



Projecto de Mestrado em Engenharia Informática

Computação Móvel

Interface for Audit Download

I. F. A. D.

Cristopher Daniel da Silva Pereira

Projecto de Mestrado realizado sob a orientação da Professora Doutora Dulce Gonçalves, Professora da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Leiria, 2011

***À Minha Família e à
Minha Namorada***

*“O desenvolvimento de software é
e será sempre uma combinação
entre engenharia e arte”*

Nota Prévía

Este projecto foi realizado com a colaboração da *Newshift Lda.*, que prontamente se disponibilizou a acolher no seio da empresa a sua realização, assim como a disponibilizar todas as ferramentas e equipamentos necessários à realização do mesmo.

Todos os esquemas de ligações apresentados nesta dissertação encontram-se ilegíveis, assim como não foi apresentado código fonte nem os diagramas de classe finais, pois estes são propriedade intelectual da *Newshift Lda.*

Agradecimentos

Aos meus pais, Conceição e José, por todo o apoio, esforço e encorajamento que demonstraram, e por todo o tempo que abdicaram da minha companhia para que pudesse concluir este projecto.

À Audrey, a minha namorada, pela sua paciência e apoio, sem os quais não teria sido fácil superar as muitas dificuldades que surgiram.

À minha orientadora, a Professora Doutora Dulce Gonçalves, por ter aceitado orientar este projecto, por toda a sua disponibilidade e dedicação em tentar mostrar sempre o melhor caminho a seguir.

Ao Engenheiro João Parracho e ao Engenheiro João Martins, por prontamente se terem disponibilizado a acolher este projecto na *Newshift Lda.*, assim como por toda a ajuda prestada.

A todos, os meus sinceros agradecimentos.

Resumo

No decorrer dos últimos anos, tem-se assistido à proliferação de máquinas de venda automática de produtos, vulgarmente denominadas por máquinas de *vending*. A natureza de alguns dos produtos disponibilizados por estas máquinas, associado à criação de legislação em Portugal e na restante União Europeia, com o objectivo de assegurar o correcto manuseamento e acondicionamento de produtos frescos, congelados e ultracongelados, obriga a que os operadores económicos tenham a necessidade proceder ao registo da temperatura do ar a que os produtos estão sujeitos enquanto estão armazenados dentro das máquinas. Paralelamente, existe ainda a necessidade de as empresas procederem à descarga periódica da auditoria financeira dos moedeiros instalados nas máquinas.

Actualmente no mercado existe um vasto conjunto de soluções que permitem a recolha dos dados de auditoria ambiental e financeira remotamente. No entanto o elevado custo dessas soluções torna diminuta a sua utilização em Portugal.

Pretende-se com esta dissertação criar uma solução que visa proporcionar aos operadores económicos da indústria das máquinas de *vending* uma solução simples e eficaz para recolha de dados de auditoria, e que tire partido da deslocação regular dos repositores às máquinas de *vending*.

Palavras-chave: Auditoria, Vending, Microcontroladores, Protocolo 1-Wire, Dispositivos Móveis

Abstract

Over the last few years it has been witnessed the proliferation of automatic vending machines industry. The nature of some of the products offered by these machines, coupled with the creation of legislation in European Union with the aim of ensuring the proper maintenance, handling and packaging of fresh, frozen or deep frozen products requires that traders have the need to register the air temperature at which the products are exposed while they are stored inside the machines. At the same time, there is still a need for companies to conduct the periodic download of the financial audit from the currency changers installed on machines.

Currently in the market are a wide range of solutions that allow remote data collection of environmental and financial audit. However the high cost of these solutions doesn't make it viable to use in Portugal.

The objective of this dissertation is to create a solution that gives vending machines operators a simple and effective solution to collect audit data, taking advantage of stockers move up to the machines often.

Key-Words: Audit, Vending, Microcontroller, I-Wire, Mobile Devices

Lista de Siglas

3GPP	<i>Third Generation Partnership Project</i>
ATM	<i>Authomated Teller Machines</i>
ATM	<i>Asynchronous Transfer Mode</i>
BDV	<i>Bundesverband der Deutschen Vending-Automatenwirtschaft e.V.</i>
BOM	<i>Bill of Materials</i>
CDMA	<i>Code Division Multiple Access</i>
CPU	<i>Central Processing Unit</i>
CRC	<i>Cyclic Redundancy Check</i>
CTS	<i>Clear to Send</i>
DER	<i>Diagrama Entidade-Relacionamento</i>
DIP	<i>Dual In-Line Package</i>
DoS	<i>Denial of Service</i>
EDGE	<i>Enhanced Data rates for GSM Evolution</i>
EEPROM	<i>Electrically-Erasable Programmable Read-Only Memory</i>
EUA	<i>Estados Unidos da América</i>
EVMMA	<i>European Vending Machine Manufacturers Association</i>
ESTG	<i>Escola Superior de Tecnologia e Gestão</i>
ETSI	<i>European Telecommunications Standards Institute</i>
EVA	<i>European Vending Association</i>
GPRS	<i>General Packet Radio Service</i>
GPS	<i>Global Positioning System</i>
GSM	<i>Global System for Mobile Communications</i>
HSDPA	<i>High-Speed Downlink Packet Access</i>
HSUPA	<i>High Speed Uplink Packet Access</i>
HTTP	<i>Hypertext Transfer Protocol</i>

I2C	<i>Inter-Integrated Circuit</i>
IDE	<i>Integrated Development Environment</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IIS	<i>Internet Information Services</i>
IP	<i>Internet Protocol</i>
IPL	Instituto Politécnico de Leiria
LED	<i>Light Emitting Diode</i>
LTE	<i>3GPP Long Term Evolution</i>
M2M	<i>Machine-To-Machine</i>
MEI	<i>Mars Electronics International</i>
MCU	<i>Microcontroller Unit</i>
MIPS	<i>Million instructions per second</i>
MMS	<i>Multimedia Messaging Service</i>
NAMA	<i>National Automatic Merchandising Association</i>
NIF	Número de Identificação Fiscal
PCB	<i>Printed Circuit Board</i>
PIN	<i>Personal Identification Number</i>
PVC	<i>Polyvinyl Chloride</i>
RAM	<i>Random-Access Memory</i>
RLS	<i>Radio Link Stability</i>
ROM	<i>Read-Only Memory</i>
RTC	<i>Real-Time Clock</i>
RTU	<i>Remote Terminal Unit</i>
SCADA	<i>Software de Supervisory Control And Data Acquisition</i>
SD	<i>Secure Digital</i>
SGBD	<i>Sistema de Gestão de Base de Dados</i>
SIM	<i>Subscriber Identity Module</i>
SMS	<i>Short Message Service</i>
SOAP	<i>Simple Object Access Protocol</i>
SPI	<i>Serial Peripheral Interface Bus</i>
TCP	<i>Transmission Control Protocol</i>
UART	<i>Universal Asynchronous Receiver/Transmitter</i>
UDP	<i>User Datagram Protocol</i>

UMTS	<i>Universal Mobile Telecommunication System</i>
USB	<i>Universal Serial Bus</i>
WBS	<i>Work Breakdown Structure</i>
WCMDMA	<i>Wide-Band Code-Division Multiple Access</i>
XML	<i>eXtensible Markup Language</i>

Índice

NOTA PRÉVIA.....	VII
AGRADECIMENTOS	IX
RESUMO	XI
ABSTRACT.....	XIII
LISTA DE SIGLAS.....	XV
ÍNDICE	XIX
ÍNDICE DE FIGURAS.....	XXIII
ÍNDICE DE TABELAS.....	XXVII
1 INTRODUÇÃO	1
1.1 OBJECTIVOS.....	2
1.2 ESTRUTURA DO DOCUMENTO.....	2
2 ESTADO DA ARTE	5
2.1 COMPOSIÇÃO DAS MÁQUINAS DE <i>VENDING</i>	6
2.2 MOEDEIRO	8
2.3 PROTOCOLOS DE COMUNICAÇÃO DAS MÁQUINAS DE <i>VENDING</i>	10
2.4 TELEMETRIA.....	12
2.4.1 CUSTO ASSOCIADOS AOS SISTEMAS DE TELEMETRIA.....	16
2.5 TECNOLOGIA <i>MACHINE-TO-MACHINE</i>	18
2.6 SEGURANÇA EM SISTEMAS <i>MACHINE-TO-MACHINE</i>	19
2.7 <i>MACHINE-TO-MACHINE</i> NA INDÚSTRIA DAS MÁQUINAS DE <i>VENDING</i>	23
3 METODOLOGIA.....	27
3.1 IDENTIFICAÇÃO DO PROBLEMA.....	27
3.2 PROCESSO DE INVESTIGAÇÃO	28
3.3 DESENVOLVIMENTO	29
4 EQUIPAMENTO UTILIZADO	31
4.1 <i>IBUTTON</i> ®	31
4.2 PROTOCOLO <i>1-WIRE</i>	32
4.3 MICROCONTROLADORES	35
4.3.1 MICROCONTROLADORES MICROCHIP® VS MICROCONTROLADORES ATMEL®	37
4.3.1.1 Preço e Principais Características.....	37
4.3.1.2 Características Extra.....	38

4.3.1.3	Encapsulamento.....	38
4.3.1.4	Linguagens de Programação Suportadas.....	39
4.4	MODEM GSM	40
5	CONCEPÇÃO DA SOLUÇÃO	41
5.1	ARQUITECTURA DA SOLUÇÃO	41
5.1.1	COMUNICAÇÃO SOCKET	42
5.1.2	APLICAÇÃO CLIENTE	43
5.1.3	SERVIDOR APLICACIONAL.....	43
5.1.4	SISTEMA DE GESTÃO DE BASE DE DADOS	44
5.2	ESPECIFICAÇÃO DOS REQUISITOS.....	44
5.2.1	ANÁLISE DOS REQUISITOS	44
5.2.1.1	Modelo do Domínio.....	44
5.2.1.2	Casos de Uso	47
5.2.2	MODELO DE DADOS	52
6	DESENHO DE PROTÓTIPOS.....	53
6.1	DISPOSITIVO MÓVEL DE RECOLHA DE AUDITORIA.....	53
6.1.1	AVALIAÇÃO DO HARDWARE UTILIZADO	53
6.1.1.1	Modem.....	53
6.1.1.2	Microcontrolador	54
6.1.1.3	LCD	54
6.1.2	PROTOTIPAGEM.....	54
6.1.3	FLUXO DE EVENTOS DOS PRINCIPAIS PROCESSOS.....	57
6.1.3.1	Processo Principal.....	57
6.1.3.2	Descarga de Auditoria.....	59
6.1.3.3	Oclusão do Equipamento	60
6.2	MÓDULO DE RECOLHA DE AUDITORIA	61
6.2.1	PROTOTIPAGEM.....	61
6.2.2	FLUXO DE EVENTOS	62
6.2.2.1	Processo Principal.....	62
6.2.2.2	Obtenção de Auditoria Ambiental.....	63
6.2.2.3	Obtenção de Auditoria Financeira.....	65
6.3	EMULADOR DE MOEDEIRO MEI® SÉRIE 6 E SÉRIE 7.....	66
6.3.1	PROTOTIPAGEM.....	66
6.3.2	FLUXO DE EVENTOS DO PROCESSO PRINCIPAL DO EMULADOR.....	67
6.4	APLICAÇÃO DE GESTÃO E CONFIGURAÇÃO.....	67
6.4.1	PROTOTIPAGEM.....	68
7	IMPLEMENTAÇÃO.....	71
7.1	FERRAMENTAS UTILIZADAS	71
7.1.1	DOCKLIGHT.....	71
7.1.2	MIKROC PRO FOR PIC.....	72
7.1.3	MPLAB®	75
7.1.4	PICKIT 2.....	76
7.1.5	MPLAB® ICD 2.....	76
7.2	DISPOSITIVO MÓVEL DE RECOLHA DE AUDITORIA.....	77
7.2.1	DEFINIÇÃO DO PROTOCOLO DE TRANSFERÊNCIA DE DADOS	78
7.2.2	INTERFACE DE LIGAÇÃO ENTRE DISPOSITIVO MÓVEL E O MÓDULO DE RECOLHA.....	82

7.2.3	DESENVOLVIMENTO DO FIRMWARE	82
7.2.3.1	<i>Integração com o Modem GSM</i>	83
7.2.3.2	<i>Mecanismo de Segurança Desenvolvido</i>	84
7.2.3.3	<i>Comunicação Dispositivo Móvel – Módulo de Recolha</i>	86
7.2.3.4	<i>Comunicação Dispositivo Móvel – Servidor Socket</i>	88
7.2.3.5	<i>Integração com o LCD</i>	89
7.2.3.6	<i>Armazenamento de Informação</i>	90
7.2.3.7	<i>Modo de Funcionamento Off-Line</i>	91
7.2.3.8	<i>Integração com a Rede 1-Wire</i>	92
7.2.3.9	<i>Oclusão Automática do Equipamento</i>	92
7.2.4	SOLUÇÃO FINAL DE HARDWARE	93
7.2.4.1	<i>Esquema de Ligações Final</i>	93
7.2.4.2	<i>Lista de Componentes</i>	96
7.3	MÓDULO DE RECOLHA DE AUDITORIA	97
7.3.1	ORGANIZAÇÃO DO CÓDIGO FONTE	98
7.3.2	INTERFACE DE LIGAÇÃO ENTRE MÓDULO DE RECOLHA E MOEDEIROS MEI®	98
7.3.3	DESENVOLVIMENTO DO FIRMWARE	98
7.3.3.1	<i>Integração com Moedeiro MEI®</i>	98
7.3.3.2	<i>Integração com a Rede 1-Wire</i>	98
7.3.4	SOLUÇÃO DE HARDWARE FINAL	99
7.3.4.1	<i>Esquemático Final</i>	99
7.3.4.2	<i>Lista de Componentes</i>	101
7.4	SERVIDOR SOCKET	101
7.4.1	DESENVOLVIMENTO DO SERVIDOR SOCKET	101
7.5	SERVIDOR DE SERVIÇOS	102
7.5.1	DESENVOLVIMENTO DO WEBSERVICE	103
8	TESTES	105
8.1	ESPECIFICAÇÃO DE TESTES A REALIZAR	106
8.2	EXECUÇÃO DOS TESTES	107
8.2.1	TESTES DE INTEGRAÇÃO DE COMPONENTES	107
8.2.2	TESTES DE INTEGRAÇÃO DO SERVIDOR SOCKET	107
8.2.2.1	<i>Resultados</i>	108
8.2.3	TESTES DE SISTEMA	108
9	CONCLUSÃO	109
9.1	RESULTADOS	109
9.2	PRINCIPAIS CONTRIBUTOS	110
9.3	TRABALHO FUTURO	111
10	BIBLIOGRAFIA	113
ANEXO 1	PLANO DE PROJECTO.....	119
ANEXO 2	SOLUÇÕES DE TELEMETRIA PARA MÁQUINAS DE VENDING	133
ANEXO 3	ESPECIFICAÇÃO DE REQUISITOS.....	135
ANEXO 4	ESTRUTURAÇÃO DO MODELO DE DADOS	149
ANEXO 5	CASOS DE USO	161
ANEXO 6	DESCRIÇÃO DOS PINOS E CONFIGURAÇÃO DOS JUMPERS DE FUNÇÃO DO LCD LM6060CBY181	
ANEXO 7	LISTA DE COMANDOS AT	183

ANEXO 8	LISTA DE COMANDOS DE INICIALIZAÇÃO DO LCD.....	187
ANEXO 9	ORGANIZAÇÃO DO CÓDIGO FONTE DO DISPOSITIVO MÓVEL E DO MÓDULO DE RECOLHA DE AUDITORIA	189
ANEXO 10	ESTRUTURA DOS TICKETS DOS MOEDEIROS MEI® SÉRIE 6 E SÉRIE 7	191
ANEXO 11	ESPECIFICAÇÃO DOS TESTES REALIZADOS.....	193
ANEXO 12	ESPECIFICAÇÃO DO CENÁRIO DE TESTES	197

Índice de Figuras

Figura 1 Exemplo de um moedeiro MEI® 690 Series	9
Figura 2 Exemplo de <i>datalogger</i> com ecrã.....	14
Figura 3 <i>iButton</i> ®	31
Figura 4 Exemplo de uma rede <i>1-Wire</i>	32
Figura 5 Processo de programação de microcontrolador.....	36
Figura 6 Exemplo de um microcontrolador com encapsulamento DIP.....	39
Figura 7 Arquitectura definida para a solução.....	41
Figura 8 Modelo de domínio	47
Figura 9 Diagrama global dos casos de uso do sistema.....	50
Figura 10 Diagrama do conjunto de casos de uso de autenticação.....	50
Figura 11 Esquema de ligações da unidade central de processamento.....	55
Figura 12 Esquema de ligações do modem GSM.....	55
Figura 13 Esquema de ligações do LCD	56
Figura 14 Esquema de ligações aos módulos de transmissão de dados.....	56
Figura 15 Esquema de ligações do leitor de cartões SD.....	56
Figura 16 Esquema de ligações da interface USB de <i>debug</i>	57
Figura 17 Esquema de ligações do circuito de alimentação	57
Figura 18 Fluxograma do funcionamento geral do firmware do dispositivo móvel.....	59

Figura 19 Fluxograma da operação de descarga de auditoria.....	60
Figura 20 Fluxograma da operação de oclusão do dispositivo móvel.....	61
Figura 21 Esquemático geral do dispositivo de recolha de auditoria	62
Figura 22 Fluxograma do processo principal	63
Figura 23 Fluxograma do processo de obtenção de auditoria ambiental.....	64
Figura 24 Fluxograma do processo de obtenção de auditoria financeira	65
Figura 25 Protótipo do emulador de moedeiro	66
Figura 26 Esquema de ligações do emulador de moedeiro MEI®	66
Figura 27 Fluxograma do funcionamento do emulador de moedeiro MEI®	67
Figura 28 Janela principal - vista de recolhas.....	68
Figura 29 Janela principal - vista de estatísticas.....	68
Figura 30 Janela de gestão (genérica).....	69
Figura 31 Janela de detalhes de auditoria financeira	69
Figura 32 Janela de detalhes de auditoria ambiental	70
Figura 33 Janela de configurações.....	70
Figura 34 Captura de ecrã do Docklight.....	72
Figura 35 Captura de ecrã do <i>mikroC PRO for PIC</i>	73
Figura 36 Captura de ecrã do gestor de bibliotecas do <i>mikroC PRO for PIC</i>	73
Figura 37 Captura de ecrã do assistente de código do <i>mikroC PRO for PIC</i>	74
Figura 38 Captura de ecrã do assistente de parâmetros do <i>mikroC PRO for PIC</i>	74
Figura 39 Captura de ecrã do editor de projecto do <i>microC PRO for PIC</i>	75
Figura 40 Programador <i>PICkit 2</i> idêntico ao utilizado	76

Figura 41 Programador <i>Microchip MPLAB® ICD 2</i> idêntico ao utilizado	77
Figura 42 Protótipo do dispositivo móvel de recolha de auditoria	77
Figura 43 Fluxograma do processo de tratamento de resposta do modem.....	84
Figura 44 Fluxograma do processo de cifragem de dados.....	85
Figura 45 Fluxograma do processo de decifragem de dados.....	86
Figura 46 Fluxograma do processo de transferência de dados entre o dispositivo móvel e o módulo de recolha de auditoria.....	87
Figura 47 Esquema de funcionamento do LCD em modo série	90
Figura 48 Fluxograma do processo de armazenamento de dados em ficheiro	91
Figura 49 Esquema de ligações do circuito de alimentação	93
Figura 50 Esquema de ligações do conector de transmissão de dados e ligação ao módulo de recolha de auditoria.....	93
Figura 51 Esquema de ligações do modem GSM.....	94
Figura 52 Esquema de ligações da unidade central de processamento.....	95
Figura 53 Esquema de ligações do LCD	95
Figura 54 Esquema de ligações do leitor de cartões SD.....	95
Figura 55 Protótipo do módulo de recolha de auditoria	97
Figura 56 Esquema de ligações da unidade central de processamento e interface de comunicação com o moedeiro	100
Figura 57 Esquema de ligações da interface de ligação ao dispositivo móvel	100
Figura 58 Aplicação de emulação de envio de dados do dispositivo móvel	108
Figura 59 Gráfico de Gantt.....	119
Figura 60 Plano de Comunicações	129

Figura 61 Diagrama Entidade-Relacionamento da base de dados de sistema.....	152
Figura 62 Diagrama Entidade-Relacionamento da base de dados de serviços.....	153
Figura 63 Diagrama do conjunto de casos de uso de configuração.....	161
Figura 64 Diagrama do conjunto de casos de uso do controlo de calibrações	161
Figura 65 Diagrama do conjunto de casos de uso da gestão de identificadores.....	162
Figura 66 Diagrama do conjunto de casos de uso da gestão de localizações	162
Figura 67 Diagrama do conjunto de casos de uso da gestão de máquinas de <i>vending</i>	162
Figura 68 Diagrama do conjunto de casos de uso da gestão de módulos de recolha de auditoria	163
Figura 69 Diagrama do conjunto de casos de uso da gestão de registadores	163
Figura 70 Diagrama do conjunto de casos de uso da gestão de utilizadores	163
Figura 71 Diagrama do conjunto de casos de uso da visualização de auditoria.....	164
Figura 72 Cenário utilizado na execução dos testes de sistema	197

Índice de Tabelas

Tabela 1 Evolução histórica da indústria das máquinas de <i>vending</i>	5
Tabela 2 Principais fabricantes de máquinas de <i>vending</i>	8
Tabela 3 Protocolos utilizados em interfaces série das máquinas de <i>vending</i>	11
Tabela 4 Planos de <i>internet</i> das principais operadoras móveis nacionais	17
Tabela 5 Descrição dos principais ataques realizados a sistemas M2M.....	22
Tabela 6 Operadores económicos portugueses de máquinas de <i>vending</i>	24
Tabela 7 Vendedores portugueses de máquinas de <i>vending</i>	25
Tabela 8 Comparação das principais características dos microcontroladores comparados.	37
Tabela 9 Característica extra dos microcontroladores comparados.....	38
Tabela 10 Comparação das linguagens de programação suportadas pelos microcontroladores	39
Tabela 11 Descrição sucinta de cada classe identificada.....	46
Tabela 12 Fluxo de eventos do caso de uso "Autenticar"	51
Tabela 13 Estrutura do pacote de dados de auditoria ambiental.....	78
Tabela 14 Estrutura do pacote de dados de auditoria financeira	80
Tabela 15 Estrutura do pacote de erros.....	80
Tabela 16 Estrutura do pacote de estabelecimento de comunicação	81
Tabela 17 Estrutura do pacote de <i>acknowledge</i>	82

Tabela 18 Estrutura do pacote de dados de auditoria financeira	88
Tabela 19 Lista de componentes do dispositivo móvel de recolha de auditoria.....	96
Tabela 20 BOM do módulo de recolha de auditoria.....	101
Tabela 21 Pacote de resultado de operação	102
Tabela 22 Plano de comunicações detalhado	127
Tabela 23 Nomenclatura de componentes não gráficos	130
Tabela 24 Nomenclatura de componentes gráficos e objectos	130
Tabela 25 Restantes convenções utilizadas	131
Tabela 26 Soluções de telemetria para máquinas de <i>vending</i>	133
Tabela 27 Descrição das entidades da base de dados de sistema	149
Tabela 28 Descrição das entidades da base de dados de serviços	151
Tabela 29 Tabelas resultantes da base de dados de sistema	153
Tabela 30 Tabelas resultantes da base dados de serviços.....	157
Tabela 31 Fluxo de eventos do caso de uso "Configurar Dispositivo Móvel"	164
Tabela 32 Fluxo de eventos do caso de uso "Visualizar Histórico de Calibrações".....	166
Tabela 33 Fluxo de eventos do caso de uso "Registar Calibração"	167
Tabela 34 Fluxo de eventos do caso de uso "Adicionar Identificador"	170
Tabela 35 Fluxo de eventos do caso de uso "Editar Identificador"	173
Tabela 36 Fluxo de eventos do caso de uso "Apagar Identificador"	176
Tabela 37 Descrição dos pinos do <i>LCD LM6060CBY</i>	181
Tabela 38 Configuração dos <i>jumpers</i> de função do <i>LCD LM6060CBY</i> para modo de funcionamento série.....	182
Tabela 39 Lista de comandos AT de inicialização básica do modem GSM.....	183

Tabela 40 Lista de comandos AT de inicialização de rede do modem GSM.....	184
Tabela 41 Lista de comandos AT de configuração do perfil de ligação à <i>internet</i>	184
Tabela 42 Lista de comandos AT de configuração do perfil do serviço de <i>internet</i>	185
Tabela 43 Lista de comandos AT de ligação à <i>internet</i> e de transferência de dados	186
Tabela 44 Lista de comandos de inicialização do LCD.....	187
Tabela 45 Especificação dos testes de integração efectuados aos componentes do dispositivo móvel.....	193
Tabela 46 Especificação dos testes de integração efectuados à comunicação entre o dispositivo móvel e o servidor socket.....	194
Tabela 47 Especificação dos testes de sistema efectuados	194
Tabela 48 Especificações dos equipamentos utilizados no cenário de testes	198

Introdução

Ao longo dos últimos anos a indústria das máquinas de *vending* tem vindo a aumentar. Este processo de venda directa tem aumentado pois proporciona diversas vantagens para as empresas, nomeadamente, o baixo valor das despesas gerais, no sentido que muitos operadores não necessitam de escritórios ou lojas dispendiosas. Outra vantagem é o facto de os operadores comprarem os produtos directamente ao fabricante e revenderem-nos directamente ao consumidor, evitando assim intermediários que ficam com parte do lucro (Hawkins, 1992).

Na indústria do *vending* são comercializados os mais diversos produtos, desde selos e postais, a tabaco, revistas e jornais. No entanto, alguns dos produtos mais vendidos são bebidas quentes e frias e comida.

A actual legislação criada pela União Europeia e em Portugal pretende assegurar o correcto manuseamento, transporte e acondicionamento de produtos frescos, congelados e ultracongelados, obrigando, entre diversos aspectos, a que os operadores económicos da área alimentar controlem a temperatura a que os produtos estão expostos através de equipamentos de medição manual ou automática (Guerra, 2009).

Para além da obrigação do controlo da temperatura a que os alimentos se encontram expostos, os operadores económicos tem ainda a necessidade de obter os dados de auditoria financeira relativa às transacções efectuadas pelas máquinas. Normalmente são os moedeiros instalados nas máquinas de *vending* que disponibilizam essa informação, vindo dotados de uma interface que permite aos repositores obterem um relatório dos dados de auditoria financeira.

A constante evolução dos sistemas de informação permite que haja uma vasta oferta de sistemas de telemetria e tendencialmente mais baratos. Existem actualmente diversas soluções de telemetria no mercado vocacionadas para o *vending* que permitem efectuar a reco-

lha dos dados de auditoria ambiental e financeira, assim como a configuração e controlo das máquinas remotamente. Estas soluções, no entanto, acabam por ser demasiado complexas e conseqüentemente caras.

Sendo que cada operador económico de máquinas de venda possui centenas e por vezes milhares de máquinas, efectuar a instalação de soluções de telemetria em todas as máquinas acarreta um elevado investimento. Dada a actual situação económica que se vive em Portugal, e a dimensão dos operadores económicos da indústria do *vending*, a possibilidade de investimento em soluções de telemetria é diminuta.

1.1 Objectivos

Pretende-se com este projecto criar uma solução com um custo reduzido que permita aos operadores económicos, de uma forma simples e automatizada, recolher e armazenar a informação referente às condições ambientais a que se encontram sujeitos os alimentos armazenados, assim como informação financeira dos moedeiros.

Esta solução irá permitir descarregar a informação recolhida pelos registadores de temperatura instalados nas máquinas de *vending*, bem como a informação das transacções monetárias contida nos moedeiros. A informação deverá ser recolhida para um dispositivo móvel aquando da visita de um repositor à máquina de *vending*, e posteriormente enviada para um servidor a fim de poder ser analisada pelos operadores económicos.

1.2 Estrutura do Documento

A presente dissertação encontra-se organizada em nove capítulos. Para além do capítulo introdutório, existem os capítulos referentes ao estado da arte, à metodologia, ao equipamento utilizado, à arquitectura proposta, à especificação dos requisitos, ao desenho de protótipos, à implementação, aos testes e por fim à conclusão.

Após este capítulo introdutório onde são apresentados os objectivos e estrutura da dissertação é apresentado o capítulo o estado da arte. O segundo capítulo revelou-se fundamental para compreender a actual situação da indústria do *vending* e as tecnologias associadas. No terceiro capítulo é abordada a metodologia utilizada para a elaboração deste projecto, sendo apresentado o problema e o processo de investigação e o desenvolvimento realizado. No quarto capítulo são apresentados os equipamentos utilizados na implementação da solução

proposta. Neste capítulo são abordados os modos de funcionamento dos equipamentos tendo sido fundamental para uma maior compreensão dos mesmos. No quinto capítulo é apresentada a concepção da solução e a análise dos requisitos. No sexto capítulo é apresentado o processo de desenho dos diversos elementos que compõe a solução, nomeadamente os esquemas de ligação dos protótipos dos equipamentos a desenvolver, a descrição dos principais processos, e os protótipos não funcionais da aplicação de gestão e configuração. No sétimo capítulo é descrito o processo de implementação da solução, onde são apresentadas as ferramentas utilizadas durante a implementação, assim como os aspectos considerados relevantes durante o desenvolvimento dos equipamentos e das restantes aplicações que compõe a solução. No oitavo capítulo são abordados os testes realizados à solução implementada. Por último, no nono capítulo, é apresentada a conclusão, onde são abordados os resultados obtidos e ainda indicado o trabalho futuro a realizar.

No final do documento encontram-se os anexos que complementam a dissertação e que pela sua importância não poderiam ser omissos. Nos anexos encontram-se o plano de projecto, a apresentação de algumas soluções de telemetria direccionadas ao *vending*, a especificação de requisitos, a estruturação do modelo de dados, os casos de uso da solução proposta, documentação técnica, e a especificação dos testes realizados.

Estado da Arte

A vasta proliferação da indústria das máquinas de *vending* surge da necessidade de satisfazer uma necessidade que tem vindo a crescer consideravelmente no quotidiano das pessoas, a falta de tempo. O ritmo acelerado que se vive actualmente leva a que se procurem serviços rápidos, de fácil acesso e cómodos. A indústria do *vending* oferece a possibilidade às pessoas de terem acesso a produtos alimentares, e não só, de uma forma rápida e cómoda, 24 horas por dia, 365 dias por ano.

As máquinas de *vending* são máquinas que, através de processos automatizados, permitem a dispensa de diferentes e variados produtos. A sua expansão em locais como empresas, fábricas, hospitais, escolas entre outros estabelecimentos fez com que a venda de bebidas engarrafadas ou enlatadas e de *snacks* aumentasse.

Na Tabela 1 pode ser consultada uma breve apresentação da evolução histórica da indústria das máquinas de *vending*.

Tabela 1 Evolução histórica da indústria das máquinas de *vending*

Fonte: (Lee, 2005; NAMA, 2008)

Evolução Histórica das Máquinas de <i>Vending</i>	
Data	Descrição
215 A.C	No Egipto, é já utilizado um dispositivo (urna inventada pelos Gregos) para a dispensa de água benta nos templos.
1700 - 1799	Nas tabernas inglesas começam a ser utilizadas caixas que funcionam com moedas para a venda de tabaco.
1886 - 1888	Nos EUA (Estados Unidos da América) são concedidas várias patentes de dispositivos de distribuição que funcionam com base em moedas. Surtem máquinas de distribuição baseadas em moedas (para a venda, por exemplo, de pastilhas elásticas nos EUA e de postais em Londres).
1905 - 1950	Nos EUA começam a ser vendidos selos nos correios através de máquinas para o efeito.

	<p>Surge a primeira máquina de <i>vending</i> para venda de tabaco.</p> <p>É inventado o dispensador que permitiu ampliar a utilização das máquinas de <i>vending</i> a diferentes produtos.</p> <p>É fundada a NAMA (<i>National Automatic Merchandising Association</i>).</p> <p>Surgem as primeiras máquinas de <i>vending</i> de café e sandes.</p>
1957 - 1978	<p>Aparecem normas de controlo sanitário e é estabelecido o primeiro programa de certificação de equipamentos de <i>vending</i> pela NAMA.</p> <p>Surgem máquinas de <i>vending</i> de batidos.</p> <p>São aplicados novos componentes electrónicos nas máquinas de <i>vending</i>.</p> <p>As máquinas de <i>vending</i> de <i>snacks</i> com um painel frontal de vidro são introduzidas no mercado, assim como as máquinas de <i>vending</i> de água.</p>
1985 - 1987	<p>Surgem máquinas de <i>vending</i> que suportam notas e cartões de crédito/débito.</p> <p>São utilizados os primeiros computadores portáteis para captura electrónica de dados das máquinas de <i>vending</i>.</p>
1991 - 1993	<p>Surgem as primeiras máquinas de café aromatizado, e outras bebidas quentes solúveis.</p> <p>A NAMA aprova padrões industriais para a transferência de dados.</p> <p>É efectuada a primeira transmissão remota sem fios de dados das máquinas para os armazéns.</p>
1998 – Actualmente	<p>São revistos e aprovados novos padrões de comunicação.</p> <p>Desenvolvidos novos mecanismos de segurança de detecção de dinheiro falso.</p>

2.1 Composição das Máquinas de *Vending*

As principais matérias-primas utilizadas na construção das máquinas de *vending* são o aço galvanizado, o plástico, pó acrílico (para revestimento) e poliuretano (para o isolamento).

A composição destes equipamentos inclui, normalmente, uma estrutura exterior em aço que determina a dimensão da máquina de *vending* e é responsável pela protecção dos componentes internos da mesma. No interior dessa estrutura pode ser encontrado um compartimento interno designado por tanque. Entre a estrutura exterior e o tanque existe um isolamento sob a forma de espuma responsável por manter a temperatura interna estável e proteger assim os produtos de temperaturas extremas. As superfícies externas das máquinas de *vending* são normalmente revestidas com materiais resistentes e de elevada durabilidade de modo a evitar abusos dos clientes (Roberts, 2011).

Para o armazenamento e dispensa de produtos podem ser utilizados alimentadores em formato de colunas empilhadas ou de bandejas. Os alimentadores em formato de colunas empilhadas contêm mecanismos motorizados para empurrar fisicamente os produtos para a

frente até serem libertados da pilha e caírem na área acessível ao cliente. Os alimentadores em formato de bandeja são constituídos por espirais de arame rotativas que detém os produtos e que os vão libertando para o cliente à medida que vão rodando. No entanto, existem constantes ajustamentos às máquinas de *vending* de acordo com a própria evolução das embalagens dos produtos que estas distribuem para que estes sejam dispensados de uma forma prática e eficiente (Roberts, 2011).

Existem máquinas de *vending* que apresentam duas portas: uma interna e outra externa. Geralmente, a porta interna funciona como um isolamento adicional, e a porta externa inclui os componentes electrónicos e de iluminação que permitem aos clientes seleccionar, pagar e receber os seus produtos, e ainda diversos mecanismos de segurança de modo a evitar furtos (Roberts, 2011).

Actualmente, as máquinas de *vending* incluem componentes, denominados por moedeiros, permitem verificar a autenticidade de moedas e notas, que possibilitam a utilização de cartões de crédito/débito e permitem dar diferentes tipos de *feedback* ao cliente (por exemplo, visuais através de ecrãs ou vocais) (Roberts, 2011).

O controlo de qualidade das máquinas de *vending* é bastante rigoroso e inclui testes aos componentes electrónicos que os constituem, aos alimentadores, à precisão e à segurança com que os produtos são dispensados. De acordo com a tipologia das máquinas, podem ser feitos, por exemplo, testes de refrigeração (Roberts, 2011).

Na Tabela 2 são apresentados alguns dos fabricantes de máquinas de *vending* mais utilizadas no mercado português.

Tabela 2 Principais fabricantes de máquinas de vending

Principais Fabricantes de Máquinas de Vending		
Logótipo	Fabricante	Tipos de Máquinas Produzidas
	<i>Bianchi</i>	Máquinas de café e máquinas de venda automática de bebidas quentes, frias e snacks.
	<i>Saeco</i>	Máquinas de café e máquinas de venda automática de bebidas quentes, frias e snacks.
	<i>GPE Vendors</i>	Máquinas de café, bebidas quentes e bebidas frias.
	<i>N&W Global Vending</i>	Máquinas de café e máquinas de venda automática de bebidas quentes, frias e snacks.
	<i>Crane Merchandising Systems</i>	Máquinas de café e máquinas de venda automática de bebidas quentes, frias e snacks.
	<i>Jofemar</i>	Máquinas de café, máquinas de venda automática de bebidas quentes, frias, snacks, tabaco e sistemas de pagamento.

2.2 Moedeiro

Como referido anteriormente, uma máquina de vending é composta por diversos componentes, sendo um dos principais componentes o moedeiro (Figura 1).



Figura 1 Exemplo de um moedeiro MEI® 690 Series

O moedeiro trata-se de um equipamento de verificação da autenticidade e tipo das moedas ou notas introduzida, e pode ser encontrado para além de em máquinas *vending* também em máquinas de jogo, em máquinas de trocos, em ATMs (*Automated Teller Machines*), em caixas de pagamento automático (wiseGEEK, 2011). Ao receber uma moeda, e após verificar a sua validade, esta poderá ir para os tubos do moedeiro, ou então para o cofre. O tubo trata-se do compartimento onde ficam armazenadas as moedas que poderão ser devolvidas aos utilizadores. O cofre é compartimento onde ficam armazenadas as moedas introduzidas e que serão posteriormente recolhidas por um operador/repositor.

Os moedeiros actuais poderão utilizar vários métodos para detecção de notas falsas. Um dos métodos passa pela utilização de uma cabeça de leitura magnetizada para verificar se a tinta magnética da nota introduzida reflecte ao ser submetida a uma determinada frequência. Outro método, um pouco mais simples, passa pela utilização de solução de iodo que não vai reagir com as notas verdadeiras, mas irá marcar as notas falsas devido à sua composição de materiais diferentes. Outro método de detecção de notas falsas passa pelo apro-

veitamento dos mecanismos de segurança incorporados nas notas verdadeiras e ainda pela medição da sua dimensão (wiseGEEK, 2011).

A detecção de moedas falsas é geralmente mais simples, pois as moedas são geralmente de materiais, peso, forma e tamanho diferentes. Os moedeiros geralmente verificam a veracidade das moedas pelo peso, forma e tamanho, existindo no entanto alguns que fazem o teste através da medição do magnetismo da moeda ou verificando a sua composição (wiseGEEK, 2011).

Cada vez mais os falsificadores de moedas e notas criam formas de contornar os sistemas de segurança, fazendo com que muitos países dêem alta prioridade na melhoria dos sistemas de detecção de dinheiro falso. No entanto, a constante evolução da tecnologia, para além de possibilitar aos falsificadores criarem formas de contornar os sistemas de segurança, tem também permitido que sejam criados mais e melhores sistemas de detecção (wiseGEEK, 2011).

Um dos maiores fabricantes de moedeiros é a MEI® (*Mars Electronics International*), sendo os seus moedeiros vastamente utilizados nas máquinas de *vending* a operar em Portugal. A MEI® é uma empresa do grupo *Mars*, criada em 1969 e actualmente sediada nos EUA, com pontos de venda e produção espalhados por todo mundo (*International Directory of Company Histories, Vol. 7, 1993*). É considerada uma das maiores e mais fiáveis empresas de produção de moedeiros, estimando-se que ocorram 2 mil milhões de transacções por semana em mais de 100 países utilizando os seus moedeiros (MEI, 2007). A MEI® foi a primeira empresa a criar um moedeiro electrónico durante a década de 60 (MEI, 2007), e durante a década de 80 criou o primeiro sistema electrónico de pagamento por notas e cartões de crédito/débito (*International Directory of Company Histories, Vol. 7, 1993*). Actualmente possui moedeiros para máquinas de *vending*, caixas *self-service* de supermercados, em caixas de pagamento automático em parques de estacionamento, e em máquinas de trocos e de jogo nos casinos.

2.3 Protocolos de Comunicação das Máquinas de *Vending*

Para a comunicação entre os diversos componentes das máquinas de *vending* poderão ser utilizadas várias interfaces. As interfaces das máquinas de *vending* estão divididas em duas categorias, interfaces electromecânicas e interfaces série (EVA, 2010).

As interfaces electromecânicas surgiram na década de 60, não possuíam nenhum microcontrolador e controlavam directamente os vários componentes da máquina de *vending* através de um elevado número de cabos e conectores, e operava com tensões elevadas o que as tornava perigosas (EVA, 2010).

As interfaces série são as mais utilizadas actualmente e não são tão complexas e perigosas como as interfaces electromecânicas. Neste tipo de interfaces são utilizados microcontroladores para enviar mensagens entre os diversos componentes da máquina de *vending*, como por exemplo entre o moedeiro e a placa de controlo(EVA, 2010).

Para ambas as interfaces mencionadas existem diversos protocolos criados. Para as interfaces electromecânicas foram criados protocolos diferentes para a Europa, para os Estados Unidos da América e para a Ásia. Relativamente aos protocolos de comunicação utilizados nas interfaces série, vários foram criados pelos fabricantes de máquinas de *vending* e os seus componentes ao longo dos últimos e posteriormente adoptados pelas várias associações de associações de operadores da indústria do *vending* (EVA, 2010). Na Tabela 3 são apresentados alguns dos principais protocolos especificados para as interfaces série das máquinas de *vending*.

Tabela 3 Protocolos utilizados em interfaces série das máquinas de *vending*

Fonte: (Azkoyen, 2004; EVA, 2011; EVA & NAMA, 2007; MEI, 1995)

Protocolos de Interfaces Série das Máquinas de <i>Vending</i>	
Protocolo	Descrição
Protocol A	Este protocolo, também conhecido como Executive, foi desenvolvido pela MEI® no início da década de 80 e permite a ligação entre periféricos, por exemplo o moedeiro, à máquina de <i>vending</i> . Neste protocolo a transacção é controlada pelo moedeiro, e os preços dos produtos tanto poderão ser definidos ou na máquina ou no moedeiro. Neste protocolo é ainda definido o tipo de conectores a utilizar entre os diversos componentes e a tensão de operação dos equipamentos.
BDV001	O protocolo BDV001 foi criado pela BDV (<i>Bundesverband der Deutschen Vending-Automatenwirtschaft e.V.</i>), a associação de operadores económicos do <i>vending</i> na Alemanha, e baseia-se no <i>Protocol A</i> da MEI®, em que essencialmente a maior diferença é o conector de comunicação e de alimentação terem sido juntos num só conector. Este protocolo apenas foi adoptado em países de língua alemã.
MDB/ICP	Inicialmente surgiu o protocolo MDB (<i>Multi-Drop Bus</i>), tendo sido desenvolvido pela CoinCo para a Coca-Cola no início da década de 90. Este protocolo foi criado para permitir a ligação de moedeiros de baixo custo que apenas servissem para a colocação

	de moedas e todo o restante processamento fosse efectuado pela máquina de <i>vending</i> , tendo sido adoptado em 1994 pela NAMA . De seguida a EVMMA (<i>European Vending Machine Manufacturers Association</i>) adoptou o protocolo tendo feito algumas alterações de modo a suportar periféricos de pagamento sem dinheiro, dando origem ao ICP (<i>Internal Communications Protocol</i>). Em 1998 ambos os protocolos foram uniformizados dando origem ao MDB/ICP, sendo actualmente utilizado pela NAMA, pela EVMMA e pela EVA (<i>European Vending Association</i>).
Micromech	Este protocolo foi inicialmente criado para a interligação entre moedeiros e unidades de troco, tendo sido posteriormente revisto e actualizado de modo a permitir que o controlador da máquina de <i>vending</i> tenha controlo directo sobre os diversos periféricos. Apesar de inicialmente o protocolo ter sido especificado para moedeiros de três tubos, este foi alterado para poder suportar moedeiros de quatro tubos, tendo sido alterado o conector da interface de ligação de 12 pinos por um de 15 pinos. Com esta alteração foi possível adicionar a opção de ligação em 24V em vez de 110V e suportar quatro tubos em vez de três.
VCCS	O protocolo VCCS trata-se de um protocolo para suporte a transacções com moedas, notas ou sistemas de pagamento sem dinheiro, e foi criado pela Coca-Cola® para utilização nos países Asiáticos. Neste protocolo é utilizado apenas um conector que disponibiliza a alimentação e comunicação.

2.4 Telemetria

Actualmente pretende-se melhorar a recolha de dados, a manutenção e a eficiência das máquinas de *vending* através da utilização de diagnósticos remotos que permitam, por exemplo, conhecer em tempo real, o *stock* de cada máquina de *vending*, quais os produtos que estão a ser mais vendidos ou efectuar a mudança de preços dos produtos remotamente. Com a utilização de sistemas de telemetria é possível reduzir a utilização de computadores portáteis para a execução de acções directamente nas máquinas ou para a recolha de dados relativos às vendas. Pretende-se, igualmente, reduzir a quantidade de dinheiro armazenado nestas máquinas de forma a reduzir os actos de vandalismos e furtos das mesmas através de uma maior utilização de cartões de crédito/débito (Roberts, 2011).

O conceito de telemetria surgiu da necessidade de efectuar medições em locais inacessíveis. Os telemetristas utilizavam telémetros para medir a distância entre o observador e um ponto inacessível. Actualmente o termo telemetria aplica-se a várias formas de medição à distância, ou seja, à obtenção, processamento e transmissão de dados à distância (Rozas, 2004).

