"
        value= \" $Identificacao_espaco\">
    <input type= \"submit\" class= \"buttons\" value= \"Submeter\"></input>
    </form>

    </CENTER>

    <p><br><br>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'><a href= \"../iae_espacos.php\">
<img src='botao_b.gif' name='botao1' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

?>

```

modificarespacos3.php

<?php

```

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio.php");

?>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
<!-- Resultado da Altera&#231&#227o &#224 Tabela Espa&#231os -->
Altera&#231&#227o do Espa&#231o
</b></FONT>
<HR size="2" width="60%" color="#663300">

<?php

$identificacao_original = $_POST['identificacao_original'];

$identificacao = $_POST['identificacao'];
$descricao = $_POST['descricao'];
$tipo = $_POST['tipo'];
$coordenadas_geo = $_POST['coordenadas_geo'];
$estado = $_POST['estado'];
$presencas = $_POST['presencas'];
$num_unidades = $_POST['num_unidades'];

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<CENTER>";

switch ($identificacao)
{
    case $identificacao_original: /*Vai-se alterar o registo existente, sem mudar a
                                   identificação*/

        $query = "UPDATE espacos SET id_esp = '$identificacao',desc_esp = '$descricao',
                                   tipo_esp = '$tipo', coordgeo_esp = '$coordenadas_geo', estado_esp =
                                   '$estado', presencas_esp = '$presencas', numunid_esp =
                                   '$num_unidades'
                                   WHERE id_esp = '$identificacao_original'";

        $result = mysql_db_query("dbname",$query);
        if ($result)
        {
            echo "<P><FONT class=\"h3\">Altera&#231&#227o sem mudar a Identifica&#231&#227o
                    efectuada com sucesso !</font>";

            include("tab_val_alt4_7.php");

            echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
            <FONT class='h8' color='#aa0010'>
            <a href='modificar_espacos2.php?Identificacaol=$identificacao_original'>
            <img src='botao_b.gif' name='botaol' border='none' height=30 width=30
            align='middle'> Voltar (Menu Anterior)</a></td></tr>";

            include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

            echo"<meta http-equiv=\"refresh\"
            content=\"3;URL=modificar_espacos2.php?Identificacaol=$identificacao_original\"";
            exit();
        }

        echo "<FONT class=\"h3\">Erro na Altera&#231&#227o</FONT><p><br>";

        echo"<meta http-equiv=\"refresh\"
        content=\"3;URL=modificar_espacos2.php?Identificacaol=$identificacao_original\"";

        break;

    default: /*Vai-se alterar também o código, mas é preciso verificar se o código já
              existe*/
        $i=0;
        $query = "SELECT * FROM espacos "; /* vou ver se a identificação existe*/

```

```

$result = mysql_db_query("dbname",$query);
$rows = mysql_numrows($result);

while ($i < $rows)
{
    $row = mysql_fetch_row($result);
    $resultado = $row[1]; /* Nota: $row[1] e não $row[0] Porque a identificação do
                           espaço está na 2ª linha */
    if ($resultado == $identificacao)
    {
        echo "<br><br><FONT class=\"h3\">A Identifica&#231&#227o <FONT color=\"Maroon\"
              class=\"h3\">$identificacao</FONT>
              <FONT class=\"h3\"> n&#227o pode ser alterada</FONT><p>
              <FONT color=\"Maroon\" class=\"h3\"><b>JÁ EXISTE !</b></FONT>";

        /* Introdução do botão "Voltar (Menu Anterior) */
        echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
        <FONT class='h8' color='#aa0010'>
        <a href='modificar_espacos2.php?Identificacao1=$identificacao_original'>
        <img src='botao_b.gif' name='botao1'border='none' height=30 width=30
        align='middle'> Voltar (Menu Anterior)</a></td></tr>";

        echo"<meta http-equiv=\"refresh\"
        content=\"3;URL=modificar_espacos2.php?Identificacao1=$identificacao_original\">";
        exit();
    }

    $i++;
}

$query = "UPDATE espacos SET id_esp = '$identificacao',desc_esp = '$descricao',
        tipo_esp = '$tipo', coordgeo_esp = '$coordenadas_geo',
        estado_esp = '$estado', presencas_esp = '$presencas',
        numunid_esp = '$num_unidades'
        WHERE id_esp = '$identificacao_original'";

$result = mysql_db_query("dbname",$query);
if ($result)
{
    echo "<p><FONT class=\"h3\">Altera&#231&#227o efectuada com sucesso !</FONT>";
    include("tab_val_alt4_7.php");

    /* Para Integridade Referencial */
    $query = "UPDATE permissoes SET id_esp = '$identificacao'
        WHERE id_esp = '$identificacao_original'";
    $result = mysql_db_query("dbname",$query);

    $query = "UPDATE log_acessos SET id_esp = '$identificacao'
        WHERE id_esp = '$identificacao_original'";
    $result = mysql_db_query("dbname",$query);
}

}

echo"</CENTER>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'>
<a href='modificar_espacos2.php?Identificacao1=$identificacao'> <img src='botao_b.gif'
name='botao1' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

echo"<meta http-equiv=\"refresh\"
content=\"3;URL=modificar_espacos2.php?Identificacao1=$identificacao\">";

?>

```

tab_val_alt4_7.php

```
<?php
echo "<p>";
echo "<TABLE class=\"comBordaSimples\" width=400><p>
    <TR><TH width=30%><FONT class=\"h4_2\" color=\"Maroon\">Atributos</FONT></TH>
    <TH><FONT class=\"h4_2\" color=\"Maroon\">Novos Dados</FONT></TH>
    </TR>";

    echo"<TR><TD class=\"h4_2\">Identifica&#231&#227o</TD>
        <TD class=\"t_left\">$identificacao</TD>
        </TR>
        <TR><TD class=\"h4_2\">Descri&#231&#227o</TD>
        <TD class=\"t_left\">$descricao</TD>
        </TR>
        <TR><TD class=\"h4_2\">Tipo</TD>
        <TD class=\"t_left\">$tipo</TD>
        </TR>
        <TR><TD class=\"h4_2\">Localização</TD>
        <TD class=\"t_left\">$coordenadas_geo</TD>
        </TR>
        <TR><TD class=\"h4_2\">Estado</TD>
        <TD class=\"t_left\">$estado</TD>
        </TR>
        <TR><TD class=\"h4_2\">Presen&#231as</TD>
        <TD class=\"t_left\">$presencas</TD>
        </TR>
        <TR><TD class=\"h4_2\">Nº de Unidades</TD>
        <TD class=\"t_left\">$num_unidades</TD>
        </TR>
    </TR>";
echo"</TABLE><p>";

?>
```

eliminar_espacos2.php

```
<?php
include("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio.php");

?>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
<!-- Resultado da Elimina&#231&#227o na Tabela Espa&#231os -->
Elimina&#231&#227o do Espa&#231o
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

$Identificacao_espaco = ltrim($_GET['Identificacao1'],"."); /* Nota: Identificação do
                                                                nodo a ser eliminado */
include("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

/* Eliminação de um nodo e de todos os seus filhos */
$query = "SELECT @myLeft := lft, @myRight := rgt, @myWidth := rgt-lft+1
FROM espacos
WHERE id_esp = '$Identificacao_espaco'";
$result = mysql_db_query("dbname",$query);

/* Nota: Gera a tabela com o espaço a eliminar e todos os espaços nele contidos */
$query = "SELECT * FROM espacos WHERE lft BETWEEN @myLeft AND @myRight ORDER BY
espacos.lft;";
$result = mysql_db_query("dbname",$query);
```

