Universidade de Aveiro Departamento de Engenharia Mecânica
2015

David Rafael
Pimentel Cardoso

Controlo de acessos no sector turístico

Universidade de Aveiro Departamento de Engenharia Mecânica
2015

David Rafael
Pimentel Cardoso

Controlo de acessos no sector turístico

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestrado em Engenharia Mecânica, realizada sob orientação científica de José Paulo Oliveira Santos, Professor Auxiliar do Departamento de Engenharia Mecânica da Universidade de Aveiro.

O júri / The jury

Presidente / President

Prof. Doutor Margarida Isabel Cabrita Marques Coelho
Professora Auxiliar da Universidade de Aveiro

Vogais / Committee

Prof. Doutor José Paulo Oliveira Santos
Professor Auxiliar da Universidade de Aveiro (orientador)

Prof. Doutor André Ventura da Cruz Marnoto Zúquete
Professor Auxiliar da Universidade de Aveiro

Agradecimentos / Acknowledgements

Em primeiro lugar gostaria de agradecer aos meus pais e família por todo o apoio e carinho que me ofereceram durante o meu percurso académico, por acreditarem sempre em mim e por me terem ajudado em tudo o que lhes foi possível. Ao Professor Doutor José Paulo Oliveira Santos, meu orientador de dissertação, deixo aqui o meu agradecimento pela disponibilidade e apoio durante a realização deste trabalho e pelos conhecimentos oferecidos enquanto professor e orientador. Por fim, agradeço aos meus amigos e colegas que, direta ou indiretamente, me ajudaram a concluir este trabalho.

Palavras-chave Sistema de controlo de acessos; ESP8266; Wi-Fi; Web

Resumo

A presente dissertação propõe o desenvolvimento de um sistema de controlo de acessos que irá recorrer a uma rede Wi-Fi como método de transmissão de dados no processo de identificação do utilizador e de autenticação do mesmo, permitindo que este possa aceder a um lugar pretendido. Uma vez que esta tecnologia de comunicação de dados ainda não foi explorada na criação destes sistemas, pretende-se desenvolver um protótipo inovador que cumpra todos os objetivos colocados na realização do controlo de acessos.

Este sistema foi desenvolvido para eliminar a necessidade de se recorrer a terceiros para se conseguir aceder ao local reservado. Deste modo o cliente não tem a necessidade de efetuar o check-in na receção do hostel, podendo dirigir-se diretamente ao local, permitindo reduzir as horas de funcionamento da receção. No caso do arrendamento de apartamentos, o proprietário evita ter de se deslocar ao local para ter de entregar as chaves do mesmo, eliminando os custos colocados na viagem que teria de realizar e permitindo ao cliente aceder ao local de forma mais autónoma. Uma vez que o sistema desenvolvido utiliza elementos de baixo custo, permite também reduzir os custos relativamente aos sistemas de cartões magnéticos utilizados.

Inicialmente, o trabalho consistiu na investigação dos conceitos teóricos sobre o controlo de acessos e os diferentes tipos de sistemas existentes e os seus métodos de comunicação. De seguida procurou-se definir uma solução que permitisse satisfazer as ideias encontradas para a redução dos custos nestas unidades turísticas, utilizando uma tecnologia nova na implementação deste tipo de sistema e que permitisse agradar também ao cliente.

Desta forma, pretende-se incentivar o desenvolvimento de soluções em controlo de acessos com esta tecnologia, para que num futuro próximo sejam considerados um produto robusto, flexível e fiável.

Keywords Acess control system; ESP8266; Wi-Fi; Web

Abstract

This thesis proposes the development of an access control system that will use a Wi-Fi network as a data transmission method in the identification and authentication of the user, allowing this to acess a desired place. Since this data communications technology has not been exploited in the creating of these systems, it is intended to develop an innovative prototype that fulfills all the goals set in the realization of the access control.

This system was developed to eliminate the need to rely on third parties to gain access to the reserved place. This way the client does not have the need to make the check-in at the reception of the hostel and can go directly to the place, reducing the operating hours of reception. In the rental apartments case, the owner avoids having to travel to the place to hand over it's keys, eliminating the costs placed on the trip he would have to make and allowing the client to access the place more autonomously. Since the system developed uses low-cost elements, it also allows to reduce the costs in comparison with the magnetic card systems used.

Initially the work consisted on the investigation of theoretical concepts of access control and the different systems types and their communication methods. Then sought to define a solution that can enable the ideas found to reduce costs in this touristic units, using a new technology on the implementation of this type of system and also pleasing the customer.

In this way, we intend to encourage the development of access control solutions based on the proposed model so that in the near future is considered a robust, flexible and reliable product.