O avanço da tecnologia permitiu que soluções de telemetria sejam cada vez mais acessíveis. O custo dos sistemas de telemetria sem fio é actualmente consideravelmente mais barato do que há uns anos atrás. A expansão do GSM (*Global System for Mobile Communications*) foi um dos factores que mais contribuiu ao desenvolvimento de novos sistemas de telemetria. Através da tecnologia GPRS (*Global System for Mobile Communications*) é possível garantir que, ainda que virtualmente, seja possível comunicar de praticamente todo o lado, com um custo reduzido (Metriolog, 2005).

As unidades físicas mais comuns medidas por sistemas de telemetria incluem temperatura, humidade, pressão, luminosidade, movimento, velocidade e ritmo cardíaco (Vodafone, 2010). Apesar das diferentes aplicações que um sistema de telemetria pode ter, a sua base de funcionamento é idêntica, sendo os principais componentes que o compõem os seguintes (Metriolog, 2005):

- Sensores;
- Actuadores;
- RTU (*Remote Terminal Unit*);
- *Base Stations*;
- SCADA (*Software de Supervisory Control and Data Acquisition*).

Sensores

Um sensor trata-se de um dispositivo que mede unidades físicas e converte-as para uma unidade eléctrica. Os sensores podem ser divididos em duas famílias, sensores analógicos e sensores digitais.

A utilização de sensores para transformação de unidades físicas em unidades eléctricas traz diversos benefícios, nomeadamente a elevada sensibilidade e precisão, a duração e fraca exigência de manutenção dos equipamentos electrónicos, o controlo remoto e registo contínuo, a supervisão automática em diversos pontos de medida, a possibilidade de visualização digital, o controlo automático, o tratamento computadorizado de um elevado número de dados, e a troca de informação através de computadores (Galvão, 2004).

Existem actualmente sensores com e sem fios, assim como *dataloggers*. Um *datalogger* trata-se de um dispositivo electrónico, geralmente de pequenas dimensões, alimentado por

uma bateria e com um sistema de armazenamento, para registo de dados ao longo do tempo através de um sensor interno ou externo.

Existem *dataloggers* com interface de ligação a computadores pessoais para visualização dos dados recolhidos. Existem ainda *dataloggers* com um pequeno ecrã (Figura 2) para apresentação de dados ao utilizador e assim funcionar autonomamente.



Figura 2 Exemplo de *datalogger* com ecrã

Fonte: (Testo, 2011)

Actuadores

Um actuador é um dispositivo que reage ao receber um impulso eléctrico provocando uma acção. Os actuadores são muito utilizados em funções de controlo, como por exemplo abrir/fechar portas e abrir/fechar válvulas.

Remote Terminal Unit

Um RTU trata-se de um dispositivo electrónico composto por um microprocessador, memória não volátil, módulos de entrada/saída e uma interface de comunicação que serve de interface entre os equipamentos que estão ligados no meio físico com a *Base Station* do sistema.

Os RTU poderão ter dois sentidos de funcionamento. Tanto podem enviar dados recebidos dos sensores para a *Base Station*, como podem receber dados da *Base Station* e fazer accionar actuadores.

A comunicação entre os diversos RTU e os sistemas de controlo é geralmente feita através de interfaces série RS-232, RS-485, RS-422, interfaces *Ethernet* e ainda interfaces sem

fios, sendo que estas últimas poderão ser baseadas em GSM, GPRS ou em soluções proprietárias.

As soluções sem fio proprietárias têm a vantagem de geralmente utilizarem frequências rádio livres ou com um custo reduzido, pelo que reduz consideravelmente o custo das comunicações. Estas soluções poderão no entanto ser mais caras de produzir assim como o raio de alcance é consideravelmente mais baixo.

As soluções com base em GSM comunicam com os restantes elementos do sistema através de um modem sem fios analógico. Este tipo de solução tem um custo elevado de operação devido ao preço das comunicações ser geralmente taxado ao minuto. A vantagem deste tipo de soluções é a vasta proliferação da rede GSM, tornando virtualmente possível a comunicação entre os vários elementos do sistema independentemente da distância a que se encontram uns dos outros.

Por fim, as soluções com base em GPRS são agora muito comuns. Apesar do custo das comunicações continuarem a ser um ponto negativo, estas são mais baratas aquando comparadas com o GSM dado que geralmente são taxados com base na quantidade de dados transmitidos. Um aspecto importante e vantajoso é o de que as comunicações GPRS permitem a utilização de protocolos utilizados na *internet* como é o caso do TCP/IP (*Transmission Control Protocol/Internet Protocol*).

Existem actualmente RTUs mais complexos, podendo estes desempenhar algumas acções autonomamente sem ser necessário qualquer indicação externa, armazenar dados e efectuar gestão de consumo energético.

Base Stations

Uma *Base Station* não é mais que um equipamento que centralizará a recolha e envio de informação para os RTU.

As *Base Stations* poderão ser de diversos tipos. Na sua forma mais simplificada as *Base Stations* poderão não ser mais que um software a ser executado num computador que recolhe os dados dos diversos RTUs armazenando-os numa base de dados ou em ficheiros. As *Base Stations* poderão ser também dispositivos com capacidade de armazenamento com interfaces para ligação a computadores ou a redes cabeadas ou sem fios.

As *Base Stations* são no entanto equipamentos caros, pois são geralmente produzidos em baixas quantidades e com tecnologias proprietárias.

Ao contrário do que acontece actualmente, no início do desenvolvimento de sistemas de recolha de telemetria os recursos para criação de RTUs viáveis eram escassos e os sistemas informáticos eram pouco fiáveis para suportar sistemas de recolha constante pelo que era necessário investir no desenvolvimento de *Base Stations* que dariam alguma autonomia ao sistema em caso de falha. Actualmente é possível desenvolver RTUs com quantidades de memória consideráveis e instalar os sistemas em redes informáticas com servidores disponíveis 24 horas, 7 dias por semana com uma alta taxa de fiabilidade. Desta forma, actualmente o conceito de *Base Station* começa tornar-se obsoleto (Metriolog, 2005).

Software Control and Data Acquisition

Um software SCADA é geralmente o software de recolha e apresentação de dados recolhidos pelos sensores e enviados pelos RTUs. Os *softwares* SCADA são também responsáveis por enviar a informação para accionar os actuadores.

Este tipo de sistemas, permite centralizar a monitorização de diversos parâmetros e actuar sobre diversos dispositivos de controlo existentes num ou mais complexos existentes numa vasta área.

Os sistemas SCADA poderão ser aplicados na indústria de fabrico e produção, sistemas de geração de energia, refinarias, em infra-estruturas de tratamento e fornecimento de água, em infra-estruturas de recolha de resíduos domésticos, oleodutos e gasodutos, sistemas de comunicação, em edifícios no controlo de consumo de energia e controlo de acessos em aeroportos, barcos e até mesmo em estações espaciais.

Os sistemas de telemetria existentes para as máquinas de *vending* baseiam-se na tecnologia M2M (*Machine-To-Machine*), que será apresentada na secção 2.5.

2.4.1 Custo Associados aos Sistemas de Telemetria

Um dos factores que mais é tido em conta na aquisição de sistemas telemetria é o seu custo. Os preços actuais dos equipamentos, apesar da tendência de ficarem mais baratos em comparação há uns anos, são ainda bastante elevados.

O custo das comunicações móveis tem sido igualmente um factor inibidor na aquisição de sistemas telemetria. No entanto, tem-se assistido nos últimos anos a uma redução considerável no preço das comunicações móveis assim como a criação de vários planos de comunicação no que se refere ao acesso à *internet* a partir de dispositivos móveis (Vodafone, 2010).

Actualmente as três principais operadoras móveis no mercado português disponibilizam planos de *internet* para dispositivos móveis. Na Tabela 4 são apresentados os principais planos de *internet* da Vodafone, TMN e Optimus.

Tabela 4 Planos de *internet* das principais operadoras móveis nacionais

Fonte: (Optimus, 2011; TMN, 2011; Vodafone, 2011)

Planos de <i>Internet</i> Móvel das Principais Operadoras Nacionais		
Plano	Preço	Tráfego
Vodafone		
<i>Tarifa Diária</i>	€0.95/Dia	10MB
<i>Aditivo Internet 25</i>	€1.29/Semana	25MB
<i>Aditivo Internet 100</i>	€5.19/Mês	100MB
<i>Aditivo Internet 300</i>	€10.38/Mês	300MB
<i>Aditivo Internet 600</i>	€15.58/Mês	600MB
Optimus		
<i>Diário</i>	€0.99/Dia	15MB
<i>Internet Já</i>	€1.39/Semana	30MB
<i>Internet Smart</i>	€2.49/Semana	75MB
<i>Internet Power</i>	€4.99/Semana	250MB
TMN		
<i>IT Diário</i>	€1.04/Dia	15MB
<i>IT Semanal</i>	€1.30/Semana	25MB
<i>IT Standard</i>	€7.99/Mês	200MB
<i>IT Super</i>	€10.39/Mês	300MB

No caso em particular do projecto a desenvolver, estima-se que a média mensal de *Bytes* a enviar seja no máximo de 10MB por cada 100 máquinas segundo o seguinte cálculo:

TBE (Total de Bytes a Enviar)

$$= \text{N}^{\circ} \text{ M\acute{a}ximo de Bytes a Enviar por M\acute{a}quina} \times 100 \text{ M\acute{a}quinas} \times 30 \text{ Dias}$$

$$= 2791 \times 100 \times 30 = 8373000 \approx 8MB$$

Verifica-se desta forma, que o serviço mensal de menor tráfego será suficiente, não acarretando assim uma despesa mensal de grande valor em comunicações móveis para os operadores económicos.

2.5 Tecnologia *Machine-To-Machine*

A vasta proliferação da *internet* e o aumento da largura de banda tem permitido à sociedade actual alterar vários aspectos do seu dia-a-dia. A computação e a comunicação móvel têm igualmente evoluído bastante ao longo dos últimos anos. Este rápido desenvolvimento de tecnologias ubíquas tem permitido que haja poder computacional em qualquer altura, em qualquer lugar, em qualquer dispositivo e com qualquer tipo de dados (Metrilog, 2005).

Cada vez mais as máquinas têm utilizado a *internet* para comunicar entre si. O desenvolvimento dos microcontroladores, das redes e das tecnologias sem fio, tem estimulado ainda mais o rápido crescimento de tecnologias ubíquas (Metrilog, 2005).

O actual panorama tecnológico é bastante diferente de o de há uns anos atrás, a proliferação das tecnologias sem fio fez com que cada vez menos se assista ao aparecimento de soluções sem fio proprietárias. O aparecimento de padrões como o GSM, o CDMA (*Code Division Multiple Access*), o IEEE (*Institute of Electrical and Electronics Engineers*) 802.11a/b/g, o *Bluetooth* e o mais recente IEEE 802.11.14 (*Zig Bee*) praticamente inviabilizam a necessidade de criar soluções proprietárias, assim como foram grandes impulsionadoras das tecnologias M2M (Metrilog, 2005).

Apesar da grande utilização da tecnologia GPRS para a comunicação, outras tecnologias como o LTE (*3GPP Long Term Evolution*), WiFi e WiMAX poderão ser utilizadas (Vodafone, 2010).

A comunicação entre máquinas permite criar uma série de soluções inovadoras. Actualmente já existem diversas aplicações para a tecnologia M2M, por exemplo, controlo de frotas, controlo de tráfego, controlo de dispositivos remotos, segurança, agricultura, etc (Metrilog, 2005; Vodafone, 2010).

A utilização de sistemas M2M permitirá alterar o modo de operação de muitas empresas. O acesso remoto a informação em tempo real a partir de qualquer máquina ou dispositivo

permitirá às empresas não só melhorar a sua eficiência e reduzir custos, mas também aumentar a satisfação do cliente (Vodafone, 2010).

Em suma, através da tecnologia M2M é possível interligar máquinas que possuam um meio de comunicação e desta forma trocar informação de forma automática com outras máquinas ou com outros sistemas de tecnologias de informação sem que haja intervenção humana (Vodafone, 2010).

A utilização na Internet de padrões como o TCP/IP e o HTTP (*Hypertext Transfer Protocol*) assim como formatos de dados como o XML (*eXtensible Markup Language*) permite que se possa garantir interoperabilidade entre diversos sistemas de telemetria (Metrilog, 2005).

2.6 Segurança em Sistemas *Machine-To-Machine*

O aspecto da segurança é já um requisito geral na maioria das aplicações modernas, pelo que, também os sistemas de telemetria levantam várias questões de segurança.

A utilização de comunicação M2M interliga diversas máquinas com outros sistemas, criando desta forma um grande número de interfaces de ligação. Para além das interfaces de ligação entre sistemas, existe ainda a ligação aos vários componentes de medição do sistema de telemetria. Todas estas ligações criam naturalmente vários pontos vulneráveis a serem atacados. É importante garantir que toda a informação recolhida seja transmitida de forma segura e sem perdas (Vodafone, 2010).

Sendo um dos principais objectivos da comunicação M2M o baixo custo dos equipamentos, e considerando que a sua utilização será vasta, a aplicação global de aspectos de segurança não será prática (Cha, Shah, Andreas, Andreas, & Michael, 2009).

A tendência futura passa cada vez mais por descentralizar os sistemas. Este facto cria a necessidade de complementar a segurança com risco controlado.

As políticas de segurança poderão ser complementadas com o factor confiança. Se uma entidade tem o comportamento esperado poder-se-á concluir que esta é uma entidade segura. Assim sendo, ao passar parte da aplicação de segurança para os elementos que compõem o sistema, poder-se-á criar uma rede transaccional segura (Cha, Shah, Andreas, Andreas, & Michael, 2009).

Algumas das principais características de um equipamento M2M são ser pequeno, ter um custo de produção reduzido, utilizar redes sem fio como meio de comunicação, e operar por longos períodos de tempo sem que haja a necessidade de intervenção humana. Outro aspecto relevante nos equipamentos M2M é o facto de poderem ser implementados em grande número e localizações distantes, pelo que muitas vezes a sua manutenção é feita remotamente. Todos estes aspectos poderão tornar os equipamentos de M2M bastante susceptíveis a ataques.

De modo a identificar os mecanismos de segurança a utilizar, será necessário primeiro identificar e classificar os possíveis atacantes.

Os atacantes poderão ser classificados como sendo (Meinel & AlNemr, 2008):

- Atacantes activos: são atacantes que têm acesso directo aos dispositivos de recolha de informação;
- Atacantes passivos: são atacantes que procuram ter interferência com os dispositivos de recolha de informação através de ligações paralelas de modo a interceptar as comunicações entre o dispositivo e outro sistema;
- *Insiders*: são geralmente os atacantes mais comuns dos sistemas, sendo estes os próprios operadores dos sistemas.

Outro aspecto a ter em conta é o nível de segurança do sistema. Para que se possa identificar os requisitos de segurança do sistema, é necessário perceber os diversos tipos de ameaças existentes e quais as que mais poderão afectar os sistemas M2M.

Apesar de ser bastante eficiente, o protocolo IP tem as suas vulnerabilidades. Com os actuais mecanismos existentes de encaminhamento de pacotes, deixa-os vulneráveis a acções de *spoofing*, *sniffing*, roubo de identidade assim como não garante o não-repúdio. A falta de segurança existente na *Internet* é uma preocupação a ter em conta, pois torna as redes públicas e privadas susceptíveis de serem monitorizadas e acedidas por utilizadores/entidades não autorizadas (Istepanian, Laxminarayan, & Pattichis, 2006).

Existem diversos tipos de ataque, sendo os mais comuns os ataques de *eavesdropping* modificação de dados, *spoofing*, DoS (*Denial of Service*), *Man in the Middle* e *sniffing* (Istepanian, Laxminarayan, & Pattichis, 2006).

Segundo o projecto 3GPP (*Third Generation Partnership Project*) os ataques poderão ser divididos em várias categorias, nomeadamente (Cha, Shah, Andreas, Andreas, & Michael, 2009):

- Ataques físicos: este tipo de ataques inclui a utilização de *tokens* de autenticação válidos em equipamentos modificados, ataques de *reflashing* (alteração do *firmware* por *firmware* alterado e/ou fraudulento);
- Comprometimento de credenciais: este tipo de ataques inclui os ataques de força bruta a *tokens* e os ataques de chave comprometida. Estão também incluídos nesta categoria os ataques de intrusão física, ataques *side-channel*, e clonagem maliciosa dos *tokens* de autenticação;
- Ataques de configuração: esta categoria de ataques inclui alteração de configurações e/ou actualização fraudulenta de *software*, configuração incorrecta do sistema por parte do operador e má configuração e/ou adulteração da lista de controlo de acesso;
- Ataques de protocolo: os ataques inseridos nesta categoria são ataques directos aos dispositivos, incluindo ataques de *men-in-the-middle* no primeiro acesso à rede, *DoS*, comprometer os dispositivos explorando falhas nos serviços da rede, e ataques ao processo de manutenção remota;
- Ataques ao núcleo da rede: esta categoria refere-se aos ataques feitos ao operador de comunicações móveis. Os ataques mais comuns são a personificação de dispositivos, *tunneling* de tráfego entre dispositivos personificados, alteração de configurações de *firewalls*, modems, *routers* e *gateways*. Esta categoria inclui ainda ataque de *DoS* ao núcleo da rede e *sniffing*.
- Ataques aos dados de utilizador e privacidade da identidade: esta categoria de ataques inclui os ataques de *eavesdropping* aos dados enviados por utilizadores e/ou dispositivos, *spoofing*, e disponibilização de credenciais de acesso a entidades não autorizadas.

Na Tabela 5 são apresentados os principais ataques realizados aos sistemas M2M.

Tabela 5 Descrição dos principais ataques realizados a sistemas M2M

Principais Ataques a Sistemas M2M	
Ataque	Descrição
<i>Eavesdropping</i>	Refere-se aos ataques que ocorrem quando o atacante tem acesso à rede e consegue ler os dados transferidos.
Modificação de dados	É geralmente o próximo ataque a realizar após os ataques de eavesdropping. Este tipo de ataques não é mais do que a alteração dos dados interceptados sem o conhecimento do emissor ou do receptor.
<i>Spoofing</i>	São ataques que ocorrem quando um atacante gera pacotes de modo a simular que estes são emitidos por um endereço IP válido obtendo assim ligação a uma rede. Após obter ligação à rede atacada, o atacante poderá reencaminhar, apagar ou alterar informação.
<i>DoS</i>	Este tipo de ataques ocorre quando um atacante, após ter acesso à rede, consegue provocar o mau funcionamento das aplicações ou até mesmo provocar a inutilização dos sistemas.
<i>Man-in-the-middle</i>	Tal como o nome indica, são ataques que ocorrem quando o atacante consegue “colocar-se” entre dois pontos em comunicação, conseguindo assim interceptar todas as suas comunicações.
Chave comprometida	São os ataques em que o atacante consegue decifrar uma chave. A partir do momento que o atacante tem em sua posse uma chave, este pode aceder à rede, descriptar e modificar dados ou até mesmo gerar novas chaves e assim ter acesso à rede sem ser descoberto.
<i>Sniffing</i>	São os ataques feitos com recurso a programas que interceptam as comunicações numa rede e caso os pacotes não sejam encriptados o atacante tem acesso a toda a informação neles contidos.

Os principais aspectos de segurança a ter em conta nos sistemas M2M são os mesmos que na generalidade dos sistemas informáticos, sendo estes a confidencialidade, integridade dos dados, autenticidade, o controlo de acesso, disponibilidade, não repúdio, e anonimato.

Conclui-se que a segurança é portanto uma questão importante a ter em conta em todos os sistemas que envolvam informação sensível, como por exemplo dados comerciais, dados clínicos e dados de transferências financeiras.

A fim de garantir um ambiente seguro em sistemas dispersos, deverá existir um conjunto relevante de elementos de segurança (Cha, Shah, Andreas, Andreas, & Michael, 2009). Os equipamentos de M2M deverão incluir recursos que garantam um ambiente de funcionamento seguro e confiável para a execução do *software* e armazenamento de dados.

Mecanismos de encriptação, palavras-chave seguras, utilização de *firewalls* e anti-vírus poderão facilmente ser aplicados para evitar ataques a dispositivos remotos. Este tipo de mecanismos de segurança permite ainda que o grande número de dispositivos que compõe o sistema seja facilmente configurado remota e centralmente (Vodafone, 2010).

2.7 *Machine-To-Machine* na Indústria das Máquinas de *Vending*

A indústria das máquinas de *vending* tem sido uma das quais se tem verificado um aumento da utilização de soluções M2M, nomeadamente em sistemas de telemetria.

A maioria dos sistemas de telemetria existentes para máquinas de *vending* fornece informação em tempo real sobre o *stock* de produtos e informação de auditoria financeira. Este tipo de soluções permite que os operadores económicos saibam previamente quais os produtos que são necessários reabastecer nas máquinas. Desta forma é possível planear a ronda de reabastecimento previamente, economizando assim tempo nas rondas e consequentemente dinheiro.

Apesar dos avanços tecnológicos e consequente redução nos custos das soluções de telemetria, estas continuam a ter um valor elevado. As soluções de telemetria passam na sua grande maioria pela instalação de equipamentos que permitam efectuar a ligação a um servidor através da *internet*, particularmente através de uma ligação GPRS. Este factor faz com que muitas soluções se tornem inviáveis para os operadores económicos de máquinas de *vending* em Portugal.

No Anexo 2 é apresentada uma tabela com algumas soluções de telemetria, respectivas características e os seus preços dentro do que foi possível apurar.

Na Tabela 6 são apresentadas as principais empresas portuguesas da área do *vending* e as suas principais áreas de acção.

Tabela 6 Operadores económicos portugueses de máquinas de vending

Principais Operadores Económicos de Máquinas de Vending em Portugal		
Logótipo	Nome	Área de Acção
	<i>NVending</i>	Todo território de Portugal Continental.
	<i>Serdial Vending</i>	Braga, Porto, Coimbra, Lisboa e região do Algarve.
	<i>A Super 2000</i>	Região norte de Portugal e zona de Lisboa.
	<i>Coffee & Snack</i>	Margem Sul, Lisboa, Sintra e Porto.
	<i>LeiriVending</i>	Distritos de Leiria, Coimbra e Santarém.
	<i>WeAreCoffee</i>	Zona de Lisboa.
	<i>Grão Frio</i>	Zona de Lisboa.

Na Tabela 7 são apresentados alguns dos vendedores de máquinas de *vending* portugueses.

Tabela 7 Vendedores portugueses de máquinas de *vending*

Vendedores Portugueses de Máquinas de <i>Vending</i>		
Logótipo	Nome	Tipo de Produtos
	<i>Lucavending</i>	Comercialização de equipamentos de <i>vending</i> e sistemas de pagamento.
	<i>VendusVending</i>	Comercialização de equipamentos de <i>vending</i> da <i>Crane Merchandising Systems</i> .
	<i>A Guia Portugal</i>	Comercialização de equipamentos de <i>vending</i> da <i>Jofemar</i> , <i>F2S</i> e <i>Züimex</i> .

Metodologia

Neste capítulo é efectuada uma identificação do problema, do processo de investigação seguido e por último é apresentada uma síntese do processo desenvolvimento.

O desenvolvimento de *software* é composto por um conjunto de tarefas, realizadas por uma ou mais pessoas. A realização dessas tarefas é um processo complexo, e difícil cumprir todas as variáveis definidas, tempo de execução e custo (Silva & Videira, 2008).

Não existem processos ideais para a realização de *software*, pelo que o processo utilizado deverá ser sempre adaptado a quem o realiza e ao próprio projecto. As metodologias de desenvolvimento, permitem definir que técnicas, notações e ferramentas utilizar que torna possível a realização de um projecto de *software* (Silva & Videira, 2008).

3.1 Identificação do Problema

A tendência actual na indústria do *vending* vai no sentido de instalar sistemas que permitam gerir e controlar as máquinas de *vending* remotamente. Juntamente a esta tendência, a criação de legislação obriga aos operadores de produtos alimentares a controlarem a temperatura a que os produtos se encontram expostos, sendo desta forma necessário instalar equipamentos de medição de temperatura dentro das máquinas de *vending*.

Os actuais sistemas de telemetria existentes no mercado para a indústria do *vending* permitem o controlo e a gestão remota das máquinas de *vending*, possibilitando controlar os *stocks* das máquinas, controlar o número de vendas, alterar preços e obter dados de auditoria. Estes sistemas dão a possibilidade aos operadores identificar previamente as máquinas com menor *stock* e quais os produtos a repor nas máquinas, podendo assim realizar uma melhor gestão da volta de reposição e consequentemente poupar dinheiro.

Os sistemas de telemetria comportam, no entanto, um elevado custo. Apesar do preço dos equipamentos que compõe os sistemas tender a baixar, estes são ainda muito caros. A maioria dos operadores de *vending* em Portugal opera centenas de máquinas, e nalguns

casos milhares, pelo que o preço de instalação de equipamentos de telemetria por máquina implica um grande investimento. Dado que a maioria das empresas em Portugal são de pequena e média dimensão, e muitas da indústria do *vending* chegam por vezes a ser pequenas empresas familiares, assim como a actual conjuntura que se vive, o investimento em soluções de telemetria torna-se inoportuno.

Pretende-se com este projecto desenvolver uma solução, composta por um dispositivo móvel e um módulo de recolha de auditoria, que tire partido das deslocações realizadas às máquinas de *vending* pelos repositores, que permita recolher os dados de auditoria ambiental e financeira e posterior envio automático para um servidor. Desta forma pretende-se evitar a instalação de equipamentos com elevado preço em cada máquina de *vending*, pretendendo-se que o preço final de produção do dispositivo móvel seja 100€ e o do módulo de recolha de auditoria 50€.

3.2 Processo de Investigação

O estudo efectuado para o desenvolvimento deste projecto baseou-se na observação por contacto directo com a indústria a que se destina o produto que se pretende desenvolver, assim como no levantamento bibliográfico junto de diversas fontes, nomeadamente documentação técnica, artigos, livros, sites, e revistas. Através desta pesquisa foi possível verificar o actual estado da arte e assim compreender melhor o mercado para o qual se destina a solução proposta.

Como referido anteriormente, pretendeu-se neste projecto desenvolver um sistema que permitisse agilizar o processo de obtenção de dados de auditoria na indústria do *vending*. De modo a conseguir alcançar esse objectivo, e como o projecto envolve tanto uma vertente de programação de alto nível como de baixo nível, a metodologia de desenvolvimento baseou-se em dois ciclos distintos.

Para a componente de alto nível optou-se por efectuar o levantamento e posterior análise dos requisitos do sistema que permitiram desenhar o modelo de domínio. Posteriormente foram identificados os actores do sistema, assim como definidos e descritos os casos de uso. Após a descrição dos casos de uso procedeu-se ao desenho dos primeiros protótipos não funcionais da aplicação. Por último, desenhou-se o diagrama de classes detalhado e procedeu-se ao desenvolvimento aplicativo.

Relativamente à componente de baixo nível efectuou-se a análise de requisitos e respectivas funcionalidades a implementar, procedendo-se à elaboração de diagramas de fluxo das principais funcionalidades. Seguiu-se a fase de implementação dos diversos equipamentos a desenvolver.

3.3 Desenvolvimento

Para uma melhor adaptação à tecnologia e à ferramenta de desenvolvimento, foram criados numa fase inicial projectos separados. Os projectos criados permitiram uma melhor adaptação e compreensão:

- Comunicação com a interface UART (*Universal Asynchronous Receiver/Transmitter*);
- Integração com a tecnologia *I-Wire*;
- Ligação ao modem GSM;
- Integração com o módulo de cartões SD (*Secure Digital*);
- Integração com o LCD (*Liquid Crystal Display*).

Após a conclusão da criação dos diversos projectos independentes, procedeu-se à criação dos dois projectos finais, o dispositivo móvel de recolha de auditoria, e o módulo de recolha de auditoria, nos quais foram integrados os projectos criados anteriormente. Como o acesso a moedeiros foi limitado durante o desenvolvimento do projecto, procedeu-se ainda à implementação de um emulador de moedeiros que permitiu desta forma validar o funcionamento do módulo de recolha de auditoria.

Relativamente às restantes aplicações, foram desenvolvidas os servidores que compõe a arquitectura proposta, nomeadamente o servidor *socket* e o servidor de serviços.

Equipamento Utilizado

Neste capítulo são caracterizados os diversos componentes electrónicos utilizados no desenvolvimento do projecto e principais conceitos associados.

Para o desenvolvimento deste projecto foi necessário compreender o funcionamento de alguns equipamentos electrónicos e respectivos protocolos de comunicação, particularmente conhecer o modo de funcionamento dos *iButtons*® e o seu protocolo de comunicação, compreender o que são microcontroladores e as suas principais características, e ainda compreender o modo de funcionamento dos modems GSM.

De seguida são caracterizados os componentes referidos anteriormente.

4.1 *iButton*®

Um *iButton*® (Figura 3) trata-se de um *datalogger*, produzido pela *Maxim*, composto por um *microprocessador* encapsulado numa pequena embalagem de aço inoxidável com cerca de 6mm de espessura. Dadas as suas dimensões reduzidas e a sua elevada robustez, é possível utilizar estes dispositivos nos mais diversificados ambientes sem perigo de que este possa ser danificado.



Figura 3 *iButton*®

Fonte: (Products, 2011e)

O *iButton*® utiliza o seu encapsulamento como interface de comunicação. Os contactos da interface são feitos através da “tampa” e da “base”. A “tampa” é o elemento superior do encapsulamento, a “base” é todo o resto do encapsulamento. Ambos os componentes estão ligados ao *chip* que se encontra no interior, e estão separados através de uma anilha de polipropileno (Products, 2011f).

A comunicação com o *iButton*® é efectuada através do protocolo *1-Wire* através dos contactos referidos anteriormente.

4.2 Protocolo 1-Wire

Numa abordagem tradicional de dois fios, o dispositivo *master* necessita de ter dois portos disponíveis para dados e para o sinal de relógio para comunicar com um dispositivo *slave*, sendo que o dispositivo *slave* necessita ainda de um pino extra para alimentação (Products, 2011d).

O protocolo *1-Wire* trata-se de um simples protocolo de comunicação série desenvolvido pela *Dallas Semiconductor*, e que utiliza apenas um fio tanto para dados como para alimentação, podendo ser encontrado em diversos componentes, como por exemplo memórias, sensores, conversores analógicos/digitais e RTC (*Real-Time Clock*) (Products, 2011b).

Tipicamente uma rede *1-Wire* é composta por um dispositivo *master* ligado a vários dispositivos *slave* (Figura 4) através de um barramento *1-Wire*, em que a comunicação é bidireccional *half-duplex*, em que a transmissão de dados é feita em modo série com o *bit* menos significativo a ser transmitido em primeiro lugar (Products, 2011d).

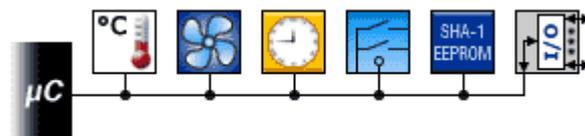


Figura 4 Exemplo de uma rede *1-Wire*

Fonte: (Products, 2011a)

O protocolo suporta duas velocidades de transmissão, 15.4kbps em modo padrão e 125kbps em modo *overdrive* (Products, 2011d).

Todos os dispositivos *slave* vêm programados de fábrica com um identificador único e inalterável que lhes permite serem identificados numa rede *I-Wire*. Todos os identificadores são compostos por 64 *bits*, estando estes subdivididos em 8 *bits* para identificação da família, 48 *bits* para o número de série e 8 *bits* com um *CRC (Cyclic Redundancy Check)* que serve para verificação da integridade dos dados (Products, 2011d).

O dispositivo *master* não tem no entanto, a necessidade de conhecer os identificadores dos dispositivos *slave*, pois pode enviar o pedido aos dispositivos *slave* para que estes lhe enviem os seus identificadores (Products, 2011d).

Todas as comunicações *I-Wire* são iniciadas e controladas pelo dispositivo *master* e feitas digitalmente através de períodos de curta duração, tendo todos os dispositivos *slave* um relógio interno que é sincronizado com o dispositivo *master* (Products, 2011d).

Como referido anteriormente, a comunicação *I-Wire* é feita através do conceito de intervalos de tempo de pequena duração, sendo que o intervalo de tempo é caracterizado pelo instante que o valor lógico 1 ou 0 é lido/escrito na linha *I-Wire*. O dispositivo *master* para comunicar com um dispositivo *slave* inicia um intervalo controlado de tempo pequena duração colocando a linha a 0. Para enviar o valor lógico 0 o dispositivo *master* envia um impulso de longa duração ao passo que para enviar o valor lógico 1 é enviado um impulso de curta duração. A duração de um intervalo de tempo é de 60 microssegundos em modo padrão ou 8 microssegundos em modo *overdrive*. Durante o intervalo de tempo da comunicação existe uma janela de tempo em que o dispositivo *slave* irá ler o estado da linha e assim detectar se o valor lógico enviado é 0 ou 1.

O protocolo de comunicação *I-Wire* é dividido em 3 fases. Na primeira fase o dispositivo *master* efectua um *reset* à linha, sincronizando assim todos os dispositivos *slave* e colocando-os num estado conhecido. De seguida são enviados os comandos de selecção de dispositivo e os comandos de função (Products, 2011d).

Para efectuar o *reset* da linha o dispositivo *master* coloca a linha 0 entre 480 a 640 microssegundos, de seguida liberta a linha ficando no modo de recepção de dados entre 15 a 60 microssegundos, ficando a linha nesta fase no seu estado inactivo. Após o dispositivo *master* libertar a linha, todos os dispositivos *slave* enviam um sinal de *acknowledge* ao qual se dá o nome de impulso de presença, colocando para tal a linha a 0 entre 60 a 240 microssegundos. Após ser enviado o impulso de presença, todos os dispositivos *slave* libertam a

linha e esperam durante um período de 45 a 180 microssegundos para que a linha volte a estabilizar, ficando sincronizados após este período. Num ambiente com diversos *slaves* o dispositivo *master* só irá conseguir determinar que existe pelo menos um dispositivo na linha, pelo que será necessário implementar uma sequência de detecção de dispositivos *slave* (Products, 2011d).

Após ter sido efectuada a sequência de *reset* dá-se início à sequência de selecção, também conhecido por sequência de comandos ROM (*Read-Only Memory*). Nesta fase o dispositivo *master* selecciona o dispositivo *slave* com que pretende comunicar através do seu identificador único. Após o dispositivo *master* seleccionar qual o dispositivo *slave* com que pretende comunicar, os restantes libertam a linha (Products, 2011d).

Finalmente, após o dispositivo *master* ter seleccionado o dispositivo com que pretende comunicar, dá-se início à sequência de comandos funcionais, como por exemplo ler ou escrever da memória (Products, 2011d).

Como referido anteriormente, o protocolo *I-Wire* utiliza apenas uma linha para dados e alimentação dos dispositivos ligados à rede, isto é possível pois os dispositivos *I-Wire* utilizam o conceito de energia parasita. Através de um circuito de alimentação parasita, um condensador é carregado enquanto a linha se encontra liberta, ou seja, no estado *high*. Quando a linha é colocada a 0, o circuito irá utilizar a energia acumulada no condensador para alimentar o oscilador e o circuito de controlo do dispositivo (Products, 2011d).

Destacam-se os seguintes benefícios da tecnologia *I-Wire* (Products, 2011c):

- Necessidade de apenas uma linha para controlo e operação;
- Contém um identificador único pré-programado de fábrica;
- Dispositivos alimentados através da linha de comunicação;
- Possibilidade de ligar diversos dispositivos na mesma linha de comunicação;
- Boa tolerância a descargas electrostáticas.

As redes *I-Wire* têm no entanto algumas limitações, existem diversos factores que podem limitar o seu alcance. O dispositivo *master* deverá de ter a capacidade de fornecer a corrente suficiente para superar a capacidade do cabo, assim como deverá conseguir gerar impulsos com a duração estipulada nas especificações do protocolo *I-Wire*.

Outro aspecto a ter em consideração no planeamento de redes *I-Wire* de maior dimensão, como por exemplo o tipo de cabo a utilizar, dever-se-á ter em consideração o tempo de reflexão de onda, o tempo de atraso produzido pelo cabo, a resistência do cabo, e a degradação dos níveis de sinal (Products, 2008).

Estudos efectuados indicam a possibilidade de redes com um total máximo de 500m de fio utilizando dispositivos *master* mais complexos (Products, 2008).

4.3 Microcontroladores

O rápido desenvolvimento dos componentes electrónicos assistido ao longo dos últimos anos tem permitido que diversas tecnologias tenham crescido no mercado. Muita da evolução deve-se à introdução dos microcontroladores, visto que estes são programados com relativa facilidade e possuem um elevado poder computacional apesar do seu baixo custo, sendo um componente comum em soluções de domótica, robótica, telecomunicações e electrónica doméstica e industrial (Rocha, 2006).

Um microcontrolador, também conhecido por MCU (*Microcontroller Unit*), trata-se de um circuito integrado com poder computacional, possuindo um processador, memória, um oscilador e um conjunto de pinos de entrada/saída (Parallax, 2004).

Os microcontroladores podem ser programados utilizando várias linguagens de programação, entre elas encontra-se a linguagem *C* e o *Assembly*, sendo que esta última torna a programação do microcontrolador mais difícil (Rocha, 2006). A possibilidade de desenvolver firmware para os microcontroladores dá a capacidade de processar e relacionar vários níveis de informação aos circuitos digitais que os integram, dando-lhes assim algum nível de autonomia e capacidade de decisão (Rocha, 2006).

Os microcontroladores ao saírem da fábrica vêm com a memória vazia. Para enviar código para a memória a fim de ser executado é necessário utilizar um programador. O programador poderá enviar qualquer *firmware* desenvolvido ou um *bootloader* (Rocha, 2006).

Para programar um microcontrolador como referido anteriormente é necessário um programador, mas não só, é também necessário um editor de código, um compilador e um *software* de programação. Já existem no entanto vários IDEs (*Integrated Development Environment*) que incluem o editor de código, o compilador e *software* de programação.

O processo de programação (Figura 5) passa pelo desenvolvimento do código, que posteriormente será compilado e dará origem a um ficheiro *assembler*. De seguida o ficheiro é *assembler* é compilado por um compilador de *assembler* do qual resulta um ficheiro hexadecimal. Por fim o ficheiro hexadecimal será carregado para o programador e posteriormente enviado para a memória do microcontrolador.

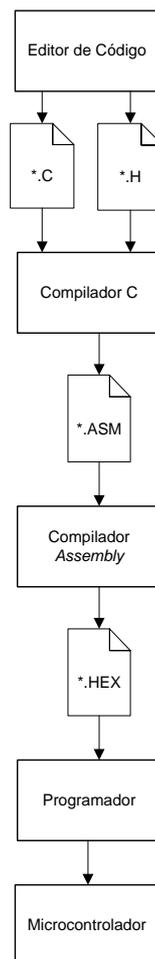


Figura 5 Processo de programação de microcontrolador

Existem diversas famílias de microcontroladores, sendo os microcontroladores de 8 *bits* os mais comuns. Existem diversas gamas de microcontroladores de 8 *bits*, podendo estes custar entre 0.58€ e 960€, e ser programados através de um computador pessoal conjuntamente com um programador com um custo a partir de 39€.

Entre os vários fabricantes de microcontroladores, destacam-se a *Microchip*® e a *Atmel*®, sendo que a *Microchip*® desenvolve os PIC® e a *Atmel*® os AVR®. De seguida é apresentada uma comparação entre os microcontroladores de 8 bits dos fabricantes mencionados.

4.3.1 Microcontroladores Microchip® vs Microcontroladores Atmel®

Já é longa a discussão sobre quais serão os melhores microcontroladores, se os PIC® ou os AVR®, pelo que uma análise para concluir qual o melhor deverá recair sobre algumas características importantes, nomeadamente:

- Preço e principais características;
- Características extra.
- Encapsulamento;
- Linguagens de programação suportadas.

De seguida serão apresentadas as comparações efectuadas aos microcontroladores disponibilizados pelos fabricantes acima referidos nos pontos mencionados anteriormente.

4.3.1.1 Preço e Principais Características

Ambos os fabricantes disponibilizam uma vasta gama de produtos, com diversas características reflectindo-se numa variada gama de preços.

Foram seleccionados três microcontroladores idênticos de ambos os fabricantes, com base no número de pinos, quantidade de memória RAM (*Random-Access Memory*), quantidade de memória ROM, velocidade de CPU (*Central Processing Unit*), velocidade do oscilador interno, e tensão de funcionamento. Da *Microchip*® foram seleccionados o *PIC18F26k20* e o *PIC18F4620*. Da *Atmel*® foi seleccionado o *ATmega644/V*.

Os preços utilizados para comparação referem-se ao valor unitário praticado pela *Farnell* a 9 de Julho de 2011 e toda a informação apresentada foi obtida nos *datasheets* técnicos dos respectivos microcontroladores.

Tabela 8 Comparação das principais características dos microcontroladores comparados

Fonte: (Atmel, 2010; Microchip, 2008, , 2010)

Principais Características do Microcontroladores Comparados			
Fabricante	<i>Microchip</i> ®	<i>Microchip</i> ®	<i>Atmel</i> ®
Modelo	<i>PIC18F26K20</i>	<i>PIC18F4620</i>	<i>ATmega644/V</i>
Nº de Pinos (E/S)	28 (25)	40 (36)	40 (32)
Quantidade de Memória de Programação (Bytes)	65536	65536	65536
Quantidade de Memória	3936	3936	4096

<i>RAM (Bytes)</i>			
Quantidade de Memória EEPROM (Bytes)	1024	1024	2048
Velocidade do CPU (MIPS)	16	10	20
Velocidade do Oscilador Interno	31kHz – 16MHz	31kHz – 16MHz	4MHz – 10MHz
Tensão de Operação	1.8 – 3.6	2 – 5.5	2.7 – 5.5
Preço	2.97€	7.41€	9.68€

4.3.1.2 Características Extra

Na tabela seguinte são apresentadas outras características consideradas relevantes num microcontrolador.

Tabela 9 Característica extra dos microcontroladores comparados

Fonte: (Atmel, 2010; Microchip, 2008, , 2010)

Características Extra dos Microcontroladores Comparados		
Modelo	Interfaces	Periféricos
<i>PIC18F26k20</i>	<i>I2C; SPI; UART.</i>	<i>ADC; Comparator.</i>
<i>PIC18F4620</i>	<i>UART; I2C; PSP; SPI.</i>	<i>ADC; Comparator; PWM; Timer.</i>
<i>ATmega644V</i>	<i>JTAG; SPI; UART.</i>	<i>ADC; Comparator; RTC.</i>

4.3.1.3 Encapsulamento

O encapsulamento é outro factor importante a ter em consideração. Durante a fase de prototipagem poderá ser interessante utilizar encapsulamento do tipo *DIP (Dual In-Line Package)*. Neste aspecto tanto a *Microchip®* como a *Atmel®* disponibilizam diversos equipamentos com encapsulamento *DIP*.

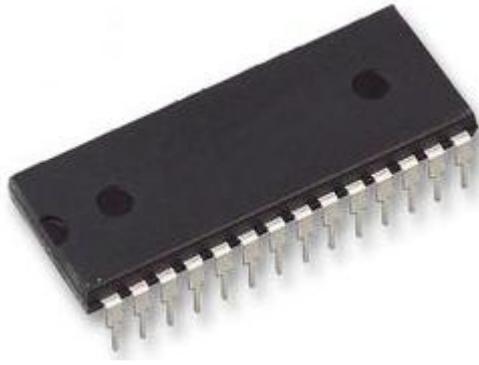


Figura 6 Exemplo de um microcontrolador com encapsulamento DIP

Fonte: (Microchip, 2011e)

4.3.1.4 Linguagens de Programação Suportadas

Na tabela apresentada de seguida poderão ser consultados os diversos tipos de linguagem de programação suportados pelos microcontroladores *Microchip*® e *Atmel*®.

Tabela 10 Comparação das linguagens de programação suportadas pelos microcontroladores

Comparação das Linguagens de Programação Suportadas pelos Microcontroladores		
Linguagem de Programação	Suportado por Microchip®	Suportado por Atmel®
<i>Assembly</i>	✓	✓
<i>C</i>	✓	✓
<i>BASIC</i>	✓	✓

Os aspectos analisados são os que se considerou serem os mais relevantes para uma primeira análise. No entanto existem outras características que poderiam ser analisadas, como por exemplo a qualidade dos *IDEs* existentes, o desempenho dos compiladores e a facilidade de programação. Estas características para uma maior precisão dos resultados exigiam que fosse efectuado um estudo prático.

De acordo com as características analisadas entre os microcontroladores *Microchip*® e os *Atmel*®, pode-se concluir que são muito idênticos na gama analisada, pelo que não se pode considerar que os microcontroladores *Microchip*® são melhor ou pior que os microcontroladores *Atmel*®.

Desta forma conclui-se que a escolha sobre um fabricante de microcontroladores irá recair essencialmente sobre a familiarização com o desenvolvimento de *firmware* para microcon-

troladores de um dos fabricantes. No entanto, para quem não estiver familiarizado com nenhum dos fabricantes, ou não tiver à partida uma limitação quanto à sua escolha, poderá experimentar a desenvolver tanto para um fabricante como para o outro pois ambos disponibilizam placas de iniciação com um preço acessível e ferramentas de desenvolvimento gratuitas ou de demonstração com tempo limitado.