```

$num_linhas = mysql_numrows($result);

if ($num_linhas > 0)
{
    /* Escrita do cabeçalho da tabela */
    echo "<CENTER>";

    echo "<br><FONT class=\"h3\">O Espaço com a Identificação <FONT class=\"h3\">
        <FONT color=\"Maroon\" class=\"h3\"> $Identificacao_espaco</FONT>
        <FONT class=\"h3\"> foi ELIMINADO !</FONT><p>";

    echo "<TABLE class=\"comBordaSimples1\" width=1100><p>";

    echo "<TR>";
    echo "<TH><FONT class=\"h4_2\" color=\"Maroon\">Identificação</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Descrição</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Tipo</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Localização</FONT></TH>";
    echo "</TR>";

    $i = 0;
    while ($i < $num_linhas)
    {
        $linha = mysql_fetch_row($result);
        echo "<TR>";
        echo "<TD class=\"t_left\">".$linha[1].</TD>
            <TD class=\"t_left\">".$linha[2].</TD>
            <TD class=\"t_left\">".$linha[5].</TD>
            <TD class=\"t_left\">".$linha[6].</TD>";
        echo "</TR>";

        /* Para Integridade Referencial */
        $Identificacao_espaco_eliminar = ltrim($linha[1]); /* NOTA: Identificação do
            espaço a eliminar nas tabelas permissoes e log_acessos */
        $query1 = "DELETE FROM permissoes WHERE id_esp =
            $Identificacao_espaco_eliminar";
        $result1 = mysql_db_query("dbname", $query1);

        $query2 = "DELETE FROM log_acessos WHERE id_esp =
            '$Identificacao_espaco_eliminar'";
        $result2 = mysql_db_query("dbname", $query2);
        $i++;
    }

    echo "</TABLE>";

    echo "</Select><p><br>";
    echo "<FONT color=\"Maroon\" class=\"h3\"><b>Nota: </b></FONT>
        <FONT class=\"h3\">Também foram eliminados todos os Espaços 'incluídos' em
        </FONT> <FONT color=\"Maroon\" class=\"h3\"> $Identificacao_espaco</FONT><p>";
}
else
{
    echo "<br><br><FONT class=\"h3\">O Espaço a eliminar com a Identificação
        <FONT class=\"h3\">
        <FONT color=\"Maroon\" class=\"h3\"> $Identificacao_espaco</FONT><p>
        <FONT color=\"Maroon\" class=\"h3\"> NÃO EXISTE !</FONT>";
}

/* Eliminação de um nodo e de todos os seus filhos (continuação) */
$query = "DELETE FROM espacos WHERE lft BETWEEN @myLeft AND @myRight;";
$result = mysql_db_query("dbname", $query);

$query = "UPDATE espacos SET rgt = rgt-@myWidth WHERE rgt > @myRight;";
$result = mysql_db_query("dbname", $query);

$query = "UPDATE espacos SET lft = lft-@myWidth WHERE lft > @myRight;";
$result = mysql_db_query("dbname", $query);

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */

```

```
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'><a href=\"../../iae_espacos.php\">
<img src='botao_b.gif' name='botao1' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

?>
```

C.2 – Código de “Auditar Acessos a um Espaço por Utilizador”

c_acessos_utilizador_espaco.php

```
<?php

include("gera_pagina_ate_meio.php");

include("acessos_utilizador_espaco/listar/c_acessos_utilizador_espaco1.php");

include("gera_fim.php");

?>
```

c_acessos_utilizador_espaco1.php

```
<SCRIPT language=Javascript>

function MouseSobre(numero,tipo) //
{
    if(tipo==1){
        document.images[numero+9].src = "acessos_utilizador_espaco/listar/consultaron.gif";
        document.images[numero+9].border = "0";
    }
}

function MouseFora(numero, tipo)
{
    if(tipo==1){
        document.images[numero+9].src = "acessos_utilizador_espaco/listar/consultarout.gif";
        document.images[numero+9].border = "0";
    }
}

</SCRIPT>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Consultar Acessos dum Utilizador a um Espaço
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

include("ligabd_pedro.php");

/* Nota: Para ordenar pelos títulos das diferentes colunas das tabelas */
$Flag_Ordenacao = $_GET['Flag_Ordenacao'];
if ($Flag_Ordenacao == 'Nome')
{
    $query = "SELECT * FROM utilizadores ORDER BY nome_utiliz;";
}
else
{
    $query = "SELECT * FROM utilizadores ORDER BY id_utiliz;";
}

$result = mysql_db_query("dbname",$query);

$num_linhas = mysql_numrows($result);

if ($num_linhas > 0)
```

```
{
    echo "<CENTER>";

    echo "<TABLE class=\"comBordaSimples3\" width=500><p>";
        echo "<TR>";
            echo "<ul id='menuver'>";
                echo "<TH width=90>";
                    <a href=\"c_acessos_utilizador_espaco.php?Flag_Ordenacao=Identificacao\"
                    title='Ordenar por Identificação' ><FONT class=\"h4_2\" color=\"Maroon\">
                    Identificação </FONT></a></TH>
                    <TH><a href=\"c_acessos_utilizador_espaco.php?Flag_Ordenacao=Nome\"
                    title='Ordenar por Nome'><FONT class=\"h4_2\" color=\"Maroon\"> Nome
                    </FONT></a></TH>
                    <TH width=70 colspan='3'><FONT class=\"h4_2\"
                    color=\"Maroon\">Espaços</FONT></TH>";
                echo "</ul>";
            echo "</TR>";

    $i = 0;
    while ($i < $num_linhas)
    {
        $linha = mysql_fetch_row($result);

        echo "<TR>";
            echo "<TD class=\"t_left\">".$linha[0].</TD>";
            <TD class=\"t_left\">".$linha[1].</TD>";
            <TD class=\"t_center\"><a
href=\"acessos_utilizador_espaco/listar/c_acessos_utilizador_espaco2.php?Identificacao1=
$linha[0]&onmouseover=\"MouseSobre($i,1);&onmouseout=\"MouseFora($i,1);&\">
<img src=\"acessos_utilizador_espaco/listar/consultarout.gif\" name =\"$i\" border =
\"none\">
                </TD>";
            echo "</TR>";

            $i++;
        }

        echo "</TABLE>";

        echo "</Select><p><br><br>";
    }
    else
    {
        echo"<FONT class=\"h3\">A TABELA DOS UTILIZADORES ESTÁ VAZIA !!!</FONT>";
        echo"<br><p>";
        echo"<FONT class=\"h3\">NÃO EXISTEM UTILIZADORES PARA SE CONSULTAREM OS SEUS
        ACESSOS</FONT>";
        echo"<br><p>";
    }
}

mysql_close();

?>

</form>
```

c_acessos_utilizador_espaco2.php

```
<?php

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio_sem_login.php");

?>

<meta http-equiv="content-type" content="text/xml; charset=iso-8859-1" />

<link rel="stylesheet" type="text/css" media="all" href="skins/aqua/theme.css"
title="Aqua" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-blue.css"
title="winter" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-blue2.css"
      title="blue" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-brown.css"
      title="summer" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-green.css"
      title="green" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-1.css"
      title="win2k-1" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-2.css"
      title="win2k-2" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-cold-
1.css" title="win2k-cold-1" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-cold-
2.css" title="win2k-cold-2" />
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-system.css"
      title="system" />

<!-- import the calendar script -->
<script type="text/javascript" src="calendar.js"></script>

<!-- import the language module -->
<script type="text/javascript" src="lang/calendar-en.js"></script>

<!-- other languages might be available in the lang directory; please check
your distribution archive. -->

<!-- helper script that uses the calendar -->
<script type="text/javascript">

var oldLink = null;
// code to change the active stylesheet
function setActiveStyleSheet(link, title) {
  var i, a, main;
  for(i=0; (a = document.getElementsByTagName("link")[i]); i++) {
    if(a.getAttribute("rel").indexOf("style") != -1 && a.getAttribute("title")) {
      a.disabled = true;
      if(a.getAttribute("title") == title) a.disabled = false;
    }
  }
  if (oldLink) oldLink.style.fontWeight = 'normal';
  oldLink = link;
  link.style.fontWeight = 'bold';
  return false;
}