4.4 Modem GSM

Um modem GSM é um tipo de modem no qual é introduzido um cartão SIM (*Subscriber Identity Module*) e que funciona com base num serviço subscrito junto de uma operadora e que suporta os protocolos GSM, como é caso das tecnologias 2,5G GPRS e EDGE (*Enhanced Data rates for GSM Evolution*), assim como tecnologia 3G, tais como o WCDMA (*Wide-Band Code-Division Multiple Access*), UMTS (*Universal Mobile Telecommunication System*), HSDPA (*High-Speed Downlink Packet Access*) e HSUPA (*High Speed Uplink Packet Access*). O modem GSM é de facto equiparado pelas operadoras de comunicações móveis a um telemóvel.

Existem modems GSM de dois tipos distintos. Podem ser equipamentos externos que poderão ser ligados a um computador ou qualquer outro dispositivo através de uma interface série, USB (*Universal Serial Bus*) ou *Bluetooth*, ou podem ainda ser dispositivos móveis do tipo telemóvel ou *smartphone*. Ambos os casos permitem que o equipamento ao qual estiver ligado o modem comunique através da rede de comunicações móveis, sendo a utilização mais comum para estabelecer uma ligação à *internet*, podendo no entanto ser usado para enviar e receber mensagens SMS (*Short Message Service*) e MMS (*Multimedia Messaging Service*). No entanto para ser considerado um modem GSM, este deverá suportar a listagem de comandos AT definida pelas normas ETSI (*European Telecommunications Standards Institute*), GSM 07.05 e 3GPP TS 27.005 (Limited, 2011).

Concepção da Solução

Neste capítulo é apresentada a arquitectura proposta para a solução que se pretende criar, assim como descritos os diversos elementos que a compõe. É ainda efectuada a análise aos requisitos da solução implementada, assim como é definido o modelo de dados.

5.1 Arquitectura da Solução

A arquitectura proposta baseou-se em dois aspectos fundamentais, nomeadamente o modo como é pretendido vender o produto ao cliente final e as limitações inerentes à tecnologia utilizada.

A arquitectura definida para a solução é a típica arquitectura cliente-servidor como apresentada na Figura 7.

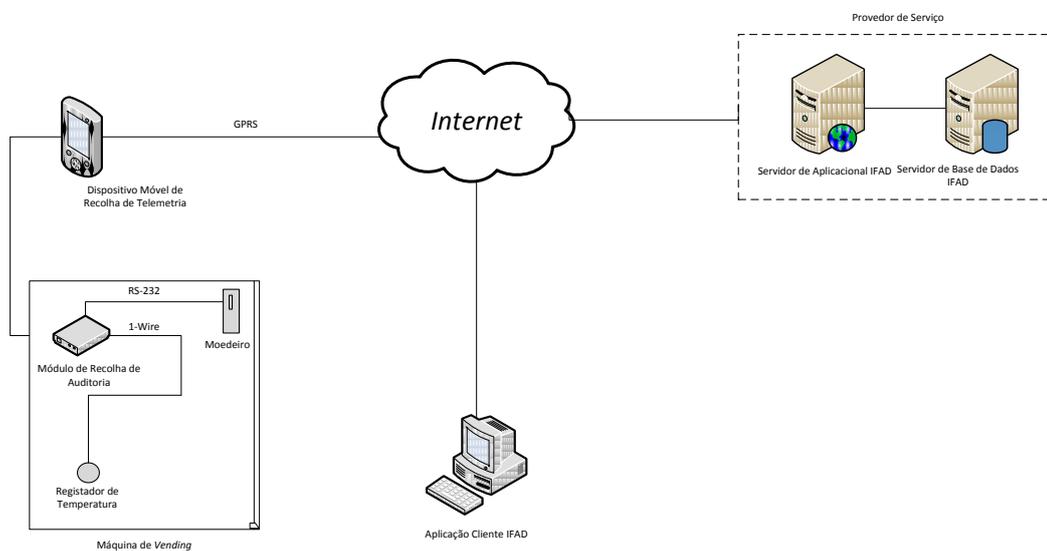


Figura 7 Arquitectura definida para a solução

Como é pretendido que parte do produto seja vendido como um serviço, é o cliente que tem a ónus de iniciar a comunicação quando necessita de algum serviço, e posteriormente o servidor processa esse pedido e retorna a resposta para o cliente. Nesta secção é explicado o protocolo de comunicação utilizado. É efectuada uma introdução às plataformas usa-

das em cada um dos componentes da arquitectura e quais as razões que levaram a sua adopção.

5.1.1 Comunicação Socket

Um *socket* trata-se de uma interface de comunicação que permite criar um canal de comunicação entre uma aplicação cliente e um servidor (Vault, 2008). A função do servidor *socket* é a de mapear a informação recebida na rede para o respectivo processo que a irá processar.

Os servidores *socket* poderão ser classificados em diversos tipos consoante as propriedades de comunicação utilizadas. Cada *socket* tem um tipo associado que define a sua semântica de comunicação, assim como a segurança, ordem, prevenção e duplicação das mensagens (IBM, 2009). Apesar de normalmente as comunicações *socket* serem efectuadas entre *sockets* do mesmo tipo, poderão existir comunicações entre *sockets* de tipo diferentes, desde que os protocolos de comunicação subjacentes sejam compatíveis (IBM, 2009). Os diferentes tipos de *socket* são (IBM, 2009):

- *Stream Socket*;
- *Datagram*;
- *Raw Socket*;
- *Connection Datagram*.

Os *socket* do tipo *Stream Socket* são tipicamente utilizados para transferência de mensagens grande dimensão. Este tipo de *socket* disponibiliza um canal de transmissão bidireccional, com a garantia de que os pacotes de dados chegam na ordem correcta e sem repetições pois este é implementado sobre o protocolo TCP (IBM, 2009).

Os *socket* do tipo *Datagram* são geralmente utilizados com mensagens curtas e com um comprimento máximo fixo. Este tipo de *socket* é implementado sobre o protocolo UDP (*User Datagram Protocol*), por este motivo o *socket Datagram* suporta uma comunicação bidireccional mas no entanto não é sequencial, segura, ou com garantia de que os pacotes de dados chegam todos na mesma ordem ou duplicados (IBM, 2009).

Os *socket* do tipo *Raw Socket* são normalmente orientados a datagramas, sendo que no entanto as suas características dependem do tipo de interface fornecida pelo protocolo. Este

tipo de *socket* permite que uma aplicação tenha acesso directo a protocolos de comunicação de baixo nível, e são normalmente destinados a utilizadores que pretendam tirar partido de alguma característica do protocolo que esteja a ser utilizado ou que não esteja directamente acessível, ou então para criar novos protocolos sob algum protocolo já existente (IBM, 2009).

Os *socket* do tipo *Connection Datagram*, à semelhança do tipo *Stream Socket*, suporta um fluxo de dados bidireccional, sequencial e sem duplicação de pacotes, no entanto não é confiável. Este tipo de *Socket* não é confiável pois, é um serviço orientado à ligação, o *Socket* deverá ter já uma ligação estabelecida antes da transferência de dados. Actualmente, apenas o protocolo ATM (*Asynchronous Transfer Mode*) suporta esse tipo de *socket* (IBM, 2009).

5.1.2 Aplicação Cliente

Neste projecto podem-se identificar dois clientes distintos, a aplicação de gestão e configuração, e o servidor para o qual o dispositivo móvel irá enviar os dados recolhidos.

A aplicação de gestão e configuração será uma aplicação *Windows® Forms* desenvolvida sobre a plataforma *.NET*. A escolha de desenvolver a aplicação em *.NET* foi feita com base na familiarização do desenvolvimento de aplicações *Windows® Forms* em *C#* e pela simplicidade de integração com *WebServices* desenvolvidos também sobre a plataforma *.NET*.

O dispositivo móvel irá enviar os dados através de uma ligação *Socket* para um servidor. O servidor *Socket* desenvolvido é uma aplicação consola desenvolvida sobre a plataforma *.NET* que ficará à escuta de comunicações num determinado porto e endereço local.

5.1.3 Servidor Aplicacional

O servidor aplicacional utilizado foi o *Microsoft® IIS (Internet Information Services)* porque foi adoptada a plataforma *.NET*. A escolha foi feita essencialmente pela familiarização com o desenvolvimento de *WebServices* em *C#* e por se considerar que a plataforma reunia todas as condições para cumprir os requisitos do projecto. A linguagem de programação *C#* é uma linguagem orientada a objectos, simples e com um conjunto de abstracções que permitem acelerar o processo de desenvolvimento.

Outra das razões que se teve em conta na escolha do *C# .NET* foi o facto do objectivo principal de um *WebService* ser a interoperabilidade entre plataformas. Quando desenhado e implementado de forma correcta um *WebService* comunica de forma neutra ou seja, deverá ser indiferente a tecnologia utilizada para desenvolver as aplicações cliente, bastando para tal que estas suportem o protocolo SOAP (*Simple Object Access Protocol*).

5.1.4 Sistema de Gestão de Base de Dados

O SGBD (Sistema de Gestão de Base de Dados) adoptado foi o *Oracle® MySQL™* por ter uma versão livre de custos, ser compacto, robusto, ter uma boa performance e um conjunto de ferramentas gráficas para gestão e manutenção das bases de dados existentes num servidor, como é o caso do *MySQL™ Workbench*. O *MySQL™ Workbench* é uma ferramenta gráfica para desenho de bases de dados disponível para *Windows®*, *Linux* e *OS X*. O *MySQL™* possui ainda um conector para *.NET*, permitindo assim integrar mais facilmente aplicações *.NET* com o SGBD *Oracle® MySQL™*.

Para além das características mencionadas anteriormente, o facto da empresa colaboradora já utilizar em outros projectos o *Oracle® MySQL™*, foi outra razão que levou à sua adopção.

5.2 Especificação dos Requisitos

Seguidamente é apresentada a análise dos requisitos funcionais e não funcionais do sistema após levantamento dos mesmos, assim como apresentar e descrever os casos de uso a eles associados.

5.2.1 Análise dos Requisitos

De seguida é apresentado o modelo de domínio identificado após o levantamento de requisitos efectuado e que pode ser consultado no Anexo 3.

5.2.1.1 Modelo do Domínio

O modelo do domínio trata-se do conjunto de termos utilizados na descrição inicial dos casos de uso, sendo que este é obtido após um conjunto tarefas, nomeadamente, identificar quais as classes que compõe o sistema, o relacionamento entre elas e por fim desenhar o diagrama de classes preliminar (Ferreira, 2007b).

Nesta secção será abordado o processo da definição do modelo de domínio, nomeadamente a identificação e a descrição das classes identificadas, assim como o seu relacionamento.

Classes Identificadas

Após a primeira análise dos requisitos foram identificadas as seguintes classes:

- Utilizador;
- Administrador;
- Operador;
- Repositor;
- Auditoria;
- Financeira;
- Ambiental;
- Recolha;
- Módulo;
- Máquina;
- Localização;
- Identificador;
- Registador;
- Calibração.

Relacionamentos

A classe “Calibração” está relacionada com a classe “Registador” pois cada registador irá ser alvo de calibrações periódicas.

A classe “Registador” está relacionada com a classe “Ambiental” pois são os registadores que efectuem a obtenção de auditoria ambiental.

A classe “Financeira” está relacionada com a classe “Administrador” e “Operador”, pois o administrador e o operador são responsáveis por verificar se o valor obtido na recolha confere com o valor recebido em numerário.

A classe “Recolha” está relacionada com a classe “Auditoria” e “Módulo” pois não existem recolhas que não obtenham dados de auditoria e porque as recolhas de dados de auditoria são efectuadas por um determinado módulo de recolha.

A classe “Módulo” está relacionada com a classe “Maquina” pois, todos os módulos de recolha irão estar instalados em máquinas de *vending*.

A classe “Máquina” está relacionada com a classe “Localização” pois as máquinas de *vending* irão estar instaladas num determinado local.

A classe “Identificador” está relacionada com a classe “Repositor” pois, todos os repositores irão possuir um identificador que servirá para sua identificação na recolha de auditoria.

Na Tabela 11 é apresentada uma descrição sucinta das classes identificadas anteriormente.

Tabela 11 Descrição sucinta de cada classe identificada

Descrição Sucinta das Classes Identificadas	
Classe	Descrição
Calibração	Acção de aferição do erro de medição do registador.
Registador	Elemento instalado nas máquinas de <i>vending</i> que efectua o registo de dados das condições ambientais das máquinas.
Auditoria	Medição efectuada pelos diversos elementos de recolha de informação ligados às máquinas de <i>vending</i> . A auditoria recolhida poderá ser do tipo “Financeira” ou “Ambiental”.
Utilizador	Elemento que interage com o sistema. Os utilizadores podem pertencer a três perfis diferentes, “Administrador”, “Operador”, e “Repositor”.
Identificador	Elemento que irá identificar um repositor no momento da recolha de auditoria.
Recolha	Acção de obter dados de auditoria.
Máquina	Elemento onde são dispensados os produtos a vender.
Módulo	Elemento ao qual estão ligados os diversos elementos de recolha de auditoria e ao qual é ligado o dispositivo móvel a fim de obter dados de auditoria recolhidos.
Localização	Descrição do local onde se encontram instaladas as máquinas de <i>vending</i> .

Obteve-se assim o modelo de domínio apresentado na Figura 8.

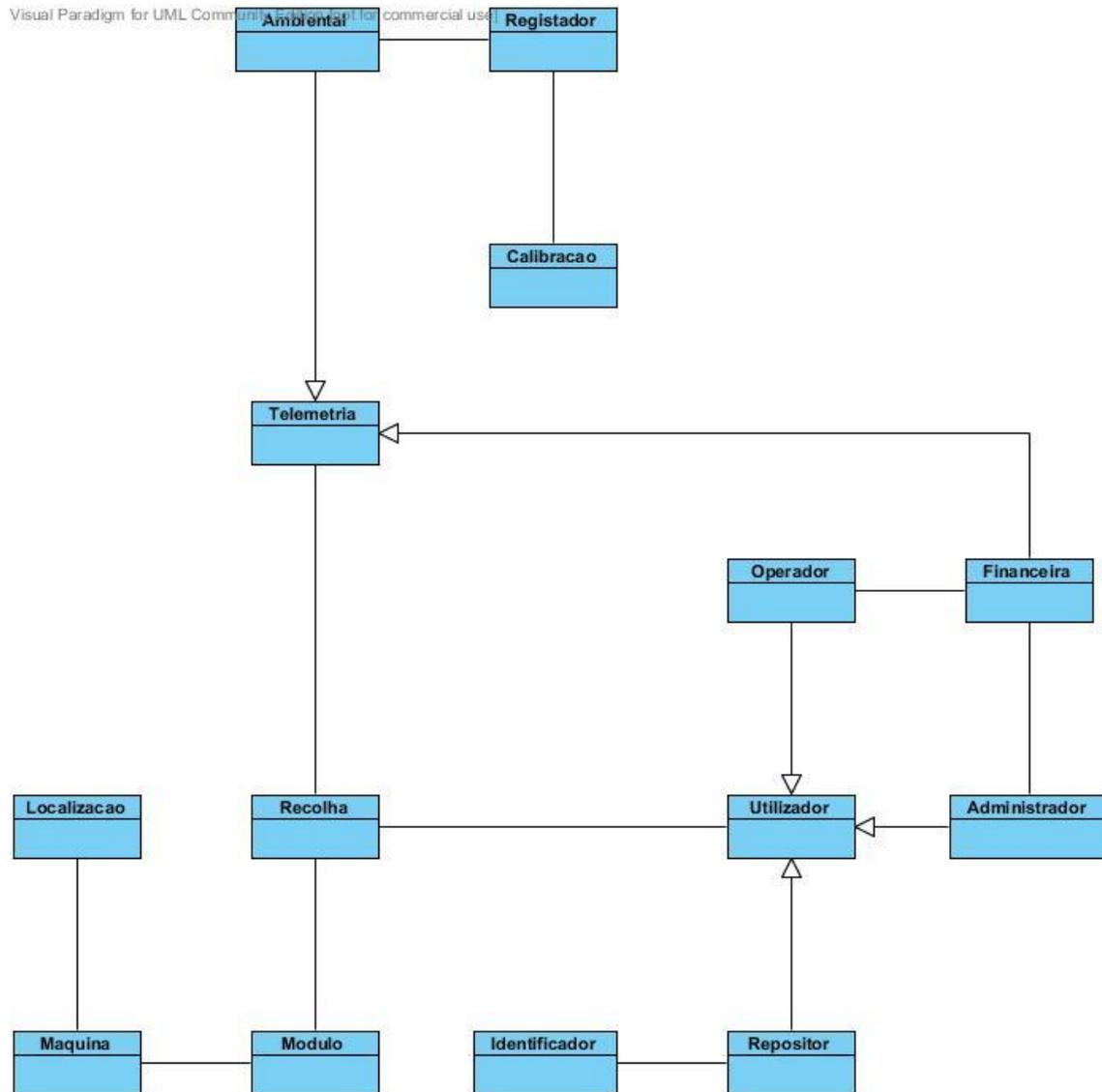


Figura 8 Modelo de domínio

5.2.1.2 Casos de Uso

Um caso de uso trata-se de uma sequência de acções realizadas por um actor de forma a atingir um objectivo, descrevendo os aspectos de utilização do sistema sem serem focalizados os detalhes da implementação (Ferreira, 2007b).

Os modelos de caso de uso são desenvolvidos juntamente com o modelo de domínio do sistema, e permitem identificar os objectos que compõe cada caso de uso, e detectar os fluxos de mensagens entre objectos sendo possível desta forma analisar a forma como estes interagem no caso de uso. (Ferreira, 2007b).

De seguida são identificados e descritos os actores do sistema, os casos de uso e ainda apresentados os seus diagramas.

Identificação dos Actores

Um actor representa o papel que um utilizador ou entidade desempenha no sistema em análise, pelo que um utilizador pode representar vários actores e um actor pode representar vários utilizadores (Ferreira, 2007a).

Um actor é aquele que realiza ou participa num caso de uso, ou seja, vários utilizadores podem desempenhar o mesmo papel (representado por um único actor), ou o mesmo utilizador pode desempenhar papéis diferentes (vários actores) (Ferreira, 2007a).

Um actor pode ser classificado como activo, um actor que desencadeia o caso de uso, ou como passivo, um actor que participa no caso de uso (Ferreira, 2007a).

Os actores podem ser identificados com base nas seguintes regras (Ferreira, 2007a):

- Regra 1 – Pensar em papéis e não nas pessoas ou profissões;
- Regra 2 – Pensar nas entradas e saídas de informação do sistema;
- Regra 3 – Um actor pode não ser um ser humano. Pode tratar-se de um sistema externo.

De acordo com as regras anteriores, os actores são obtidos analisando (Ferreira, 2007a):

- As pessoas que interagem directamente com o sistema;
- A(s) pessoa(s) responsável(eis) pela manutenção do sistema;
- Hardware externo utilizado pelo sistema;
- Outros sistemas que precisem de interagir com o sistema em análise.

Os actores são utilizados para obter os casos de uso. No entanto são particularmente importantes:

- Na configuração do sistema para diferentes perfis de utilização:
 - Cada perfil pode ser associado a um ou mais actores, limitando desta forma os casos de uso que cada utilizador pode executar.
- Na definição de políticas de segurança;

- Na negociação de competências.

De seguida são apresentados os diversos actores do sistema:

- Utilizador não autenticado: utilizador que ainda não está autenticado no sistema;
- Utilizador autenticado: utilizador que efectuou a sua autenticação no sistema com sucesso;
- Administrador: utilizador com privilégios para as seguintes funções:
 - Anular a confirmação de valores financeiros recolhidos;
 - Editar os dados das recolhas de auditoria financeira que se encontram incompletas;
 - Configurar os parâmetros de funcionamento da aplicação;
 - Efectuar a gestão de utilizadores;
 - Efectuar a gestão de máquinas de vending;
 - Efectuar a gestão de localizações de máquinas;
 - Efectuar a gestão de módulos de recolha de auditoria;
 - Efectuar a gestão de registadores de temperatura;
 - Efectuar a gestão de identificadores de repositores;
 - Introduzir dados de calibração dos registadores de temperatura.
- Operador: utilizador com privilégios para as seguintes funções:
 - Confirmação de valores financeiros recolhidos;
 - Visualizar todos os dados de auditoria recolhidos;
 - Gerar relatórios.
- Repositor: utilizador apenas com privilégios para recolha de auditoria junto das máquinas de *vending*.
- Dispositivo móvel: equipamento utilizado pelos repositores para efectuar a recolha de dados de auditoria junto das máquinas de *vending*.
- Módulo de recolha de auditoria: equipamento instalado na máquina de *vending* ao qual se encontram conectados os equipamentos de obtenção de auditoria.

De seguida são apresentados o diagrama global dos casos de uso, em que são apresentados os diversos conjuntos de casos de uso definidos, e ainda os diagramas detalhados de cada conjunto.

Diagrama Global dos Casos de Uso

Na Figura 9 é apresentado o diagrama global dos casos de uso.

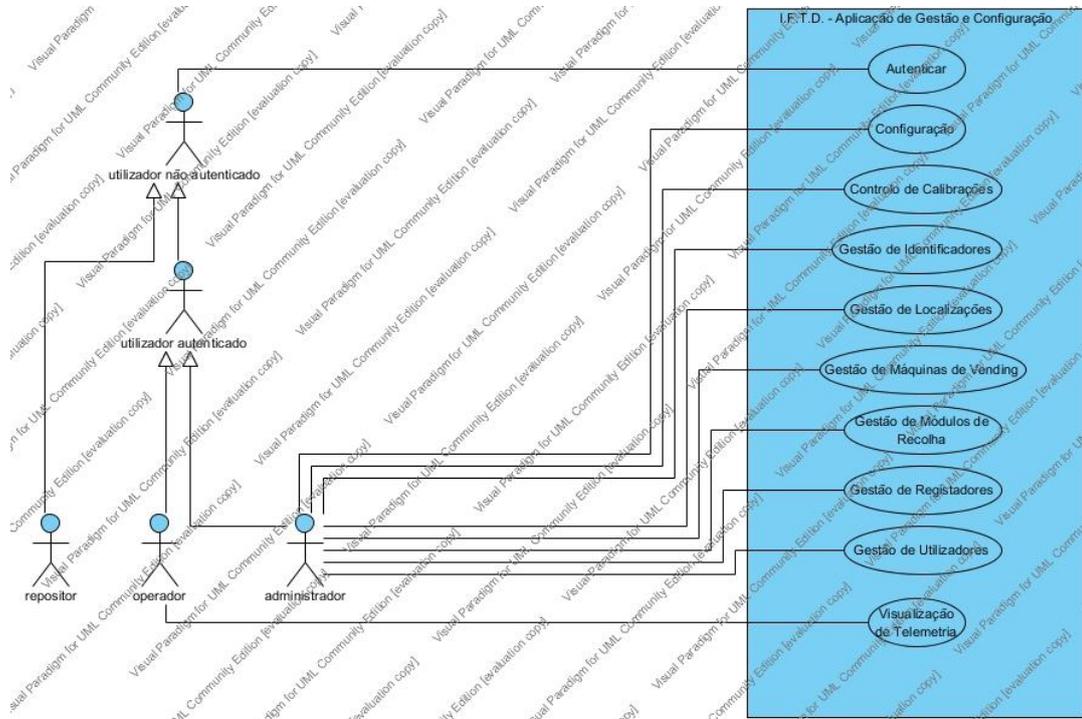


Figura 9 Diagrama global dos casos de uso do sistema

Diagramas Detalhados de Cada Conjunto de Casos de Uso

Na Figura 10 é apresentado o diagrama detalhado dos casos de uso do conjunto de casos de uso de autenticação.

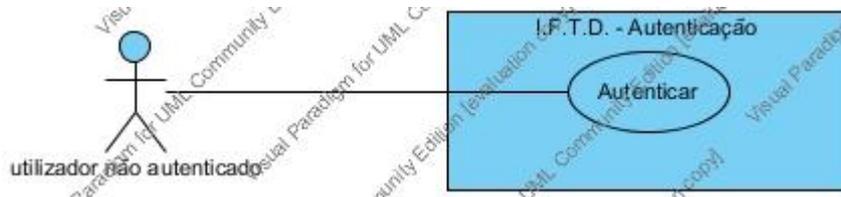


Figura 10 Diagrama do conjunto de casos de uso de autenticação

Fluxo de Eventos de Cada Caso de Uso

Na Tabela 12 é apresentada a descrição e o fluxo de eventos do caso de uso autenticar. As descrições e fluxos de eventos dos restantes casos de uso poderão ser consultados no Anexo 4.

Tabela 12 Fluxo de eventos do caso de uso "Autenticar"

Fluxo de Eventos de Caso de Uso		
Nome do Caso de Uso	Autenticar	
Descrição	Nesta secção deverá ser possível ao utilizador não autenticado autenticar-se perante o sistema.	
Actores	Utilizador não autenticado	
Caminho Principal		
Evento N°	Ação do Actor	Resposta do Sistema
1	O utilizador introduz as suas credenciais de acesso nos respectivos campos na janela de autenticação e carrega em “Entrar”;	
2		O sistema procede à validação das credenciais de acesso introduzidas pelo utilizador. Após verificar que os dados são válidos, o sistema redirecciona o utilizador para a janela principal da aplicação.
Caminhos Secundário		
Evento N°	Ação do Actor	Resposta do Sistema
1	O utilizador na janela de autenticação carrega em “Sair”;	
2		O sistema fecha a janela de autenticação e termina a aplicação.
1	O utilizador, na janela de autenticação introduz credencias de autenticação inválidas e carrega em “Entrar”;	
2		O sistema verifica que as credenciais introduzidas são inválidas e apresenta uma janela com uma mensagem de erro;

3	O utilizador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e apresenta a janela de autenticação.
1	O utilizador, na janela de autenticação, preenche apenas um dos elementos que compõe as credenciais de acesso e carrega em “Entrar”;	
2		O sistema verifica que existem elementos em falta e apresenta uma janela com uma mensagem de erro;
3	O utilizador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e apresenta a janela de autenticação.
1	O utilizador após introduzir as credenciais de acesso na janela de autenticação carrega em “Entrar”;	
2		O sistema ao tentar conectar-se ao servidor de contas verifica uma falha na ligação e apresenta uma janela com uma mensagem de erro;
3	O utilizador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e apresenta a janela de autenticação;

5.2.2 Modelo de Dados

Relativamente ao modelo de dados foram identificadas e descritas as várias entidades que compõe as base de dados da solução, desenhados os DER (Diagramas Entidade-Relacionamento), e apresentadas as tabelas resultantes após derivação das relações entre as entidades. Todo o trabalho realizado relacionado com o modelo de dados pode ser consultado no Anexo 4.

Desenho de Protótipos

Neste capítulo são apresentadas as fases de desenho do dispositivo móvel de recolha de auditoria, do módulo de recolha de auditoria, do emulador de moedeiro, e da aplicação de gestão e configuração.

Após a conclusão da fase de análise deu-se início à fase de desenho dos vários protótipos da solução. Para cada um dos equipamentos a desenvolver foi efectuada uma avaliação do *hardware* a utilizar, desenhados os esquemas de ligações, e descritos os principais processos a serem executados pelo *firmware* a desenvolver. Para além do desenho dos protótipos dos equipamentos, são também apresentados os primeiros protótipos não funcionais da aplicação de gestão e configuração.

6.1 Dispositivo Móvel de Recolha de Auditoria

Nesta secção é apresentada a fase de desenho do dispositivo móvel de recolha de auditoria, nomeadamente a abordagem que foi feita relativamente ao *hardware* utilizado, os esquemas de ligações do protótipo desenvolvido e a descrição dos principais processos do *firmware* a desenvolver.

6.1.1 Avaliação do Hardware Utilizado

No desenvolvimento do dispositivo móvel, de entre os diversos componentes electrónicos, destacam-se o modem, o microcontrolador e o LCD utilizados. De seguida será apresentada uma breve descrição de cada um dos componentes utilizados.

6.1.1.1 Modem

O modem utilizado, um *Cinterion/Siemens TC-65i*, trata-se de um modem GSM de classe 12, *Quad-Band*, com capacidade de 86kbps de *uplink* e *downlink*. Duas características interessantes deste modem são a *Java Virtual Machine* integrada no modem e a utilização do protocolo TCP/IP através de comandos AT, tendo esta última, demonstrado ser bastante útil no desenvolvimento do projecto, pois através de comandos AT foi possível estabelecer uma ligação *socket*.

Para além das características referidas anteriormente, destacam-se ainda a possibilidade de ligação ao modem através de interfaces USB, I2C (*Inter-Integrated Circuit*), SPI (*Serial Peripheral Interface Bus*) e série, e ainda a capacidade de monitorização de RLS (*Radio Link Stability*) para detecção de *jamming*.

6.1.1.2 Microcontrolador

O microcontrolador escolhido foi o *PIC18F26k20* da *Microchip*®. O *PIC18F26k20* trata-se de um microcontrolador de arquitectura de 8 *bits* de baixo custo. Deste microcontrolador destaca-se os 3,936 *Bytes* de memória RAM, os 1024 *Bytes* de memória EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), uma interface de comunicação UART, o baixo consumo energético e o baixo custo.

6.1.1.3 LCD

O LCD utilizado foi escolhido com base em dois aspectos, a capacidade de ser facilmente conectado ao microcontrolador e o baixo custo.

Dados os dois aspectos mencionados optou-se por utilizar o LCD monocromático *LM6060CBY* da *Topway*. Este LCD utiliza o controlador *ST7565P*, que permite utilizar o LCD em modo de funcionamento 6800 e 8080, sendo estes modos de funcionamento em paralelo, e em modo série. A fim de se poder reduzir o número de pinos do microcontrolador a serem utilizados para a ligação ao LCD, optou-se por colocar o LCD em modo de funcionamento série, conseguindo-se assim reduzir o número de pinos necessários de 13 para 8.

A descrição dos pinos do LCD e a configuração dos *jumper*s função do LCD pode ser consultada no Anexo 6.

6.1.2 Prototipagem

Nas Figuras 11, 12, 13, 14, 15, 16, e 17 são apresentados os esquemas de ligação dos vários componentes que compõe o esquema de ligações do protótipo do dispositivo móvel de recolha de auditoria.

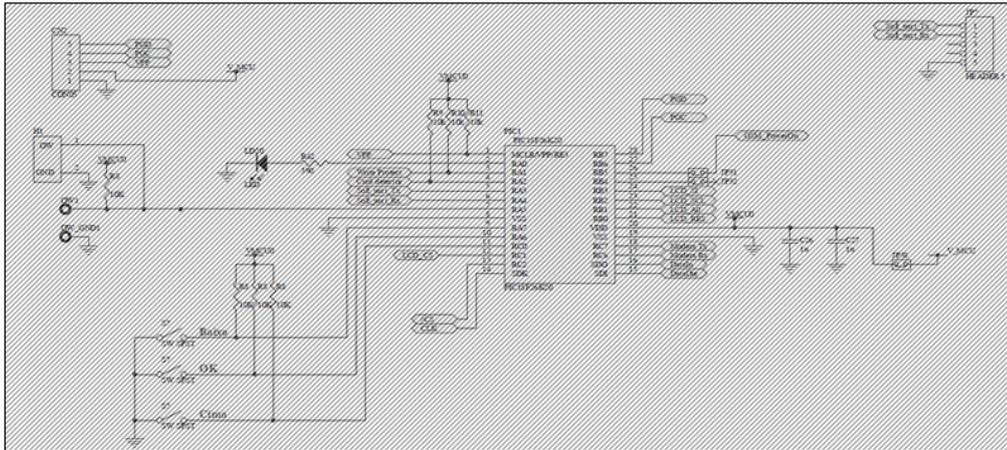


Figura 11 Esquema de ligações da unidade central de processamento

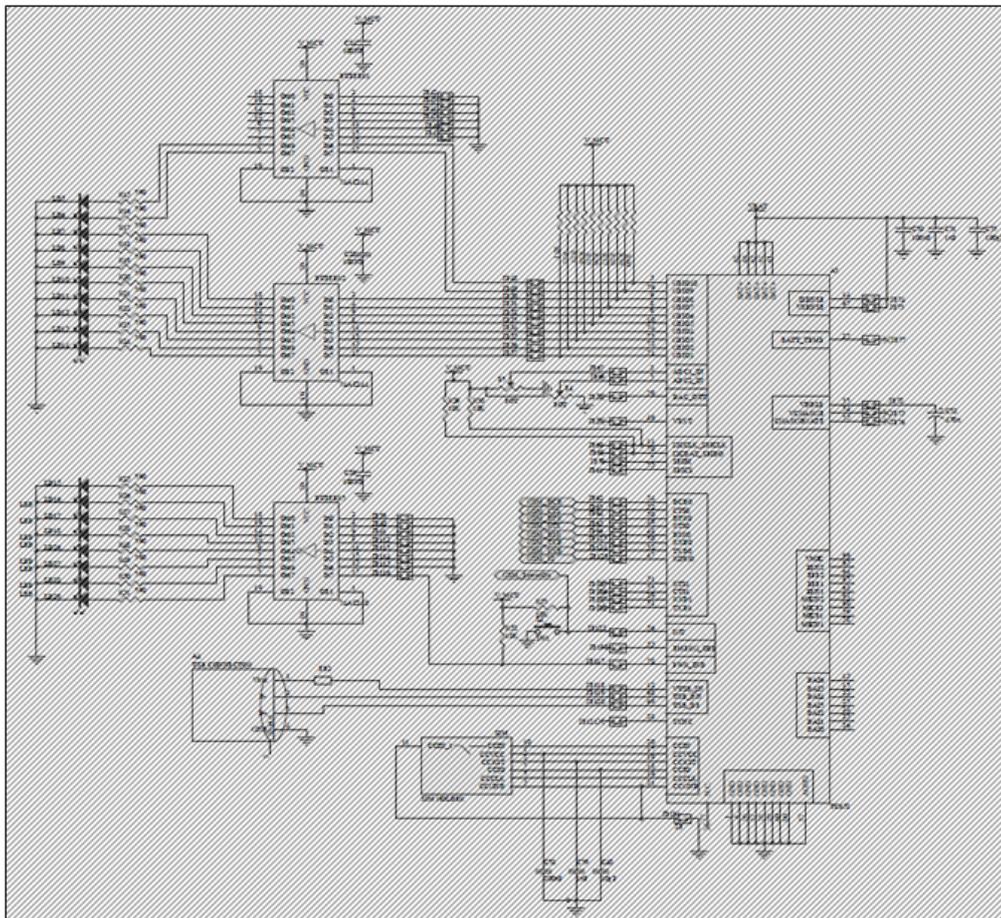


Figura 12 Esquema de ligações do modem GSM

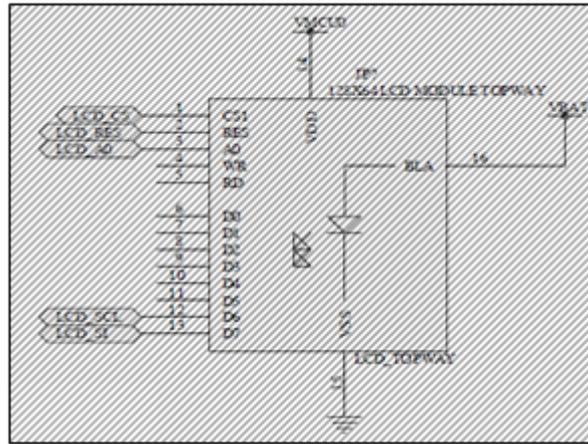


Figura 13 Esquema de ligações do LCD

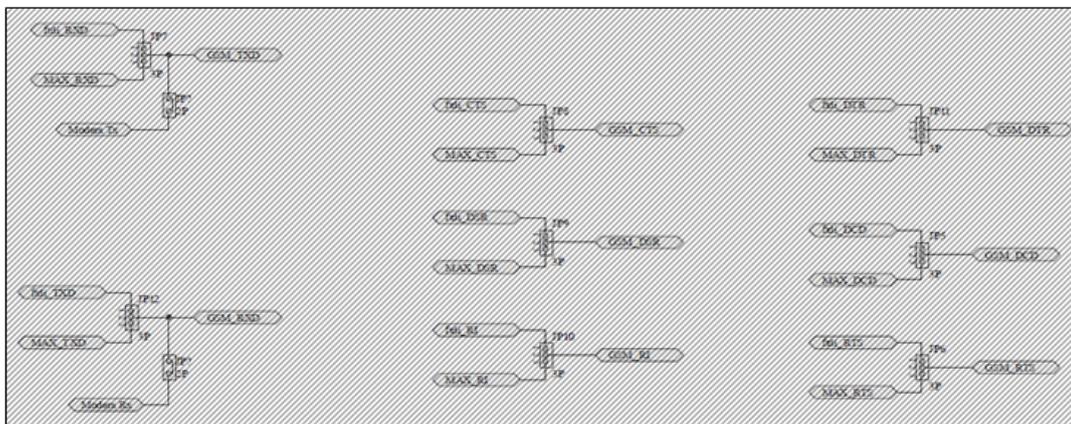


Figura 14 Esquema de ligações aos módulos de transmissão de dados

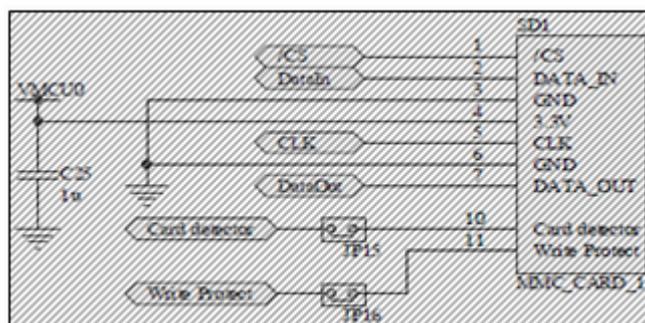


Figura 15 Esquema de ligações do leitor de cartões SD

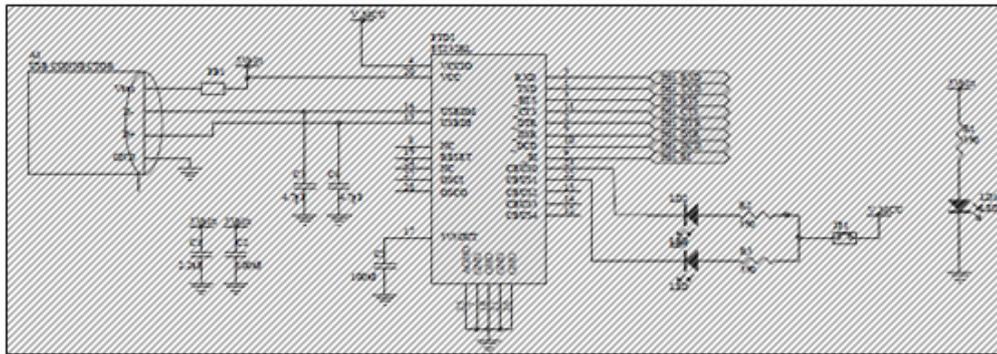


Figura 16 Esquema de ligações da interface USB de *debug*

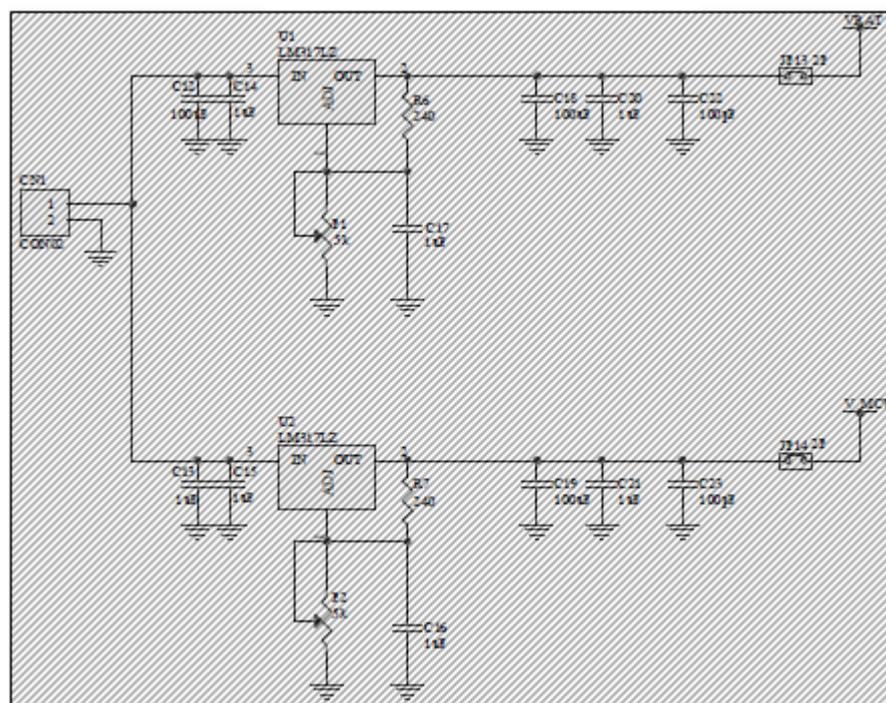


Figura 17 Esquema de ligações do circuito de alimentação

6.1.3 Fluxo de Eventos dos Principais Processos

De seguida será apresentada uma descrição do fluxo de eventos dos principais processos a serem executados pelo *firmware* do dispositivo móvel de recolha de auditoria.

6.1.3.1 Processo Principal

Após o arranque do dispositivo e após serem executadas as inicializações necessárias, é apresentado ao utilizador o menu principal do sistema, ficando o dispositivo a partir deste momento num ciclo infinito a verificar se o utilizador introduziu alguma opção.

Caso a opção introduzida seja “Descarregar Auditoria” é apresentado ao utilizador o menu de descarga de auditoria. Após ser apresentado o menu de descarga de auditoria o dispositivo fica novamente a aguardar que o utilizador introduza a opção pretendida. Caso o utilizador seleccione descarregar todos os tipos de auditoria, será enviado para o dispositivo de recolha o comando de descarga de auditoria financeira e após descarga da auditoria financeira é enviado o comando de descarga de auditoria ambiental. No final do processo de descarga de auditoria ambiental é novamente apresentado o menu de descarga de auditoria. No entanto, se o utilizador seleccionar apenas a opção de descarga de auditoria financeira ou a opção de descarga de auditoria ambiental é enviado o comando respectivo para o dispositivo de recolha.

Caso a opção seleccionada pelo utilizador no menu principal seja “Configurações” é apresentado o menu de configuração do dispositivo, ficando o dispositivo de seguida a aguardar que o utilizador seleccione a operação que pretende executar. Se o utilizador seleccionar a opção de definir o intervalo entre leituras é-lhe apresentado o menu de definição do código PIN (*Personal Identification Number*). Após definir o código PIN é apresentado novamente ao utilizador o menu de configuração. No entanto, se o utilizador seleccionar a opção de definir o intervalo entre leituras é apresentado o menu de definição de intervalo entre leituras sendo redireccionado novamente para o menu de configuração no final da operação.

Por fim, se o utilizador seleccionar a opção de desligar o dispositivo, são efectuadas as operações de verificação da existência de dados de auditoria e de seguida desliga o dispositivo.

O processo descrito é ilustrado no fluxograma apresentado na Figura 18.

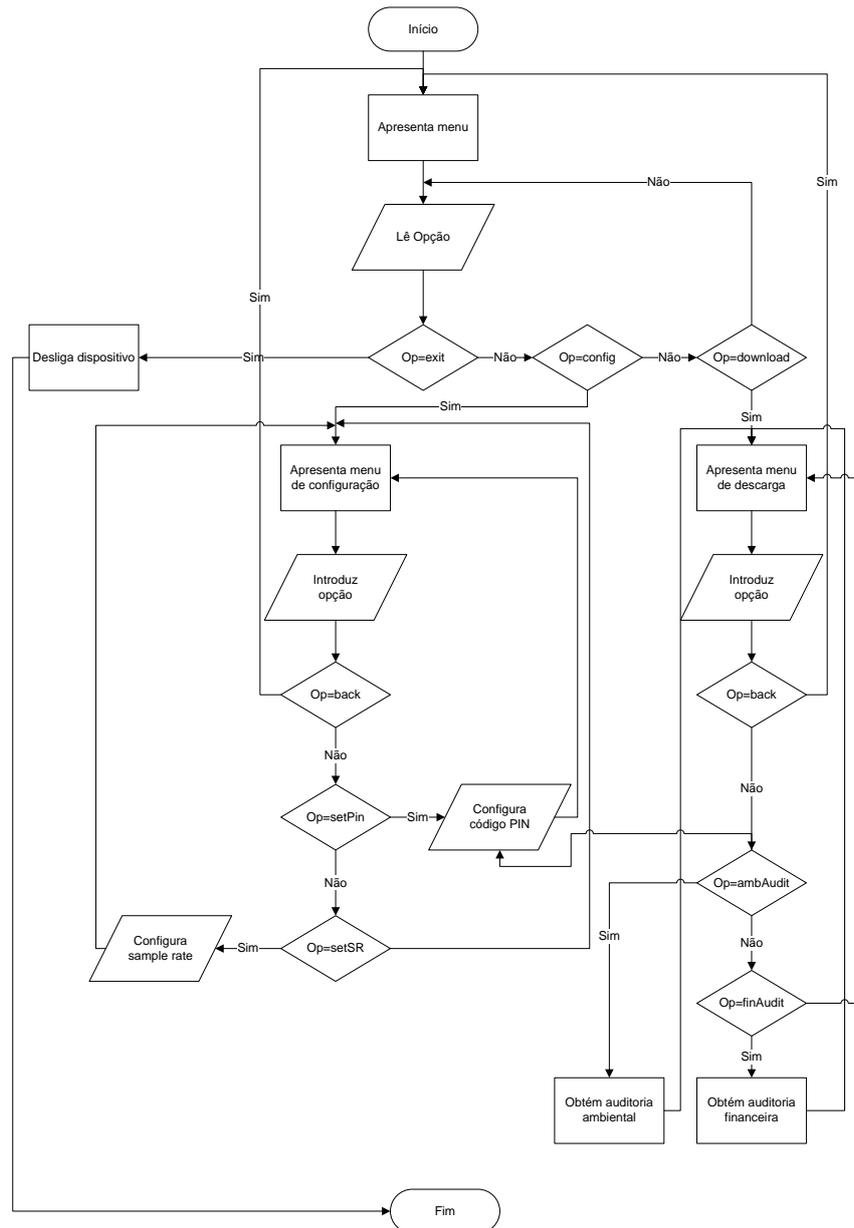


Figura 18 Fluxograma do funcionamento geral do firmware do dispositivo móvel

6.1.3.2 Descarga de Auditoria

Após verificação do tipo de auditoria a descarregar, o dispositivo móvel envia o comando respectivo para o dispositivo de recolha de auditoria. Após envio do comando de descarga de auditoria o dispositivo móvel lê os dados obtidos pelo dispositivo de recolha e guarda-os num ficheiro no cartão SD. Após os dados serem descarregados do dispositivo de recolha o dispositivo móvel procede ao envio dos dados para o servidor. Caso os dados sejam enviados com sucesso é apresentada uma mensagem de sucesso ao utilizador e apaga o

ficheiro onde foram armazenados os dados. Pelo contrário, caso os dados não sejam enviados com sucesso, é apresentada uma mensagem de erro ao utilizador.

Na Figura 19 é pode ser consultado o fluxograma do processo de descarga de auditoria.

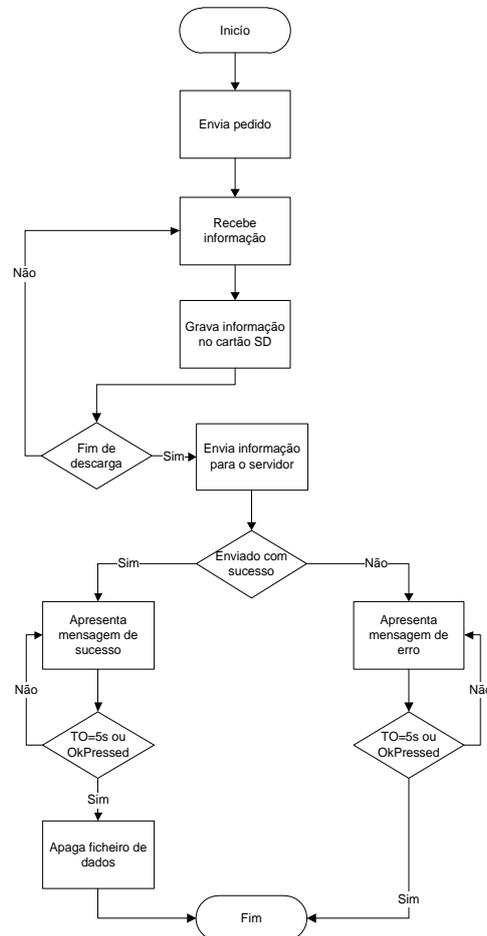


Figura 19 Fluxograma da operação de descarga de auditoria

6.1.3.3 Oclusão do Equipamento

O utilizador ao seleccionar a opção para desligar o dispositivo móvel, é verificado se existem ficheiros com dados de auditoria. Caso existam, o dispositivo móvel tenta enviar os dados para o servidor, e em caso de sucesso apaga o ficheiro correspondente aos dados enviados seguindo-se a apresentação de uma mensagem de sucesso. Caso os dados não sejam enviados com sucesso é apresentada uma mensagem de erro ao utilizador.

Na Figura 20 é apresentado o fluxograma representativo do processo descrito.

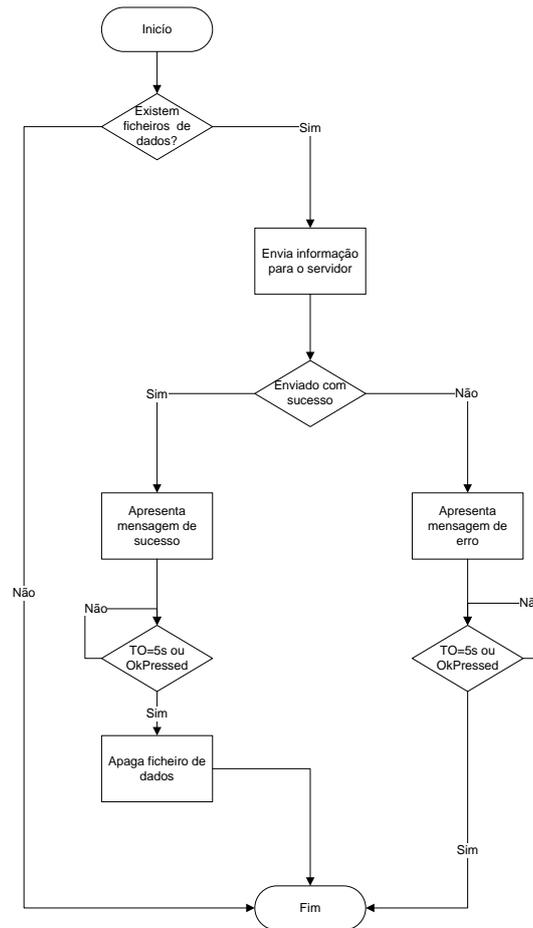


Figura 20 Fluxograma da operação de oclusão do dispositivo móvel

6.2 Módulo de Recolha de Auditoria

Nesta secção é apresentada a fase de desenho do dispositivo móvel de recolha de auditoria, nomeadamente a descrição do microcontrolador utilizado, o esquemático do protótipo desenvolvido e a descrição dos principais processos do *firmware* a desenvolver.

6.2.1 Prototipagem

Na Figura 21 é apresentado o esquema de ligações do protótipo do módulo de recolha de auditoria.

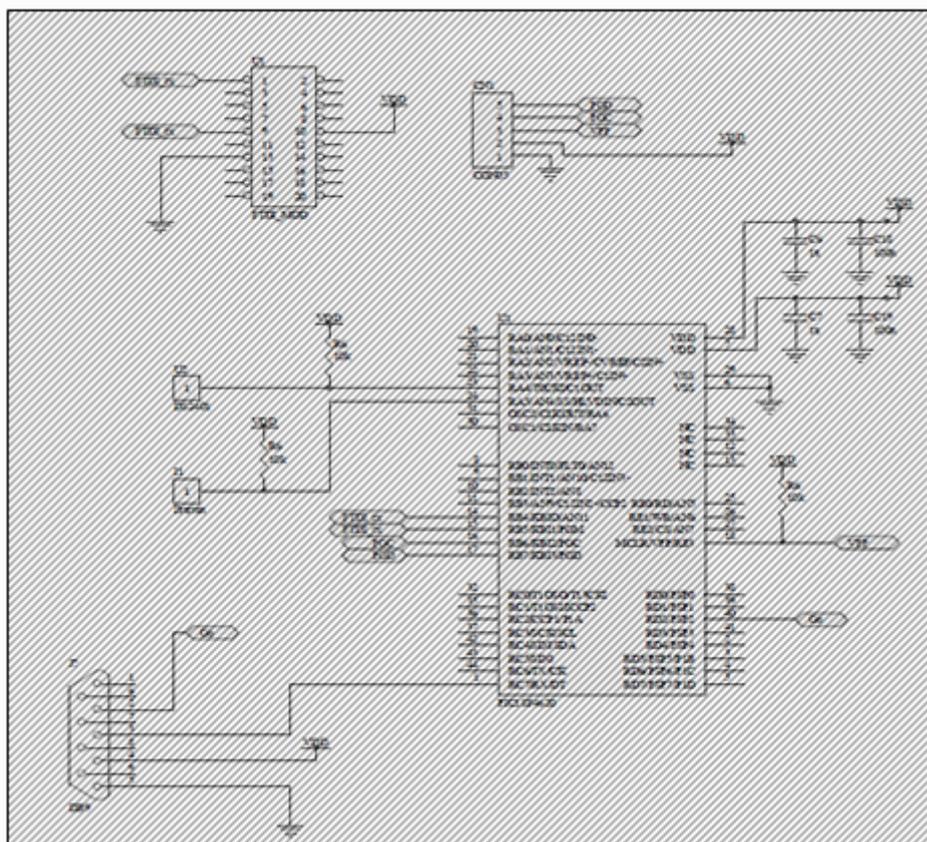


Figura 21 Esquemático geral do dispositivo de recolha de auditoria

6.2.2 Fluxo de Eventos

De seguida são apresentados os diagramas de fluxo de eventos juntamente com uma breve descrição dos aspectos mais relevantes do *firmware* a ser executado no módulo de recolha de auditoria.

6.2.2.1 Processo Principal

O dispositivo de recolha de auditoria encontra-se num ciclo infinito a verificar a recepção de um comando de descarga de auditoria. Ao receber um comando é verificado qual o tipo de auditoria que é pretendido. Se for o comando de recolha de auditoria financeira, o dispositivo de recolha procede à obtenção de dados existentes no moedeiro, se pelo contrário for o comando de descarga de auditoria ambiental o dispositivo de recolha procede à obtenção dos dados existentes no registador de temperatura, ou seja, no *iButton DS1921G*.

No fluxograma apresentado na Figura 22 é ilustrado o processo descrito.

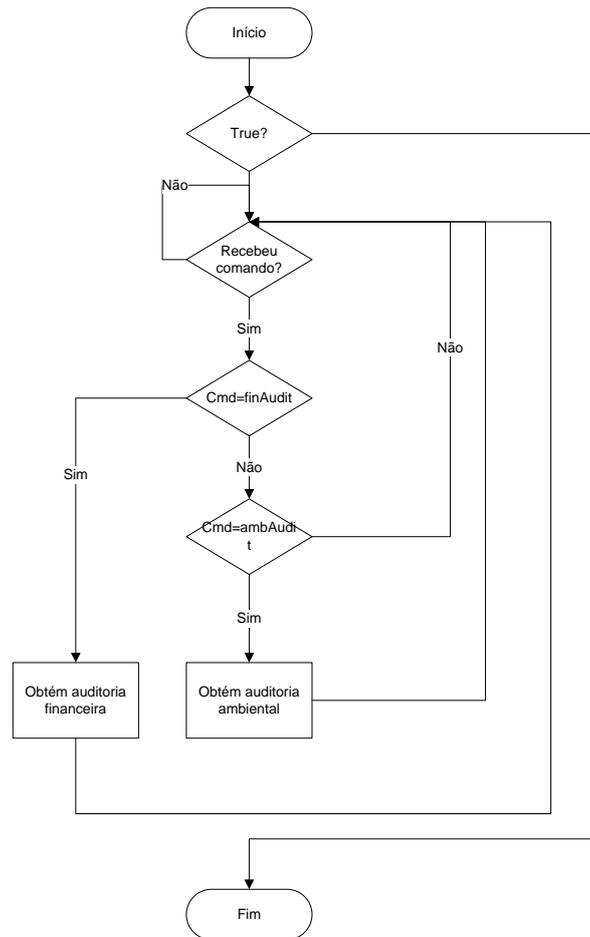


Figura 22 Fluxograma do processo principal

6.2.2.2 Obtenção de Auditoria Ambiental

O dispositivo de recolha ao receber o comando de descarga de auditoria ambiental dá início ao processo de obtenção dos dados recolhidos pelo registador de temperatura.

Inicialmente é verificado se o registador se encontra ligado ao dispositivo de recolha, caso o registador não se encontre ligado é interrompida a descarga e enviado um pacote de erro para o dispositivo móvel. Se o registador de temperatura tiver sido detectado, o dispositivo de recolha obtém os parâmetros de configuração do período de registo em curso no registador obtendo de seguida os valores de temperatura registados.

Após obter todos os valores de temperatura registados, o dispositivo de recolha cria o pacote de dados a enviar para o dispositivo móvel e procede ao seu envio. Se o ocorrer alguma falha no envio procede-se a uma nova tentativa de envio, até a um máximo de três tentativas.

Após o envio de dados com sucesso para o dispositivo móvel, o dispositivo de recolha termina o período de registo a decorrer no registador e começa um novo período com os mesmos parâmetros com que o período anterior se encontrava configurado, à excepção do intervalo entre leituras que é recebido juntamente com o comando de descarga de auditoria ambiental.

No fluxograma apresentado na Figura 23 é ilustrado o processo descrito.

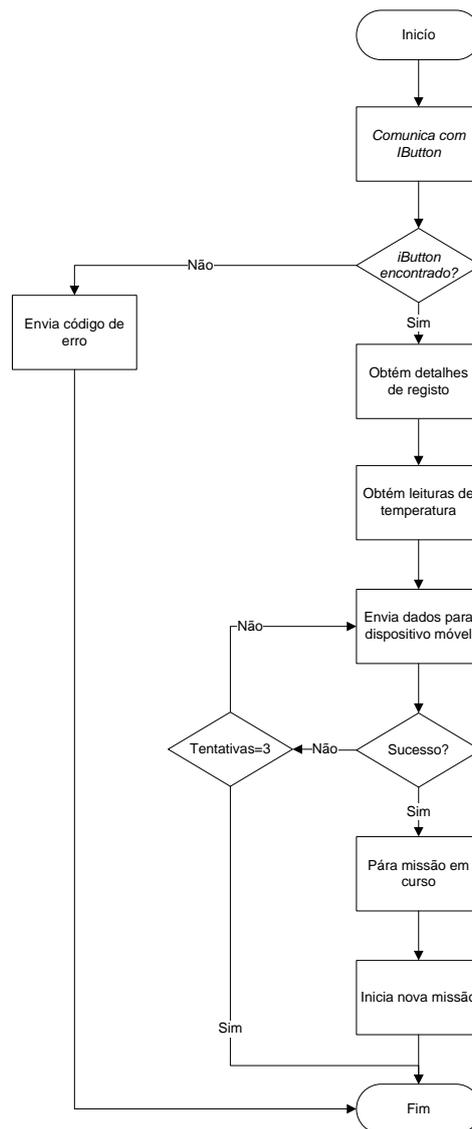


Figura 23 Fluxograma do processo de obtenção de auditoria ambiental

6.2.2.3 Obtenção de Auditoria Financeira

O dispositivo de recolha ao receber o comando de descarga de auditoria financeira dá início ao processo de obtenção dos dados fornecidos pelo moedeiro instalado na máquina de vending.

Para dar início à obtenção dos dados de auditoria financeira o dispositivo de recolha coloca a linha para sinalização de início de descarga a 0. Se o moedeiro não tiver iniciado o envio de dados, a obtenção de dados será interrompida e é enviado um pacote de erro para o dispositivo móvel. Após o moedeiro ter procedido à descarga da informação é criado o pacote a enviar para o dispositivo móvel com os dados obtidos, procedendo de seguida ao seu envio. À semelhança do que acontece com a descarga de auditoria ambiental, caso ocorra algum erro, procede-se à tentativa de reenvio até um máximo de três vezes.

No fluxograma apresentado na Figura 24 é ilustrado o processo descrito.

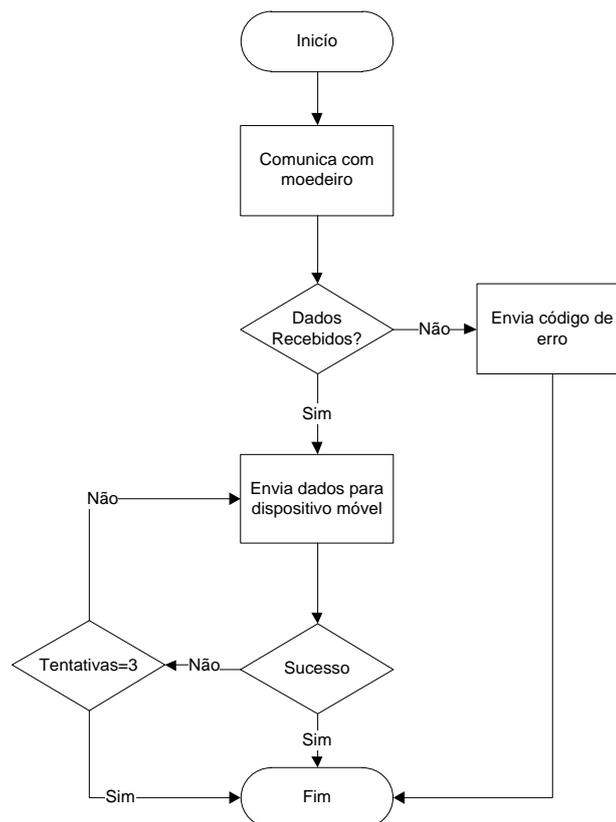


Figura 24 Fluxograma do processo de obtenção de auditoria financeira

6.3.2 Fluxo de Eventos do Processo Principal do Emulador

O *firmware* a ser executado no emulador trata-se de uma função muito simples, ilustrada na Figura 27, e consiste na verificação constante do valor do pino de CTS (*Clear to Send*). Ao detectar que o pino de CTS foi colocado a 0, acende o LED (*Light Emitting Diode*) para dar indicação de que foi estabelecida comunicação. De seguida envia um exemplar de um *ticket* semelhante aos emitidos pelos moedeiros MEI® e conclui o processo desligando o LED. O processo de envio do *ticket* poderá ainda ser despoletado ao carregar no botão colocado no emulador.

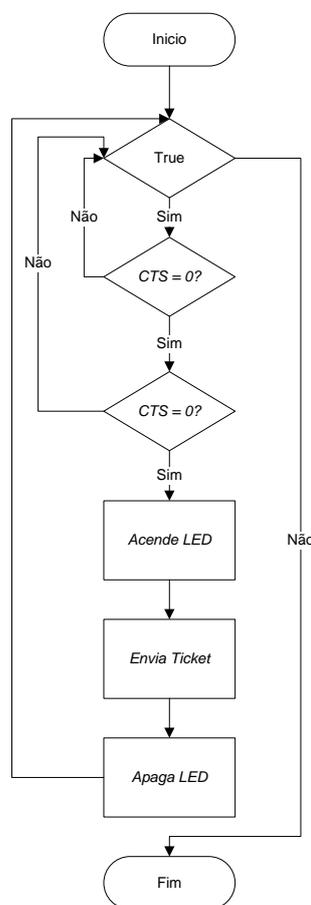


Figura 27 Fluxograma do funcionamento do emulador de moedeiro MEI®

6.4 Aplicação de Gestão e Configuração

Nesta secção são apresentados os protótipos não funcionais da interface da aplicação de gestão e configuração.

6.4.1 Prototipagem

De seguida são apresentados os protótipos desenhados, particularmente os protótipos da janela principal, da janela de gestão, da janela de detalhes de auditoria e a janela de configuração.

Nas Figuras 28, 29, 30, 31, 32 e 33 são apresentados os vários protótipos não funcionais da aplicação de gestão e configuração desenhados.

Figura 28 Janela principal - vista de recolhas

Figura 29 Janela principal - vista de estatísticas

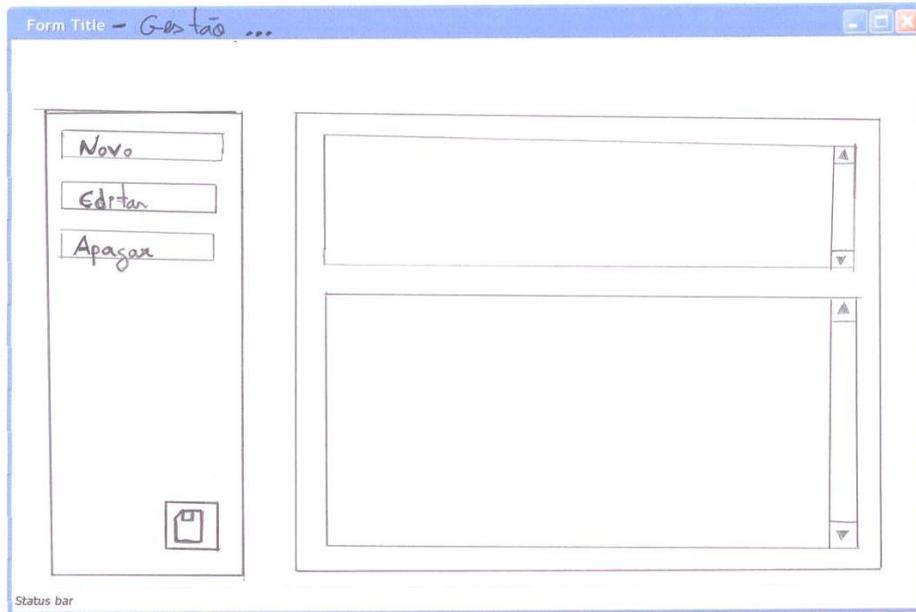


Figura 30 Janela de gestão (genérica)

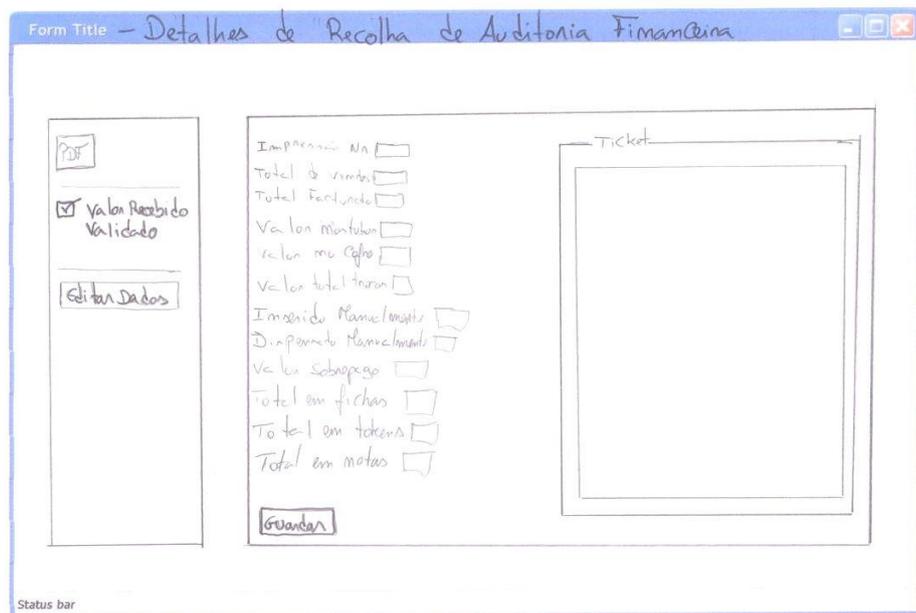


Figura 31 Janela de detalhes de auditoria financeira

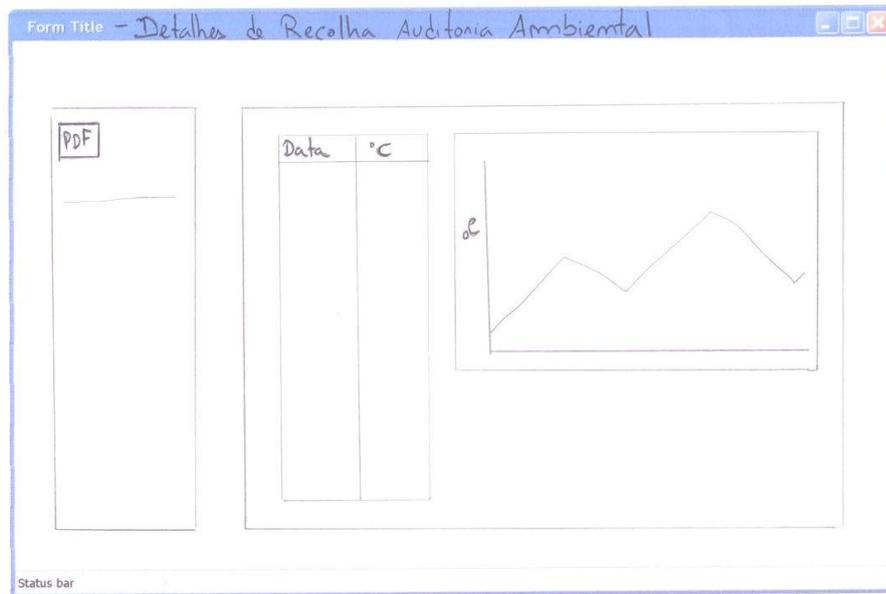


Figura 32 Janela de detalhes de auditoria ambiental

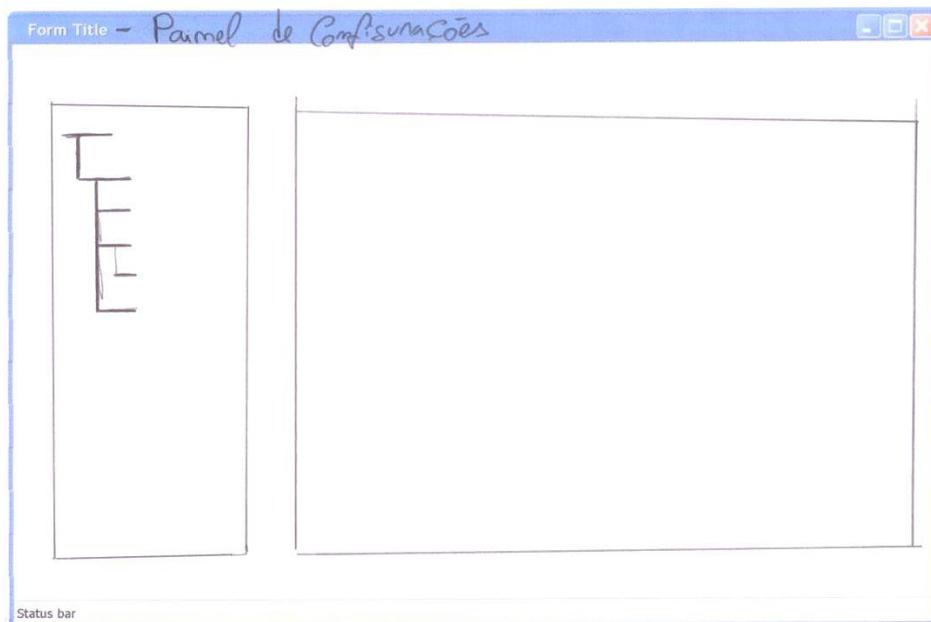


Figura 33 Janela de configurações

Implementação

Neste capítulo são apresentados os pormenores considerados relevantes durante a fase de implementação da solução proposta.

De seguida serão abordados os pormenores relativos à implementação do sistema, nomeadamente da implementação do *firmware* do dispositivo móvel, do *firmware* do módulo de recolha de auditoria e finalmente do *WebService*.

Inicialmente são apresentadas as ferramentas utilizadas durante a implementação da solução, particularmente a ferramenta direccionada às interfaces série, o IDE utilizado para o desenvolvimento de *firmware*, o *software* utilizado para efectuar o carregamento do *firmware* desenvolvido para os microcontroladores, e ainda os programadores utilizados. Após a descrição das ferramentas utilizadas é apresentada a fase de implementação do *firmware* e servidores desenvolvidos.

7.1 Ferramentas Utilizadas

Segue-se uma listagem das ferramentas utilizadas consideradas relevantes no desenvolvimento deste projecto.

7.1.1 Docklight

O *Docklight* é uma ferramenta de teste, análise e simulação direccionada às portas que utilizam o protocolo série (entre eles, o protocolo RS-232 e o RS-485/422). Com esta ferramenta é possível monitorizar a comunicação com um ou dois dispositivos. O *Docklight* é de fácil instalação e utilização, e pode ser utilizado na maioria dos computadores que utilizem o *Windows*® 7, o *Windows*® Vista, o *Windows*® XP ou o *Windows*® 2000/NT 4 (Heggelbacher, 2011).

Deste modo, esta ferramenta foi utilizada neste projecto para monitorizar as comunicações efectuadas via porta série, nomeadamente entre o dispositivo móvel e o dispositivo de recolha, e as comunicações efectuadas com o modem inserido no dispositivo móvel.

Interface for Audit Download

O *Docklight* (Figura 34) foi ainda essencial para testar e definir a ordem correcta dos comandos *AT* a serem enviados para o modem, assim como para testar o funcionamento do dispositivo de recolha.

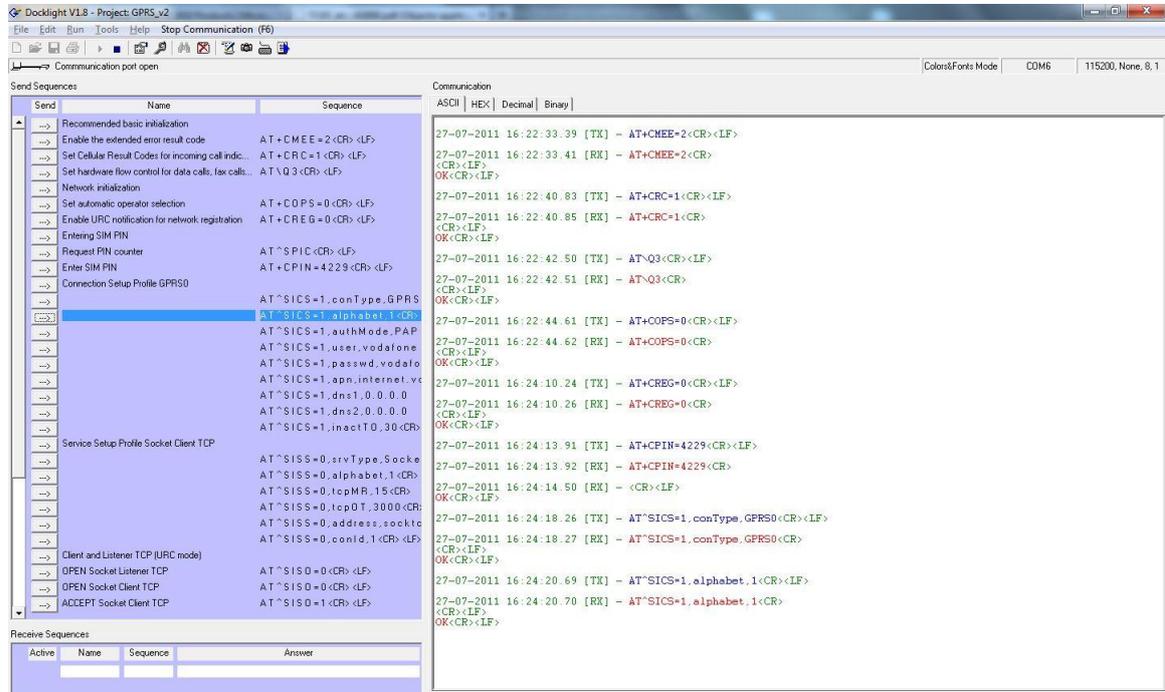


Figura 34 Captura de ecrã do Docklight

7.1.2 mikroC PRO for PIC

O *mikroC PRO for PIC* (Figura 35) é um IDE produzido pela *MikroElektronika* para desenvolvimento e programação de microcontroladores PIC. Com esta ferramenta é possível desenvolver *firmware* para uma vasta gama de microcontroladores PIC®.

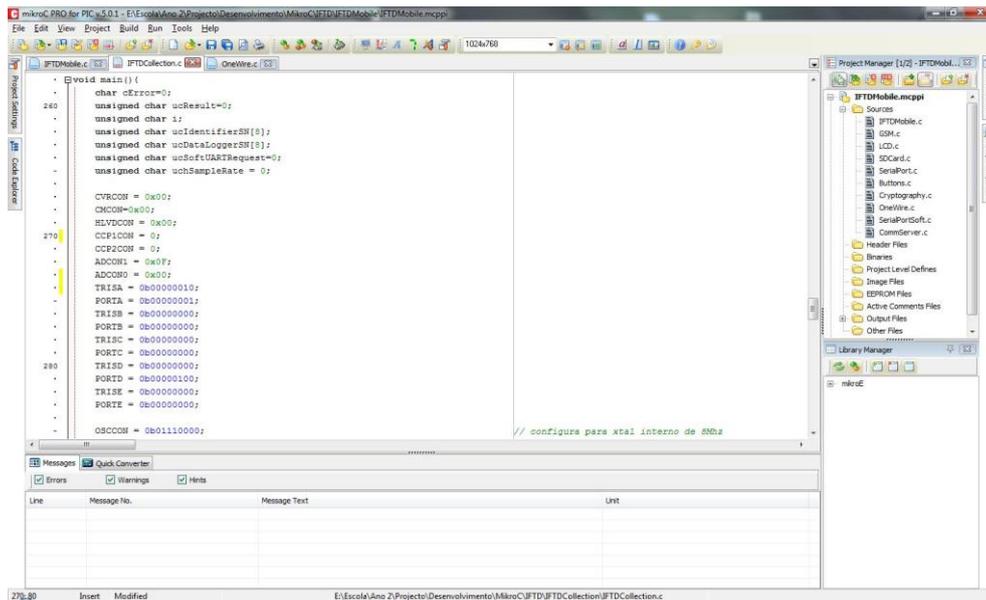


Figura 35 Captura de ecrã do *mikroC PRO for PIC*

Entre as diversas características do IDE, destacam-se o gestor de bibliotecas (Figura 36), o assistente de código, o assistente de parâmetros, o editor de projecto, o simulador de *software*, e o *in-circuit debbuger*.

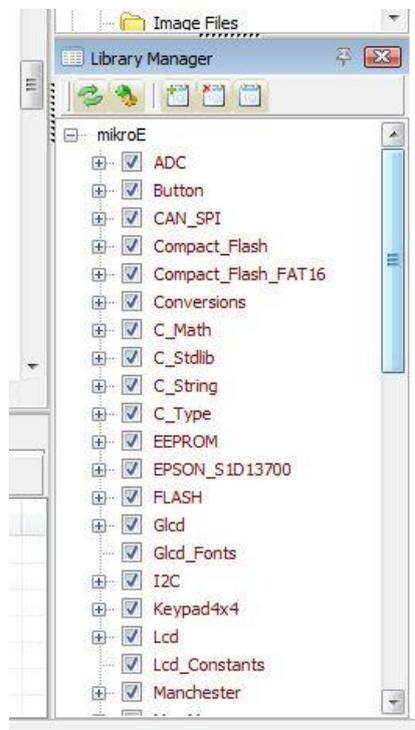


Figura 36 Captura de ecrã do gestor de bibliotecas do *mikroC PRO for PIC*

O gestor de bibliotecas permite ao programador facilmente escolher qual a biblioteca que pretende utilizar no seu projecto. Através da selecção da *checkbox* correspondente é possível incluir as bibliotecas necessárias ao projecto sem ser necessário fazer os *#include* das mesmas. É possível ainda com o gestor de bibliotecas incluir bibliotecas de terceiros após estas terem sido instaladas com gestor de pacotes (MikroElektronika, 2011). Entre as diversas bibliotecas estão incluídos conjuntos de bibliotecas de comunicação e de armazenamento, dos quais foram utilizadas algumas bibliotecas para o desenvolvimento deste projecto.

O assistente de código (Figura 37), apesar de ser uma característica comum nos IDEs recentes, merece o seu destaque visto tratar-se uma característica muito útil ao programador, permitindo com a combinação *ctrl* + barra de espaço aceder a funções, constantes e variáveis, minimizando desta forma erros de sintaxe (MikroElektronika, 2011).



Figura 37 Captura de ecrã do assistente de código do *mikroC PRO for PIC*

À semelhança do assistente de código, o assistente de parâmetros (Figura 38) permite, através da combinação de teclas *ctrl* + *shift* + barra de espaço, aceder à listagem de parâmetros das funções, evitando assim que o programador tenha a necessidade de memorizar o nome e os tipos dos parâmetros das funções (MikroElektronika, 2011).



Figura 38 Captura de ecrã do assistente de parâmetros do *mikroC PRO for PIC*

O editor de projecto (Figura 39) permite configurar todos os bits de configuração do microcontrolador que se está a programar, seleccionando apenas opções válidas e sendo possível guardar as configurações efectuadas e reutiliza-las noutro projecto (MikroElektronika, 2011).

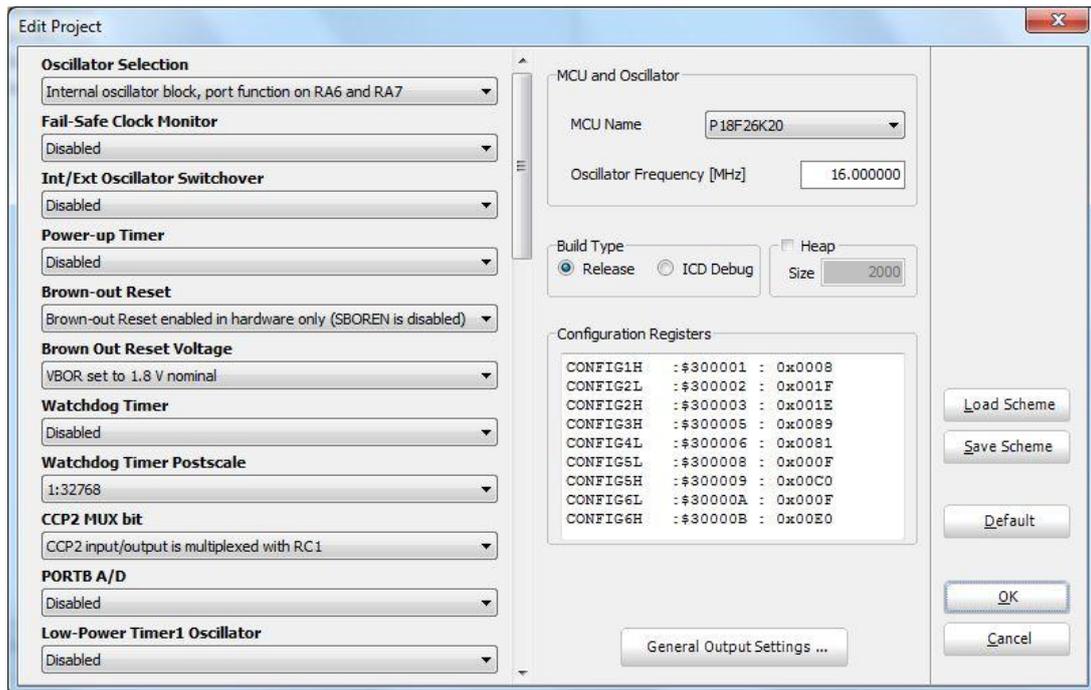


Figura 39 Captura de ecrã do editor de projecto do *mikroC PRO for PIC*

O simulador de *software* permite monitorizar valores de variáveis através da simulação de execução do *software* desenvolvido no computador, permitindo ainda através da utilização do *Watch Clock* medir os tempos de execução das funções tanto em milissegundos como em ciclos de relógio (MikroElektronika, 2011).

O *mikroC PRO for PIC* quando utilizado juntamente com o programador USB *mikroProg* suporta *In-Circuit Debug*. Com esta funcionalidade é possível efectuar as operações comuns de *debug*, tais como, *Step-over*, *Step-into*, *Step-out*, *Run*, *Run to cursor* (MikroElektronika, 2011).

7.1.3 MPLAB®

O *MPLAB®* trata-se de um IDE livre produzido pela *Microchip®* para desenvolvimento de *firmware* para microcontroladores de 8, 16 e 32 *bits* fabricados pela *Microchip®*. Para além dos compiladores incluídos, o *MPLAB®* suporta a instalação e utilização de compiladores produzidos por terceiros.

O *MPLAB®*, à semelhança do *mikroC PRO for PIC*, contém um gestor de projecto, um simulador de *software*, um *debugger*, e ainda possui suporte para os programadores da

Microchip® como por exemplo o *ICD 3*, o *ICD 2*, e os *PICKits 1, 2 e 3* (Microchip, 2011b).

O *MPLAB*® foi utilizado em conjunto com o *ICD2* e o *PICKit 2* para carregar para os microcontroladores o *firmware* desenvolvido.

7.1.4 PICKit 2

O *PICKit 2* (Figura 40) é um programador de baixo custo desenvolvido pela *Microchip*® para programação e *debugging* de microcontroladores da *Microchip*®. Quando integrado com o IDE *MPLAB*®, o *PICKit 2* permite efectuar *debug* na maioria dos microcontroladores PIC®, podendo desta forma serem analisados e modificados os valores contidos nos registos (Microchip, 2011d).



Figura 40 Programador *PICKit 2* idêntico ao utilizado

Fonte: (Microchip, 2011c)

7.1.5 MPLAB® ICD 2

O *MPLAB*® *ICD 2* (Figura 41), à semelhança do *PICKit 2*, é um programador de baixo custo desenvolvido pela *Microchip*® para programação e *debugging* de microcontroladores da *Microchip*®. As suas funcionalidades são semelhantes às do *PICKit 2*, suportando no entanto um maior número de microcontroladores (Microchip, 2004).



Figura 41 Programador *Microchip MPLAB® ICD 2* idêntico ao utilizado

Fonte: (Microchip, 2011a)

7.2 Dispositivo Móvel de Recolha de Auditoria

Nesta secção serão apresentados os aspectos considerados relevantes no desenvolvimento do *firmware* do dispositivo móvel de recolha de auditoria (Figura 42).

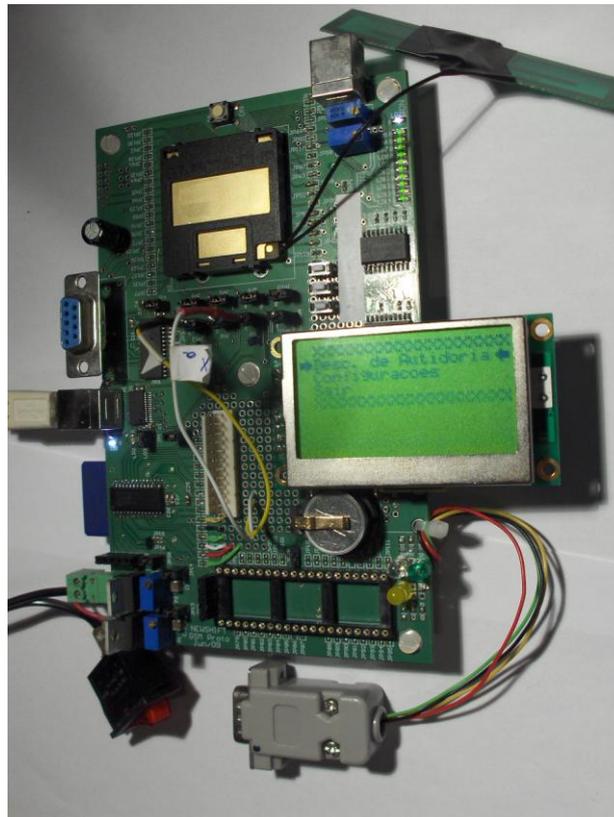


Figura 42 Protótipo do dispositivo móvel de recolha de auditoria

A organização do código fonte do dispositivo móvel recolha de auditoria pode ser consultada no Anexo 9.

7.2.1 Definição do Protocolo de Transferência de Dados

Para a transferência de dados entre o dispositivo de recolha de auditoria e o dispositivo móvel foi implementado um simples protocolo de comunicação.

O protocolo de comunicação baseia-se no conceito de *handshacking*, em que o emissor comunica ao receptor que pretende estabelecer uma comunicação e a quantidade de dados a serem enviados na comunicação. Após o receptor enviar a confirmação de estabelecimento de ligação, o emissor dá início ao processo de envio de dados.

De modo a garantir a integridade dos dados enviados, é aplicado um algoritmo CRC de 16 *bits*.

De seguida são apresentadas as estruturas dos diversos pacotes utilizados na comunicação entre o dispositivo de recolha de auditoria e o dispositivo móvel.

Na Tabela 13 é apresentada a estrutura do pacote de envio de dados de auditoria ambiental. Neste pacote para além da identificação do módulo de recolha de auditoria, são enviados o número de série do *datalogger* que se encontra na máquina de *vending*, os parâmetros do período de registo do *datalogger*, e as várias leituras efectuadas.

Tabela 13 Estrutura do pacote de dados de auditoria ambiental

Pacote de Dados Auditoria Ambiental		
Posição	Índice	Bytes
1	0	<i>DL</i>
2	1	<i>PT</i>
3	2	<i>SN</i>
4	3	<i>SN</i>
5	4	<i>SN</i>
6	5	<i>SN</i>
7	6	<i>SN</i>
8	7	<i>SN</i>
9	8	<i>SN</i>
10	9	<i>SN</i>
11	10	<i>DLSN</i>
12	11	<i>DLSN</i>
13	12	<i>DLSN</i>
14	13	<i>DLSN</i>
15	14	<i>DLSN</i>

16	15	<i>DLSN</i>
17	16	<i>DLSN</i>
18	17	<i>DLSN</i>
19	18	<i>MTSH</i>
20	19	<i>MTSMM</i>
21	20	<i>MTSD</i>
22	21	<i>MTSM</i>
23	22	<i>MTSY</i>
24	23	<i>NMSH</i>
25	24	<i>NMSC</i>
26	25	<i>NMSL</i>
27	26	<i>SR</i>
28	27	<i>TLAT</i>
29	28	<i>THAT</i>
30	29	<i>SI</i>
31	30	<i>S2</i>
...
31+n	30+n	<i>Sn</i>
32+n	31+n	<i>CRCH</i>
33+n	32+n	<i>CRCL</i>
34+n	33+n	<i>DL</i>
Legenda		
<i>DL</i>	<i>Delimiter</i>	
<i>PT</i>	<i>Packet Type</i>	
<i>SN</i>	<i>Identifier Serial Number</i>	
<i>DLSN</i>	<i>Datalogger Serial Number</i>	
<i>MTSH</i>	<i>Mission Time Stamp Hour</i>	
<i>MTSMM</i>	<i>Mission Time Stamp Minutes</i>	
<i>MTSD</i>	<i>Mission Time Stamp Day</i>	
<i>MTSM</i>	<i>Mission Time Stamp Month</i>	
<i>MTSY</i>	<i>Mission Time Stamp Year</i>	
<i>NMSH</i>	<i>Number of Mission Samples High Byte</i>	
<i>NMSC</i>	<i>Number of Mission Samples Center Byte</i>	
<i>NMSL</i>	<i>Number of Mission Samples Low Byte</i>	
<i>SR</i>	<i>Sample Rate</i>	
<i>TLAT</i>	<i>Temperature Low Alarm Threshold</i>	
<i>THAT</i>	<i>Temperature High Alarm Threshold</i>	
<i>S#</i>	<i>Sample #</i>	
<i>CRCH</i>	<i>CRC High Byte</i>	
<i>CRCL</i>	<i>CRC Low Byte</i>	

Na Tabela 14 é apresentada a estrutura do pacote de envio de dados de auditoria financeira. Neste pacote é enviada a identificação do módulo de recolha de auditoria, assim como o *ticket* emitido pelo moedeiro.