// This function gets called when the end-user clicks on some date.
function selected(cal, date) {
  cal.sel.value = date; // just update the date in the input field.
  if (cal.dateClicked && (cal.sel.id == "sel1" || cal.sel.id == "sel3"))
    // if we add this call we close the calendar on single-click.
    // just to exemplify both cases, we are using this only for the 1st
    // and the 3rd field, while 2nd and 4th will still require double-click.
    cal.callCloseHandler();
}

// And this gets called when the end-user clicks on the _selected_ date,
// or clicks on the "Close" button. It just hides the calendar without
// destroying it.
function closeHandler(cal) {
  cal.hide(); // hide the calendar
  // cal.destroy();
  _dynarch_popupCalendar = null;
}

// This function shows the calendar under the element having the given id.
// It takes care of catching "mousedown" signals on document and hiding the
// calendar if the click was outside.
function showCalendar(id, format, showsTime, showsOtherMonths) {
  var el = document.getElementById(id);
  if (_dynarch_popupCalendar != null) {
    // we already have some calendar created
    _dynarch_popupCalendar.hide(); // so we hide it first.
  }
}
```

```

    } else {
        // first-time call, create the calendar.
        var cal = new Calendar(1, null, selected, closeHandler);
        // uncomment the following line to hide the week numbers
        // cal.weekNumbers = false;
        if (typeof showsTime == "string") {
            cal.showsTime = true;
            cal.time24 = (showsTime == "24");
        }
        if (showsOtherMonths) {
            cal.showsOtherMonths = true;
        }
        _dynarch_popupCalendar = cal; // remember it in the global var
        cal.setRange(1900, 2070); // min/max year allowed.
        cal.create();
    }
    _dynarch_popupCalendar.setDateFormat(format); // set the specified date format
    _dynarch_popupCalendar.parseDate(el.value); // try to parse the text in field
    _dynarch_popupCalendar.sel = el; // inform it what input field we use

    // the reference element that we pass to showAtElement is the button that
    // triggers the calendar. In this example we align the calendar bottom-right
    // to the button.
    _dynarch_popupCalendar.showAtElement(el.nextSibling, "Br"); // show the calendar

    return false;
}

var MINUTE = 60 * 1000;
var HOUR = 60 * MINUTE;
var DAY = 24 * HOUR;
var WEEK = 7 * DAY;

// If this handler returns true then the "date" given as
// parameter will be disabled. In this example we enable
// only days within a range of 10 days from the current
// date.
// You can use the functions date.getFullYear() -- returns the year
// as 4 digit number, date.getMonth() -- returns the month as 0..11,
// and date.getDate() -- returns the date of the month as 1..31, to
// make heavy calculations here. However, beware that this function
// should be very fast, as it is called for each day in a month when
// the calendar is (re)constructed.
function isDisabled(date) {
    var today = new Date();
    return (Math.abs(date.getTime() - today.getTime()) / DAY) > 10;
}

function flatSelected(cal, date) {
    var el = document.getElementById("preview");
    el.innerHTML = date;
}

function showFlatCalendar() {
    var parent = document.getElementById("display");

    // construct a calendar giving only the "selected" handler.
    var cal = new Calendar(0, null, flatSelected);

    // hide week numbers
    cal.weekNumbers = false;

    // We want some dates to be disabled; see function isDisabled above
    cal.setDisabledHandler(isDisabled);
    cal.setDateFormat("%A, %B %e");

    // this call must be the last as it might use data initialized above; if
    // we specify a parent, as opposite to the "showCalendar" function above,
    // then we create a flat calendar -- not popup. Hidden, though, but...
    cal.create(parent);

    // ... we can show it here.

```

```
        cal.show();
    }

function MouseSobre(numero,tipo) //
{
    if(tipo==1){
        document.images[numero+9].src = "consultaron.gif";
        document.images[numero+9].border = "0";
    }
}

function MouseFora(numero, tipo)
{
    if(tipo==1){
        document.images[numero+9].src = "consultarout.gif";
        document.images[numero+9].border = "0";
    }
}

</script>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Consultar Acessos do Utilizador a um Espaço
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

$Identificacao_utilizador = $_GET['Identificacao1'];

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<FONT class=\"h7\">Identifica&#231&#227o do Utilizador: </FONT>
<FONT color=\"Maroon\" class=\"h7\"> $Identificacao_utilizador</FONT><p>";

echo"<CENTER>";

echo " <TABLE class=\"comBordaSimples2\" width=400><p>

    <TR>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Atributos</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Dados do Utilizador</FONT></TH>
    </TR>

    <TR>
        <TD><FONT class=\"h4_2\">Identifica&#231&#227o</FONT></TD>
        <TD class=\"t_left\">$Identificacao_utilizador</TD>
    </TR>";

    $query = "SELECT * FROM utilizadores WHERE id_utiliz =
        '$Identificacao_utilizador';"; Instrução SELECT
    $result = mysql_db_query("dbname",$query);
    $row = mysql_fetch_row($result);

    echo"<TR>
        <TD class=\"h4_2\">Nome</TD>
        <TD class=\"t_left\">".$row[1]."</TD>";
    echo"</TR>";

echo"</TABLE> <BR>

</CENTER>";

$Identificacao_utilizador = $_GET['Identificacao1'];

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<FONT class=\"h7\">Espaços a que o Utilizador </FONT>
<FONT color=\"Maroon\" class=\"h7\"> $Identificacao_utilizador</FONT>
```

```

        <FONT class=\ "h7\">tem acesso (ou permissão) </FONT><p>;

$query = "SELECT DISTINCT espacos.esp_id, espacos.id_esp, espacos.desc_esp, espacos.lft,
        espacos.rgt, espacos.tipo_esp, espacos.coordgeo_esp
        FROM papeis_utilizadores, papeis, permissoes, espacos
        WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
              AND papeis_utilizadores.id_papel = papeis.id_papel
              AND papeis.id_papel = permissoes.id_papel
              AND permissoes.id_esp = espacos.id_esp
        ORDER BY espacos.lft;";

$result = mysql_db_query("dbname",$query);

$num_linhas = mysql_numrows($result);
$botao = 0; /* Nota: Variável que vai conter o nº de linhas ou botões a serem inseridos
                                                    no quadro */

if ($num_linhas > 0)
{
    echo "<form action=\"c_acessos_utilizador_espaco3.php\" method=post>"; /* Nota:
        instrução método post para os botões inserir e cancelar actuarem e tb.
        para se passar para a form c_acessos_utilizador_espaco3.php */

    echo "<CENTER>";

    echo "<TABLE class=\"comBordaSimples3\" width=1100><p>";

    echo "<TR>";
        echo "<TH width=130><FONT class=\"h4_2\"
            color=\"Maroon\">Identificaç&#227o</FONT></TH>
            <TH><FONT class=\"h4_2\" color=\"Maroon\">Descri&#231&#227o</FONT></TH>
            <TH><FONT class=\"h4_2\" color=\"Maroon\">Tipo</FONT></TH>
            <TH><FONT class=\"h4_2\" color=\"Maroon\">Localização</FONT></TH>
            <TH width=70><FONT class=\"h4_2\" color=\"Maroon\">Acessos</FONT></TH>";
    echo "</TR>";