Tabela 14 Estrutura do pacote de dados de auditoria financeira

Pacote de Dados Auditoria Financeira		
Posição	Índice	Bytes
1	0	<i>DL</i>
2	1	<i>PT</i>
3	2	<i>SN</i>
4	3	<i>SN</i>
5	4	<i>SN</i>
6	5	<i>SN</i>
7	6	<i>SN</i>
8	7	<i>SN</i>
9	8	<i>SN</i>
10	9	<i>SN</i>
11	10	<i>D</i>
12	11	<i>D</i>
13	12	<i>D</i>
14	13	<i>D</i>
...
14+n	13+n	<i>Dn</i>
15+n	14+n	<i>CRCH</i>
16+n	15+n	<i>CRCL</i>
17+n	16+n	<i>DL</i>
Legenda		
<i>DL</i>	<i>Delimiter</i>	
<i>PT</i>	<i>Packet Type</i>	
<i>SN</i>	<i>Identifier Serial Number</i>	
<i>D</i>	<i>Data</i>	
<i>CRCH</i>	<i>CRC High Byte</i>	
<i>CRCL</i>	<i>CRC Low Byte</i>	

Na Tabela 15 é apresentada estrutura do pacote de envio de erros. A informação contida no pacote é a identificação do módulo de recolha de auditoria e o código de erro.

Tabela 15 Estrutura do pacote de erros

Pacote de Erros		
Posição	Índice	Bytes
1	0	<i>DL</i>
2	1	<i>PT</i>
3	2	<i>SN</i>
4	3	<i>SN</i>
5	4	<i>SN</i>
6	5	<i>SN</i>
7	6	<i>SN</i>
8	7	<i>SN</i>
9	8	<i>SN</i>

10	9	<i>SN</i>
11	10	<i>EC</i>
12	11	<i>0x00</i>
13	12	<i>CRCH</i>
14	13	<i>CRCL</i>
15	14	<i>DL</i>
Legenda		
<i>DL</i>	<i>Delimiter</i>	
<i>PT</i>	<i>Packet Type</i>	
<i>SN</i>	<i>Identifier Serial Number</i>	
<i>D</i>	<i>Error Code</i>	
<i>CRCH</i>	<i>CRC High Byte</i>	
<i>CRCL</i>	<i>CRC Low Byte</i>	

Na Tabela 16 é apresentada a estrutura do pacote enviado para dar início à transferência de dados. Para além da identificação do módulo de recolha de auditoria é também enviado o número de *Bytes* a serem enviados na transferência de dados.

Tabela 16 Estrutura do pacote de estabelecimento de comunicação

Pacote de Início de Comunicação		
Posição	Índice	Bytes
1	0	<i>DL</i>
2	1	<i>PT</i>
3	2	<i>SN</i>
4	3	<i>SN</i>
5	4	<i>SN</i>
6	5	<i>SN</i>
7	6	<i>SN</i>
8	7	<i>SN</i>
9	8	<i>SN</i>
10	9	<i>SN</i>
11	10	<i>BTSH</i>
12	11	<i>BTSL</i>
13	12	<i>CRCH</i>
14	13	<i>CRCL</i>
15	14	<i>DL</i>
Legenda		
<i>DL</i>	<i>Delimiter</i>	
<i>PT</i>	<i>Packet Type</i>	
<i>SN</i>	<i>Identifier Serial Number</i>	
<i>NRBH</i>	<i>Number of Bytes to Send High Byte</i>	
<i>NRBL</i>	<i>Number of Bytes to Send Low Byte</i>	
<i>CRCH</i>	<i>CRC High Byte</i>	
<i>CRCL</i>	<i>CRC Low Byte</i>	

Na Tabela 17 é apresentado o pacote de *acknowledge* transferido para confirmar o início da comunicação entre os dois dispositivos, sendo enviada a confirmação do número de *Bytes* a receber na transferência de dados que a iniciar.

Tabela 17 Estrutura do pacote de *acknowledge*

Pacote de <i>Acknowledge</i>		
Posição	Índice	Bytes
1	0	<i>DL</i>
2	1	<i>PT</i>
3	2	<i>SN</i>
4	3	<i>SN</i>
5	4	<i>SN</i>
6	5	<i>SN</i>
7	6	<i>SN</i>
8	7	<i>SN</i>
9	8	<i>SN</i>
10	9	<i>SN</i>
11	10	<i>NRBH</i>
12	11	<i>NRBL</i>
13	12	<i>CRCH</i>
14	13	<i>CRCL</i>
15	14	<i>DL</i>
Legenda		
<i>DL</i>	<i>Delimiter</i>	
<i>PT</i>	<i>Packet Type</i>	
<i>SN</i>	<i>Identifier Serial Number</i>	
<i>NRBH</i>	<i>Number of Bytes to Receive High Byte</i>	
<i>NRBL</i>	<i>Number of Bytes to Receive Low Byte</i>	
<i>CRCH</i>	<i>CRC High Byte</i>	
<i>CRCL</i>	<i>CRC Low Byte</i>	

7.2.2 Interface de Ligação Entre Dispositivo Móvel e o Módulo de Recolha

Como interface de ligação entre o dispositivo móvel e o módulo de recolha optou-se por utilizar um cabo com um conector *DB9* que servirá para transferência de dados e para alimentação do módulo de recolha. A escolha recaiu sobre a utilização de um cabo em detrimento de uma interface sem fios, por exemplo *Bluetooth*, porque desta forma é possível reduzir o custo tanto do dispositivo móvel como do dispositivo de recolha. Outro factor que conduziu à escolha da utilização de um cabo como interface de ligação, foi o facto de os repositores actualmente já utilizarem um cabo para ligar os moedeiros a impressoras para imprimir os *tickets* e pelo estudo que foi feito perante os possíveis clientes não foi demonstrada nenhuma relutância a esse mecanismo de ligação.

7.2.3 Desenvolvimento do Firmware

De seguida são apresentadas as justificações das opções tomadas durante o desenvolvimento do *firmware* do dispositivo móvel.

7.2.3.1 Integração com o Modem GSM

A comunicação entre o microcontrolador e o modem GSM utilizado foi efectuada através da sua interface UART.

Antes de proceder à integração entre o microcontrolador e o modem GSM foi indispensável identificar a listagem de comandos AT necessários para configuração do modem, para ligação à rede GSM, e para utilização do protocolo TCP/IP. Com o auxílio do manual do modem e do guia de desenvolvimento foi possível identificar a listagem de comandos AT apresentados no Anexo 7. Após identificados os comandos AT necessários procedeu-se à sua implementação no microcontrolador.

Como referido anteriormente a comunicação entre o microcontrolador e o modem foi efectuada através da interface UART dos equipamentos, desta forma, utilizou-se a biblioteca *UART Library*, incluída no conjunto de bibliotecas de *hardware* do *mikroC PRO for PIC*.

De modo a utilizar a interface UART do microcontrolador é necessário inicialmente proceder à sua inicialização, efectuando a chamada da função correspondente da biblioteca e onde é definido *baud rate* da comunicação. Optou-se para este caso utilizar um *baud rate* de 115200bps.

De modo a ser possível tratar as respostas enviadas pelo modem à recepção dos comandos recebidos, foi necessário habilitar as interrupções por *hardware* do microcontrolador. As interrupções por *hardware* despoletam a chamada da função *interrup*, na qual é possível identificar o tipo de interrupção gerada. Se o *bit RCIF* do registo *PIR1* se encontrar a 1, significa que foram recebidos dados na interface UART, sendo de seguida lidos os dados existentes no *buffer* e colocados dentro de um *array* auxiliar de modo a serem tratados posteriormente após a função da interrupção concluir a sua execução.

A função para tratamento da resposta enviada pelo modem consiste na verificação se na *string* da resposta se encontra a sigla *OK*. Se a resposta não contiver a sigla *OK*, é verificado se existe a palavra *ERROR*. Se a resposta contiver a palavra *ERROR* é enviado um código de erro, senão repete toda a operação até encontrar a sigla *OK* ou a palavra *ERROR*, ou então até expirar o tempo máximo estipulado para a operação, neste caso 10 segundos.

Na Figura 43 é apresentado o fluxograma representativo da função de tratamento da resposta enviada pelo *modem*.

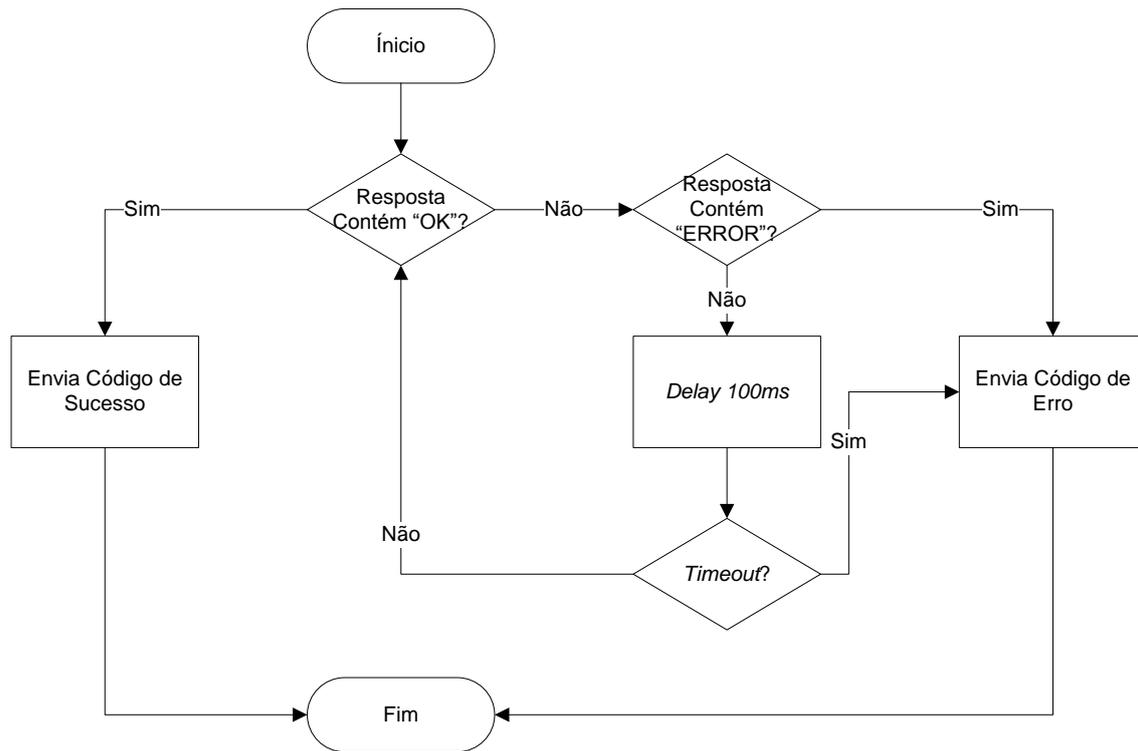


Figura 43 Fluxograma do processo de tratamento de resposta do modem

7.2.3.2 Mecanismo de Segurança Desenvolvido

Dado o conteúdo da informação recolhida ser de baixa sensibilidade, optou-se por aplicar apenas um algoritmo simples de cifragem sobre os dados enviados para o servidor.

Dada a limitação inerente aos equipamentos utilizados, o algoritmo de cifragem utilizado tem por base a aplicação da operação lógica de *XOR* a cada *Byte* transmitido. A chave utilizada terá por base o valor de CRC calculado para o pacote. Visto que o CRC calculado é de 16 *bit*, os dois *Bytes* que compõe o CRC serão utilizados alternadamente como chave de cifragem e de seguida, na ordem inversa novamente como chave de cifragem à mensagem já cifrada.

A ordem da chave será definida pela paridade do valor do CRC. Caso o valor do CRC seja impar será o *Byte* mais significativo utilizado primeiro na sequência da chave de cifragem, caso seja par será o *Byte* menos significativo a iniciar a sequência da chave de encriptação.

Na Figura 44 é apresentado o fluxograma representativo do processo de cifragem de dados desenvolvido.

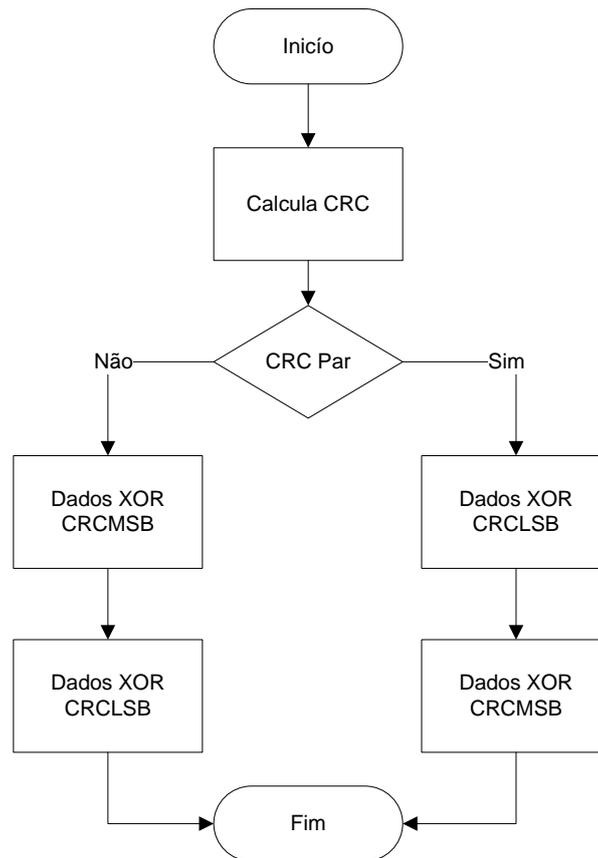


Figura 44 Fluxograma do processo de cifragem de dados

Para efectuar a decifragem dos dados é necessário aplicar a chave na ordem inversa, ou seja, se o CRC for impar a sequência da chave de decifragem começa com o *Byte* menos significativo seguindo-se o *Byte* mais significativo, caso o CRC seja par a sequência da chave de decifragem começa com o *Byte* mais significativo seguindo do *Byte* menos significativo.

Na Figura 45 é apresentado o fluxograma representativo do processo de decifragem desenvolvido.

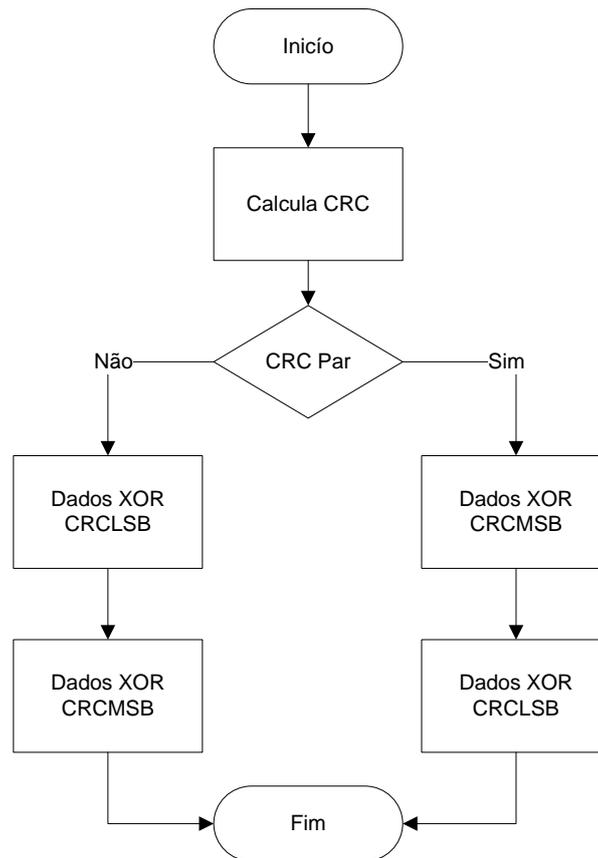


Figura 45 Fluxograma do processo de decifragem de dados

7.2.3.3 Comunicação Dispositivo Móvel – Módulo de Recolha

Como referido anteriormente o dispositivo móvel comunica com o módulo de recolha através de um cabo que se encontra ligado aos microcontroladores de ambos os equipamentos. Como foi utilizada a interface UART do microcontrolador para efectuar a ligação ao modem, para a comunicação entre o dispositivo móvel e o módulo de recolha foi criada uma *Software* UART. Para proceder à implementação da *Software* UART utilizou-se uma das bibliotecas disponibilizadas pelo compilador utilizado. A biblioteca *Software UART Library*, incluída nas bibliotecas de *hardware* do *mikroC PRO for PIC*, permite a criação de *Software* UARTs, emulando assim uma interface UART física. Para a criação de uma *Software* UART é necessário especificar o porto de transmissão de dados (*TX*), o porto de recepção de dados (*RX*) e o *baud rate* a utilizar na comunicação.

Como as *Software* UARTs não possuem nenhum *buffer* para armazenamento dos dados recebidos, foi necessário implementar um protocolo de comunicação de forma a garantir a

recepção de todos os *Bytes* ordenadamente. O protocolo implementado foi utilizado em todas as funções de troca de informação entre o dispositivo móvel e o módulo de recolha.

O protocolo de comunicação, representado Figura 46, consiste no emissor enviar um *Byte*, aguardar 10ms e efectuar a leitura de um *Byte*. Se o *Byte* lido possuir o valor 0x7F, será enviado o *Byte* seguinte do pacote de dados, repetindo o processo para todos os *Bytes* a enviar. A espera de 10ms é necessária a fim de sincronizar a comunicação entre microcontroladores de ambos os dispositivos.

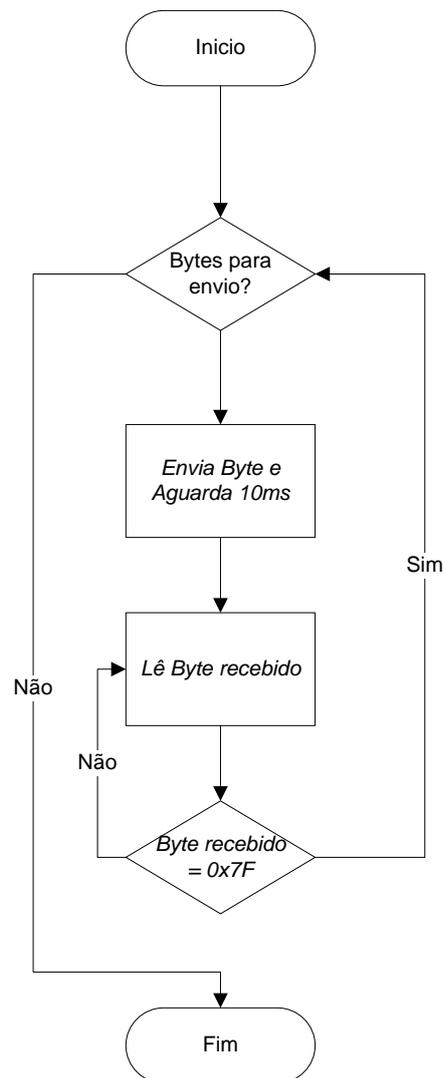


Figura 46 Fluxograma do processo de transferência de dados entre o dispositivo móvel e o módulo de recolha de auditoria

Um aspecto a ter em atenção ao implementar procedimentos que utilizem as *Software UARTs* é o facto de estas implementarem funções bloqueantes. Caso não haja nenhum

Byte para ser lido na *Software UART*, ao ser chamada a função de leitura o *firmware* ficará bloqueado até que seja recebido um *byte*. De modo a evitar o bloqueio por tempo indeterminado, é possível efectuar a chamada à função *Soft_UART_Break*, que permite interromper a leitura e continuar o fluxo normal do *firmware*. No entanto, esta função terá de ser chamada na função de interrupção por *hardware*, pelo que foi necessário colocar o *bit TMROIE*, do registo *INTCON*, a 1.

7.2.3.4 Comunicação Dispositivo Móvel – Servidor Socket

Para a comunicação entre o dispositivo móvel e o servidor *socket* foi implementado um protocolo de comunicação semelhante ao implementado para a comunicação entre o dispositivo móvel e o dispositivo de recolha de auditoria.

O protocolo de comunicação baseia-se no conceito de *handshacking*, em que o emissor comunica ao receptor que pretende estabelecer uma comunicação e a quantidade de dados a serem enviados na comunicação assim como em quantos pacotes serão enviados esses mesmos dados. Após o receptor enviar a confirmação de estabelecimento de ligação, o emissor dá início ao processo de envio de dados.

De modo a garantir a integridade dos dados enviados, é aplicado um algoritmo de CRC de 16 *bits*.

A estrutura, apresentada na Tabela 18, do pacote a enviar é idêntica à estrutura utilizada no protocolo de comunicação entre o dispositivo de recolha de auditoria e o dispositivo móvel, divergindo apenas um pouco no cabeçalho do pacote, onde é incluído o número do pacote e o número de bytes de dados contidos no pacote.

Tabela 18 Estrutura do pacote de dados de auditoria financeira

Pacote de Dados Auditoria Financeira		
Posição	Índice	Bytes
1	0	<i>DL</i>
2	1	<i>PT</i>
3	2	<i>PNR</i>
4	3	<i>NBIPH</i>
5	4	<i>NBIPL</i>
6	5	<i>SN</i>
7	6	<i>SN</i>
8	7	<i>SN</i>
9	8	<i>SN</i>
10	9	<i>SN</i>

11	10	<i>SN</i>
12	11	<i>SN</i>
13	12	<i>SN</i>
14	13	<i>D</i>
...
n-3	n-4	<i>D_n</i>
n-2	n-3	<i>CRCH</i>
n-1	n-2	<i>CRCL</i>
n	n-1	<i>DL</i>
Legenda		
<i>DL</i>	<i>Delimiter</i>	
<i>PT</i>	<i>Packet Type</i>	
<i>SN</i>	<i>Identifier Serial Number</i>	
<i>PNR</i>	<i>Packet Number</i>	
<i>NBTSH</i>	<i>Number of Bytes In Packet High Byte</i>	
<i>NBTSL</i>	<i>Number of Bytes In Packet Low Byte</i>	
<i>D</i>	<i>Data</i>	
<i>CRCH</i>	<i>CRC High Byte</i>	
<i>CRCL</i>	<i>CRC Low Byte</i>	

7.2.3.5 Integração com o LCD

Como referido anteriormente, o LCD escolhido suporta diversos modos de funcionamento, tendo-se optado por utilizar o modo série, minimizando desta forma o número de pinos de E/S do microcontrolador a utilizar.

De modo a integrar com o LCD foi necessário desenvolver as funções base, nomeadamente a função de envio de comandos, e a função de envio de dados.

Quando o LCD se encontra configurado para funcionamento em modo série, como representado na Figura 47, e após o pino */CSI* (*Chip Select*) ser colocado a 0, os dados são recebidos através do pino *SI* (*Serial Data Input*) quando o pino *SCL* (*Serial Clock*) se encontra a 1. O processo de recepção de dados para exibição e o processo de recepção de dados referentes a comandos é idêntico, diferindo apenas a configuração do pino *A0* (*Address Time*). Se o pino *A0* se encontrar a 1 significa que serão recebidos dados para exibição, e quando o pino *A0* se encontrar a 0 os dados recebidos são comandos (Shenzhen Topway Technology Co., 2007).

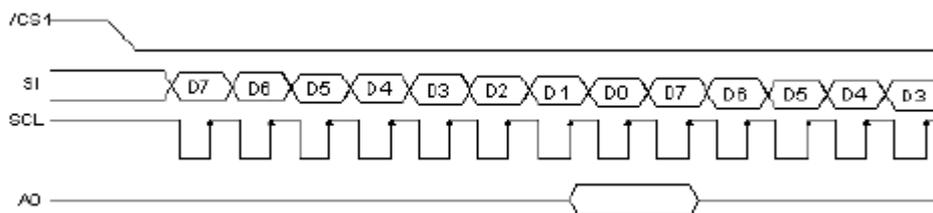


Figura 47 Esquema de funcionamento do LCD em modo série

Fonte: (Shenzhen Topway Technology Co., 2007)

Após a criação das funções de envio de dados e de comandos foi possível desenvolver as funções de apresentação de texto e imagens, assim como a função de limpeza do conteúdo do LCD e ainda a função de inicialização.

A listagem de comandos que são necessários para a inicialização do LCD poderá ser consultada no Anexo 8.

7.2.3.6 Armazenamento de Informação

O armazenamento da informação de auditoria descarregada foi efectuado com suporte a um cartão SD. A integração com o módulo de suporte ao cartão SD foi efectuada com recurso à biblioteca *Multi Media Card Library*, inserida no conjunto de bibliotecas de *hardware* do *mikroC PRO for PIC*.

A biblioteca *Multi Media Card Library* trata-se de uma biblioteca disponível apenas para microcontroladores da família *PIC18F*, e que permite comunicar através do barramento SPI com cartões MMC, SD e SDHC, sendo que estes só poderão ser utilizados num sistema de ficheiros *FAT16*.

De modo a ser possível utilizar o cartão SD é necessário efectuar a chamada à função de inicialização do barramento SPI. A inicialização do barramento SPI pode ser efectuada com recurso à biblioteca *SPI Library*, incluída no conjunto de bibliotecas de *hardware*.

Após a inicialização do barramento SPI é possível proceder à inicialização do módulo de suporte ao cartão SD. A inicialização do módulo é efectuada através da chamada de uma função da biblioteca *Multi Media Card Library*.

Para uma optimização do tempo de escrita da informação no cartão SD, optou-se por criar um buffer de 512 Bytes no qual será armazenada temporariamente a informação a ser escrita. A informação armazenada no *buffer* será escrita no cartão em duas ocasiões distintas.

Será quando o *buffer* tiver chegado à sua capacidade máxima, começando posteriormente a ser preenchido novamente desde início, e a outra ocasião será quando se fechar o ficheiro. Na Figura 48 é apresentado um esquema representativo do processo de escrita de informação para o ficheiro.

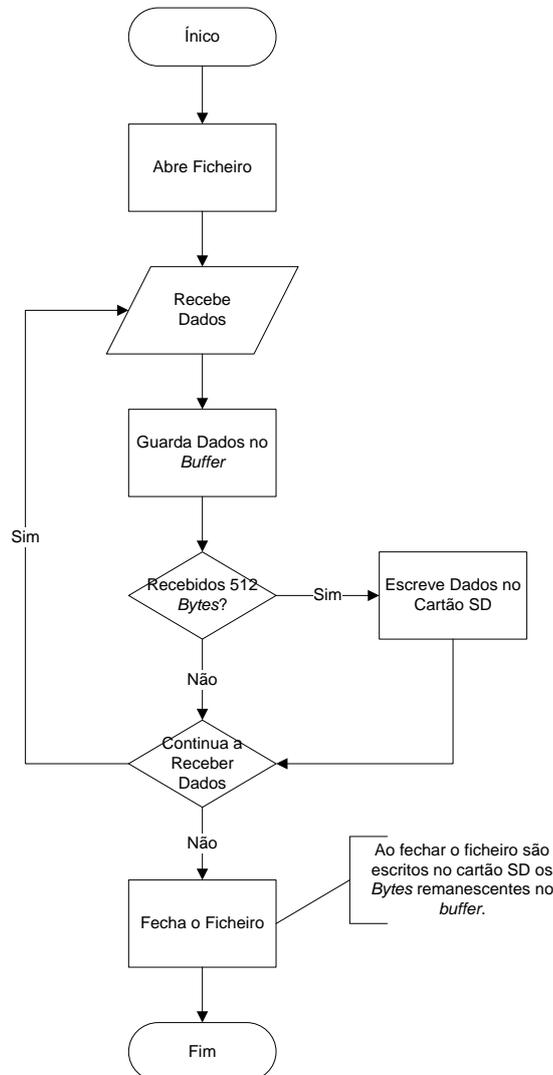


Figura 48 Fluxograma do processo de armazenamento de dados em ficheiro

7.2.3.7 Modo de Funcionamento *Off-Line*

O modo de funcionamento *off-line* permite que o dispositivo móvel seja utilizado em ambientes nos quais não há sinal de rede GSM ou então por opção dos operadores económicos. Neste modo os dados não são enviados para o servidor, estes ficam armazenados no cartão SD até que o dispositivo móvel se encontre num local com rede, ou quando é ligado a uma interface que permita o envio dos dados para a aplicação de gestão e configuração.

Visto a informação que indica que o dispositivo funcionará em modo *off-line* tratar-se de apenas um *bit*, esta ficará guardada na EEPROM do microcontrolador, em que quando ficar armazenado o valor 1 o dispositivo móvel funcionará em modo *off-line*, quando estiver o valor 0 o dispositivo móvel funcionará no modo normal.

7.2.3.8 Integração com a Rede 1-Wire

Como o dispositivo de identificação do repositor trata-se de um *iButton DS1990R*, foi necessário implementar a comunicação entre o microcontrolador e a rede *1-Wire*. A integração com a rede *1-Wire* foi efectuada com recurso à biblioteca *OneWire Library*, incluída no conjunto de bibliotecas de *hardware* do *mikroC PRO for PIC*.

A biblioteca utilizada implementa funções de comunicação através do protocolo *1-Wire* da *Dallas Semiconductor Corp.*. Como referido anteriormente, o protocolo *1-Wire*, trata-se de um protocolo de comunicação que necessita apenas de um fio para comunicação com os diversos dispositivos na rede e que assenta sobre uma filosofia de comunicação *master/slave*.

As funções disponibilizadas pela biblioteca implementam as três operações base do protocolo *1-Wire*, sendo estas, escrita, leitura e *reset* do sinal da rede.

No caso do dispositivo móvel, foi necessário implementar a função de procura de dispositivos *1-Wire* da família 01, família na qual estão incluídos os *iButtons DS1990R*. Para tal é necessário efectuar *reset* ao sinal da linha, momento no qual é indicado qual o pino do microcontrolador utilizado para a rede *1-Wire*. Após o *reset* à linha é enviado o comando para leitura do número de série do dispositivo *1-Wire* seguindo-se a leitura dos 8 *bytes* enviados pelo dispositivo *1-Wire* que se encontra na rede. Se o número de série corresponder ao de um equipamento da família 01 é retornado o código de sucesso ficando o número de série armazenado num vector de *Bytes*. No caso de não ser encontrado nenhum dispositivo *1-Wire* da família 01, é retornado um código de erro.

7.2.3.9 Oclusão Automática do Equipamento

Utilizar um sistema manual para desligar o dispositivo móvel é passível de o utilizador se esquecer de o fazer. Como o dispositivo móvel é alimentado através de pilhas considerou-se de extrema importância implementar um mecanismo que desligue automaticamente o dispositivo móvel.

O mecanismo implementado não é mais que a verificação sistemática de actividade no dispositivo móvel, considerando-se actividade, toda a interacção do utilizador com o dispositivo móvel. Este mecanismo consiste num contador, que ao atingir o limiar de 30 segundos de inactividade, coloca o pino de *power hold* a 0. O sistema electrónico que se encontra ligado ao pino mencionado anteriormente, ao verificar que este foi colocado com o valor 0 provoca um corte no circuito de alimentação do sistema desligando assim o dispositivo móvel.

7.2.4 Solução Final de Hardware

Nesta secção é apresentado o esquema de ligações final do dispositivo móvel, assim como a lista de componentes a utilizar.

7.2.4.1 Esquema de Ligações Final

Nas Figuras 49, 50, 51, 52, 53 e 54 são apresentados os esquemas de ligação dos diversos componentes que compõe o esquema de ligações final do dispositivo móvel de recolha de auditoria. Com base nos esquemas de ligações apresentados deverão ser desenvolvidos PCBs (*Printed Circuit Boards*) do produto a entrar em produção.

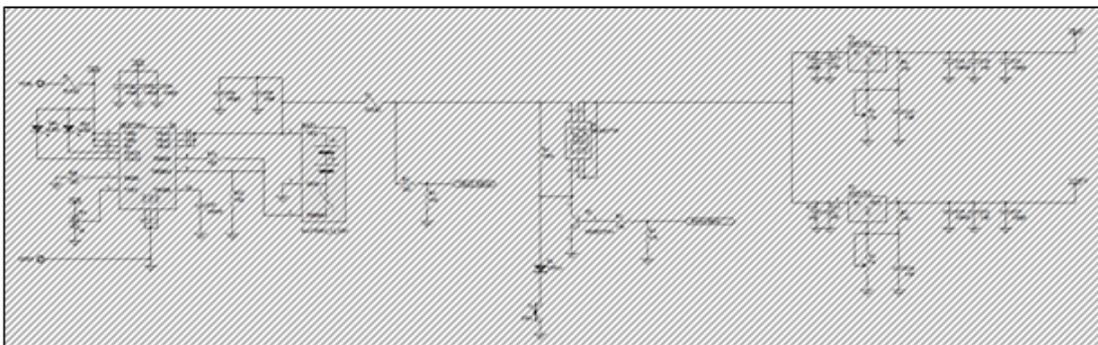


Figura 49 Esquema de ligações do circuito de alimentação

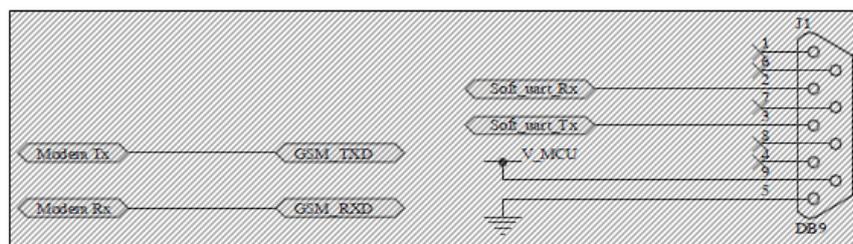


Figura 50 Esquema de ligações do conector de transmissão de dados e ligação ao módulo de recolha de auditoria

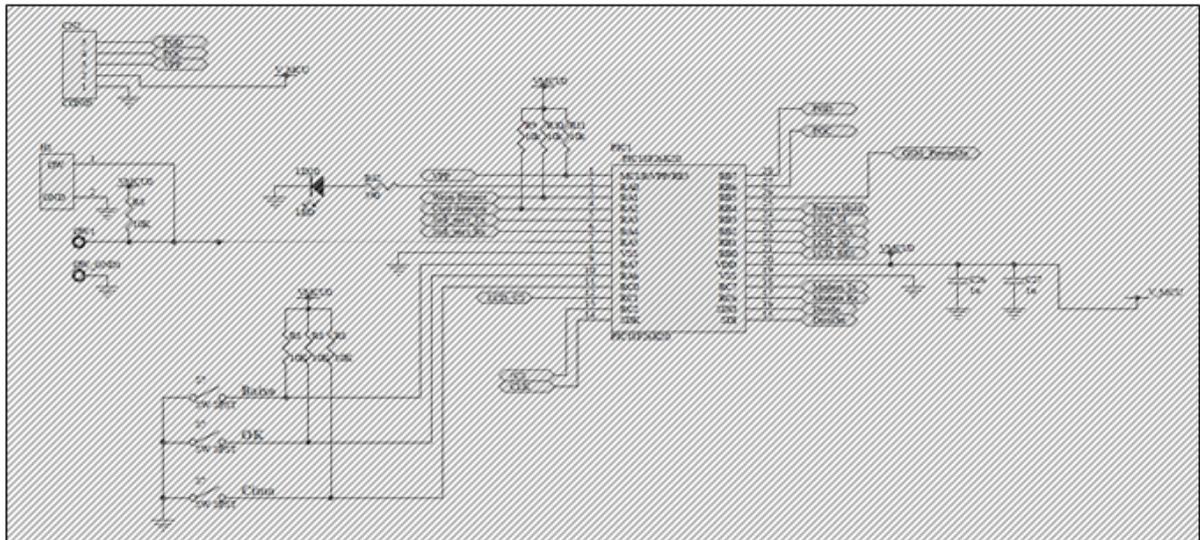


Figura 52 Esquema de ligações da unidade central de processamento

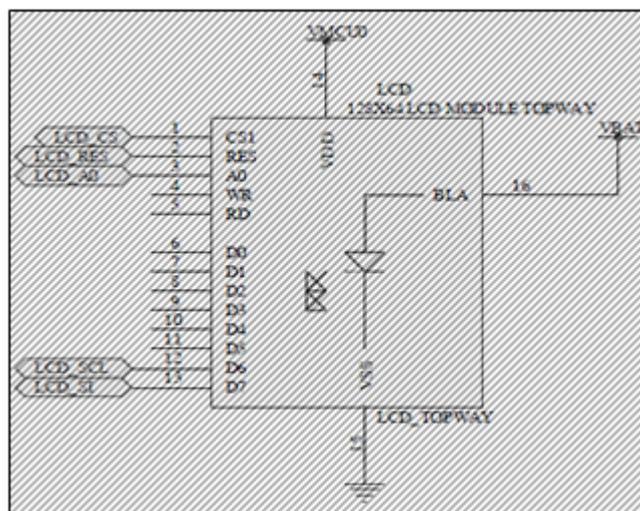


Figura 53 Esquema de ligações do LCD

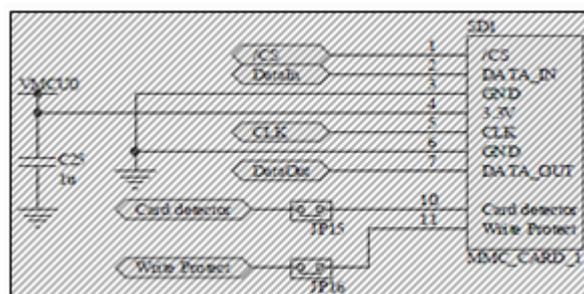


Figura 54 Esquema de ligações do leitor de cartões SD

7.2.4.2 Lista de Componentes

De seguida, na Tabela 19, é apresentada a BOM (*Bill of Materials*) final do dispositivo móvel. Na BOM é apresentada a lista de componentes electrónicos e mecânicos, e as quantidades necessárias de cada para a fabricação do produto final.

Tabela 19 Lista de componentes do dispositivo móvel de recolha de auditoria

Bill of Material - Dispositivo Móvel de Recolha de Auditoria					
Descrição	Encapsulamento	Qt.	Componente	Preço Unitário	Preço Final
Autocolante PVC	N/A	1	Autocolante PVC	1,000 €	1,00 €
Bateria Li-ion	SIP3	1	Bateria de iões de lítio	8,000 €	8,00 €
Switch	N/A	4	Botões	0,200 €	0,80 €
Caixa	N/A	1	Caixa	11,000 €	11,00 €
100nF	0805(2)	1	Condensador	0,006 €	0,01 €
100pF	0805(2)	5	Condensador	0,067 €	0,34 €
100uF	1206(2)	4	Condensador	1,750 €	7,00 €
10pF	0805(2)	1	Condensador	0,031 €	0,03 €
10uF	1206(2)	2	Condensador	0,080 €	0,16 €
1nF	0805(2)	1	Condensador	0,039 €	0,04 €
1uF	0805(2)	3	Condensador	0,010 €	0,03 €
1uF	1206(2)	8	Condensador	0,007 €	0,06 €
200NF	0805(2)	2	Condensador	0,064 €	0,06 €
470uF	RADIAL100	1	Condensador	0,430 €	0,43 €
DB9	DB-9/F	1	Conector	0,940 €	0,94 €
iButton Fob	N/A	1	Conector	0,900 €	0,90 €
MCP73864	SOIC16	1	Controlador de Carga de Bateria	3,130 €	3,13 €
1N914	0805(2)	1	Díodo	0,540 €	0,54 €
250mA	1206(2)	1	Fusível	0,420 €	0,42 €
2A	1206(2)	1	Fusível	0,460 €	0,46 €
DS1990A	ibutton	1	iButton DS1990A	1,010 €	1,01 €
LCD Topway	N/A	1	LCD	6,000 €	6,00 €
LED	0805(2)	3	LED	0,040 €	0,12 €
SD Card Holder	N/A	1	Leitor de Cartões SD/MMC	1,340 €	1,34 €
PIC18F26K20	SOIC28	1	Microcontrolador	2,970 €	2,97 €
Cinterion TC65I	N/A	1	Modem GSM	33,000 €	33,00 €

PCB	N/A	1	PCB	5,310 €	5,31 €
5k Ω	N/A	2	Potenciómetro	0,250 €	0,50 €
LM317LZ	N/A	2	Regulador de Tensão Ajustável	0,690 €	1,38 €
100k Ω	0805(2)	1	Resistência	0,050 €	0,05 €
10K Ω	0805(2)	16	Resistência	0,050 €	0,80 €
1,3k Ω	1206(2)	1	Resistência	0,050 €	0,05 €
1M Ω	0805(2)	1	Resistência	0,050 €	0,05 €
240 Ω	0805(2)	2	Resistência	0,050 €	0,10 €
2M Ω	0805(2)	1	Resistência	0,050 €	0,05 €
390 Ω	0805(2)	1	Resistência	0,050 €	0,05 €
3,1k Ω	0805(2)	1	Resistência	0,050 €	0,05 €
7K5	0805(2)	1	Resistência	0,050 €	0,05 €
SIM Holder	ICA-567	1	Suporte de Cartão SIM	0,730 €	0,73 €
MMBT2904	SOT-23	1	Transístor NPN	0,130 €	0,13 €
Total					89,08 €

7.3 Módulo de Recolha de Auditoria

Neste subcapítulo são apresentadas as justificações das opções tomadas durante o desenvolvimento do *firmware* do módulo de recolha de auditoria (Figura 55).

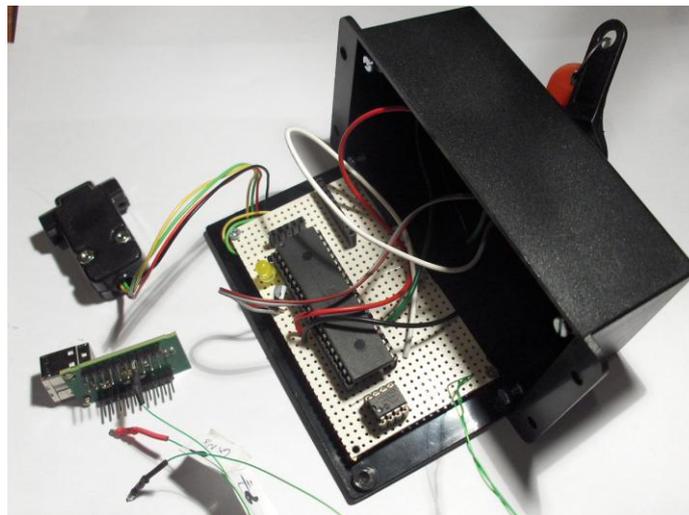


Figura 55 Protótipo do módulo de recolha de auditoria

7.3.1 Organização do Código Fonte

A organização do código fonte do módulo de recolha de auditoria pode ser consultada no Anexo 9.

7.3.2 Interface de Ligação Entre Módulo de Recolha e Moedeiros MEI®

Para interface de ligação entre o módulo de recolha e os moedeiros MEI® foi aproveitada a ligação fornecida pelos moedeiros, ou seja, uma ligação série utilizando um cabo e um conector *DB15*. Desta forma foi utilizada a interface UART física do microcontrolador do módulo de recolha para efectuar a ligação ao moedeiro.

7.3.3 Desenvolvimento do Firmware

De seguida são apresentadas as justificações das principais opções tomadas durante o desenvolvimento do *firmware* do módulo de recolha.

7.3.3.1 Integração com Moedeiro MEI®

Como referido anteriormente a ligação ao moedeiro foi efectuada com recurso à interface UART física do microcontrolador pelo que, à semelhança do que aconteceu com a integração com o modem no dispositivo móvel, foi utilizada a biblioteca *UART Library*, incluída no conjunto de bibliotecas de *hardware* do *mikroC PRO for PIC*.

7.3.3.2 Integração com a Rede 1-Wire

À semelhança do dispositivo móvel, foi também necessário implementar a comunicação entre o microcontrolador do módulo de recolha e a rede *1-Wire*, tendo esta sido efectuada com recurso à biblioteca *OneWire Library*, incluída no conjunto de bibliotecas de *hardware* do *mikroC PRO for PIC*.

No caso do módulo de recolha, foi necessário implementar a função de procura de dispositivos *1-Wire*, sendo que neste caso para além da família 01 onde se encontra incluído o identificador *DS2401*, foi também incluída a família 21 que é a família que inclui os *data-loggers* de temperatura *DS1921G*. Apesar de no módulo de recolha estarem incluídas mais famílias, todo o processo de detecção do dispositivo *1-Wire* na rede é feito de forma análoga ao que foi efectuada no dispositivo móvel.

Para além da função de detecção de dispositivos *I-Wire*, foi necessário implementar as funções de obtenção dos parâmetros de configuração do registador de temperatura, as funções de obtenção dos valores de temperatura, de terminar o período de registo em curso no registador e a função para iniciar um novo período de registo.

7.3.4 Solução de Hardware Final

Nesta secção é apresentado o esquema de ligações final do módulo de recolha de auditoria, assim como a lista de componentes a utilizar.

7.3.4.1 Esquemático Final

Nas Figuras 56 e 57 são apresentados os esquemas de ligações dos componentes que compõem o esquema de ligações final do módulo de recolha de auditoria. Com base no esquemático apresentado deverão ser desenvolvidos os *PCBs* do produto a entrar em produção.

7.3.4.2 Lista de Componentes

Na Tabela 20 pode ser consultada a BOM final do módulo de recolha de auditoria.

Tabela 20 BOM do módulo de recolha de auditoria

<i>Bill of Materials - Módulo de Recolha de Auditoria</i>					
Descrição	Encapsulamento	Qt.	Componente	Preço Unitário	Preço Final
Caixa	N/A	1	Caixa	2,940 €	2,94 €
100nF	0805(2)	4	Condensador	0,006 €	0,02 €
100pF	0805(2)	1	Condensador	0,310 €	0,31 €
1uF	1206(2)	3	Condensador	0,007 €	0,02 €
DB15	DB-15/M	1	Conector	0,750 €	0,75 €
DB9	DB-9/F	1	Conector	0,940 €	0,94 €
iButton Fob	N/A	1	Conector	0,900 €	0,90 €
MAX3223	SSO-G20/C6.7	1	Conversor de Tensão (TTL-RS232)	1,840 €	1,84 €
DS2401	N/A	1	Identificador 1-Wire	0,650 €	0,65 €
PIC18F4620	DIP	1	Microcontrolador	6,660 €	6,66 €
PCB	N/A	1	PCB	2,800 €	2,80 €
2,2kΩ	0805(2)	1	Resistência	0,050 €	0,05 €
5kΩ	0805(2)	1	Resistência	0,050 €	0,05 €
Total					17,94 €

7.4 Servidor Socket

Nesta secção são apresentados os aspectos de maior relevo relativo à implementação do servidor *socket* desenvolvido.

7.4.1 Desenvolvimento do Servidor Socket

Como referido anteriormente, o servidor *socket* trata-se de uma aplicação consola desenvolvida sob a plataforma *.NET* em *C#*. Esta aplicação fica à escuta de *sockets* do tipo *Stream Sockets*.

A aplicação após o seu arranque entra num ciclo a aguardar por ligações de clientes, e ao chegar um pedido é lançada uma nova *thread* que irá processar todas as comunicações efectuadas ficando de seguida novamente à escuta de novas ligações.

Na *thread* é efectuada a recepção dos dados enviados pelo cliente *socket*, após serem recebidos todos os dados do pacote enviado este é processado. No processamento do pacote é verificado se este é um pacote válido e se os dados nele enviados não se encontram corrompidos, ou seja, os dados recebidos são decifrados com base no algoritmo descrito anteriormente e posteriormente é calculado o CRC dos mesmos. Se o CRC calculado corresponder ao CRC enviado no pacote de dados, o pacote é considerado válido e procede-se ao restante processamento do mesmo.

Após validação da integridade do pacote é obtido o número de série do identificador do repositório que procedeu à recolha da auditoria e de seguida o tipo de auditoria que está a ser enviado.

No fim de terem sido tratados todos os pacotes enviados pelo cliente, consoante o tipo de auditoria recebido é invocado o *WebService* que irá proceder ao processamento dos dados recebidos e posterior registo na base de dados.

Após o processamento dos dados por parte do *WebService* ou em caso de falha de comunicação com este, é criado um pacote de resposta para ser enviado ao cliente. A estrutura do pacote com o resultado da operação pode ser consultada na tabela seguinte.

Tabela 21 Pacote de resultado de operação

Pacote de Resultado de Operação		
Posição	Índice	Bytes
1	0	DL
2	1	PT
3	2	ORH
4	3	ORL
5	4	CRCH
6	5	CRCL
7	6	DL
Legenda		
DL	<i>Delimiter</i>	
PT	<i>Packet Type</i>	
SN	<i>Operation Result High</i>	
PNR	<i>Operation Result Low</i>	
CRCH	<i>CRC High Byte</i>	
CRCL	<i>CRC Low Byte</i>	

7.5 Servidor de Serviços

Nesta secção são apresentados os aspectos de maior relevo relativo à implementação do servidor de serviços desenvolvido.

7.5.1 Desenvolvimento do Webservice

O *Webservice* foi desenvolvido sob a plataforma *.NET* e serve de base ao funcionamento das aplicações cliente. O *Webservice* servirá tanto o servidor *Socket* como a aplicação de gestão e configuração.

Para facilitar a transferência de dados entre as aplicações cliente e o servidor foi criada uma biblioteca de DTOs (*Data Transfer Objects*). A referência à biblioteca foi adicionada no *Webservice* e conseqüentemente encontra-se disponível a todos os clientes que o consomem.

Relativamente ao *Webservice* foram implementados os dois serviços para processamento e registo de auditoria financeira e auditoria ambiental, e respectivos métodos auxiliares.

Dos métodos auxiliares destaca-se o método de tratamento de dados de auditoria financeira. Neste método é efectuada a conversão dos dados recebidos no *ticket* e posteriormente a partir do *ticket* são obtidos os dados detalhadamente. Os dados são obtidos procurando na *string* do *ticket*, idêntico ao apresentado no Anexo 10, as palavras que identificam os diversos campos de auditoria financeira, e posteriormente obter o valor que se encontra imediatamente a seguir, sendo este convertido para o tipo de dados correspondente e armazenado na estrutura de dados de auditoria financeira.

Após serem obtidos os dados detalhados de auditoria financeira, é verificado se o número de série do identificador se encontra válido e associado a um repositório, assim como se o número de série do módulo de recolha de auditoria é válido. Após a validação, e em caso de sucesso, procede-se ao registo dos dados de auditoria na base de dados.

Testes

Neste capítulo são apresentadas e descritas as especificações dos testes realizados à solução desenvolvida.

Os testes de *software* podem ser resumidamente definidos como sendo o processo de execução de um *software* de forma controlada de modo a verificar se o mesmo se comporta conforme a sua especificação. Geralmente são utilizados o conceito de verificação e de validação nos testes de software (Processing, 2011).

O processo de verificação permite verificar se o software se encontra a fazer de forma correcta e consistente o que foi especificado, ao passo que no processo de validação é verificado se o que está a ser efectuado é o que foi especificado (Processing, 2011).

Um aspecto fundamental em testes de *software* são as especificações do software a testar, considerando-se software como sendo um pequeno bloco de código ou um sistema completo. As especificações, dependendo da complexidade do sistema a implementar, poderão ser um simples documento ou um conjunto de documentos mais complexos. No entanto, independentemente da complexidade das especificações, é seguida uma hierarquia de especificações. A hierarquia de testes tem geralmente três níveis, podendo em alguns casos ter mais ou menos níveis. Os três níveis de especificação mais comuns são a especificação de requisitos, a especificação da arquitectura e a especificação detalhada de implementação (Processing, 2011).

Na especificação de requisitos, são especificadas as funcionalidades do *software*, assim como podem também ser especificadas as restrições como as funcionalidades deverão ser implementadas (Processing, 2011).

Na especificação da arquitectura é descrito como os diversos componentes que compõe o *software* se relacionam entre si (Processing, 2011).

Na especificação detalhada de implementação são descritos como cada componente que compõe o *software* deverá ser implementado (Processing, 2011).

Existem diversos tipos de teste que poderão ser executados com base nos níveis de especificação descritos anteriormente, nomeadamente, testes unitários, testes de integração, testes de sistema e testes de aceitação.

Com os testes unitários é possível verificar se cada componente do *software* foi correctamente implementado com base nos detalhes especificados (Processing, 2011). Nos testes de integração é possível testar os diversos componentes previamente testados à medida que estes vão sendo integrados até ao momento em que o *software* funciona como um todo (Processing, 2011). Nos testes de sistema, o *software* já se encontra concluído e integrado no produto final e é testado a para verificar se todos os requisitos especificados foram cumpridos (Processing, 2011). Por fim, os testes de aceitação consistem num conjunto de testes de sistema realizados na presença do cliente que dará a sua aprovação relativamente às funcionalidades do *software* (Processing, 2011).

Neste capítulo serão apresentados os cenários dos testes efectuados, as especificações e os resultados obtidos dos próprios testes.

8.1 Especificação de Testes a Realizar

Para além dos testes que foram sendo realizados durante a implementação, definiram-se e realizaram-se outros após finalização dessa fase. Foram realizados testes de integração e testes de sistema.

Os testes de integração tiveram por objectivo validar o correcto funcionamento dos diversos componentes que compõe o dispositivo móvel, particularmente o LCD, o modem GSM, o leitor de cartões SD e a rede *I-Wire*. Para além dos testes efectuados aos componentes do dispositivo móvel, foram ainda realizados testes ao servidor *socket* para validar o seu funcionamento e ainda verificar qual o número médio de ligações concorrentes suportadas.

Por fim, foi realizado o teste de sistema que consistiu na execução de um circuito completo de descarga de auditoria financeira em cinco condições diferentes.

Deste modo, a listagem dos testes de sistema realizados podem ser consultada no Anexo 11.

8.2 Execução dos Testes

A execução dos testes decorreu em três fases distintas, no final do desenvolvimento dos projectos independentes de integração com os componentes que compõe o dispositivo móvel, após a conclusão do desenvolvimento do dispositivo móvel, e finalmente após a conclusão do desenvolvimento dos serviços de tratamento de auditoria.

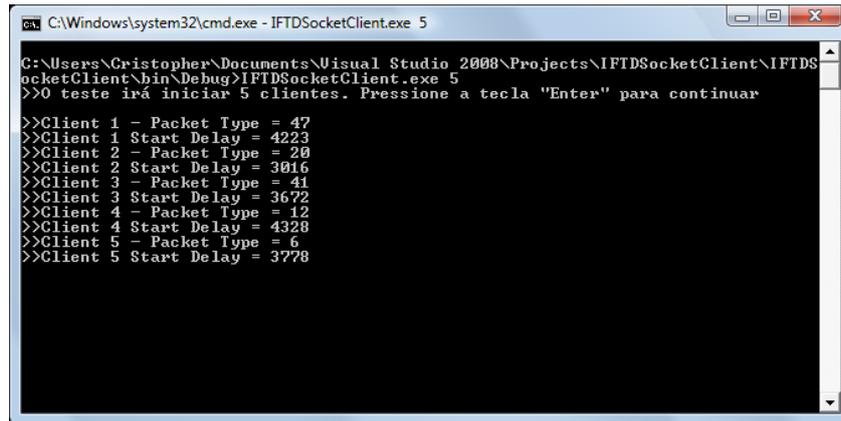
8.2.1 Testes de Integração de Componentes

Como referido anteriormente, numa fase inicial do desenvolvimento foram criados diversos projectos independentes com o objectivo de agilizar a integração dos diversos componentes existentes no dispositivo móvel. Após a conclusão de cada projecto foram realizados os testes de integração especificados no Anexo 11 e tiveram por objectivo a validação do funcionamento de cada componente utilizado nos equipamentos desenvolvidos, sendo que só após conclusão com sucesso dos testes de um componente se procedeu para o projecto do próximo componente.

8.2.2 Testes de Integração do Servidor Socket

A par com o desenvolvimento do dispositivo móvel foi desenvolvido o servidor *socket* e ainda uma aplicação consola (Figura 58) que emularia o dispositivo móvel.

A aplicação de emulação do dispositivo móvel, trata-se de uma aplicação consola desenvolvida sob a plataforma *.NET*, e que estabelece ligações ao servidor *Socket*. Esta aplicação envia pacotes de dados idênticos aos enviados pelo dispositivo móvel, permitindo desta forma emular o dispositivo móvel.



```
C:\Windows\system32\cmd.exe - IFTDSocketClient.exe 5
C:\Users\Cristopher\Documents\Visual Studio 2008\Projects\IFTDSocketClient\IFTDSocketClient\bin\Debug>IFTDSocketClient.exe 5
>>O teste irá iniciar 5 clientes. Pressione a tecla "Enter" para continuar
>>Client 1 - Packet Type = 47
>>Client 1 Start Delay = 4223
>>Client 2 - Packet Type = 20
>>Client 2 Start Delay = 3016
>>Client 3 - Packet Type = 41
>>Client 3 Start Delay = 3672
>>Client 4 - Packet Type = 12
>>Client 4 Start Delay = 4328
>>Client 5 - Packet Type = 6
>>Client 5 Start Delay = 3778
```

Figura 58 Aplicação de emulação de envio de dados do dispositivo móvel

A aplicação poderá receber por parâmetro na linha de comandos o número total de clientes *socket* a serem criados, se estes não forem definidos a aplicação por defeito cria apenas um cliente. Por cada cliente criado é obtido um valor aleatório entre 0 e 100, se o valor obtido for um número par será enviado um pacote com dados de auditoria financeira para o servidor senão, se for ímpar, é enviado um pacote com dados de auditoria ambiental.

Desta forma, foi possível executar os testes de integração especificados no Anexo 10, e ainda obter uma ferramenta que permitiu diminuir o custo do desenvolvimento do projecto, pois permitiu evitar o estabelecimento constante de ligações à rede GSM por parte do dispositivo móvel.

8.2.2.1 Resultados

Os testes de integração com o servidor *socket* permitiram concluir que o sistema, no cenário de testes suporta facilmente a ligação concorrente de 500 clientes, sendo que acima deste número começam a verificar-se falhas no estabelecimento das ligações.

8.2.3 Testes de Sistema

Os testes de sistema foram realizados após a conclusão do desenvolvimento dos serviços de tratamento dos pacotes de auditoria recebidos. Os testes consistiram na execução das tarefas descritas na especificação dos testes de sistema apresentados no Anexo 11 no cenário de testes apresentado no Anexo 12, sendo que todos passaram com sucesso.

Conclusão

Neste capítulo são apresentadas as principais conclusões do estudo da solução proposta.

As actuais soluções de telemetria vocacionadas para a área do *vending* permitem aos operadores económicos obter remotamente informações sobre o estado das máquinas. No entanto, estas soluções acarretam um elevado custo em equipamentos e em comunicações móveis.

Com a actual oferta de planos de acesso à *internet* móvel disponibilizados pelas operadoras móveis, é possível estabelecer uma ligação à *internet* sem implicar um elevado esforço económico. No entanto, se aplicados às soluções de telemetria actuais, em que é necessária uma ligação à *internet* por cada máquina o custo em comunicações é consideravelmente incrementado.

Paralelamente ao elevado custo em comunicações, os equipamentos a instalar nas máquinas de *vending*, dada a tecnologia que envolve, comportam também um elevado investimento.

A solução proposta visa tirar partido da deslocação frequente dos repositores às máquinas de *vending* para efectuar nessa altura a descarga dos dados de maior importância para os operadores económicos, ou seja, os dados de auditoria financeira e os dados de auditoria ambiental. Desta forma, será apenas necessário um dispositivo com capacidade de ligação à *internet*, e o equipamento a instalar na máquina de *vending* que servirá de interface de ligação do dispositivo móvel aos *dataloggers* e ao moedeiro.

9.1 Resultados

Com a realização deste projecto constatou-se que os principais objectivos foram atingidos, ou seja, criar uma solução economicamente viável para os operadores de máquinas de *vending*, estimando-se o valor do dispositivo móvel em 89€ e do módulo de recolha de auditoria em 18€, valores consideravelmente menores do que foi inicialmente definido. Apesar

de ainda não ser possível determinar qual será o custo final do restante sistema, pode-se considerar ter atingido o objectivo de disponibilizar uma solução económica, que permita aos operadores de máquinas de *vending* a recolha e o tratamento automático de dados relevantes no seu negócio, isto é, a auditoria ambiental e financeira.

Ao longo da implementação foram ultrapassadas diversas dificuldades, particularmente:

- A adaptação ao desenvolvimento de *firmware* para microcontroladores;
- A identificação dos comandos AT a utilizar para configuração do modem e estabelecimento de ligações TCP/IP;
- A identificação dos comandos de inicialização do LCD;
- As dificuldades inerentes às limitações da tecnologia utilizada, particularmente a baixa capacidade de memória, e sincronização do funcionamento entre microcontroladores.

Um dos principais obstáculos no desenvolvimento da solução, para além das dificuldades inerentes à adaptação com a tecnologia, foi a baixa capacidade de memória dos microcontroladores. Este factor exigiu um maior esforço para otimizar ao máximo a utilização de variáveis, de modo a que de futuro fosse possível escalar o sistema sem haver a necessidade imediata de trocar de microcontrolador. Assim sendo, conseguiu-se no dispositivo móvel uma utilização de 93% da memória RAM e de 70% da memória ROM, e no módulo de recolha, sendo este o equipamento mais susceptível a ser actualizado de futuro, uma utilização de 69% da memória RAM e 19% da memória ROM.

9.2 Principais Contributos

O contributo deste projecto é a apresentação de uma solução alternativa economicamente mais viável aos sistemas actuais de telemetria para a indústria do *vending*.

A solução proposta disponibiliza aos operadores de máquinas de *vending* um sistema que lhes permite obter dados de auditoria ambiental de uma forma mais simples, facilitando assim o cumprimento da legislação em vigor, assim como obter os dados de auditoria financeira referentes às transacções realizadas nas máquinas.

No entanto, a solução apresentada foi desenhada tendo em conta futuras extensões que a complementem, na medida em que foi minimizada a utilização de memória do microcontrolador e o número de pinos utilizados, sendo desta forma apenas necessário efectuar uma actualização de *firmware* e a inclusão dos conectores necessários.

9.3 Trabalho Futuro

De modo a complementar os requisitos definidos para a solução, será ainda necessário desenvolver os seguintes pontos:

- Desenvolvimento da aplicação de gestão e configuração.
- Desenvolvimento dos serviços de suporte à aplicação de gestão e configuração.
- Dispositivo móvel
 - Permitir a substituição dos parâmetros de configuração do modem para funcionamento com outras operadoras de telecomunicações móveis;
 - Desenhar os PCBs finais que entrarão na produção dos equipamentos;
 - Implementação de um *bootloader* para permitir o carregamento de *firmware* pela interface UART do microcontrolador;
 - Complementar o suporte a moedeiros de outros fabricantes.
- Módulo de recolha de auditoria
 - Desenhar os PCBs finais que entrarão na produção dos equipamentos;
 - Implementação de um *bootloader* para permitir o carregamento de *firmware* pela interface UART do microcontrolador.

Para além dos pontos referidos poderão ainda ser testes complementares, nomeadamente testes funcionais com potenciais clientes, e ainda implementar mecanismos de segurança no acesso aos serviços, particularmente a cifragem do canal de comunicação.

Bibliografia

- Alibaba.com. Vending Machine Telemetry System. Retrieved 04 de Setembro, 2011, from http://www.alibaba.com/products/387760670/Vending_Machine_Telemetry_System.html
- Atmel. (2010). 8-bit AVR Microcontroller with 64K Bytes In-System Programmable Flash. Retrieved 23 de Julho, 2011, from http://www.atmel.com/dyn/resources/prod_documents/doc2593.pdf
- Azkoyen. (2004). AN 800 Payout Units Technical Information. Retrieved 27 de Setembro, 2011, from <http://www.wrzutniki.com/w-produkty/an8000.pdf>
- BITX. (2011). BITX for Vending Telemetry and remote control system for the automatic distribution industry. Retrieved 4 de Setembro, 2011, from http://www.bitx.com/sites/bitx.mediagrouptv.com/files/attachments_public/BITX_brochure_A5_Eng.pdf
- Cha, I., Shah, Y., Andreas, S. U., Andreas, L., & Michael, M. V. (2009). Trust In M2M Communication. 69-75.
- EVA. (2010). Information for Members - Subject Area: Overview of Vending Machine Interfaces.
- EVA. (2011). Information for Members - Subject Area: Overview of Vending Machine Interfaces.
- EVA, & NAMA. (2007). Data Transfer Standard EVA DTS 6.1.
- Ferreira, M. P. M. (2007a). Linguagem UML, Diagramas de Casos de Uso, Apontamentos Teóricos Engenharia de Software I.
- Ferreira, M. P. M. (2007b). Processo ICONIX, Meta 1, Apontamentos Teóricos de Engenharia de Software I.
- Galvão, D. E. E. J. R. (2004). Apontamentos de Física Aplicada, ano 2004/2005, curso Engenharia Informática ESTG/IPL.
- GB. Telemetry solution for vending machines.
- Guerra, S. d. E. A. A. J. d. C. (2009). Portaria 1129/2009: Jornal Oficial da União Europeia.

- Hawkins, L. S. (1992). *How To Succeed in Network Marketing*. EUA: Judy Piatkus Publishers.
- Heggelbacher, F. (2011). Docklight RS232 Terminal/RS232 Monitor Version 1.9. Retrieved 23 de Julho, 2011, from <http://www.docklight.de/>
- IBM. (2009). AIX 6.1 Information Center - Socket Types and Protocols. Retrieved 2011, 20 de Agosto, from http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=/com.ibm.aix.prোগcomm/doc/progcomc/skt_types.htm
- International Directory of Company Histories, Vol. 7.* (1993.): St. James Press.
- Istepanian, R. S. H., Laxminarayan, S., & Pattichis, C. S. (2006). *M-Health Emerging Mobile Health Systems*. Estados Unidos da América.
- Lee, L. (2005). History of Vending Machine. Retrieved 20 de Setembro, 2011, from <http://ezinearticles.com/?History-of-Vending-Machine&id=99988>
- Limited, N. c. (2011). What is a GSM Modem? Retrieved 2011, 19 de Agosto, from <http://www.newsms.com/faq/what-is-a-gsm-modem>
- MEI. (1995). MEI 20 mA Protocol-A Specification.
- MEI. (2007). Sobre a MEI. Retrieved 20 de Setembro, 2011, from http://www.meigroup.com/global/about_mei/?region=/emea/
- Meinel, C., & AlNemr, R. (2008). *Security Issues and Aspects in Healthcare Pervasive Systems*. Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.
- Metriolog. (2005). M2M: The New Age Of Telemetry. Retrieved 4 de Dezembro, 2010, from http://www.metriolog.at/download/M2M_WhitePaper.pdf
- Microchip. (2004). In-Circuit Debugger/Programmer,MPLAB,ICD 2,USB,DV164005. Retrieved 2 de Setembro, 2011
- Microchip. (2008). PIC18F2525/2620/4525/4620 Data Sheet Enhanced Flash Microcontrollers with 10-Bit A/D and nano Watt Technology. Retrieved 23 de Julho, 2011, from <http://ww1.microchip.com/downloads/en/DeviceDoc/39626e.pdf>
- Microchip. (2010). PIC18F23K20/24K20/25K20/26K20/43K20/44K20/45K20/46K20 Data Sheet 28/40/44-Pin Flash Microcontrollers with nanoWatt XLP Technology. Retrieved 23 de Julho, 2011, from <http://ww1.microchip.com/downloads/en/DeviceDoc/80404E.pdf>
- Microchip. (2011a). MPLAB ICD 2. Retrieved 27 de Julho, 2011, from http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en010046

- Microchip. (2011b). MPLAB Integrated Development Environment. Retrieved 27 de Julho, 2011, from http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en019469&part=SW007002
- Microchip. (2011c). PICkit 2. Retrieved 2 de Setembro, 2011, from http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en023805
- Microchip. (2011d). PICkit 2 Development Programmer/Debugger User's Guide. Retrieved 27 de Julho, 2011
- Microchip. (2011e). SDPI PIC. from <http://pt.farnell.com/productimages/farnell/standard/GE28DIPXLP-40.jpg>
- MikroElektronika. (2011). mikroElektronika - mikroC PRO for PIC. Retrieved 24 de Julho, 2011, from <http://www.mikroe.com/eng/products/view/7/mikroc-pro-for-pic/>
- Modules, C. W. (2008a). Application Developer's Guide.
- Modules, C. W. (2008b). TC65i AT Command Set.
- NAMA. (2008). History of Vending and Coffee Service. Retrieved 20 de Setembro, 2011, from <http://www.vending.org/industry/history.php>
- Optimus. (2011). Tarifários Internet no Telemóvel. Retrieved 16 de Julho, 2011, from <http://www.optimus.pt/Particulares/Movel/Services/InternetNoTelemovel/Tarifarios>
- Parallax. (2004). What's a Microcontroller? Student Guide. Retrieved 20 de Setembro, 2011, from http://www.parallax.com/dl/docs/books/edu/wamv2_2.pdf
- Processing, I. I. (2011). An Introduction to Software Testing. Retrieved 18 de Agosto, 2011, from <http://www.ipl.com/pdf/p0820.pdf>
- Products, M. I. (2008). Application Note 148 Guidelines for Reliable Long Line 1-Wire® Networks. Retrieved 6 de Abril, 2011, from <http://pdfserv.maxim-ic.com/en/an/AN148.pdf>
- Products, M. I. (2011a). 1-Wire Network Example. from <http://www.maxim-ic.com/products/1-wire/images/1wiremain.gif>
- Products, M. I. (2011b). Analog, linear, and mixed-signal devices from Maxim/Dallas Semiconductor. Retrieved 27 de Abril, 2011, from http://www.maxim-ic.com/company/dallas/1_wire.cfm
- Products, M. I. (2011c). Analog, linear, and mixed-signal devices from Maxim/Dallas semiconductor. Retrieved 7 de Abril, 2011, from <http://www.maxim-ic.com/products/1-wire/>

- Products, M. I. (2011d). Analog, linear, and mixed-signal devices from Maxim/Dallas Semiconductor -1-Wire Tutorial Presentation Retrieved 7 de Abril, 2011, from <http://www.maxim-ic.com/products/1-wire/flash/overview/index.cfm>
- Products, M. I. (2011e). Generic iButton. from <http://www.maxim-ic.com/products/ibutton/products/images/genericibutton.jpg>
- Products, M. I. (2011f). What Is an iButton? Retrieved 30 de Julho, 2011, from <http://www.maxim-ic.com/products/ibutton/ibuttons/>
- Protel. Protel Remote Vending Monitoring System. Retrieved 4 de Setembro, 2011, from http://www.protelinc.com/ProtelWeb/vending_main.asp
- Roberts, J. W. (2011). How Products Are Made Volume 7 - Vending Machine Retrieved 20 de Setembro, 2011, from <http://www.madehow.com/Volume-7/Vending-Machine.html>
- Rocha, R. (2006). Microcontroladores. *Programar - A revista portuguesa de programação* Retrieved 20 de Setembro, 2011, from <http://revista-programar.info/?action=editions&type=viewmagazine&n=4>
- Rozas, N. (2004). O que é a Telemetria. *Revista Gás Brasil*, 13-15.
- Shenzhen Topway Technology Co., L. (2007). LM6060CBY LCD Module User Manual. Retrieved 15 de Novembro, 2010, from <http://www.topwaydisplay.com/Pub/Manual/LM6060CBY-Manual-Rev0.1.pdf>
- Silva, A., & Videira, C. (2008). *UML, Metodologias e Ferramentas CASE* (2 ed. Vol. 2): Centro Atlântico.
- Sitronix. (2008). ST7565P 65 x 132 Dot Matrix LCD Controller/Driver.
- Testo. (2011). Testo 174T. Retrieved 21 de Setembro, 2011, from http://www.testo.pt/online/img/products/normal/regular/0572_1560_01.jpg
- TMN. (2011). it internetnotemóvel. Retrieved 16 de Julho, 2011, from <http://www.tmn.pt/portal/site/tmn/menuitem.0143d3546741f79ae8f48210751056a0/?vgnnextoid=26625dbb7fd02210VgnVCM1000005401650aRCRD>
- Vault, G. (2008). Sockets e aplicações em rede. Retrieved 20 de Agosto, 2011, from <http://www.geekvault.org/2008/02/sockets-e-aplicacoes-em-rede/>
- Vending, K. (2010). GPRS Communication Module. Retrieved 04 de Setembro, 2011, from http://www.kimmavending.com/gprs_communication.htm
- Vodafone. (2010). Global Machine to Machine Communication. Retrieved 4 de Dezembro, 2010, from http://enterprise.vodafone.com/products_solutions/machine_to_machine/
- Vodafone. (2011). Internet no Telemóvel, Quanto custa? Retrieved 16 de Julho, 2011, from <http://www.vodafone.pt/main/Particulares/Internetmovel/Tarifarios/>

wiseGEEK. (2011). What Is a Currency Detector? Retrieved 20 de Setembro, 2011, from <http://www.wisegeek.com/what-is-a-currency-detector.htm>

Zahn, M. (2003). Naming Conventions for .NET/C# Projects. Retrieved 18 de Outubro, 2010, from http://www.akadia.com/services/naming_conventions.html

Anexo 1 Plano de Projecto

Neste anexo é apresentado o plano de projecto elaborado para a realização deste projecto. Desta forma, é apresentado inicialmente a descrição do produto a desenvolver, a definição dos objectivos, das entregas, das fronteiras, dos pressupostos, das restrições, dos requisitos e do organograma técnico do próprio projecto.

Em relação à gestão de tempo foi efectuado o planeamento baseado nas macro actividades identificadas conforme apresentado na Figura 59.

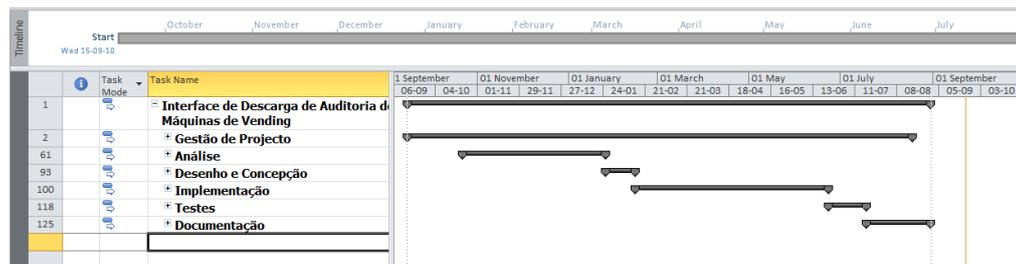


Figura 59 Gráfico de Gantt

1.1 Descrição do Produto

Pretende-se com este projecto implementar um sistema de recolha de dados de auditoria de máquinas de *vending*. Este sistema irá permitir obter a informação recolhida pelos registadores de temperatura instalados nas máquinas de *vending*, bem como a informação contida nos moedeiros. A informação deverá ser descarregada para um dispositivo móvel aquando a visita de um funcionário à máquina de *vending*, posteriormente enviada para um servidor a fim de poder ser analisada pelos operadores económicos.

A grande maioria das empresas a operar no mercado do *vending* opera centenas e por vezes mesmo milhares de máquinas pelo que o custo de instalação por máquina deverá ser reduzido. O sistema deverá portanto ser alvo de uma análise a fim de minimizar o custo final do produto para o cliente.

Desta forma, o projecto será dividido em quatro componentes distintos: o dispositivo móvel, o módulo de ligação à máquina de *vending* para recolha de auditoria, a aplicação servidor, e a aplicação de gestão e configuração.

1.1.1 Objectivos do Projecto

Segue-se uma listagem dos objectivos do projecto:

- Dispositivo móvel
 - Ligação ao módulo de recolha de auditoria da máquina de *vending*;
 - Suportar modo de funcionamento *off-line* em caso de falhas de comunicação;
 - Ligação ao servidor efectuada através de ligação *GPRS*;
 - Possibilidade de *upload* do *firmware*.
- Módulo de recolha de auditoria da máquina de vending
 - Possuir interface para ligação ao dispositivo móvel;
 - Possuir interface para ligação ao registador de temperatura;
 - Possuir interface para ligação ao moedeiro;
 - Deverá ser escalável;
 - Possibilidade de *upload* de *firmware*.
- Aplicação servidor
 - Recepção e processamento de dados de auditoria financeira;
 - Recepção e processamento de dados de auditoria de temperatura;
 - Disponibilizar os dados recolhidos.
- Aplicação de gestão e configuração
 - Aplicação multi-posto;
 - Apresentação dos dados de auditoria recolhidos;
 - Criação de relatórios;
 - Gestão de parâmetros do sistema;
 - Configuração e actualização do dispositivo móvel.

1.2 Entregas do Projecto

As entregas do projecto deverão ser as seguintes:

- Entregas ao júri de avaliação e serviços académicos:

- Dissertação.
- Entregas à empresa colaboradora:
 - Especificação de requisitos;
 - Esquemas de ligações do dispositivo móvel;
 - Esquemas de ligações do módulo de recolha de auditoria;
 - Dispositivo móvel;
 - Módulo de recolha de auditoria;
 - Aplicação servidor;
 - Aplicação de gestão e configuração;
 - Manuais de instalação;
 - Manuais de utilização.

1.3 Fronteiras do Projecto

Segue-se uma listagem das fronteiras do projecto:

- O *firmware* da primeira versão do dispositivo móvel irá apenas contemplar descargas de auditoria ambiental e financeira;
- O sistema não irá efectuar descarga de auditoria remotamente.

1.4 Pressupostos do Projecto

Os pressupostos assumidos neste projecto são os seguintes:

- O sistema será compatível apenas com os moedeiros MEI® série 6 e série 7;
- O sistema será compatível apenas com os registadores de temperatura da *Maxim* modelo *DS1921G*;
- Os registadores de temperatura deverão ter sido previamente iniciados por um sistema externo ao sistema a desenvolver;
- Para efectuar a descarga de auditoria o repositon deverá deslocar-se à máquina de *vending*;
- Os microcontroladores utilizados serão da *Microchip*®

1.5 Restrições do Projecto

O projecto apresenta as seguintes restrições:

- O dispositivo móvel deverá comunicar através de uma ligação *GPRS* com o servidor;
- O preço de produção dos módulos de recolha de auditoria das máquinas de *vending* não deverá ultrapassar os 50€ por motivos de concorrência.

1.6 Requisitos do Projecto

Segue-se uma listagem dos requisitos do projecto relativos ao dispositivo móvel, ao módulo de recolha de auditoria, à aplicação servidor e à aplicação de gestão e configuração.

Desta forma o dispositivo móvel deverá:

- Possuir interface de ligação ao módulo de recolha de auditoria da máquina de *vending*;
- Permitir a identificação do repositório que efectuou a recolha de auditoria;
- Recolher e enviar os dados de auditoria recolhidos;
- Permitir o funcionamento em modo off-line;
- Possibilitar o *upload* de *firmware*;
- Desligar-se sozinho após um período de tempo de inactividade;
- Permitir inserir o código PIN do cartão SIM;
- Permitir configurar o intervalo entre leituras do registador de temperatura.

O módulo de recolha de auditoria deverá:

- Possuir interface para ligação de registador *Maxim DS1921G*;
- Possuir interface para ligação de moedeiros MEI® série 6 e série 7;
- Possuir interface com o dispositivo móvel de recolha de auditoria;
- Possuir interface para expansões futuras;
- Ser alimentado através do dispositivo móvel de recolha de auditoria;
- Possuir um número de série para fins de identificação da máquina de *vending*;
- Possibilitar o *upload* de *firmware*.

Por sua vez, a aplicação servidor deverá:

- Permitir a recepção dos dados de auditoria;
- Disponibilizar os dados a outras aplicações.

Finalmente a aplicação de gestão e configuração deverá:

- Ser uma aplicação multi-posto;
- Apresentar a listagem de recolhas de auditoria efectuadas;
- Indicar quais as máquinas com um valor de trocos inferior ao mínimo especificado;
- Indicar a listagem as máquinas que tenham um volume de vendas inferior ao mínimo especificado;
- Permitir aplicar filtros de pesquisa para apresentação das listagens de recolha de auditoria;
- Permitir a criação de relatórios com a informação de auditoria financeira e auditoria ambiental;
- Apresentar nos relatórios de auditoria ambiental os valores registados em forma de gráfico e listagem, assim como apresentar o valor de temperatura máxima, mínima e média;
- Apresentar nos relatórios de auditoria financeira o valor total de vendas efectuadas pela máquina, o valor total facturado e o valor que se encontra nos tubos do moedeiro;
- Suportar vários perfis de utilizador;
- Permitir efectuar a gestão de utilizadores;
- Permitir efectuar a gestão de localizações;
- Permitir efectuar a gestão de identificadores de repositores;
- Permitir efectuar a gestão de máquinas de *vending*;
- Permitir efectuar a gestão de módulos de recolha de auditoria;
- Possuir três perfis de utilizador: administrador, operador e repositor;
- Permitir que os utilizadores do perfil operador possam:
 - Marcar que o valor indicado na recolha de auditoria financeira confere com o valor recebido em numerário por parte dos repositores;
- Permitir que os utilizadores do perfil administrador possam:
 - Especificar o valor mínimo de trocos;
 - Especificar o valor mínimo de volume de vendas;
 - Alterar a marcação indicativa de valor financeiro correcto;
 - Editar os dados recebidos nas recolhas;
 - Efectuar a gestão de utilizadores;

- Efectuar a gestão de máquinas de *vending*;
- Efectuar a gestão de localização de máquinas;
- Efectuar a gestão de módulos de recolha de auditoria;
- Efectuar a gestão de registadores de temperatura;
- Introduzir dados de calibração de registadores de temperatura;
- Permitir efectuar o *upload* de *firmware* para o dispositivo móvel;
- Permitir configurar o endereço da aplicação servidor no dispositivo móvel;
- Permitir configurar o intervalo entre leituras do registador de temperatura;
- Permitir configurar o código *PIN* no dispositivo móvel.

1.7 Organograma Técnico

O organograma técnico é um grupo dos componentes do projecto (orientado às entregas), que organiza e define o âmbito total do projecto.

Os componentes do último nível do organograma técnico são chamados de pacotes de trabalho. A descrição dos componentes de trabalho é agrupada num dicionário do organograma técnico.

O organograma técnico ou *WBS (Work Breakdown Structure)* deste projecto é de seguida apresentado, enumerando os diversos componentes de trabalho, constituindo desta forma o dicionário do organograma técnico:

1. Interface for Audit Download

1.1. Gestão de Projecto

1.1.1. Planeamento

- 1.1.1.1. Definição de Âmbito
- 1.1.1.2. Gestão de Tempo
- 1.1.1.3. Gestão de Comunicação
- 1.1.1.4. Gestão de Qualidade

1.1.2. Controlo de Progresso

- 1.1.2.1. Reuniões internas
- 1.1.2.2. Reuniões com orientadora de projecto

1.2. Análise

1.2.1. Recolha de Informação

- 1.2.1.1. Reuniões
- 1.2.1.2. Prospecção de Mercado
- 1.2.1.3. Elaboração do Caderno de Especificação de Requisitos
- 1.2.2. Análise do Dispositivo Móvel
 - 1.2.2.1. Definição da Arquitectura
 - 1.2.2.2. Escolha da Tecnologia a Utilizar
 - 1.2.2.3. Escolha dos Componentes a Utilizar
 - 1.2.2.4. Análise de Integração
 - 1.2.2.5. Elaboração de Diagramas
- 1.2.3. Análise do Módulo de Recolha de Auditoria da Máquina de *Vending*
 - 1.2.3.1. Definição da Arquitectura
 - 1.2.3.2. Escolha da Tecnologia a Utilizar
 - 1.2.3.3. Escolha dos Componentes a Utilizar
 - 1.2.3.4. Análise de Integração
 - 1.2.3.5. Elaboração de Diagramas
- 1.2.4. Análise da Aplicação Servidor
 - 1.2.4.1. Estruturação do Modelo de Dados
 - 1.2.4.2. Definição da Arquitectura
 - 1.2.4.3. Escolha da Tecnologia a Utilizar
 - 1.2.4.4. Análise de Integração
 - 1.2.4.5. Elaboração de Diagramas
- 1.2.5. Análise da Aplicação de Gestão e Configuração
 - 1.2.5.1. Definição da Arquitectura
 - 1.2.5.2. Escolha da Tecnologia a Utilizar
 - 1.2.5.3. Análise de Integração
 - 1.2.5.4. Elaboração de Diagramas
- 1.3. Desenho
 - 1.3.1. Desenho de Esquemas de Ligações
 - 1.3.2. Desenho de Interface
 - 1.3.3. Desenho de Navegação
 - 1.3.4. Reuniões
- 1.4. Implementação
 - 1.4.1. Implementação Dispositivo Móvel

- 1.4.1.1. Desenvolvimento da Placa de Prototipagem
- 1.4.1.2. Desenvolvimento do *Firmware*
- 1.4.2. Implementação Módulo de Recolha de Auditoria
 - 1.4.2.1. Desenvolvimento da Placa de Prototipagem
 - 1.4.2.2. Desenvolvimento do *Firmware*
- 1.4.3. Implementação Aplicação Servidor
 - 1.4.3.1. Desenvolvimento do Modelo de Dados
 - 1.4.3.2. Desenvolvimento da Camada de Acesso a Dados
 - 1.4.3.3. Desenvolvimento da Camada de Lógica de Negócio
- 1.4.4. Implementação Aplicação de Gestão e Configuração
 - 1.4.4.1. Desenvolvimento da Interface
 - 1.4.4.2. Desenvolvimento da Camada de Lógica de Negócio
- 1.4.5. Inspeção de Código
 - 1.4.5.1. Revisões
 - 1.4.5.2. Correções
- 1.5. Testes
 - 1.5.1. Desenho
 - 1.5.2. Realização de Testes de Integração
 - 1.5.3. Realização de Testes de Sistema
- 1.6. Documentação
 - 1.6.1. Redacção da Documentação do Dispositivo Móvel
 - 1.6.2. Redacção da Documentação do Módulo de Recolha de Auditoria
 - 1.6.3. Redacção da Documentação da Aplicação Servidor
 - 1.6.4. Redacção da Documentação da Aplicação de Gestão e Configuração

1.8 Gestão da Comunicação

A gestão de comunicações é o conjunto de processos que são necessários para assegurar a geração, colecção, disseminação, armazenamento e disposição apropriada e atempada de informação acerca de todo o projecto. Desta forma, a gestão da comunicação deverá incluir o planeamento, os requisitos e as tecnologias das comunicações, e o próprio plano de gestão das comunicações.

O planeamento de comunicações visa determinar quais as necessidades de informação por parte dos intervenientes do projecto e os processos de comunicação entre eles: quem precisa e de que informação, quando esta necessitará de estar disponível, como lhes será fornecida e por quem. Na Tabela 22 é apresentado o plano de comunicação detalhado com os diversos canais de comunicação utilizados durante a execução do projecto.

Tabela 22 Plano de comunicações detalhado

Plano de Comunicações Detalhado			
Canal de comunicação	Periodicidade	Tipo de informação Transmitida	Interna
Reunião	Uma vez, após o planeamento	Levantamento dos requisitos dos módulos, esclarecimento de dúvidas que podem ter surgido na fase de planeamento	✓
Especificação de Requisitos		Especificação dos requisitos do projecto	
Reunião	Quinzenal	Relato do progresso das actividades para prevenção de deslizamentos	✓
Reunião	Uma vez, após elaboração da especificação de requisitos	Apresentação do documento de especificação de requisitos para aprovação	✓
Telefone	Após elaboração do caderno de requisitos	Contacto com empresas operadoras económicas de máquinas de vending para marcação de reuniões	-
Reunião	Quinzenalmente	Relato do progresso das actividades e esclarecimento de dúvidas com a orientadora do projecto	-
Email	Ocasionalmente	Envio de documentação para revisão por parte da orientadora do projecto	-
Email/Telefone	Ocasionalmente	Remarcação de data da reunião de orientação de projecto	-
Email	Ocasionalmente	Pedido de informações referentes a produtos	-
Intranet	Após realização dos testes de acei-	Reportar bugs detectados	✓

	tação e testes de carga		
Pessoalmente/Questionários	Após levantamento de requisitos	Recolha de opiniões dos operadores económicos relativas a sistemas de recolha de auditoria	-

Para evitar falhas de comunicação deverão ser claramente definidos os meios necessários para a comunicação ser estabelecida sem falhas. Assim, para as reuniões internas será necessária uma sala para cerca de quatro pessoas, enquanto, para as reuniões com a orientadora de projecto será necessária uma sala com capacidade para cerca de três pessoas com respectivos computadores portáteis.

A comunicação interna requer que estejam disponíveis e em pleno funcionamento três telemóveis, um telefone, um fax, três computadores de secretária e um servidor.

Deverão ser igualmente marcadas as reuniões internas e externas com antecedência. As reuniões internas deverão ser marcadas com um dia de antecedência, enquanto as reuniões com a orientadora deverão ser marcadas com duas semanas de antecedência.

Os métodos e tecnologias de comunicação utilizados neste projecto foram:

- A *intranet* – serve de repositório a todos os documentos gerados no âmbito do projecto;
- O dossier de projecto – contém todos os documentos resultantes do processo de comunicação desde os relatórios de progresso até aos resultados dos diversos testes efectuados;
- O *email* – para divulgação do agendamento das reuniões;
- O *Bugzilla* – para reportar *bugs* detectados na fase de testes do projecto e após entrada em produção;
- O *Orcanos QPack* – para redacção e criação do caderno de requisitos assim como planeamento dos testes a realizar.

1.1.8 Plano de Gestão de Comunicações

O plano de comunicações do projecto pode ser ilustrado através da Figura 60.