    $num_linhas = mysql_numrows($result);
    $i = 0;
    while ($i < $num_linhas)
    {
        $linha = mysql_fetch_row($result);
        echo "<TR>";
            echo "<TD class=\"t_left\">".$linha[1]."</TD>
                <TD class=\"t_left\">".$linha[2]."</TD>
                <TD class=\"t_left\">".$linha[5]."</TD>
                <TD class=\"t_left\">".$linha[6]."</TD>
                <TD width=70 class=\"t_left\"><A
                href=\"c_acessos_utilizador_espaco3.php?Identificacao1=$linha[1]&#227o=$Identificacao_utilizador\" onclick=\"return validar()\"
                onmouseover=\"MouseSobre($i+$botao,1);\" onmouseout=\"MouseFora($i+$
                botao,1);\"><img src=\"consultarout.gif\" name =\"$i+$botao\"
                border = \"none\">
                </TD>";
            echo "</TR>";
            $i++;
        }

    echo"</TABLE><p>";

    echo "</CENTER>";

    echo "</form>"; /* Nota: fecha formulário ou instrução de método post */
}
else
{
    echo"<FONT color=\"Maroon\" class=\"h3\"><b>NÃO EXISTEM</b></FONT>";
}

    echo"<p>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */

```

```
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'><a href=\"../../c_acessos_utilizador_espaco.php\">
<img src='botao_b.gif' name='botao1' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";
```

```
include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");
```

```
?>
```

c_acessos_utilizador_espaco3.php

```
<?php
```

```
include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio_sem_login.php");
```

```
?>
```

```
<meta http-equiv="content-type" content="text/xml; charset=iso-8859-1" />
```

```
<link rel="stylesheet" type="text/css" media="all" href="skins/aqua/theme.css"
      title="Aqua" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-blue.css"
      title="winter" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-blue2.css"
      title="blue" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-brown.css"
      title="summer" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-green.css"
      title="green" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-1.css"
      title="win2k-1" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-2.css"
      title="win2k-2" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-cold-
1.css" title="win2k-cold-1" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-win2k-cold-
2.css" title="win2k-cold-2" />
```

```
<link rel="alternate stylesheet" type="text/css" media="all" href="calendar-system.css"
      title="system" />
```

```
<!-- import the calendar script -->
```

```
<script type="text/javascript" src="calendar.js"></script>
```

```
<!-- import the language module -->
```

```
<script type="text/javascript" src="lang/calendar-en.js"></script>
```

```
<!-- other languages might be available in the lang directory; please check
your distribution archive. -->
```

```
<!-- helper script that uses the calendar -->
```

```
<script type="text/javascript">
```

```
var oldLink = null;
```

```
// code to change the active stylesheet
```

```
function setActiveStyleSheet(link, title) {
```

```
    var i, a, main;
```

```
    for(i=0; (a = document.getElementsByTagName("link")[i]); i++) {
```

```
        if(a.getAttribute("rel").indexOf("style") != -1 && a.getAttribute("title")) {
```

```
            a.disabled = true;
```

```
            if(a.getAttribute("title") == title) a.disabled = false;
```

```
        }
```

```
    }
```

```
    if (oldLink) oldLink.style.fontWeight = 'normal';
```

```
    oldLink = link;
```

```
    link.style.fontWeight = 'bold';
```

```
    return false;
```

```
}
```

```
// This function gets called when the end-user clicks on some date.
```

```
function selected(cal, date) {
```

```

cal.sel.value = date; // just update the date in the input field.
if (cal.dateClicked && (cal.sel.id == "sel1" || cal.sel.id == "sel3"))
    // if we add this call we close the calendar on single-click.
    // just to exemplify both cases, we are using this only for the 1st
    // and the 3rd field, while 2nd and 4th will still require double-click.
    cal.callCloseHandler();
}

// And this gets called when the end-user clicks on the _selected_ date,
// or clicks on the "Close" button. It just hides the calendar without
// destroying it.
function closeHandler(cal) {
    cal.hide(); // hide the calendar
    // cal.destroy();
    _dynarch_popupCalendar = null;
}

// This function shows the calendar under the element having the given id.
// It takes care of catching "mousedown" signals on document and hiding the
// calendar if the click was outside.
function showCalendar(id, format, showsTime, showsOtherMonths) {
    var el = document.getElementById(id);
    if (_dynarch_popupCalendar != null) {
        // we already have some calendar created
        _dynarch_popupCalendar.hide(); // so we hide it first.
    }
    else {
        // first-time call, create the calendar.
        var cal = new Calendar(1, null, selected, closeHandler);
        // uncomment the following line to hide the week numbers
        // cal.weekNumbers = false;
        if (typeof showsTime == "string") {
            cal.showsTime = true;
            cal.time24 = (showsTime == "24");
        }
        if (showsOtherMonths) {
            cal.showsOtherMonths = true;
        }
        _dynarch_popupCalendar = cal; // remember it in the global var
        cal.setRange(1900, 2070); // min/max year allowed.
        cal.create();
    }
    _dynarch_popupCalendar.setDateFormat(format); // set the specified date format
    _dynarch_popupCalendar.parseDate(el.value); // try to parse the text in field
    _dynarch_popupCalendar.sel = el; // inform it what input field we use

    // the reference element that we pass to showAtElement is the button that
    // triggers the calendar. In this example we align the calendar bottom-right
    // to the button.
    _dynarch_popupCalendar.showAtElement(el.nextSibling, "Br"); // show the calendar

    return false;
}

var MINUTE = 60 * 1000;
var HOUR = 60 * MINUTE;
var DAY = 24 * HOUR;
var WEEK = 7 * DAY;

// If this handler returns true then the "date" given as
// parameter will be disabled. In this example we enable
// only days within a range of 10 days from the current
// date.
// You can use the functions date.getFullYear() -- returns the year
// as 4 digit number, date.getMonth() -- returns the month as 0..11,
// and date.getDate() -- returns the date of the month as 1..31, to
// make heavy calculations here. However, beware that this function
// should be very fast, as it is called for each day in a month when
// the calendar is (re)constructed.
function isDisabled(date) {
    var today = new Date();
    return (Math.abs(date.getTime() - today.getTime()) / DAY) > 10;
}

```

```
}

function flatSelected(cal, date) {
    var el = document.getElementById("preview");
    el.innerHTML = date;
}

function showFlatCalendar() {
    var parent = document.getElementById("display");

    // construct a calendar giving only the "selected" handler.
    var cal = new Calendar(0, null, flatSelected);

    // hide week numbers
    cal.weekNumbers = false;

    // We want some dates to be disabled; see function isDisabled above
    cal.setDisabledHandler(isDisabled);
    cal.setDateFormat("%A, %B %e");

    // this call must be the last as it might use data initialized above; if
    // we specify a parent, as opposite to the "showCalendar" function above,
    // then we create a flat calendar -- not popup. Hidden, though, but...
    cal.create(parent);

    // ... we can show it here.
    cal.show();
}

function validar()
{
    var formulario = document.formulario

    var dataini = formulario.dataini.value

    var datafim = formulario.datafim.value

    var submitOK="True"

    if (!dataini)
    {
        alert("Deve preencher o campo Data Inicio!!")
        submitOK="False"
    }

    if (datafim<=0)
    {
        alert("Deve preencher o campo Data Fim!!")
        submitOK="False"
    }

    if (submitOK=="False")
    {
        return false
    }
}

</script>

<CENTER>
<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Acessos do Utilizador a um Espaço
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php
```

```

/* Nota: para retirar as variáveis $identificacao_espaco e $identificacao_utilizador que
foram passadas do menu anterior em identificacao1 */
$identificacoes = $_GET['Identificacao1'];
$vector_identificacoes = explode("||||", $identificacoes);
$Identificacao_espaco = $vector_identificacoes[0];
$Identificacao_utilizador = $vector_identificacoes[1];

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<FONT class=\"h7\">Identifica&#231&#227o do Utilizador: </FONT>
    <FONT color=\"Maroon\" class=\"h7\"> $Identificacao_utilizador</FONT><p>";

echo"<CENTER>";

echo "<TABLE class=\"comBordaSimples2\" width=400><p>

    <TR>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Atributos</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Dados do Utilizador</FONT></TH>
    </TR>

    <TR>
        <TD width=150><FONT class=\"h4_2\">Identifica&#231&#227o</FONT></TD>
        <TD class=\"t_left\">$Identificacao_utilizador</TD>
    </TR>";

$query = "SELECT * FROM utilizadores WHERE id_utiliz = '$Identificacao_utilizador'";

$result = mysql_db_query("dbname", $query);
$row = mysql_fetch_row($result);

    echo"<TR>
        <TD class=\"h4_2\">Nome</TD>
        <TD class=\"t_left\">".$row[1]."</TD>";
    echo"</TR>";

echo"</TABLE>

</CENTER>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<table align='center' border='0'>

    <tr>
        <td><p align='center'><FONT class=\"h7\">Acessos do Utilizador </FONT></td>
        <td><p align='center'>
            <FONT color=\"Maroon\" class=\"h7\"> $Identificacao_utilizador</FONT></td>
        <td><p align='center'><FONT class=\"h7\">ao Espaço </FONT></td>
        <td><p align='center'>
            <FONT color=\"Maroon\" class=\"h7\"><b>$Identificacao_espaco</b></FONT></td>
        <td><p align='center'>
            <FONT class=\"h7\"> entre duas Datas (Assinale as Datas !)</FONT></td>
        <td><p align='center'>
            <a><img src='mickey.gif' width='100' height='100' border='0'></a></td>
    </tr>

</table>";

echo "<CENTER>";

    echo "<TABLE class=\"t_center\" border=0 bgcolor=\"#ffffcc\" cellpadding=\"5\"
        cellspacing=\"1\" width=200><p>";

    echo "<TR bgcolor=\"#f5deb3\">";
        echo "<TH width=20% colspan='2'>
            <FONT class=\"h4_2\" color=\"Maroon\">Data Início</FONT></TH>
            <TH><FONT class=\"h4_2\" color=\"Maroon\"></FONT></TH>
            <TH width=20% colspan='2'>
                <FONT class=\"h4_2\" color=\"Maroon\">Data Fim</FONT></TH>";
    echo "</TR>";

```

```

echo "<TR>";
echo "<TD><FONT class=\"h4_2\" color=\"Maroon\"><b></b></FONT></TD>
    <TD class=\"t_center\"><form method=post name =\"formulario\"
        action=\"c_acessos_utilizador_espaco4.php\"
        onsubmit=\"return validar()\"><input type=text class=\"caixatexto\"
        length=\"10\" name=\"dataini\" id=\"sel3\"size=\"10\" value =
        $dataini></input><input type=\"reset\" class=\"buttons\" value=\"...\"
        onclick=\"return showCalendar('sel3', '%d/%m/%Y');\"></TD>";
echo "<TD></TD>";

echo "<TD><FONT class=\"h4_2\" color=\"Maroon\"><b></b></FONT></TD>
    <TD class=\"t_center\"><form method=post name =\"formulario\"
        action=\"c_acessos_utilizador_espaco4.php\"
        onsubmit=\"return validar()\"><input type=text class=\"caixatexto\"
        length=\"10\" name=\"datafim\"
        id=\"sel4\" size=\"10\" value = $datafim></input><input type=\"reset\"
        class=\"buttons\" value=\"...\"
        onclick=\"return showCalendar('sel4', '%d/%m/%Y');\"></TD>";
echo "</TR>";

echo "</TABLE>";

echo "<TABLE>";
echo "<input type=\"hidden\" name=\"Identificacao_utilizador\"
    value=\"\$Identificacao_utilizador\">";
echo "<input type=\"hidden\" name=\"Identificacao_espaco\"
    value=\"\$Identificacao_espaco\">";
echo "<td><input type = \"submit\" name=\"cmdsubmit\" class=\"buttons\"
    value=\"Submeter\"></input></td>";
echo "<td></td>";
echo "<td><input type=\"reset\" name=\"cmdcancelar\" class=\"buttons\"
    value=\"Cancelar\" ></input></td>";
echo "</TABLE><p>";

echo "</CENTER>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */
echo "<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='aa0010'>
<a href='c_acessos_utilizador_espaco2.php?Identificacao1=Identificacao_utilizador'>
<img src='botao_b.gif' name='botao1' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

?>

```

c_acessos_utilizador_espaco4.php

```

<?php

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_pagina_ate_meio.php");

?>

<CENTER>

<HR size="2" width="60%" color="#663300">
<FONT class="h2" COLOR="#663300"><b>
Acessos do Utilizador a um Espaço
</b></FONT>
<HR size="2" width="60%" color="#663300">
<p>

<?php

$Identificacao_utilizador = $_POST['Identificacao_utilizador'];
$Identificacao_espaco = $_POST['Identificacao_espaco'];

```

```

$dataini = $_POST['dataini'];
$datafim = $_POST['datafim'];

/* Nota: Utilização para o caso de ordenação pelos títulos das diferentes colunas das
tabelas */
if ($Identificacao_utilizador == '' AND $Identificacao_espaco == '')
{
    $identificacoes = $_GET['Flag_Ordenacao'];
    $vector_identificacoes = explode(";;", $identificacoes);
    $Flag_Ordenacao = $vector_identificacoes[0];
    $Identificacao_utilizador = $vector_identificacoes[1];
    $Identificacao_espaco = $vector_identificacoes[2];
    $dataini = $vector_identificacoes[3];
    $datafim = $vector_identificacoes[4];
}

/* Nota: Para transformar a data início que vem no formato string (dd/mm/aaaa) para o
formato (aaaa-mm-dd) igual ao formato do campo da base de dados mysql */
$vectorini = explode("/", $dataini);
$diasini = $vectorini[0];
$mesesini = $vectorini[1];
$anosini = $vectorini[2];
$datainicio_formatada = $anosini."-".$mesesini."-".$diasini;

/* Nota: Para transformar a data fim, que vem no formato string (dd/mm/aaaa), no formato
(aaaa-mm-dd), igual ao formato do campo da base de dados mysql */
$vectorfim = explode("/", $datafim);
$diasfim = $vectorfim[0];
$mesesfim = $vectorfim[1];
$anosfim = $vectorfim[2];
$datafim_formatada = $anosfim."-".$mesesfim."-".$diasfim;

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<FONT class=\"h7\">Identifica&#231&#227o do Utilizador: </FONT>
<FONT color=\"Maroon\" class=\"h7\"> $Identificacao_utilizador</FONT><p>";

echo"<CENTER>";

echo "<TABLE class=\"comBordaSimples2\" width=400><p>

    <TR>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Atributos</FONT></TH>
        <TH><FONT class=\"h4_2\" color=\"Maroon\">Dados do Utilizador</FONT></TH>
    </TR>

    <TR>
        <TD width=150><FONT class=\"h4_2\">Identifica&#231&#227o</FONT></TD>
        <TD class=\"t_left\">$Identificacao_utilizador</TD>
    </TR>";

    $query = "SELECT * FROM utilizadores WHERE id_utiliz =
        '$Identificacao_utilizador'";
    $result = mysql_db_query("dbname", $query);
    $row = mysql_fetch_row($result);

    echo"<TR>
        <TD class=\"h4_2\">Nome</TD>
        <TD class=\"t_left\">".$row[1]."</TD>";
    echo"</TR>";

echo"</TABLE>

</CENTER>
<p>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/ligabd_pedro.php");

echo"<FONT class=\"h7\">Acessos do Utilizador </FONT>
<FONT color=\"Maroon\" class=\"h7\">$Identificacao_utilizador</FONT>
<FONT class=\"h7\"> ao Espaço </FONT>

```