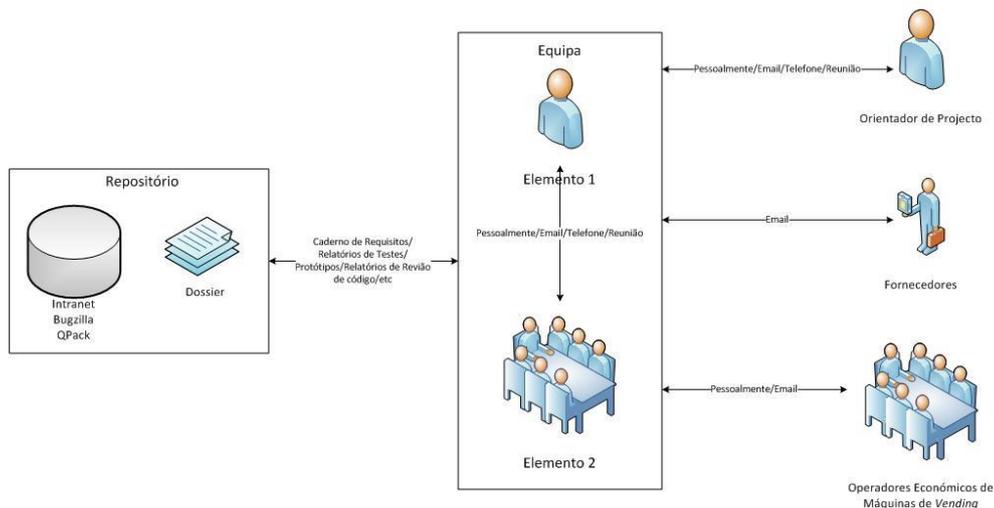


Figura 60 Plano de Comunicações

1.9 Gestão de Qualidade

A qualidade do projecto será garantida através da execução de diversos procedimentos, nomeadamente através de:

- Reuniões periódicas de acompanhamento com a orientadora do projecto;
- Reuniões periódicas de progresso com a empresa parceira;
- Realização de testes:
 - Integração;
 - Sistema;
 - Realização de revisões periódicas de código;
 - Seguimento das convenções e regras de desenvolvimento de código apresentadas de seguida.

A nomenclatura e convenções utilizadas durante a implementação foram definidas antes da inicialização do projecto de modo a uniformizar e a tornar mais legível todo o código realizado. Deste modo, definiu-se a designação que iria ser utilizada para atributos de classes, parâmetros e variáveis dentro de métodos e/ou funções, de acordo com o tipo de dados apresentados na Tabela 23.

Tabela 23 Nomenclatura de componentes não gráficos

Nomenclatura de Componentes Não Gráficos			
Tipo de Dado	Atributos de Classe	Parâmetros de métodos/funções	Variáveis dentro de métodos/funções
<i>byte</i>	<i>m_bt_[nomeVariavel]</i>	<i>bt_[nomeVariavel]</i>	<i>bt[NomeVariavel]</i>
<i>boolean</i>	<i>m_b_[nomeVariavel]</i>	<i>b_[nomeVariavel]</i>	<i>b[NomeVariavel]</i>
<i>char</i>	<i>m_ch_[nomeVariavel]</i>	<i>ch_[nomeVariavel]</i>	<i>ch[NomeVariavel]</i>
<i>decimal</i>	<i>m_dc_[nomeVariavel]</i>	<i>dc_[nomeVariavel]</i>	<i>dc[NomeVariavel]</i>
<i>double</i>	<i>m_d_[nomeVariavel]</i>	<i>d_[nomeVariavel]</i>	<i>d[NomeVariavel]</i>
<i>float</i>	<i>m_f_[nomeVariavel]</i>	<i>f_[nomeVariavel]</i>	<i>f[NomeVariavel]</i>
<i>int</i>	<i>m_i_[nomeVariavel]</i>	<i>i_[nomeVariavel]</i>	<i>i[NomeVariavel]</i>
<i>long</i>	<i>m_l_[nomeVariavel]</i>	<i>l_[nomeVariavel]</i>	<i>l[NomeVariavel]</i>
<i>object</i>	<i>m_o_[nomeVariavel]</i>	<i>o_[nomeVariavel]</i>	<i>o[NomeVariavel]</i>
<i>short</i>	<i>m_s_[nomeVariavel]</i>	<i>s_[nomeVariavel]</i>	<i>s[NomeVariavel]</i>
<i>signed byte</i>	<i>m_sbt_[nomeVariavel]</i>	<i>sbt_[nomeVariavel]</i>	<i>sbt[NomeVariavel]</i>
<i>string</i>	<i>m_str_[nomeVariavel]</i>	<i>str_[nomeVariavel]</i>	<i>str[NomeVariavel]</i>
<i>unsigned char</i>	<i>m_uch_[nomeVariavel]</i>	<i>uch_[nomeVariavel]</i>	<i>uch[NomeVariavel]</i>
<i>unsigned int</i>	<i>m_ui_[nomeVariavel]</i>	<i>ui_[nomeVariavel]</i>	<i>ui[NomeVariavel]</i>
<i>unsigned long</i>	<i>m_ul_[nomeVariavel]</i>	<i>ul_[nomeVariavel]</i>	<i>ul[NomeVariavel]</i>
<i>unsigned short</i>	<i>m_us_[nomeVariavel]</i>	<i>us_[nomeVariavel]</i>	<i>us[NomeVariavel]</i>

Determinou-se igualmente a nomenclatura (maioritariamente baseada) utilizada para os componentes gráficos e outro tipo de objectos com base na nomenclatura húngara como pode ser consultado na Tabela 24.

Tabela 24 Nomenclatura de componentes gráficos e objectos

Fonte: (Zahn, 2003)

Nomenclatura de Componentes Gráficos e Objectos	
Tipo de Componente	Nome do Componente
<i>Boolean</i>	<i>bln[Nome]</i>
<i>Button</i>	<i>btn[Nome]</i>
<i>Char</i>	<i>ch[Nome]</i>
<i>CheckBox</i>	<i>cbx[Nome]</i>
<i>ComboBox</i>	<i>cmb[Nome]</i>
<i>Container</i>	<i>ctr[Nome]</i>
<i>DataColumn</i>	<i>dcol[Nome]</i>
<i>DataGrid</i>	<i>dgrid[Nome]</i>
<i>DataGridDateTimePickerColumn</i>	<i>dgdtpc[Nome]</i>
<i>DataGridTableStyle</i>	<i>dgts[Nome]</i>
<i>DataGridTextBoxColumn</i>	<i>dgtbc[Nome]</i>
<i>DataReader</i>	<i>dreader[Nome]</i>
<i>DataRow</i>	<i>drow[Nome]</i>
<i>DataSet</i>	<i>dset[Nome]</i>
<i>DataTable</i>	<i>dtable[Nome]</i>
<i>DateTime</i>	<i>date[Nome]</i>
<i>Dialog</i>	<i>dialog[Nome]</i>
<i>DialogResult</i>	<i>dr[Nome]</i>
<i>Double</i>	<i>dbl[Nome]</i>

<i>Exception</i>	<i>ex[Nome]</i>
<i>GroupBox</i>	<i>gbx[Nome]</i>
<i>HashTable</i>	<i>htbl[Nome]</i>
<i>ImageList</i>	<i>iml[Nome]</i>
<i>Integer</i>	<i>int[Nome]</i>
<i>Label</i>	<i>lbl[Nome]</i>
<i>ListBox</i>	<i>lbx[Nome]</i>
<i>ListView</i>	<i>lv[Nome]</i>
<i>Mainmenu</i>	<i>mm[Nome]</i>
<i>MenuItem</i>	<i>mi[Nome]</i>
<i>MDI-Frame</i>	<i>frame[Nome]</i>
<i>MDI-Sheet</i>	<i>sheet[Nome]</i>
<i>NumericUpDown</i>	<i>nud[Nome]</i>
<i>Panel</i>	<i>pnl[Nome]</i>
<i>PictureBox</i>	<i>pbx[Nome]</i>
<i>RadioButton</i>	<i>rbtn[Nome]</i>
<i>SDI-Form</i>	<i>form[Nome]</i>
<i>SqlCommand</i>	<i>sqlcom[Nome]</i>
<i>SqlCommandBuilder</i>	<i>sqlcomb[Nome]</i>
<i>SqlConnection</i>	<i>sqlcon[Nome]</i>
<i>SqlDataAdapter</i>	<i>sqlda[Nome]</i>
<i>StatusBar</i>	<i>stb[Nome]</i>
<i>String</i>	<i>str[Nome]</i>
<i>StringBuilder</i>	<i>strb[Nome]</i>
<i>TabControl</i>	<i>tabctrl[Nome]</i>
<i>TabPage</i>	<i>tabpage[Nome]</i>
<i>TextBox</i>	<i>tbx[Nome]</i>
<i>ToolBar</i>	<i>tbr[Nome]</i>
<i>ToolBarButton</i>	<i>tbb[Nome]</i>
<i>Timer</i>	<i>tmr[Nome]</i>

Na Tabela 25 pode ser consultada a listagem das restantes convenções usadas.

Tabela 25 Restantes convenções utilizadas

Outras Convenções		
Nomenclatura		Notas
Nome de Classe	Iniciado com maiúscula.	As classes de acesso a dados deverão começar com o prefixo <i>DAO</i> , as classes de transferência de dados deverão começar com o prefixo <i>DTO</i> , e as classes de lógica de negócio deverão começar com <i>BLO</i> .
Nome de Métodos/Funções	Iniciado com maiúscula.	
Nome de Namespaces	Iniciado com maiúscula.	
Nome de Interfaces	I[NomeDaInterface]	
Nome de Constantes	NOME_DA_CONSTANTE	Todas as palavras que compõe o nome da constante deverão ser separados pelo

		caracter “_”.
Idioma do código fonte	Inglês.	

Anexo 2 Soluções de Telemetria para Máquinas de Vending

Na Tabela 26 é são apresentadas as principais características de algumas soluções de telemetria para máquinas de *vending* e o seu preço.

Tabela 26 Soluções de telemetria para máquinas de *vending*
Fonte: (Alibaba.com; BITX, 2011; GB; Protel; Vending, 2010)

Soluções de Telemetria para Máquinas de <i>Vending</i>		
Solução	Principais Características	Preço
<i>Kimma Vending Machine Management System/Telemetry System</i>	Ligação ao servidor remoto através de <i>GSM/GPRS</i> ; Gestão remota da máquina; Controlo de stocks; Alertas por e-mail e SMS.	Entre \$200 a \$50000
<i>Protel Remote Vending Monitoring System</i>	Possibilidade de criação de uma rede de máquinas interligadas por rádio frequência ou protocolo <i>RS485</i> ; Emissão de alertas; Controlo de stocks;	N/D
<i>BITX for Vending</i>	Ligação ao servidor remoto através de ligação <i>GSM/GPRS</i> ; Monitorização constante da máquina de vending; Alteração de preços remotamente; Emissão de alertas via e-mail e <i>SMS</i> .	N/D
<i>GB024, GB024-25</i>	Ligação ao servidor remoto através de ligação <i>GSM/GPRS</i> ; Emissão de alertas por e-mail, SMS e Fax; Envio de informação para o servidor diariamente; Monitorização de stocks;	N/D

Anexo 3 Especificação de Requisitos

A solução proposta passa pela criação de quatro componentes distintos, nomeadamente um dispositivo móvel de recolha de auditoria, um módulo de recolha de auditoria, uma aplicação servidor, e ainda uma aplicação de gestão e configuração.

3.1 Aplicação de Gestão e Configuração

Aplicação de gestão e configuração deverá ser uma aplicação multi-posto que terá por objectivo visualizar todos os dados de auditoria recolhidos, assim como proceder à configuração dos dispositivos móveis.

Desta forma a aplicação deverá:

- Apresentar a listagem de recolhas de auditoria efectuadas;
- Permitir a gestão de parâmetros do sistema;
 - Indicar quais as máquinas com um valor de trocos inferior ao mínimo especificado;
 - Indicar na listagem as máquinas que tenham um volume de vendas inferior ao mínimo especificado.
- Permitir aplicar filtros de pesquisa para apresentação das listagens de recolha de auditoria;
- Permitir a criação de relatórios com a informação de auditoria financeira e de temperatura do ar;
- Apresentar nos relatórios de auditoria de temperatura do ar os valores registados em forma de gráfico e listagem, assim como apresentar o valor de temperatura máximo, mínimo e médio;
- Apresentar nos relatórios de auditoria financeira o valor total de vendas efectuadas pela máquina, o valor total facturado e o valor que se encontra nos tubos do moedeiro;
- Possuir três perfis de utilizador: administrador, operador e repositor;

- Permitir que os utilizadores do perfil operador possam:
 - Marcar que o valor indicado na recolha de auditoria financeira confere com o valor recebido em numerário por parte dos repositores;
- Permitir que os utilizadores do perfil administrador possam:
 - Especificar o valor mínimo de trocos;
 - Especificar o valor mínimo de volume de vendas;
 - Alterar a marcação indicativa de valor financeiro correcto;
 - Editar os dados de auditoria financeira recebidos nas recolhas;
 - Efectuar a gestão de utilizadores;
 - Efectuar a gestão de máquinas de *vending*;
 - Efectuar a gestão de localização de máquinas;
 - Efectuar a gestão de módulos de recolha de auditoria;
 - Efectuar a gestão de registadores de temperatura;
 - Efectuar a gestão de identificadores de repositores;
 - Introduzir dados de calibração de registadores de temperatura;
 - Configuração e actualização do dispositivo móvel.
- Permitir configurar o endereço da aplicação servidor no dispositivo móvel;
- Permitir configurar o intervalo entre leituras do registador de temperatura;
- Permitir configurar o código *PIN* no dispositivo móvel;
- Apresentar dados estatísticos.

3.1.1 Configuração do Dispositivo Móvel

A aplicação deverá possuir uma zona de configuração do dispositivo móvel. Ao entrar nesta zona a aplicação deverá verificar se o dispositivo móvel se encontra ligado ao computador.

Deverá ser possível configurar os seguintes parâmetros:

- Endereço da aplicação servidor;
- Intervalo entre leituras dos registadores de temperatura;
- Código *PIN* do cartão *SIM*.

Se o dispositivo ainda não se encontrar ligado ao computador, deverá ser apresentada uma mensagem ao utilizador a informar que deverá proceder à ligação do equipamento.

3.2.1 Criação de Relatórios

A aplicação deverá suportar a criação de relatórios em formato *pdf* com os dados de auditoria recolhidos.

Os relatórios de auditoria ambiental deverão ter a seguinte estrutura:

- Cabeçalho
 - Período a que se refere o relatório;
 - Máquina de *vending* a que se refere o relatório;
 - Localização(ões) da máquina de *vending*;
- Resumo
 - Gráfico de linhas com o histórico de temperatura do período de apresentação;
 - Tabela de estatísticas de temperatura. Deverá incluir os valores mínimo, máximo e médio atingidos no período de apresentação;
- Corpo
 - Informações das recolhas que compõe o relatório:
 - Detalhes de cada recolha:
 - Data da recolha;
 - Identificação do repositores que efectuou a recolha;
 - Localização da máquina de *vending*;
 - Detalhes de auditoria
 - Gráfico de linhas com os valores de temperatura recolhidos;
 - Tabela de estatísticas de temperatura. Deverá incluir o valor mínimo, máximo e médio atingidos no período de apresentação.

Os relatórios de auditoria financeira deverão ter a seguinte estrutura:

- Cabeçalho
 - Período a que se refere o relatório;
 - Máquina de *vending* a que se refere o relatório;
 - Localização(ões) da máquina de *vending*;
 - Total de trocos nos tubos do moedeiro;
- Resumo

- Número total de vendas efectuadas no período de apresentação;
- Valor total facturado no período de apresentação;
- Corpo
 - Informações das recolhas que compõe o relatório:
 - Detalhes de cada recolha:
 - Data da recolha;
 - Identificação do reposititor que efectuou a recolha;
 - Localização da máquina de *vending*;
 - Detalhes de auditoria
 - Total de vendas;
 - Total facturado;
 - Total de trocos nos tubos do moedeiro;

Ao gerar os relatórios de auditoria financeira deverá ser verificado se todas as recolhas foram tratadas correctamente. Caso seja verificado que existem recolhas incompletas, deverá ser apresentado ao utilizador uma mensagem de confirmação a perguntar se pretende continuar com a criação do relatório. Se o utilizador responder afirmativamente, o relatório gerado deverá apresentar uma nota a indicar que existem recolhas incompletas.

Edição de Dados de Auditoria Financeira

Aos utilizadores pertencentes ao perfil de administrador, deverá ser permitido editar os dados de auditoria financeira, por forma permitir a correcção de dados tratados incorrectamente.

3.3.1 Filtros de Pesquisa

A aplicação deverá suportar a aplicação de filtros de pesquisa. Os parâmetros dos filtros poderão ser:

- Data;
- Repositor;
- Local de registo;
- Máquina de *vending*;
- Tipo de auditoria.

3.4.1 Gestão de Identificadores

A aplicação deverá permitir introduzir e alterar dados dos identificadores que serão entregues aos repositores.

Os dados dos identificadores a guardar deverão ser:

- Número de série (obrigatório);

3.5.1 Gestão de Localizações

A aplicação deverá permitir efectuar a gestão de localizações de máquinas de vending.

Os dados a guardar deverão ser:

- Descrição (obrigatório);
- Morada (obrigatório);
- Coordenadas *GPS (Global Positioning System)*;
- Notas;

3.6.1 Gestão de Máquinas de Vending

A aplicação deverá permitir introduzir e alterar dados de máquinas de *vending*.

Os dados a guardar referentes às máquinas de *vending* serão os seguintes:

- Descrição (obrigatório);
- Localização (obrigatório);
- Modelo;
- Tipo de moedeiro;
- Notas;

3.7.1 Gestão de Módulos de Recolha de Auditoria

A aplicação deverá permitir introduzir e alterar dados dos módulos de recolha de auditoria.

Os dados a guardar do módulo deverão ser:

- Descrição (obrigatório)
- Localização (obrigatório);
- Tipos de auditoria a recolher.

3.8.1 Gestão de Registadores de Temperatura

A aplicação deverá permitir introduzir e alterar dados dos registadores de temperatura.

Os dados a guardar do módulo deverão ser:

- Número de série (obrigatório);
- Descrição (obrigatório);
- Máquina de *vending onde se encontra instalado* (obrigatório);
- Tipo de registador.

3.9.1 Gestão de Utilizadores

A aplicação deverá permitir introduzir e alterar dados de utilizadores do sistema.

Os utilizadores poderão pertencer a três perfis, administrador, operador ou repositor. Os dados do utilizador a guardar deverão ser:

- Nome (obrigatório);
- *Username* (obrigatório);
- Palavra-chave (obrigatório);
- Contacto telefónico;
- E-mail.

Apenas o contacto telefónico, o e-mail e o nome poderão ser editados.

Ao criar um novo utilizador com o perfil de repositor deverá ser pedido o identificador que lhe será atribuído. A um novo utilizador ao efectuar o *login* pela primeira vez deverá ser solicitado que altere a palavra-chave que lhe foi atribuída.

3.10.1 Indicar Máquinas com Menor Valor de Trocos

O sistema deverá apresentar uma listagem com todas as máquinas que possuam um valor de trocos inferior a um limite especificado pelo administrador do sistema.

3.11.1 Indicar máquinas com Menor Valor de Vendas

O sistema deverá apresentar uma listagem com todas as máquinas que possuam um volume de vendas inferior a um limite especificado pelo administrador do sistema.

3.12.1 *Inserção de Dados de Calibração*

A aplicação deverá permitir introduzir os dados referentes à última calibração dos registadores de temperatura.

Os dados que a guardar deverão ser:

- Data da calibração;
- Número do certificado de calibração;
- Registador a que se refere a calibração;
- Entidade de certificação.

Todos os dados referidos são de preenchimento obrigatório.

3.13.1 *Listagem de Calibrações Efectuadas*

A aplicação deverá apresentar sobre forma de listagem todas as calibrações efectuadas aos registadores de temperatura.

Na listagem deverão ser apresentados os seguintes dados:

- Data em que foi efectuada a calibração;
- Número do certificado de calibração;
- Registador a que se refere a calibração;
- Entidade certificadora.

Os dados a apresentar na listagem poderão ser filtrados por data, sendo que por defeito deverão ser apresentados os resultados referentes a registadores que tenham sido calibrados no mês do ano anterior.

3.14.1 *Listagem de Todas as Recolhas de Auditoria*

A aplicação deverá apresentar sobre forma de listagem todas as recolhas efectuadas. Na listagem deverão ser apresentados os seguintes dados da recolha:

- Data em que foi efectuada;
- Repositor;
- Máquina de *vending*;
- Localização da máquina de *vending*;

- Tipo de auditoria.

3.15.1 Perfis de Utilizador

A aplicação deverá suportar três perfis de utilizador, sendo eles:

- Repositor;
- Operador;
- Administrador.

Os utilizadores do tipo repositore apenas servirão para identificar o repositore que efectuo a recolha dos dados de auditoria junto da máquina de *vending*. A cada repositore será associado um dispositivo de identificação que servirá para efectuar a sua identificação.

Os utilizadores do tipo operador poderão efectuar as seguintes operações:

- Confirmação de valores de auditoria financeira recolhidos;
- Visualizar todos os dados de auditoria recolhidos;
- Gerar relatórios.

Os utilizadores do tipo administrador, para além de todas as operações possíveis de realizar pelos operadores, poderão ainda:

- Anular a confirmação de valores de auditoria financeira recolhidos;
- Editar os dados das recolhas de auditoria financeira que se encontram incompletas;
- Configurar os parâmetros de funcionamento da aplicação;
- Efectuar a gestão de utilizadores;
- Efectuar a gestão de máquinas de *vending*;
- Efectuar a gestão de localizações de máquinas;
- Efectuar a gestão de módulos de recolha de auditoria;
- Efectuar a gestão de registadores de temperatura;
- Efectuar a gestão de identificadores de repositores;
- Introduzir dados de calibração dos registadores de temperatura.

3.2 Aplicação Servidor

A aplicação servidor será responsável pela recepção e tratamento de dados de todo o sistema.

Desta forma a aplicação servidor será responsável pela recepção e disponibilização dos seguintes tipos de dados:

- Dados de auditoria financeira;
- Dados de auditoria ambiental.

3.1.2 Recepção e Tratamento de Dados de Auditoria Ambiental

A aplicação servidor deverá tratar os dados de auditoria ambiental, tratando e guardando a lista de valores de temperatura registados desde a última recolha efectuada.

3.2.2 Recepção e Tratamento de Dados de Auditoria Financeira

A aplicação servidor deverá tratar os dados de auditoria financeira, tratando e guardando os seguintes campos:

- Número da impressão;
- Valor total de vendas;
- Número total de vendas;
- Valor total de dinheiro nos tubos;
- Quantidade de dinheiro no cofre;
- Valor total de troco devolvido;
- Valor total de dinheiro inserido manualmente;
- Valor total de dinheiro dispendido manualmente;
- Valor total sobre pago;
- Valor total em fichas;
- Valor total em tokens;
- Valor total em notas.

3.3 Dispositivo Móvel

O dispositivo móvel deverá ser um equipamento portátil equipado com uma interface que permitirá efectuar a ligação ao módulo de recolha de auditoria que se encontra na máquina de *vending*.

Os requisitos funcionais definidos para o dispositivo móvel são:

- Possuir interface de ligação ao módulo de recolha de auditoria da máquina de *vending*;
- Permitir a identificação do repositor que efectuou a recolha de auditoria;
- Descarregar e enviar os dados de auditoria recolhidos;
- Possibilitar o upload de *firmware*;
- Possibilitar inserir o código PIN do cartão SIM;
- Possibilitar configurar o intervalo entre leituras do registador de temperatura;
- Modo de funcionamento *off-line*.

3.1.3 Configurar Intervalo Entre Leituras dos Registadores de Temperatura

O dispositivo móvel deverá permitir, acedendo através do menu de configurações, introduzir o intervalo entre leituras dos registadores de temperatura que se encontram ligados aos módulos de recolha de auditoria.

O intervalo entre leituras deverá ser definido em minutos, com intervalos mínimos de 1 minuto.

3.2.3 Descarregar e Enviar os Dados de Auditoria Recolhidos

Após o repositor seleccionar a opção de descarga de auditoria, o dispositivo móvel deverá verificar a sua ligação ao módulo de recolha de auditoria que se encontra na máquina de *vending*. Após verificar que o dispositivo móvel se encontra ligado a um módulo de recolha de auditoria, este deverá enviar o comando de descarga correspondente e ficar a aguardar resposta. O tipo de comando de recolha deverá ter por base a opção seleccionada pelo repositor. As várias opções possíveis serão:

- Descarregar Tudo;
- Descarregar Auditoria Financeira;
- Descarregar de Auditoria Ambiental.

Após a recepção dos dados o dispositivo móvel deverá emitir os mesmos para a aplicação servidor através de uma ligação *GPRS*.

O dispositivo móvel deverá aguardar no máximo 10 segundos pela resposta do módulo de recolha de auditoria. Se ao final dos 10 segundos o dispositivo móvel não tiver obtido resposta deverá ser apresentada uma mensagem de erro ao repositório.

Se existir uma falha ao estabelecer a ligação *GRPS*, os dados deverão ser guardados para posterior envio e ser apresentada uma mensagem de erro ao repositório.

3.3.3 Identificação do Repositório que Efectuou a Recolha de Auditoria

O dispositivo móvel deverá possuir um *job* para ligação de um *iButton* do tipo *DS1990A*. O *iButton* deverá encontrar-se inserido na base de dados do sistema e associado ao repositório, para que desta forma o mesmo possa ser identificado.

3.4.3 Inserção de Código PIN do Cartão SIM

O dispositivo móvel deverá permitir a inserção do código PIN do cartão SIM.

O código PIN do cartão SIM após ser inserido deverá ficar armazenado no dispositivo móvel de modo a que não seja necessário efectuar novamente o pedido.

O código PIN poderá ser introduzido através da selecção da respectiva opção do menu de configurações, ou ainda ser pedido nas seguintes situações:

- Quando o dispositivo móvel arranca pela primeira vez;
- Quando o dispositivo móvel tenta estabelecer ligação à rede e o *PIN* introduzido seja incorrecto.

3.5.3 Interface de Ligação ao Módulo de Recolha de Auditoria

O dispositivo deverá possuir uma interface de ligação ao módulo de recolha de auditoria. A ligação será feita através de um cabo, e utilizar o protocolo *RS-232* com implementação de *handshaking*, ou seja, o módulo de recolha de auditoria deverá indicar ao dispositivo móvel de que recebeu os dados enviados. A mesma interface servirá para ligação do dispositivo móvel à *docking station* de configuração do equipamento.

3.6.3 Modo de Funcionamento Off-Line

O dispositivo móvel deverá suportar um modo de funcionamento *off-line* para as situações em que não for possível enviar os dados para a aplicação servidor.

Sempre que o ocorrer uma falha no estabelecimento da ligação à rede, ou uma falha durante o envio dos dados, estes deverão ficar armazenados num cartão SD.

Após armazenar os dados o dispositivo móvel deverá tentar estabelecer ligação à rede e enviar os dados. Em caso de insucesso os dados deverão continuar armazenados no cartão até ter sido possível enviar os dados, ou os mesmos terem sido descarregados directamente para a aplicação de gestão e configuração.

3.4 Módulo de Recolha de Auditoria

O módulo de recolha de auditoria será o equipamento ao qual se irá ligar o dispositivo móvel e que será instalado nas máquinas de *vending*, e funcionará como ponto de recolha dos valores de auditoria dos vários sensores e equipamentos a ele ligados.

De seguida são apresentados e descritos os requisitos definidos para o módulo de recolha de auditoria.

- Possuir interface de ligação para o dispositivo móvel de recolha de auditoria;
- Possuir interface de ligação para registador Maxim *DS1921G*;
- Possuir interface de ligação para moedeiros MEI® série 6 e série 7;
- Possuir interface para expansões futuras;
- Ser alimentado através do dispositivo móvel de recolha de auditoria;
- Possuir um número de série para fins de identificação da máquina de *vending*;
- Possibilitar o *upload* de *firmware*.

3.1.4 Interface de Ligação para Moedeiros

O módulo de recolha de auditoria deverá possuir uma interface de ligação para moedeiros MEI® série 6 e série 7. A interface deverá utilizar o protocolo de comunicação *RS-232*.

3.2.4 Interface de Ligação para o Dispositivo Móvel

O módulo de recolha de auditoria deverá possuir uma interface de ligação para o dispositivo móvel. A interface deverá utilizar o protocolo *RS-232* com implementação de *handshaking*.

3.3.4 Interface de Ligação para Registador Maxim DS1921G

O módulo de recolha de auditoria deverá possuir uma interface de ligação para registadores *Maxim DS1921G*. A interface deverá utilizar o protocolo *1-Wire*.

3.4.4 Possuir um Número de Serie de Identificação

O módulo de recolha de auditoria deverá estar equipado com um *chip* para fins de identificação da máquina de *vending* na qual se encontra instalado.

Anexo 4 Estruturação do Modelo de Dados

Neste anexo é abordada a estruturação do modelo de dados, nomeadamente, a descrição de cada entidade, definição dos seus atributos, a apresentação dos DER e a listagem de relações resultantes.

4.1 Lista de Entidades

O modelo de dados será composto por duas base de dados, a base de dados de sistema e a base de dados de serviços. A base de dados de sistema trata-se da base de dados que irá armazenar toda a informação do sistema de recolha de auditoria. A base de dados de serviços trata-se da base de dados onde será armazenada a informação relativa às subscrições de serviços efectuadas pelos clientes

De seguida serão apresentadas duas listagens com todas as entidades que compõe a base de dados de sistema e a base de dados de serviços.

4.1.1 Lista de Entidades da Base de Dados de Sistema

De seguida é apresentada a listagem das entidades e uma breve descrição das mesmas que compõe o modelo de dados da base de dados de sistema.

Tabela 27 Descrição das entidades da base de dados de sistema

Lista de Entidades da Base de Dados de Sistema	
Nome	Auditoria
Descrição	A entidade auditoria trata-se de uma super-entidade que armazena os dados de auditoria recolhidos. Devido às diferentes características do tipo de dados recolhidos, a auditoria está subdividida em duas categorias: Ambiental, referente aos dados de condições do ar obtidos pelos registadores.

	Financeira, referente aos dados obtidos a partir dos moedeiros instalados nas máquinas de <i>vending</i> .
Nome	Calibração
Descrição	A entidade calibração é a entidade utilizada para armazenar os dados relativos às calibrações efectuadas aos registadores de temperatura.
Nome	Contacto
Descrição	Esta entidade trata-se da entidade responsável por armazenar todos os contactos dos utilizadores.
Nome	Identificador
Descrição	Esta entidade é utilizada para guardar os dados dos identificadores atribuídos aos repositores, pelo que os identificadores deverão ser únicos.
Nome	Localização
Descrição	A entidade localização é a entidade utilizada para armazenar os dados das localizações onde se encontram instaladas as máquinas de <i>vending</i> .
Nome	Máquina
Descrição	A entidade máquina trata-se da entidade utilizada para guardar os dados das diversas máquinas de <i>vending</i> .
Nome	Recolha
Descrição	A entidade recolha é a entidade utilizada para armazenar os dados de quando foram efectuadas recolhas de auditoria assim como quem as realizou.
Nome	Módulo
Descrição	A entidade módulo é a entidade utilizada para guardar os dados relativos aos módulos de recolha de auditoria.
Nome	Perfil
Descrição	A entidade perfil é a entidade utilizada para guardar os dados relativos aos vários tipos de perfil a que os utilizadores poderão pertencer.
Nome	Registador
Descrição	A entidade registador é a entidade utilizada para guardar os dados dos registadores de temperatura instalados nas máquinas de <i>vending</i> .
Nome	Tipo de Contacto
Descrição	Esta entidade trata-se da entidade responsável por armazenar todos os tipos de contacto que poderão ser guardados no sistema.
Nome	Utilizador
Descrição	A entidade utilizador trata-se de uma super-entidade que armazena os dados dos utilizadores que irão utilizar o sistema. Devido às funções que desempenham, os utilizadores estão sub-

	<p>divididos em três categorias:</p> <p>Os administradores, têm como função gerir e configurar o sistema. Assim como validar os dados obtidos nas recolhas de auditoria.</p> <p>Os operadores, têm como função analisar os dados obtidos nas recolhas assim como criar relatórios.</p> <p>Os repositores, são os utilizadores que se deslocam junto das máquinas de vending para efectuar as recolhas, não operando directamente a aplicação de gestão e configuração, mas enviam dados através dos dispositivos móveis que levam consigo.</p>
--	--

4.2.1 Lista de Entidades da Base de Dados de Serviços

De seguida é apresentada a listagem das entidades e uma breve descrição das mesmas que compõe o modelo de dados da base de dados de serviços.

Tabela 28 Descrição das entidades da base de dados de serviços

Lista de Entidades da Base de Dados de Serviços	
Nome	Conta
Descrição	A entidade Conta trata-se da entidade onde serão armazenadas todas as contas de cliente.
Nome	Contacto
Descrição	Esta entidade trata-se da entidade responsável por armazenar todos os contactos das entidades de facturação e das contas de cliente.
Nome	Entidade de Facturação
Descrição	Esta entidade trata-se da entidade responsável por armazenar todos os dados de facturação de um cliente.
Nome	Subscrição
Descrição	A entidade Subscrição irá armazenar os dados das subscrições efectuadas pelos clientes.
Nome	Serviço
Descrição	A entidade Serviço irá armazenar os dados dos serviços que poderão ser subscritos pelos clientes.
Nome	Regra de Desconto
Descrição	A entidade regra de desconto irá armazenar os dados das regras de desconto que poderão ser aplicadas aos serviços disponibilizados.
Nome	Tipo de Contacto
Descrição	Esta entidade trata-se da entidade responsável por armazenar todos os tipos de contacto que poderão ser guardados no sistema.

4.2 Representação dos DER

Nesta apresentação dos DER estão apenas representados os atributos que farão parte das relações resultantes, todos os outros atributos não se encontram representados para não sobrecarregar o desenho dos diagramas.

4.1.2 Diagrama de Entidade-Relacionamento da Base de Dados de Sistema

Na Figura 61 é apresentado o DER da base de dados de sistema.

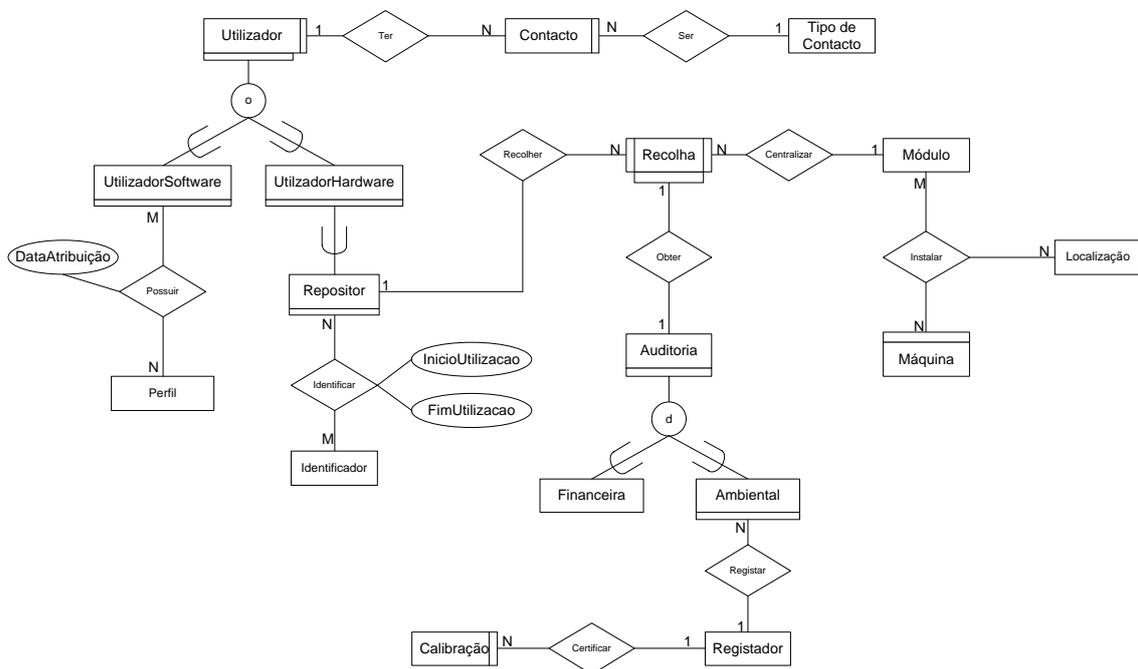


Figura 61 Diagrama Entidade-Relacionamento da base de dados de sistema

4.2.2 Diagrama de Entidade-Relacionamento da Base de Dados de Serviços

Na Figura 62 poderá ser consultado o DER da base de dados de serviços.

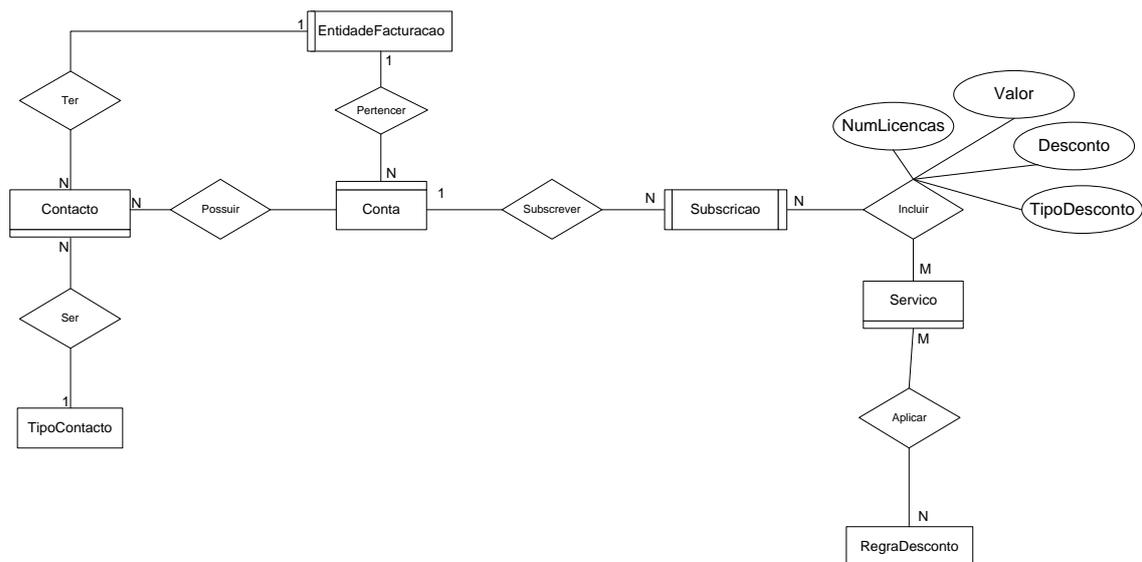


Figura 62 Diagrama Entidade-Relacionamento da base de dados de serviços

4.3 Representação das Tabelas da Base de Dados de Sistema

De seguida são apresentadas todas as tabelas resultantes da derivação das relações entre entidades que compõe o modelo de dados da base de dados de sistema.

Tabela 29 Tabelas resultantes da base de dados de sistema

Lista de Tabelas Resultantes da Base de Dados de Sistema	
Tabela	Ambiental
Chave Primária	IDAuditoriaAmbiental
Campos	Valor
	Unidade
	Data
Chaves Estrangeiras	IDRegistador
Tabela	Calibração
Chave Primária	IDCalibração
Campos	Data
	NúmeroCertificado
	EntidadeCertificadora
Chaves Estrangeiras	IDRegistador
Tabela	Contacto
Chave Primária	IDContacto
Campos	Contacto

	Activo
Chaves Estrangeiras	IDTipoContacto
Tabela	Financeira
Chave Primária	IDAuditoriaFinanceira
Campos	NúmeroImpressão
	TotalVendas
	TotalNosTubos
	TotalNoCofre
	TotalTrocós
	TotalIntroduzidoManualmente
	TotalDispendidoManualmente
	TotalSobrePago
	TotalSobrePago
	TotalChips
	TotalTokens
	TotalNotas
	Talão
Chaves Estrangeiras	N/A
Tabela	Identificar
Chave Primária	IDIdentificador
	IDUtilizador
Campos	InicioUtilização
	FimUtilização
Chaves Estrangeiras	IDIdentificador
	IDUtilizador
Tabela	Identificador
Chave Primária	IDIdentificador
Campos	NúmeroSérie
	Activo
Chaves Estrangeiras	N/A
Tabela	Instalar
Chave Primária	IDMódulo
	IDMáquina
	IDLocalização
Campos	N/A
Chaves Estrangeiras	IDMódulo

	IDMáquina
	IDLocalização
Tabela	Localização
Chave Primária	IDLocalização
Campos	Designação
	Morada
	Latitude
	Longitude
	Notas
	Activo
Chaves Estrangeiras	N/A
Tabela	Máquina
Chave Primária	IDMáquina
Campos	Designação
	Modelo
	Moedeiro
	Notas
	Activo
Chaves Estrangeiras	N/A
Tabela	Módulo
Chave Primária	IDMódulo
Campos	NúmeroSérie
	Designação
	Activo
Chaves Estrangeiras	N/A
Tabela	Obter
Chave Primária	IDAuditoria
Campos	N/A
Chaves Estrangeiras	IDAuditoria
	IDRecolha
Tabela	Perfil
Chave Primária	IDPerfil
Campos	Designação
Chaves Estrangeiras	N/A
Tabela	Utilizador
Chave Primária	IDUtilizador

Campos	Nome
	Activo
Chaves Estrangeiras	N/A
Tabela	Pertencer
Chave Primária	IDUtilizador
	IDPerfil
Campos	DataInclusão
Chaves Estrangeiras	IDUtilizador
	IDPerfil
Tabela	Recolha
Chave Primária	IDRecolha
Campos	Data
Chaves Estrangeiras	IDUtilizador
	IDMódulo
Tabela	Registador
Chave Primária	IDRegistador
Campos	NúmeroSérie
	Designação
	Modelo
	Activo
Chaves Estrangeiras	N/A
Tabela	Ter
Chave Primária	IDContacto
	FkContacto
Campos	N/A
Chaves Estrangeiras	IDContacto
	IDUtilizador
Tabela	TipoContacto
Chave Primária	IDTipoContacto
Campos	Designação
	Activo
Chaves Estrangeiras	N/A
Tabela	UtilizadorHardware
Chave Primária	IDUtilizador
Campos	N/A
Chaves Estrangeiras	IDUtilizador

	IDIdentificador
Tabela	UtilizadorSoftware
Chave Primária	IDUtilizador
Campos	Utilizador
	PalavraChave
	Tipo
Chaves Estrangeiras	IDUtilizador

4.4 Representação das Tabelas da Base de Dados de Serviços

De seguida serão apresentadas as tabelas que resultaram da derivação das relações entre as entidades que compõe o modelo de dados da base de dados de serviços.

Tabela 30 Tabelas resultantes da base dados de serviços

Lista de Tabelas Resultantes da Base de Dados de Serviços	
Tabela	Aplicar
Chave Primária	IDServiço
	IDRegraDesconto
Campos	N/A
Chaves Estrangeiras	IDServiço
	IDRegraDesconto
Tabela	Conta
Chave Primária	IDConta
Campos	Designação
	Estado
	Activo
Chaves Estrangeiras	IDEntidadeFacturação
Tabela	Contacto
Chave Primária	IDContacto
Campos	Contacto
	Activo
Chaves Estrangeiras	IDTipoContacto
Tabela	EntidadeFacturação
Chave Primária	IDEntidadeFacturação
Campos	Nome

	Morada
	MoradaFacturação
	NIF
	Activo
Chaves Estrangeiras	N/A
Tabela	Incluir
Chave Primária	IDSubscrição
	IDServiço
Campos	NúmeroLicenças
	Valor
	Desconto
	TipoDesconto
Chaves Estrangeiras	IDSubscrição
	IDServiço
Tabela	Possuir
Chave Primária	IDConta
	IDContacto
Campos	N/A
Chaves Estrangeiras	IDConta
	IDContacto
Tabela	RegraDesconto
Chave Primária	IDRegraDesconto
Campos	Designação
	MínimoLicenças
	MáximoLicenças
	Desconto
	Tipo
	Activo
Chaves Estrangeiras	N/A
Tabela	Serviço
Chave Primária	IDServiço
Campos	Designação
	Descrição
	Preço
	Activo
Chaves Estrangeiras	N/A

Tabela	Subscrição
Chave Primária	IDSubscrição
Campos	DataSubscrição
	Duração
	NúmeroLicençasSoftware
	NúmeroLicençasUtilização
	Estado
Activa	
Chaves Estrangeiras	IDConta
Tabela	Ter
Chave Primária	IDEntidadeFacturação
	IDContacto
Campos	N/A
Chaves Estrangeiras	IDEntidadeFacturação
	IDContacto
Tabela	TipoContacto
Chave Primária	IDTipoContacto
Campos	Designação
	Activo
Chaves Estrangeiras	N/A

Anexo 5 Casos de Uso

Neste anexo são apresentados os restantes casos de uso da solução que não foram apresentados previamente.