```

        <FONT color=\"Maroon\" class=\"h7\"><b>$Identificacao_espaco</b></FONT>";

echo "<FONT class=\"h7\"> entre as Datas: </FONT>
    <FONT color=\"Maroon\" class=\"h7\"> $dataini</FONT>";

echo "<FONT class=\"h7\"> e </FONT>
    <FONT color=\"Maroon\" class=\"h7\"> $datafim</FONT><p>";

/* Nota: Para ordenar pelos títulos das diferentes colunas das tabelas */
if ($Flag_Ordenacao == 'Identificacao')
{
    $query = "SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
                    espacos.coordgeo_esp, log_acessos.direc_acesso,
                    log_acessos.data_acesso, log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY espacos.id_esp, log_acessos.data_acesso, log_acessos.hora_acesso;";
    /* Nota: Clausula order by .para ordenar os acessos por identificação do
        espaço e data de acesso do utilizador ao espaço */
}
else
{
    if ($Flag_Ordenacao == 'Descricao')
    {
        $query = "SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
                        espacos.coordgeo_esp, log_acessos.direc_acesso,
                        log_acessos.data_acesso, log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY espacos.desc_esp, log_acessos.data_acesso,
          log_acessos.hora_acesso;"; /* Nota: Clausula order by
        para ordenar os acessos por descrição do espaço e data de acesso
        do utilizador ao espaço */
    }
    else
    {
        /* Nota: Por defeito ordena os acessos por datas de acesso (consoante a ordem dos
            registos do ficheiro log_acessos) */
        $query = "SELECT espacos.id_esp, espacos.desc_esp, espacos.tipo_esp,
                        espacos.coordgeo_esp, log_acessos.direc_acesso,
                        log_acessos.data_acesso, log_acessos.hora_acesso
FROM espacos, log_acessos
WHERE log_acessos.id_utiliz = '$Identificacao_utilizador'
      AND log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_esp = espacos.id_esp
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada';";
    }
}

$result = mysql_db_query("dbname", $query);

$num_linhas = mysql_numrows($result);

if ($num_linhas > 0)
{
    /* Escrita do cabeçalho da tabela */
    echo "<CENTER>";

    echo "<TABLE class=\"comBordaSimples\" width=1100><p>";

    echo "<TR>";
    echo "<ul id='menuver1'>";
    echo "<TH width=50><FONT class=\"h4_2\" color=\"Maroon\"> Direcção </FONT></TH>";

```

```

<TH><a
    href=\"c_acessos_utilizador_espaco4.php?Flag_Ordenacao=Identificacao;;$I
    dentificacao_utilizador;;$Identificacao_espaco;;$dataini;;$datafim\"
    title='Ordenar por Identificação do Espaço e Data/Hora do
    Acesso' >
    <FONT class=\"h4_2\" color=\"Maroon\"> Id. do Espaço </FONT></a></TH>

<TH><a
    href=\"c_acessos_utilizador_espaco4.php?Flag_Ordenacao=Descricao;;$I
    dentificacao_utilizador;;$Identificacao_espaco;;$dataini;;$datafim\"
    title='Ordenar por Descrição de Espaço e Data/Hora do Acesso' >
    <FONT class=\"h4_2\" color=\"Maroon\"> Descrição de Espaço
    </FONT></a></TH>

<TH><FONT class=\"h4_2\" color=\"Maroon\">Tipo</FONT></TH>

<TH><FONT class=\"h4_2\" color=\"Maroon\"> Localização </FONT></TH>

<TH width=90><a
    href=\"c_acessos_utilizador_espaco4.php?Flag_Ordenacao=Data;;$Identi
    ficacao_utilizador;;$Identificacao_espaco;;$dataini;;$datafim\"
    title='Ordenar por Data/Hora do Acesso (Ordenação por Defeito)' >
    <FONT class=\"h4_2\" color=\"Maroon\"> Data do Acesso</FONT></a></TH>
<TH width=90>

    <FONT class=\"h4_2\" color=\"Maroon\"> Hora do Acesso </FONT></TH>;
    echo "</ul>";
    echo "</TR>";

    $num_linhas = mysql_numrows($result);
    $i = 0;
    while ($i < $num_linhas)
    {
        $linha = mysql_fetch_row($result);
        echo "<TR>";
        echo "<TD class=\"t_center\"><center>".$linha[4]."</center></TD>";
        echo "<TD class=\"t_left\">".$linha[0]."</TD>";
        echo "<TD class=\"t_left\">".$linha[1]."</TD>";
        echo "<TD class=\"t_left\">".$linha[2]."</TD>";
        echo "<TD class=\"t_left\">".$linha[3]."</TD>";

        /* Nota: Para transformar a data do acesso, que vem da base de dados mysql no formato
        string (aaaa/mm/dd), no formato (dd-mm-aaaa) */
        $dataacesso=$linha[5];
        $vectoracesso = explode("-", $dataacesso);
        $anosacesso = $vectoracesso[0];
        $mesesacesso = $vectoracesso[1];
        $diasacesso = $vectoracesso[2];
        $dataacesso_formatada = $diasacesso."-".$mesesacesso."-".$anosacesso;

        echo "<TD class=\"t_center\"><center>".$dataacesso_formatada."</center></TD>";
        echo "<TD class=\"t_center\"><center>".$linha[6]."</center></TD>";
        echo "</TR>";

        $i++;
    }

    echo"</TABLE>

    </CENTER>";
}
else
{
    echo"<FONT color=\"Maroon\" class=\"h3\"><b>NÃO EXISTEM</b></FONT>";
}

echo"<p>";

mysql_close();

/* Introdução do botão "Voltar (Menu Anterior) */

```

```
echo"<tr><td width='100%' colspan='2' height='3' bgcolor='#ffffcc'><center>
<FONT class='h8' color='#aa0010'>
<a href='c_acessos_utilizador_espaco2.php?Identificacao1=$Identificacao_utilizador'>
<img src='botao_b.gif' name='botao1' border='none' height=30 width=30 align='middle'>
Voltar (Menu Anterior)</a></td></tr>";

include ("C:/Programas/wamp/www/Web_Tesev1/novo/gera_fim.php");

?>
```


Anexo D – Interrogações à Base de Dados

Neste Anexo, é apresentada a globalidade das interrogações *MySQL* de acesso à base de dados, utilizadas pela aplicação *WebGPACS*. Exceptuam-se as interrogações relacionadas com os acessos à tabela de *espaços físicos* (dados hierárquicos), incluindo as referentes ao *modelo de gestão de dados hierárquicos*, já expostas em secção anterior (ver secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””, pág.141).

D.1 – Utilizadores

- Editar Utilizadores

Criar / Inserir Utilizador

```
"INSERT INTO UTILIZADORES VALUES('$Identificacao','$Nome','$Password');";
```

Modificar Utilizador

```
"UPDATE utilizadores SET id_utiliz = '$identificacao', nome_utiliz = '$nome',  
password_utiliz = '$password'  
WHERE id_utiliz = '$identificacao_original';";
```

Eliminar Utilizador

```
"DELETE FROM utilizadores WHERE id_utiliz = '$Identificacao_utilizador';";
```

- Consultar Utilizadores

Consultar / Pesquisar Utilizador

```
"SELECT * FROM utilizadores WHERE id_utiliz = '$Identificacao_utilizador';";
```

Ordenar por Identificação de Utilizador

```
"SELECT * FROM utilizadores ORDER BY id_utiliz;";
```

Ordenar por Nome de Utilizador

```
"SELECT * FROM utilizadores ORDER BY nome_utiliz;";
```

- Editar Papéis a Utilizadores

Atribuir / Inserir Papel ao Utilizador

```
"INSERT INTO papeis_utilizadores (id_utiliz, id_papel)  
VALUES('$Identificacao_utilizador','$Identificacao_papel');";
```

Eliminar / Remover Papel ao Utilizador

```
"DELETE FROM papeis_utilizadores
WHERE id_utiliz = '$Identificacao_utilizador'
AND id_papel = '$Identificacao_papel';"
```

- Consultar Papeis de Utilizadores

Ordenar por Identificação de Papel

```
"SELECT papeis.id_papel, papeis.desc_papel
FROM papeis, papeis_utilizadores
WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
AND papeis_utilizadores.id_papel = papeis.id_papel
ORDER BY papeis.id_papel;";"
```

- Consultar Papéis (disponíveis) para o Utilizador

Consultar Papéis (disponíveis) para o Utilizador

```
"SELECT papeis.id_papel, papeis.desc_papel
FROM papeis
WHERE papeis.id_papel NOT IN (SELECT papeis.id_papel
FROM papeis, papeis_utilizadores
WHERE papeis_utilizadores.id_utiliz = '$Identificacao_utilizador'
AND papeis_utilizadores.id_papel = papeis.id_papel)
ORDER BY papeis.id_papel;";"
```

- Consultar Permissões (a Espaços) de Utilizadores

Interrogações:

- Ordenar pela Hierarquia de Espaços
- Ordenar por Descrição do Espaço
- Ordenar por Tipo de Espaço
- Ordenar por Localização do Espaço

no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””, pág. 141.

D.2 – Papéis

- Editar Papéis

Criar / Inserir Papel

```
"INSERT INTO PAPEIS VALUES('$Identificacao','$Descricao');";"
```

Modificar Papel

```
"UPDATE papeis SET id_papel = '$identificacao',desc_papel = '$descricao'
WHERE id_papel = '$identificacao_original';";"
```

Eliminar Papel

```
"DELETE FROM papeis WHERE id_papel = '$Identificacao_papel';";"
```

- Consultar Papéis

Consultar / Pesquisar Papel

```
"SELECT * FROM papeis WHERE id_papel = '$Identificacao_papel';";
```

Ordenar por Identificação do Papel

```
"SELECT * FROM papeis ORDER BY id_papel;";
```

Ordenar por Descrição do Papel

```
"SELECT * FROM papeis ORDER BY desc_papel;";
```

- Consultar Utilizadores de Papéis

Ordenar por Identificação de Utilizador

```
"SELECT utilizadores.id_utiliz, utilizadores.nome_utiliz  
FROM utilizadores, papeis_utilizadores  
WHERE papeis_utilizadores.id_papel = '$Identificacao_papel'  
      AND papeis_utilizadores.id_utiliz = utilizadores.id_utiliz  
ORDER BY utilizadores.id_utiliz;";
```

Ordenar por Nome de Utilizador

```
"SELECT utilizadores.id_utiliz, utilizadores.nome_utiliz  
FROM utilizadores, papeis_utilizadores  
WHERE papeis_utilizadores.id_papel = '$Identificacao_papel'  
      AND papeis_utilizadores.id_utiliz = utilizadores.id_utiliz  
ORDER BY utilizadores.nome_utiliz;";
```

D.3 – Espaços

- Editar Espaços

Interrogações:

- Criar / Inserir Espaço
- Modificar Espaço
- Eliminar Espaço e todos os seus Descendentes

no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””,
pág. 141.

- Consultar Espaços

Interrogações:

- Consultar / Pesquisar Espaço
- Consultar Espaços

no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””,
pág. 141.

- Consultar Caminho mais simples até um Espaço

Interrogação no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””, pág. 141.

- Consultar Utilizadores de Espaços

Ordenar por Identificação de Utilizador

```
"SELECT DISTINCT utilizadores.id_utiliz, utilizadores.nome_utiliz
FROM permissoes, papeis, papeis_utilizadores, utilizadores
WHERE permissoes.id_esp = '$Identificacao_espaco'
      AND permissoes.id_papel = papeis.id_papel
      AND papeis.id_papel = papeis_utilizadores.id_papel
      AND papeis_utilizadores.id_utiliz = utilizadores.id_utiliz
ORDER BY utilizadores.id_utiliz;";
```

Ordenar por Nome de Utilizador

```
"SELECT DISTINCT utilizadores.id_utiliz, utilizadores.nome_utiliz
FROM permissoes, papeis, papeis_utilizadores, utilizadores
WHERE permissoes.id_esp = '$Identificacao_espaco'
      AND permissoes.id_papel = papeis.id_papel
      AND papeis.id_papel = papeis_utilizadores.id_papel
      AND papeis_utilizadores.id_utiliz = utilizadores.id_utiliz
ORDER BY utilizadores.nome_utiliz;";
```

- Editar Tipos de Espaços

Criar / Inserir Tipo de Espaço

```
"INSERT INTO TIPOESPACOS VALUES('$Identificacao');";
```

Modificar Tipo de Espaço

```
"UPDATE tipospacos SET tipo_esp = '$identificacao'
WHERE tipo_esp = '$identificacao_original';";
```

Eliminar Tipo de Espaço

```
"DELETE FROM tipospacos WHERE tipo_esp = '$Identificacao_tipoespaco';";
```

- Consultar Tipos de Espaços

Ordenar por Identificação de Tipo de Espaço

```
"SELECT * FROM tipospacos ORDER BY tipo_esp;";
```

Ordenar (decrescente) por Identificação de Tipo de Espaço

```
"SELECT * FROM tipospacos ORDER BY tipo_esp desc;";
```

D.4 – Permissões (a Espaços)

- Editar Permissões de Papéis

Criar / Inserir Permissão a Papel

1ª FORMA:

```
"INSERT INTO permissoes (id_papel, id_esp)
VALUES('$Identificacao_papel','$id_espaco');";
```

2ª FORMA:

```
"INSERT INTO permissoes (id_papel, id_esp, tipoacesso_perm, condicoes_perm,
datainicio_perm, horainicio_perm, horafim_perm, datafim_perm)
VALUES('$Identificacao_papel','$Identificacao_espaco','$Tipoacesso',
'$Condicoes','$Datainicio_formatada','$Horaini','$Horafim',
'$Datafim_formatada');";
```

Modificar Permissão do Papel

```
"UPDATE permissoes SET datainicio_perm = '$Datainicio_formatada',
horainicio_perm = '$Horaini', tipoacesso_perm = '$Tipoacesso',
condicoes_perm = '$Condicoes', horafim_perm = '$Horafim',
datafim_perm = '$Datafim_formatada'
WHERE id_esp = '$Identificacao_espaco'
AND id_papel = '$Identificacao_papel';";
```

Eliminar Permissão do Papel

```
"DELETE FROM permissoes
WHERE id_esp = '$Identificacao_espaco_eliminar'
AND id_papel = '$Identificacao_papel';";
```

- Consultar Permissões (a Espaços) do Papel

Interrogação no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””, pág. 141.

- Consultar Espaços (disponíveis) para Permissões do Papel

Interrogação no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””, pág. 141.

- Consultar / Pesquisar Permissão (a Espaço) do Papel

Consultar / Pesquisar Permissão (a Espaço) do Papel

1ª FORMA:

```
"SELECT permissoes.id_papel, permissoes.id_esp
FROM permissoes
WHERE permissoes.id_papel = '$Identificacao_papel'
AND permissoes.id_esp = '$id_espaco';";
```

2ª FORMA:

```
"SELECT * FROM permissoes
WHERE id_esp = '$Identificacao_espaco'
AND id_papel = '$Identificacao_papel';";
```

3ª FORMA:

```
"SELECT * FROM permissoes
WHERE id_esp = '$Identificacao_espaco_eliminar'
AND id_papel = '$Identificacao_papel';";
```

- Consultar Datas/Horas da Permissão (a Espaço) do Papel

Consultar Datas/Horas da Permissão (a Espaço) do Papel