5.1 Diagramas de Caso de Uso

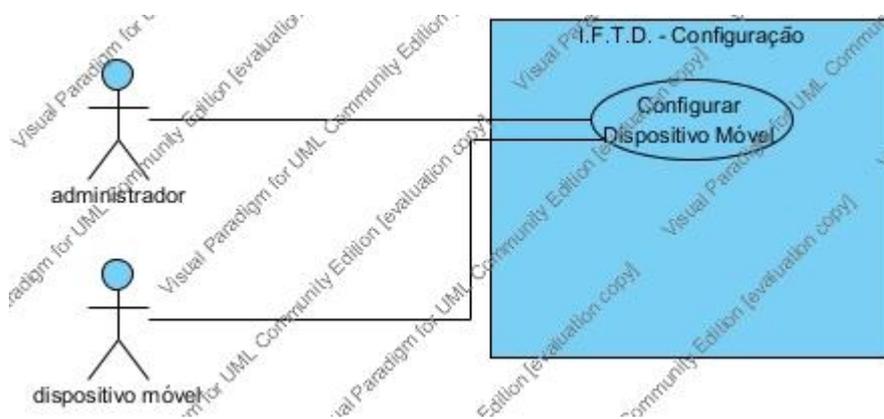


Figura 63 Diagrama do conjunto de casos de uso de configuração

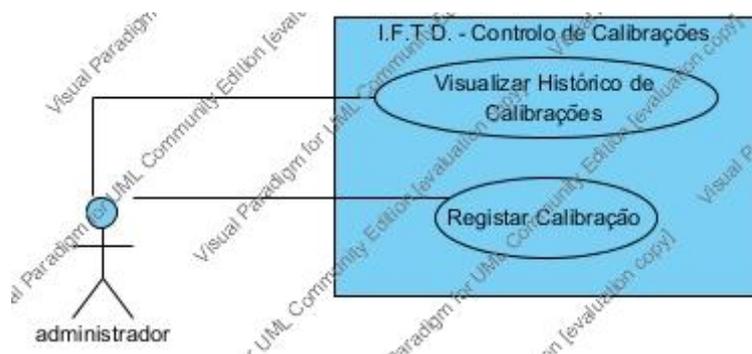


Figura 64 Diagrama do conjunto de casos de uso do controlo de calibrações

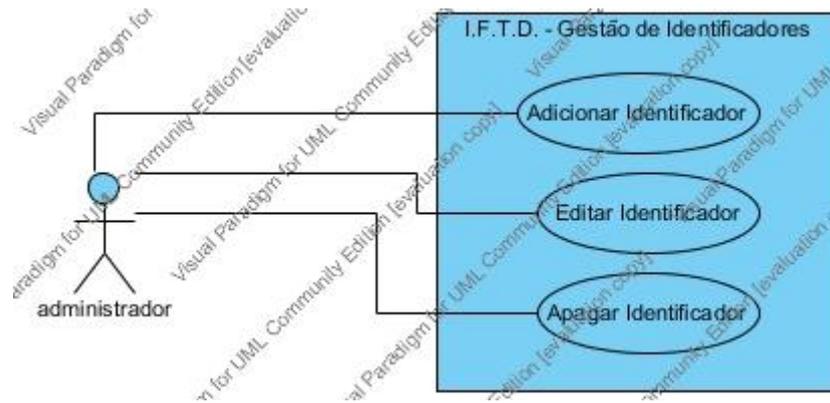


Figura 65 Diagrama do conjunto de casos de uso da gestão de identificadores

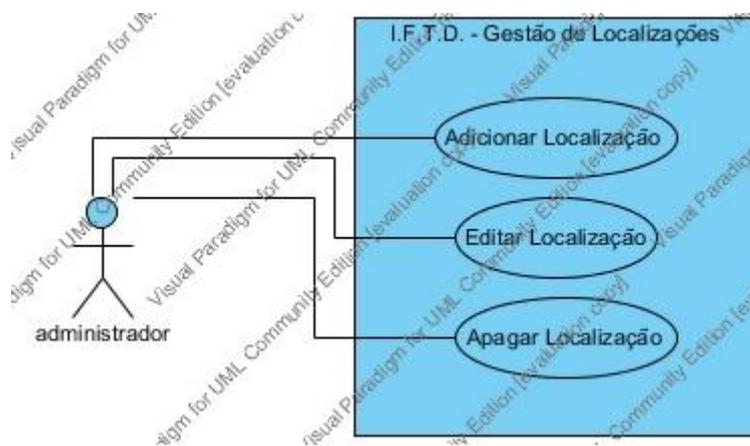


Figura 66 Diagrama do conjunto de casos de uso da gestão de localizações

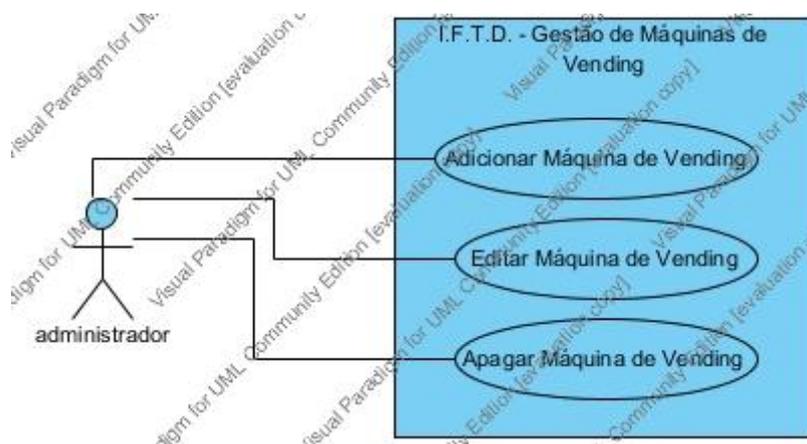


Figura 67 Diagrama do conjunto de casos de uso da gestão de máquinas de vending

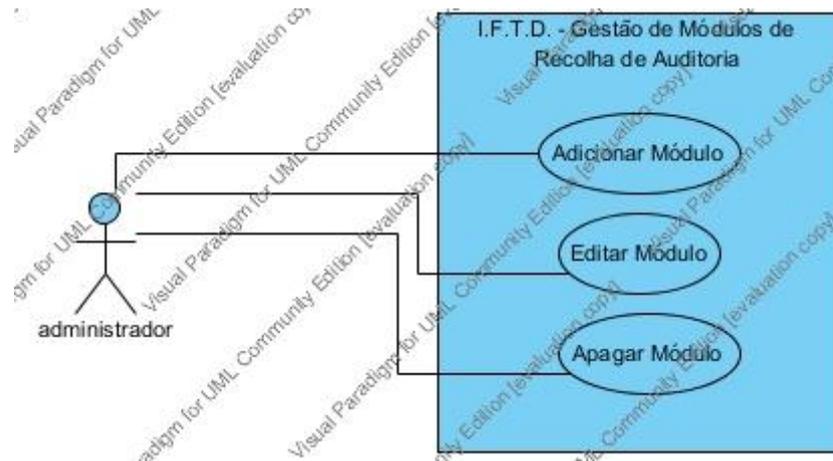


Figura 68 Diagrama do conjunto de casos de uso da gestão de módulos de recolha de auditoria

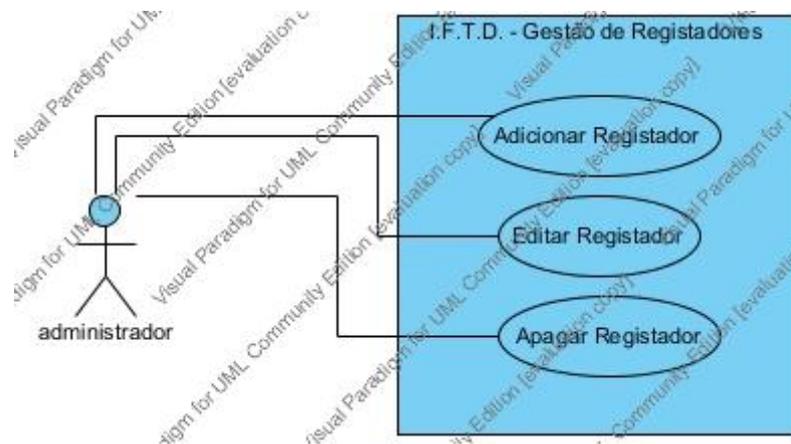


Figura 69 Diagrama do conjunto de casos de uso da gestão de registadores

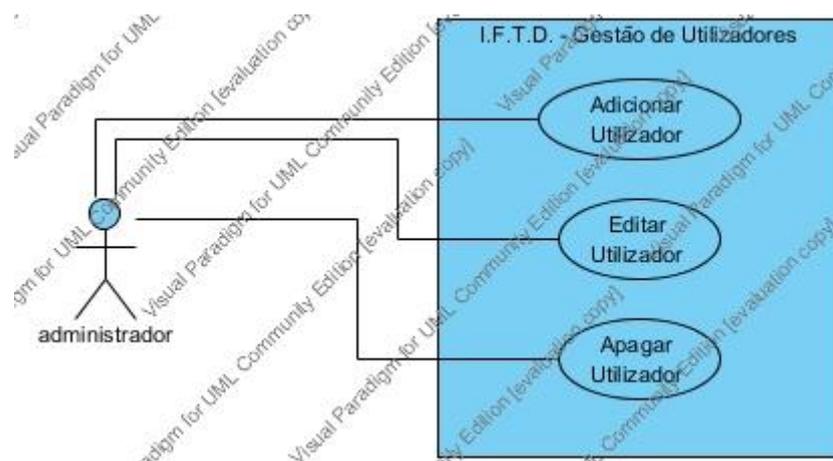


Figura 70 Diagrama do conjunto de casos de uso da gestão de utilizadores

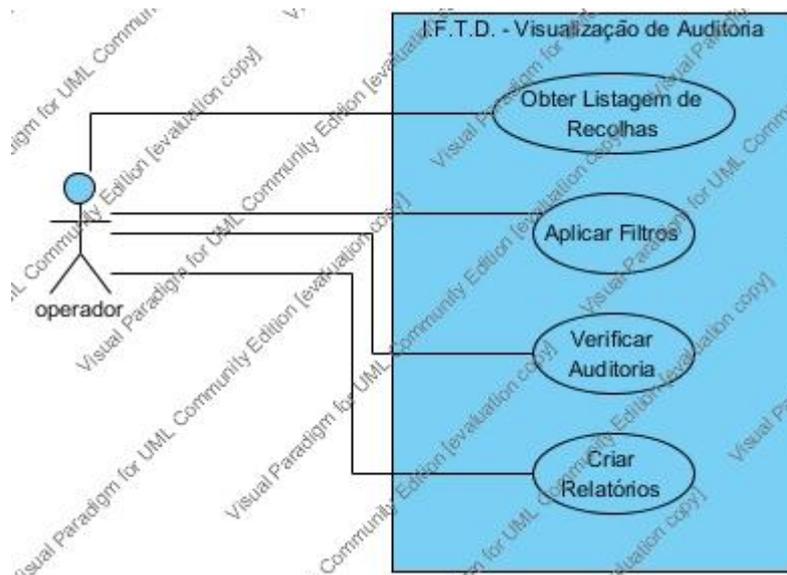


Figura 71 Diagrama do conjunto de casos de uso da visualização de auditoria

5.2 Fluxo de Eventos de Cada Caso de Uso

Tabela 31 Fluxo de eventos do caso de uso "Configurar Dispositivo Móvel"

Fluxo de Eventos do Caso de Uso		
Nome do Caso de Uso	Configurar Dispositivo Móvel	
Descrição	Nesta secção o administrador poderá configurar alguns parâmetros de funcionamento do dispositivo móvel.	
Actores	Administrador, Dispositivo Móvel	
Caminho Principal		
Evento Nº	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de configuração e carrega em "Configurar Dispositivo Móvel";	
2		O sistema apresenta a janela de configuração;
3	O utilizador introduz os parâmetros de configuração e carrega em "Ok";	
4		O sistema valida os dados introduzidos pelo utilizador e envia os dados de configuração para o dispositivo móvel. Após enviar os dados de configuração com

		sucesso para o dispositivo móvel, o sistema apresenta uma mensagem de sucesso ao utilizador;
5	O utilizador após ler a mensagem de sucesso carrega em “Ok”;	
6		O sistema fecha a janela de sucesso e a janela de configuração do dispositivo móvel.

Caminhos Secundário

Evento Nº	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de configuração e carrega em “Configurar Dispositivo Móvel”;	
2		O sistema apresenta a janela de configuração;
3	O administrador introduz os parâmetros de configuração inválidos e carrega em “Ok”;	
4		O sistema verifica que existem irregularidades nos parâmetros de configuração e apresenta uma janela com uma mensagem de erro;
5	O utilizador após ler a mensagem de erro carrega em “Ok” ;	
6		O sistema fecha a janela de erro.

1	O administrador na janela principal acede ao menu de configuração e carrega em “Configurar Dispositivo Móvel”;	
2		O sistema apresenta a janela de configuração;
3	O administrador introduz os parâmetros de configuração e carrega em “Ok”;	
4		O sistema valida os dados introduzidos pelo utilizador e verifica problemas de comunicação com o dispositivo móvel. O

		sistema apresenta uma janela com uma mensagem de erro ao utilizador;
5	O utilizador após ler a mensagem de erro carrega em “Ok”;	
6		O sistema fecha a janela de erro.

Tabela 32 Fluxo de eventos do caso de uso "Visualizar Histórico de Calibrações"

Fluxo de Eventos do Caso de Uso		
Nome do Caso de Uso	Visualizar Histórico de Calibrações	
Descrição	Nesta secção o administrador poderá consultar os dados das calibrações efectuadas aos diversos registadores utilizados no sistema.	
Actores	Administrador	
Caminho Principal		
Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema obtém a listagem das calibrações guardadas no sistema, e apresenta a janela de histórico de calibrações com a listagem obtida anteriormente;
Caminhos Secundário		
Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema não consegue estabelecer ligação ao servidor para obter a listagem de calibrações, apresenta a janela de histórico de calibrações e apresenta uma janela com uma mensagem de erro.
3	O administrador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e a janela de histórico de calibrações.

Tabela 33 Fluxo de eventos do caso de uso "Registrar Calibração"

Fluxo de Eventos do Caso de Uso		
Nome do Caso de Uso	Registrar Calibração	
Descrição	Nesta secção os administradores poderão inserir os dados de calibração referentes a um determinado registador.	
Actores	Administrador	
Caminho Principal		
Evento Nº	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema obtém a listagem das calibrações guardadas no sistema, e apresenta a janela de histórico de calibrações com a listagem obtida anteriormente;
3	O administrador acede ao menu calibração e carrega em “Adicionar Calibração”;	
4		O sistema apresenta a janela de inserção de dados de calibração;
5	O administrador introduz os dados da calibração nos respectivos campos e carrega em “Guardar”;	
6		O sistema valida os dados e envia-os para o servidor. Após ter enviado os dados com sucesso para o servidor, o sistema apresenta uma janela com uma mensagem de sucesso;
7	O administrador após a mensagem de sucesso carrega em “Ok”;	
8		O sistema fecha a janela de sucesso e a janela de inserção de dados de calibração e actualiza a listagem apresentada na janela de histórico de calibrações.
Caminhos Secundário		

Evento Nº	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema não consegue estabelecer ligação ao servidor para obter a listagem de calibrações, apresenta a janela de histórico de calibrações e apresenta uma janela com uma mensagem de erro.
3	O administrador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e a janela de histórico de calibrações.
1	O administrador na janela principal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema obtém a listagem das calibrações guardadas no sistema e apresenta a janela de histórico de calibrações com a listagem obtida anteriormente;
3	O administrador acede ao menu calibração e carrega em “Adicionar Calibração”;	
4		O sistema apresenta a janela de inserção de dados de calibração;
5	O administrador introduz os dados da calibração nos respectivos campos e carrega em “Guardar”;	
6		O sistema valida os dados e verifica falha na comunicação com o servidor, apresentando de seguida uma janela com uma mensagem de erro;
7	O administrador após a mensagem de erro carrega em “Ok”;	
8		O sistema fecha a janela de erro.

1	O administrador na janela principal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema obtém a listagem das calibrações guardadas no sistema, e apresenta a janela de histórico de calibrações com a listagem obtida anteriormente;
3	O administrador acede ao menu calibração e carrega em “Adicionar Calibração”;	
4		O sistema apresenta a janela de inserção de dados de calibração;
5	O administrador introduz os dados da calibração nos respectivos campos e carrega em “Guardar”;	
6		O sistema valida os dados e envia-os para o servidor. Após ter enviado os dados com sucesso para o servidor, o sistema apresenta uma janela com uma mensagem de sucesso;
7	O administrador após a mensagem de sucesso carrega em “Ok”;	
8		O sistema fecha a janela de sucesso e a janela de inserção de dados de calibração. Ao obter a listagem com o histórico de calibrações, o servidor detecta falha de comunicação com o servidor e apresenta uma janela com uma mensagem de erro;
9	O administrador após ler a mensagem de erro carrega em “Ok”;	
10		O sistema fecha a janela de erro e coloca uma indicação na janela de histórico de que a listagem apresentada não se encontra actualizada.
1	O administrador na janela principal	

	pal acede ao menu de calibrações e carrega em “Histórico de Calibrações”;	
2		O sistema obtém a listagem das calibrações guardadas no sistema, e apresenta a janela de histórico de calibrações com a listagem obtida anteriormente;
3	O administrador acede ao menu calibração e carrega em “Adicionar Calibração”;	
4		O sistema apresenta a janela de inserção de dados de calibração;
5	O administrador introduz dados inválidos da calibração e carrega em “Guardar”;	
6		O sistema valida os dados e envia-os para o servidor. Após ter enviado os dados com sucesso para o servidor, o sistema apresenta uma janela com uma mensagem de sucesso;

Tabela 34 Fluxo de eventos do caso de uso "Adicionar Identificador"

Fluxo de Eventos do Caso de Uso		
Nome do Caso de Uso	Adicionar Identificador	
Descrição	Nesta secção o administrador poderá adicionar um novo identificador ao sistema.	
Actores	Administrador	
Caminho Principal		
Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;

3	O administrador na janela de gestão de identificadores introduz os dados do novo identificador e carrega em “Guardar”;	
4		O sistema valida os dados e envia-os para o servidor. Após enviar os dados com sucesso para o servidor apresenta uma janela com uma mensagem de sucesso;
5	O administrador após ler a mensagem de sucesso carrega em “Ok”;	
6		O sistema acede ao servidor e obtém a lista actualizada de todos os identificadores registados no sistema, apresentando de seguida a lista obtida.

Caminhos Secundário

Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e detecta uma falha de comunicação com o servidor e apresenta uma janela com uma mensagem de erro;
3	O administrador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e a janela de gestão de identificadores;
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;

3	O administrador na janela de gestão de identificadores introduz dados inválidos do novo identificador e carrega em “Guardar”;	
4		O sistema verifica que os dados são inválidos e apresenta uma janela com uma mensagem de erro;
5	O administrador após ler a mensagem de erro carrega em “Ok”;	
6		O sistema fecha a janela de erro;
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores introduz os dados do novo identificador e carrega em “Guardar”;	
4		O sistema valida os dados e envia-os para o servidor. Após enviar os dados com sucesso para o servidor apresenta uma janela com uma mensagem de sucesso;
5	O administrador após ler a mensagem de sucesso carrega em “Ok”;	
6		O sistema verifica uma falha de comunicação com o servidor ao tentar obter a lista actualizada de todos os identificadores registados no sistema, apresentando de seguida uma janela com uma mensagem de erro;
7	O administrador após ler a mensagem de erro carrega em “Ok”;	

8		O sistema fecha a janela de erro.
---	--	-----------------------------------

Tabela 35 Fluxo de eventos do caso de uso "Editar Identificador"

Fluxo de Eventos do Caso de Uso		
Nome do Caso de Uso	Editar Identificador	
Descrição	Nesta secção o administrador poderá editar os dados de identificadores que se encontrem registados no sistema.	
Actores	Administrador	
Caminho Principal		
Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores selecciona o identificador que pretende editar e carrega em “Editar”;	
4		O sistema obtém os dados do identificador e apresenta-os na janela de gestão de identificadores;
5	O administrador edita os dados do identificador e carrega em “Guardar”;	
6		O sistema valida os dados e envia-os para o servidor. Após enviar os dados com sucesso para o servidor apresenta uma janela com uma mensagem de sucesso;
7	O administrador após ler a mensagem de sucesso carrega em “Ok”;	
8		O sistema acede ao servidor e obtém a lista

		actualizada de todos os identificadores registados no sistema, apresentando de seguida a lista obtida.
Caminhos Secundário		
Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e detecta uma falha de comunicação com o servidor e apresenta uma janela com uma mensagem de erro;
3	O administrador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e a janela de gestão de identificadores;
Caminho Secundário		
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores selecciona o identificador que pretende editar e carrega em “Editar”;	
4		O sistema obtém os dados do identificador e apresenta-os na janela de gestão de identificadores;
5	O administrador edita os dados do identificador com dados inválidos e carrega em “Gar-	

	dar”;	
6		O sistema verifica que os dados são inválidos e apresenta uma janela com uma mensagem de erro;
7	O administrador após ler a mensagem de erro carrega em “Ok”;	
8		O sistema fecha a janela de erro;
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores selecciona o identificador que pretende editar e carrega em “Editar”;	
4		O sistema obtém os dados do identificador e apresenta-os na janela de gestão de identificadores;
5	O administrador na janela de gestão de identificadores introduz os dados do novo identificador e carrega em “Guardar”;	
6		O sistema valida os dados e envia-os para o servidor. Após enviar os dados com sucesso para o servidor apresenta uma janela com uma mensagem de sucesso;
7	O administrador após ler a mensagem de sucesso carrega em “Ok”;	
8		O sistema verifica uma falha de comunicação com o servidor ao tentar obter a lista actualizada de todos os identificadores

		registados no sistema, apresentando de seguida uma janela com uma mensagem de erro;
9	O administrador após ler a mensagem de erro carrega em “Ok”;	
10		O sistema fecha a janela de erro.

Tabela 36 Fluxo de eventos do caso de uso "Apagar Identificador"

Fluxo de Eventos do Caso de Uso		
Nome do Caso de Uso	Apagar Identificador	
Descrição	Nesta secção o administrador poderá apagar o registo de identificadores.	
Actores	Administrador	
Caminho Principal		
Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores selecciona o identificador que pretende apagar;	
4		O sistema obtém os dados do identificador e apresenta-os na janela de gestão de identificadores;
5	O administrador carrega em “Apagar”;	
6		O sistema apresenta uma janela com uma mensagem de confirmação;
7	O administrador após ler a mensagem de confirmação carrega em “Sim”;	
8		O sistema fecha a janela de confirmação,

		accede ao servidor e marca o identificador como inactivo. De seguida apresenta uma janela com uma mensagem de sucesso;
9	O administrador após ler a mensagem de sucesso carrega em “Ok”;	
10		O sistema accede ao servidor e obtém a lista actualizada de todos os identificadores registados no sistema, apresentando de seguida a lista obtida.

Caminhos Secundário

Evento N°	Ação do Actor	Resposta do Sistema
1	O administrador na janela principal accede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e detecta uma falha de comunicação com o servidor e apresenta uma janela com uma mensagem de erro;
3	O administrador após ler a mensagem de erro carrega em “Ok”;	
4		O sistema fecha a janela de erro e a janela de gestão de identificadores;
1	O administrador na janela principal accede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida accede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores selecciona o identificador que pretende apagar;	
4		O sistema obtém os dados do identificador

		e apresenta-os na janela de gestão de identificadores;
5	O administrador carrega em “Apagar”;	
6		O sistema apresenta uma janela com uma mensagem de confirmação;
7	O administrador após ler a mensagem de confirmação carrega em “Não”;	
8		O sistema fecha a janela de confirmação;
1	O administrador na janela principal acede ao menu de gestão e carrega em “Gestão de Identificadores”;	
2		O sistema abre a janela de gestão de identificadores e de seguida acede ao servidor e obtém a lista de todos os identificadores activos registados no sistema, apresentando de seguida a lista obtida;
3	O administrador na janela de gestão de identificadores selecciona o identificador que pretende apagar;	
4		O sistema obtém os dados do identificador e apresenta-os na janela de gestão de identificadores;
5	O administrador carrega em “Apagar”;	
6		O sistema apresenta uma janela com uma mensagem de confirmação;
7	O administrador após ler a mensagem de confirmação carrega em “Sim”;	
8		O sistema fecha a janela de confirmação, detecta uma falha de comunicação com o servidor e apresenta uma janela com uma mensagem de erro;
9	O administrador após ler a men-	

	sagem de erro carrega em “Ok”;	
10		O sistema fecha a janela de erro;

Os restantes casos de uso referentes a acções de gestão não foram descritos, pois o fluxo de eventos é realizado de forma análoga aos que foram descritos anteriormente.

Anexo 6 Descrição dos Pinos e Configuração dos Jumpers de Função do LCD LM6060CBY

Na Tabela 37 é apresentada a descrição e função de cada um dos pinos de ligação do LCD utilizado.

Tabela 37 Descrição dos pinos do *LCD LM6060CBY*
Fonte: Adaptado de (Shenzhen Topway Technology Co., 2007)

Descrição dos Pinos de Ligação do LCD					
Nº do Pino	Nome	Tipo	Descrição		
			Modo Paralelo 8080	Modo Paralelo 6800	Modo Série
1	/CS1	Entrada	<i>Chip Select</i> /CS1=0 activa acesso ao LCD /CS1=1 desactiva o acesso ao LCD		
2	/RES	Entrada	<i>Reset Signal</i> /RES = 0 inicialização executada /RES = 1 funcionamento normal		
3	A0	Entrada	<i>Register Select</i> A0 = 0 transferência de dados de controlo A0 = 1 transferência de dados de apresentação		
4	/WR (R/W)	Entrada	/WR=0→1, /RD=1; Dados preparados para envio.	R/W=1, E=0; Leitura de dados ou estado do LCD.	Não utilizado
5	/RD (E)	Entrada	/WR=1, /RD=0; Dados preparados para	R/W=0, E=1→0; Dados preparados para	

			leitura.	envio.	
6	<i>D0</i>	Entrada/Saída	Barramento de dados de 8 bits.		Não utilizado
...	...	Entrada/Saída	Terminais de Entrada/Saída para dados de apresentação ou dados de controlo quando /CS=1 e D0~D7=1.		
11	<i>D5</i>	Entrada/Saída			
12	<i>D6 (SCL)</i>	Entrada/Saída			<i>Serial Clock Input</i>
13	<i>D7 (SI)</i>	Entrada/Saída		<i>Serial Data Input</i>	
14	<i>VDD</i>	Alimentação	Alimentação positiva		
15	<i>VSS</i>	Alimentação	Alimentação negativa, 0V		
16	<i>BLA</i>	Alimentação	Alimentação positiva da iluminação retroactiva		
17	<i>BLK</i>	Alimentação	Alimentação negativa da iluminação retroactiva, 0V		
18	<i>NC</i>	-	Não utilizado		

Na Tabela 38 são apresentadas as diversas configurações dos *jumpers* de função do *LCD*. De recordar que a configuração utilizada no projecto foi a que coloca o *LCD* em modo de funcionamento série.

Tabela 38 Configuração dos *jumpers* de função do *LCD LM6060C*BY para modo de funcionamento série

Fonte: Adaptado de (Shenzhen Topway Technology Co., 2007)

Configuração dos <i>Jumpers</i> de Função				
Jumper 1	Jumper 2	Jumper 3	Jumper 4	Modo
Aberto	Fechado	Aberto	Fechado	Série
Fechado	Aberto	Fechado	Aberto	6800
Aberto	Fechado	Fechado	Aberto	8080 (Modo Padrão)

Anexo 7 Lista de Comandos AT

Neste anexo são apresentados os comandos AT necessários para configuração do modem, para estabelecimento de ligação à rede GSM, e utilização do protocolo TCP/IP.

Para uma melhor compreensão da função dos comandos AT utilizados, estes serão divididos em cinco grupos. Inicialização básica, inicialização de rede, configuração do perfil de ligação GPRS, configuração do perfil do serviço cliente *socket* TCP, e por fim ligação à *internet* e transferência de informação.

Na Tabela 39 são apresentados os comandos necessários para a configuração básica do modo de funcionamento do modem.

Tabela 39 Lista de comandos AT de inicialização básica do modem GSM

Fonte: (Modules, 2008a, , 2008b)

Lista de Comandos de Inicialização Básica			
Comando	Descrição	Comando Utilizado	Explicação
<i>AT+CMEE</i>	Definição do formato do código de erro.	<i>AT+CMEE=2</i>	Activa os códigos de erro em formato detalhado.
<i>AT+CRC</i>	Definição do tipo de códigos para chamadas recebidas.	<i>AT+CRC=1</i>	Activa códigos em formato extenso.
<i>AT\Q</i>	Definição do tipo de controlo de fluxo.	<i>AT\Q0</i>	Desabilita o controlo de fluxo.

Na Tabela 40 são apresentados os comandos para estabelecimento de ligação do modem à rede GSM.

Tabela 40 Lista de comandos AT de inicialização de rede do modem GSM

Fonte: (Modules, 2008a, , 2008b)

Lista de Comandos de Inicialização de Rede			
Comando	Descrição	Comando Utilizado	Explicação
<i>AT+COPS</i>	Seleção da operadora móvel.	<i>AT+COPS=0</i>	Seleção automática de operadora.
<i>AT+CREG</i>	Notificação do estado da rede.	<i>AT+CREG=0</i>	Desabilita a notificação do estado da rede.
<i>AT+CPIN</i>	Introdução do código PIN.	<i>AT+CPIN=1234</i>	Introdução do código <i>PIN</i> 1234.

Na Tabela 41 são apresentados todos os comandos necessários para configuração do perfil utilizado para estabelecimento de ligação à *internet*.

Tabela 41 Lista de comandos AT de configuração do perfil de ligação à *internet*

Fonte: (Modules, 2008a, , 2008b)

Lista de Comandos de Inicialização de Configuração do Perfil de Ligação à Internet			
Comando	Descrição	Comando Utilizado	Explicação
<i>AT^SICS</i>	Criação e edição do perfil de ligação à internet.	<i>AT^SICS=1,conType,GPRS0</i>	Define o tipo de ligação como <i>GPRS</i> .
		<i>AT^SICS=1,alphabet,1</i>	Define o tipo de alfabeto a utilizar como <i>IRA (International Reference Alphabet)</i> .
		<i>AT^SICS=1,authMode,PAP</i>	Define o modo de autenticação como <i>PAP</i> .
		<i>AT^SICS=1,user,vodafone</i>	Define o <i>username</i> a utilizar na ligação.
		<i>AT^SICS=1,passwd,Vodafone</i>	Define a <i>password</i> a utilizar.
		<i>AT^SICS=1,apn,internet.vodafone.pt</i>	Define o nome do <i>access point</i> .
		<i>AT^SICS=1,dns1,0.0.0.0</i>	Define o servidor

			de <i>DNS</i> primário como sendo dinâmico.
		<i>AT^SICS=1,dns2,0.0.0.0</i>	Define o servidor de <i>DNS</i> secundário como sendo dinâmico.
		<i>AT^SICS=inactTO,30</i>	Define o tempo máximo de inatividade em 30 segundos.

Na Tabela 42 são apresentados os comandos de configuração do perfil do serviço de *internet*.

Tabela 42 Lista de comandos AT de configuração do perfil do serviço de *internet*

Fonte: (Modules, 2008a, , 2008b)

Lista de Comandos de Configuração do Perfil do Serviço de <i>Internet</i>			
Comando	Descrição	Comando Utilizado	Explicação
<i>AT^SISO</i>	Definição dos parâmetros necessários aos perfis dos serviços de <i>internet</i> .	<i>AT^SISS=0,svType,Socket</i>	Define o tipo de serviço como sendo <i>Socket</i> .
		<i>AT^SISS=0,alphabet,IRA</i>	Define o tipo de alfabeto a utilizar como <i>IRA</i> (<i>International Reference Alphabet</i>).
		<i>AT^SISS=0,tcpMR,15</i>	Define o número máximo de retransmissões em 15.
		<i>AT^SISS=0,tcpOT,3000</i>	Define o valor do período máximo de inatividade em 3000 segundos.
		<i>AT^SISS=0,address,soc tcp://newshift-remote.no-ip.org:8001</i>	Define o endereço para o serviço.
		<i>AT^SISS=0,conId,1</i>	Define qual o perfil de ligação à <i>internet</i> a utilizar.

Na Tabela 43 poderão ser consultados os comandos de estabelecimento de ligação à *internet* assim como os comandos para envio e recepção de dados.

Tabela 43 Lista de comandos AT de ligação à *internet* e de transferência de dados

Fonte: (Modules, 2008a, , 2008b)

Lista de Comandos de Ligação à <i>Internet</i> e de Transferência de Dados			
Comando	Descrição	Comando Utilizado	Explicação
<i>AT^SISO</i>	Abre uma sessão de internet definida para um perfil.	<i>AT^SISO=0</i>	Abre a sessão de internet definida no perfil 0.
<i>AT^SISW</i>	Efectua a operação de escrita (upload) de dados, assim como permite saber a quantidade de dados enviados mas dos quais ainda não foi recebido o <i>acknowledge</i> por parte da camada TCP.	<i>AT^SISW=0,10</i>	Despoleta a escrita de 10 Bytes na ligação do perfil 0.
<i>AT^SISR</i>	Efectua a operação de leitura (download) de dados, assim como permite saber a quantidade de dados existentes no <i>buffer</i> interno.	<i>AT^SISR=0,10</i>	Despoleta a leitura de 10 Bytes na ligação do perfil 0.
<i>AT^SISC</i>	Fecha a ligação TCP/IP ao porto remoto efectuada pelo comando <i>AT^SISO</i> .	<i>AT^SISC=0</i>	Fecha a ligação do perfil 0.

Anexo 8 Lista de Comandos de Inicialização do LCD

Na Tabela 44 são apresentados todos os comandos necessários para proceder à inicialização do LCD *LM6060CBY*.

Tabela 44 Lista de comandos de inicialização do LCD

Fonte: Adaptado de (Shenzhen Topway Technology Co., 2007; Sitronix, 2008)

Comandos de Inicialização do LCD <i>Topway LM6060CBY</i>												
Pinos de Controlo			Comando Binário								Comando Hexadecimal	Função
A0	E	/RD	D7	D6	D5	D4	D3	D2	D1	D0		
	RW	/WR										
0	1	0	1	0	1	0	1	1	1	1	0xAF	Liga o <i>LCD</i> .
0	1	0	0	1	0	0	0	0	0	0	0x40	Define a linha 0 como sendo a primeira linha de apresentação de dados.
0	1	0	1	0	1	0	0	0	0	0	0xA0	Selecciona a direcção padrão do <i>LCD</i> .
0	1	0	1	0	1	0	0	1	1	0	0xA6	Selecciona o funcionamento padrão do <i>LCD</i> para quando a iluminação retroactiva se encontrar activa.
0	1	0	1	0	1	0	0	1	0	0	0xA4	Desactiva a apresentação de todos os pontos ligados.
0	1	0	1	0	1	0	0	0	1	0	0xA2	Define a tensão de polarização do <i>LCD</i> .

0	1	0	1	1	0	0	1	0	0	0	0xC8	Define a direcção de varrimento do terminal de saída.
0	1	0	0	0	1	0	1	1	1	1	0x2F	Define as funções do circuito de alimentação.
0	1	0	0	0	1	0	0	1	0	1	0x25	Define o rácio da tensão da resistência interna do regulador de tensão V0.
0	1	0	1	1	1	1	1	0	0	0	0xF8	Entra no modo de definição da relação de reforço.
0	1	0	0	0	0	0	0	0	0	0	0x01	Define a relação de reforço.
0	1	0	1	0	0	0	0	0	0	1	0x81	Entra no modo de definição do volume electrónico.
0	1	0	0	0	1	0	0	0	0	1	0x21	Define o contraste.

Anexo 9 Organização do Código Fonte do Dispositivo Móvel e do Módulo de Recolha de Auditoria

Neste anexo são apresentados os ficheiros criados e sua organização durante o desenvolvimento do *firmware* do dispositivo móvel e do módulo de recolha de auditoria.

9.1 Estrutura e Organização do Código Fonte do Dispositivo Móvel

- *IFADMmobile*
 - *Buttons*
 - *Buttons.c*
 - *Buttons.h*
 - *Communication*
 - *CommCollectionDevice.c*
 - *CommCollectionDevice.h*
 - *CommServer.c*
 - *CommServer.h*
 - *Cryptography*
 - *Cryptography.c*
 - *Cryptography.h*
 - *GSM*
 - *GSM.c*
 - *GSM.h*
 - *Images*
 - *Images.h*
 - *LCD*
 - *LCD.c*
 - *LCD.h*
 - *OneWire*

- *OneWire.c*
 - *OneWire.h*
- *SDCard*
 - *SDCard.c*
 - *SDCard.h*
- *SerialPort*
 - *SerialPort.c*
 - *SerialPort.h*
 - *SerialPortSoft.c*
 - *SerialPortSoft.h*
- *UserInterface*
 - *UserInterface.c*
 - *UserInterface.h*
- *IFADMoblie.c*

9.2 Estrutura e Organização do Código Fonte do Módulo de Recolha de Auditoria

Neste anexo são apresentados os ficheiros criados e uma breve explicação do seu conteúdo no desenvolvimento do *firmware* do módulo de recolha.

- *IFADCollectionModule*
 - *Communication*
 - *CommMobileDevice.c*
 - *CommMobileDevice.h*
 - *Cryptography*
 - *Cryptography.c*
 - *Cryptography.h*
 - *OneWire*
 - *OneWire.c*
 - *OneWire.h*
 - *SerialPort*
 - *SerialPort.c*
 - *SerialPort.h*
 - *SerialPortSoft.c*
 - *SerialPortSoft.h*
 - *IFADCollectionModule.c*

Anexo 10 Estrutura dos Tickets dos Moedeiros MEI® Série 6 e Série 7

De seguida é apresentado um exemplo de um *ticket* emitido pelos moedeiros MEI® Série 6 e Série 7.

```
=====
MARS ELECTRONICS.

DADOS CONTAB. CASHFLOW

DATA-HORA
NO. MA MEI:::0968GC11794
IMPRESSAO NUMERO 17
VALOR VENDAS 325.40
NUMERO VENDAS 377
DINH. NOS TUBOS 0.00
NO INTERR. DE AL. 8
TEMPO LIGACAO 0-00:00
-----
DESDE INSTALACAO

DATA 00/00/00
IMPRESSAO NUMERO 17
VENDAS Moeda y Ca 653.08
NUMERO DE VENDAS 377
-----
VALORES PARCIAIS MOEDA

DESDE IMPRESSAO NO. 1

DINH. NO COFRE 0.00
DINH. NOS TUBOS 0.85
TROCO DEVOLVIDO 0.85
INSERIDO MANUAL 0.00
DISP. MANUAL 0.85
VALOR DE VENDAS 0.00
NUMERO VENDAS 0
SOBREPAGO 0.00
FICHAS 0.00
VALUE TOKENS 0.00
NOTAS 0.00
DINHEIRO 0.00
```

PRECOS ALTERADOS NAO

=====

APAGAR OS PARCIAIS

A5

Anexo 11 Especificação dos Testes Realizados

11.1 Testes de Integração

Na Tabela 45 são apresentadas as especificações dos testes de integração realizados aos diversos componentes que compõe o dispositivo móvel. Estes testes tiveram por objectivo a validação do funcionamento dos componentes do dispositivo móvel.

Tabela 45 Especificação dos testes de integração efectuados aos componentes do dispositivo móvel

Teste de Integração – Componentes Dispositivo Móvel		
ID do teste	Componente testado	Teste a realizar
TI001	LCD	Apresentar imagem
TI002	LCD	Apresentar texto
TI003	Leitor de cartões SD	Criar ficheiro
TI004	Leitor de cartões SD	Escrita de dados no ficheiro
TI005	Leitor de cartões SD	Leitura de dados do ficheiro
TI006	Leitor de cartões SD	Apagar ficheiro
TI007	Modem GSM	Envio de comandos AT
TI008	Rede I-Wire	Obter número de série de dispositivo I-Wire

Na Tabela 46 são apresentadas as especificações dos testes de integração realizados ao servidor *socket* desenvolvido. Com estes testes pretendeu-se verificar qual o número máximo de ligações concorrentes suportadas pelo servidor.

Tabela 46 Especificação dos testes de integração efectuados à comunicação entre o dispositivo móvel e o servidor socket

Teste de Integração – Comunicação entre Dispositivo Móvel e Servidor <i>Socket</i>	
ID do Teste	Teste a Realizar
TI009	Estabelecimento de 1 ligação socket e envio de dados
TI010	Estabelecimento de 50 ligações socket concorrentes e envio de dados
TI011	Estabelecimento de 100 ligações socket concorrentes e envio de dados
TI012	Estabelecimento de 250 ligações socket concorrentes e envio de dados
TI013	Estabelecimento de 500 ligações socket concorrentes e envio de dados

11.2 Testes de Sistema

Na Tabela 47 são apresentadas as especificações dos testes de sistema realizados no final da fase de desenvolvimento da solução proposta

Tabela 47 Especificação dos testes de sistema efectuados

Teste de Sistema – Obtenção de Auditoria e Posterior Envio para o Servidor		
ID do Teste	Teste a Efectuar	Resultado Esperado
TS001	Obtenção de dados de auditoria financeira e posterior envio para o servidor	Registo dos dados de auditoria financeira na base dados; Eliminação do ficheiro de dados correspondente no dispositivo móvel.
TS002	Obtenção dos mesmos dados de auditoria financeira e posterior envio para o servidor	Detecção de dados repetidos não sendo registados na base dados; Eliminação do ficheiro de dados correspondente no dispositivo móvel.
TS003	Obtenção de dados de auditoria financeira e envio para o servidor – servidor socket off-line	Falha no estabelecimento da ligação ao servidor Socket e apresentação de mensagem de erro; Ficheiro de dados é mantido no cartão <i>SD</i> .
TS004	Obtenção de dados de auditoria financeira e envio para o servidor – servidor de serviços off-line	Falha no estabelecimento da ligação ao servidor de serviços e apresentação de mensagem de erro; Ficheiro de dados é mantido no

		cartão <i>SD</i> .
TS005	Obtenção de dados de auditoria financeira e envio para o servidor – servidor de base de dados off-line	Falha no estabelecimento da ligação ao servidor de base de dados e apresentação de mensagem de erro; Ficheiro de dados é mantido no cartão <i>SD</i> .

Anexo 12 Especificação do Cenário de Testes

O cenário utilizado para a execução dos testes (Figura 72) é constituído por três computadores distintos inseridos numa rede local, um para alojar o servidor de base de dados, um para alojar o servidor de serviços e por último um para alojar o servidor *socket*. Para além dos computadores mencionados foi utilizado ainda o dispositivo móvel desenvolvido, que acedia ao servidor *socket* através da rede *GSM*.

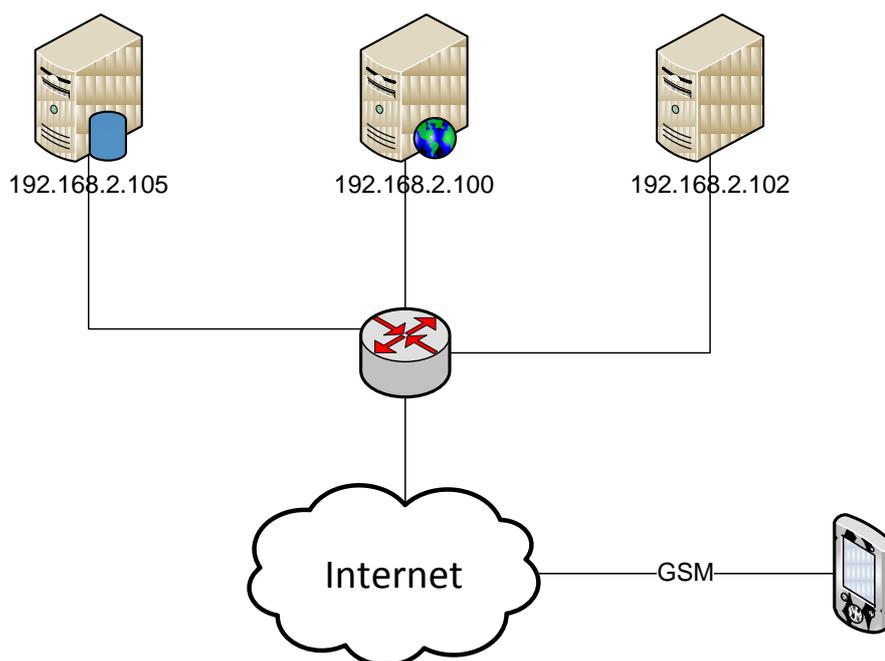


Figura 72 Cenário utilizado na execução dos testes de sistema

Na Tabela 48 são apresentadas as especificações dos equipamentos utilizados considerados relevantes para a execução dos testes.

Tabela 48 Especificações dos equipamentos utilizados no cenário de testes

Equipamentos Utilizados no Cenário de Testes	
Equipamento Utilizado para Alojamento do Servidor Socket	
Sistema Operativo	<i>Windows® Vista Home Basic + Service Pack 1</i>
Processador	<i>Intel® Pentium® Dual CPU E2180 @ 2.00Ghz</i>
Memória RAM	<i>2GB</i>
Versão .NET Framework	<i>3.5</i>
Endereço IP	<i>192.168.2.102</i>
Equipamento Utilizado para Alojamento do Servidor de Base de Dados	
Sistema Operativo	<i>Windows® XP Professional + Service Pack 3</i>
Processador	<i>Intel® Pentium® 4 CPU @ 3.00Ghz</i>
Memória RAM	<i>1GB</i>
Versão .NET Framework	<i>3.5</i>
Sistema de Gestão de Base de Dados	<i>Oracle MySql Server 5.1</i>
Endereço IP	<i>192.168.2.105</i>
Equipamento Utilizado para Alojamento do Servidor de Serviços	
Sistema Operativo	<i>Windows® XP Professional + Service Pack 3</i>
Processador	<i>Intel® Dual-Core CPU E5200 @ 2.50Ghz</i>
Memória RAM	<i>2GB</i>
Versão .NET Framework	<i>3.5</i>
Servidor Aplicacional	<i>Microsoft® Internet Information Services 5.1</i>
Endereço IP	<i>192.168.2.100</i>