```
"SELECT permissoes.datainicio_perm, permissoes.horainicio_perm,
        permissoes.horafim_perm, permissoes.datafim_perm
FROM permissoes
WHERE id_esp = '$Identificacao_espaco'
AND id_papel = '$Identificacao_papel';";
```

D.5 – Acessos e Presenças

- Auditar Acessos de Utilizadores

Interrogações:

- Ordenar por Identificação do Espaço e Data/Hora do Acesso
- Ordenar por Descrição do Espaço e Data/Hora do Acesso
- Ordenar por Data/Hora do Acesso

no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””, pág. 141.

- Auditar Acessos a Espaços

Ordenar por Nome do Utilizador e Data/Hora do Acesso

```
"SELECT utilizadores.id_utiliz, utilizadores.nome_utiliz,
        log_acessos.direc_acesso, log_acessos.data_acesso,
        log_acessos.hora_acesso
FROM utilizadores, log_acessos
WHERE log_acessos.id_esp = '$Identificacao_espaco'
AND log_acessos.id_utiliz = utilizadores.id_utiliz
AND log_acessos.data_acesso >= '$datainicio_formatada'
AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY utilizadores.nome_utiliz, log_acessos.data_acesso,
        log_acessos.hora_acesso;";
```

Ordenar por Identificação do Utilizador e Data/Hora do Acesso
--

```
"SELECT utilizadores.id_utiliz, utilizadores.nome_utiliz,
        log_acessos.direc_acesso, log_acessos.data_acesso,
        log_acessos.hora_acesso
FROM utilizadores, log_acessos
WHERE log_acessos.id_esp = '$Identificacao_espaco'
AND log_acessos.id_utiliz = utilizadores.id_utiliz
```

```
AND log_acessos.data_acesso >= '$datainicio_formatada'
AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY utilizadores.id_utiliz, log_acessos.data_acesso,
        log_acessos.hora_acesso;";
```

Ordenar por Data/Hora do Acesso e Identificação do Utilizador
--

```
"SELECT utilizadores.id_utiliz, utilizadores.nome_utiliz,
        log_acessos.direc_acesso, log_acessos.data_acesso,
        log_acessos.hora_acesso
FROM utilizadores, log_acessos
WHERE log_acessos.id_esp = '$Identificacao_espaco'
      AND log_acessos.id_utiliz = utilizadores.id_utiliz
      AND log_acessos.data_acesso >= '$datainicio_formatada'
      AND log_acessos.data_acesso <= '$datafim_formatada'
ORDER BY log_acessos.data_acesso, log_acessos.hora_acesso,
        utilizadores.id_utiliz;";
```

- Auditar Acessos por Utilizador a um Espaço

Interrogações:

- Ordenar por Identificação do Espaço e Data/Hora do Acesso
- Ordenar por Descrição do Espaço e Data/Hora do Acesso
- Ordenar por Data/Hora do Acesso

no Capítulo 7, secção §7.4.2 “Interrogações da Aplicação sobre a Tabela “Espaços””,
pág. 141.

Anexo E – Serviços de “Gestão de Controlo de Acessos”

Este Anexo, apresenta um aditamento à secção §9.2.2 “Serviços de “Gestão de Controlo de Acessos””, pág. 173, do Capítulo 9 “Conclusões” da dissertação, em que são acrescentados e mencionados alguns dos benefícios e especificidades deste tipo de *Serviços* para as organizações clientes.

(...) Os clientes, em particular, exigem não só custos reduzidos, como também conveniência e benefícios elevados. Esta proposta de serviços poderia proporcionar, às diversas organizações (instituições, empresas, condomínios residenciais,...), uma solução que, nessa perspectiva, poderia ser ajustada. Estes serviços de gestão apresentar-se-iam com as vantagens das organizações clientes poderem utilizar um *software de gestão de controlo de acessos* compreensível (em que poderiam, mesmo, efectuar as suas próprias operações administrativas ou de gestão do sistema) e sem haver necessidade de grandes investimentos (*hardware*, *software*, custos de manutenção, pessoal de *TI*,...), como sucede nos casos em que estes sistemas são totalmente implementados localmente. Os custos das organizações clientes corresponderiam somente:

- *Avença Mensal* – uma avença mensal fixa pela prestação de serviços mínimos, que incluiria:
 - ligação (*login*) ao *web site* da estação
 - “*reporting*” básico
 - registo de dados por *internet*
- *Tipo de Serviço Prestado* – custo variável, correspondente ao tipo de serviços de *gestão de controlo de acessos* mais conveniente às empresas clientes, dependendo do:
 - *Tamanho do Sistema* – quantidade de locais de acesso (leitores) ou espaços físicos controlados, número de utilizadores,...
 - *Quantidade de “Reports”*
 - ...

Benefícios:

Os principais benefícios que uma solução deste tipo poderia proporcionar às organizações clientes, seriam:

- *Custos baixos:*

- *Acesso à plataforma da aplicação por web browser*
- *Custos nulos com hardware de servidor* – a aquisição e manutenção dum servidor é dispendiosa, mas com este serviço não existe essa necessidade. Além do equipamento normal, utilizado para os sistemas de controlo de acessos físico, nenhum outro equipamento adicional ou especial é necessário no local ou nas instalações da organização cliente.
- *Custos mínimos em RH e nas TI* – os serviços são geridos pelos serviços da empresa fornecedora (estação central) e é o seu pessoal que se encarrega de gerir remotamente os sistemas de controlo de acessos (físico) das organizações clientes.

(Nota: As pequenas empresas são particularmente boas candidatas para a transferência da gestão dos seus sistemas de controlo de acessos (físico) para os serviços duma empresa deste tipo, já que normalmente não têm pessoal dedicado a estas tarefas)

- *“Backups” automáticos com a informação dos dados da base de dados*
- *Actualizações (updates) de software não necessárias*

- *Maior Segurança e Conveniência do Sistema de Controlo de Acessos:*

- *Segurança* – um sistema de controlo de acessos físico gerido por uma estação central poderá proporcionar um nível maior de segurança, pois para além de garantir que o serviço é prestado permanentemente (24h/dia e 7dias/semana), também poderá assegurar que, por exemplo, portas forçadas ou deixadas abertas terão uma acção adequada.
- *Conveniência* – pode também oferecer níveis extra de conveniência, nomeadamente, suportar o *bloqueio/abertura remoto de portas* (por ex., desbloquear remotamente uma porta, no caso de um utilizador se esquecer do seu cartão e, obviamente, depois de ser garantido que esse utilizador está devidamente autorizado a tal) e, em função ou resposta a eventos específicos, poder enviar, por *e-mail* ou *sms*, *notificações/alertas* a pessoas autorizadas (por ex., notificação da entrada dum determinado utilizador numa certa localização ou espaço físico da organização).

- *Funcionalidades de Gestão* – A prestação destes serviços poderá também proporcionar, às organizações clientes, funcionalidades para gestão ou administração própria dos sistemas (por ex., edição de utilizadores, consultas e emissão de diversos relatórios,...)

- *Serviços Adicionais:*

- *Integração com sistemas de automação* – os serviços de gestão de controlo de acessos poderão ser complementados e integrados com serviços de sistemas de automação, nomeadamente:

- *Adição de vídeo para monitorização (videovigilância)* – com base em instruções da organização cliente, os operadores da empresa prestadora do serviço, poderão monitorizar determinados locais de acesso (por ex., visualização de imagens vídeo dum determinado local de acesso, reconhecimento das condições de estado duma porta – aberta, fechada, forçada) e tomarem, se necessário, de acordo com o visualizado, as devidas acções apropriadas (por ex., notificar/alertar o responsável adequado).

- *Gestão de alarmes* – prestação de serviços complementares de integração de sistemas de alarme e outros conjuntos de equipamentos semelhantes (por ex., se o forçamento de uma porta ocorrer, a estação central receberá um sinal de alarme e, em função da opção da organização cliente, os operadores que gerem estes sistemas tomarão as correspondentes acções necessárias).

- ...