Conteúdo

Lista de Tabelas

Lista de Figuras

Lista de Acrónimos

RFID *Radio-Frequency Identification*

PIN *Personal Identification Number*

NFC *Near Field Communication*

Wi-Fi *Wireless Fidelity*

UPC *Universal Product Code*

EAN-13 *European Article Number-13*

GS1 *General Specifications 1*

PDF417 *Portable Data File 417*

AP *Acess Point*

WPA2 *Wi-Fi Protected Access 2*

OFDM *Orthogonal frequency-division multiplexing*

AES *Advanced Encryption Standard*

PHP *PHP: Hypertext Preprocessor*

HTML *HyperText Markup Language*

MySQL *My Structured Query Language*

DDF Diagrama de Dependências Funcionais

FNBC Forma Normal de Boyce Codd

Rs232 *Recommended Standard 232*

USB *Universal Serial Bus*

RX *Receiver*

TX *Transmitter*

CTX *Clear to Transmit*

RTS *Request To Send*

DB9 *D-sub 9*

DIP *dual in-line package*

PCB *Printed Circuit Board*

COM4 *Communication port 4*

I2C *Inter-Integrated Circuit*

PICC *Programmable Interface Controllers*

ASCII *American Standard Code for Information Interchange*

AT *ATTENTION*

NodeMCU *Nodejs Microcontroller Unit*

GPIO *General Purpose Input/Output*

RST *Reset*

CH-PD *Chip power-down*

VCC *Collector supply voltage*

GND *Ground*

TXD *Transmission Data*

RXD *Received Data*

LED *Light Emitting Diode*

AP MAC *Acess Point Media Access Control*

STA MAC *Stand Alone Media Access Control*

URL *Uniform Resource Locator, internet address*

CPU *Central Processing Unit*

IP *Internet Protocol*

Capítulo 1

Introdução

1.1 Enquadramento

Atualmente um dos aspetos mais importantes nas vidas das pessoas passa pela segurança e pelo modo de proteger os seus bens num determinado espaço. Estas apreciam o facto de poderem ser elas próprias a determinar quem tem a possibilidade de aceder a esse mesmo espaço.

Para resolver este problema, recorre-se a fechaduras manuais que em colaboração com um sistema de controlo de acessos e utilizando um determinado mecanismo concede permissão apenas ao seu possuidor e impede o acesso a pessoas não autorizadas a um determinado espaço, protegendo os bens ou informações que se guardaram.

No controlo de acesso das habitações pessoais é, normalmente, utilizada a chave como mecanismo de acesso, uma vez que apenas permite ao proprietário da mesma aceder ao espaço. Caso exista mais do que uma pessoa a habitar o espaço, a pessoa que possui a chave pode decidir replicá-la, de modo a permitir que as outras também tenham acesso, possibilitando assim a proteção dos seus bens.

Nas empresas, o controlo de acesso é utilizado para definir que empregados tem autorização para aceder a um determinado espaço, produto ou dados fornecidos pela mesma. Na realização deste controlo, pode ser utilizado um cartão magnético com informação sobre o utilizador com um nível de autorização e nome próprio, possibilitando ao sistema decidir se este tem ou não autorização. Para casos onde existe a necessidade de um grau de segurança muito elevado, os sistemas utilizados são os biométricos, uma vez que permitem adicionar características físicas da pessoa no processo de definição do tipo de permissão a ser atribuída. Com este sistema a empresa tem também uma forma de controlar as atividades dos seus empregados, registando todos os acessos que fazem e quando os fazem.

O processo de controlo de acesso nos hosteis consiste na entrega de cartões ao cliente na receção, permitindo que este consiga aceder ao espaço que reservou e guardar os bens que transportar com ele, sempre que tiver o cartão em sua posse. No caso do arrendamento de apartamentos o proprietário tem de se deslocar para entregar a chave ao cliente, permitindo assim que este consiga aceder ao espaço que alugou e usufruir de todos os serviços que este possui.

1.2 Motivação

Segundo os dados estatísticos recolhidos do site Turismo em Portugal, verifica-se que nos últimos anos tem existido um crescimento no número de pessoas estrangeiras a decidirem vir passar um tempo pelo nosso país (12,3 % entre 2013 e 2014 e 8,9 % durante o primeiro semestre de 2015) e pessoas nacionais a optarem por não sair do país (11,7 % entre 2013 e 2014 e 8,0 % durante o primeiro semestre 2015). Um maior número de turistas contribui para um crescimento das receitas, tendo estas no primeiro semestre de 2015 sido cerca de 498,2 milhões de euros, o que corresponde a um aumento de 12,2 % relativamente ao valor obtido no semestre inicial de 2014 [1].

As unidades hoteleiras são a grande fonte de proveitos globais no turismo correspondendo a cerca de 73,3 % dos valores obtidos até Agosto de 2015, sendo que os hosteis (hotéis-apartamentos) e o arrendamento de apartamentos representam, respetivamente, cerca de 11,2 e 5,7 % dos proveitos [1]. Atualmente as unidades hoteleiras necessitam de garantir a receção dos clientes 24 sobre 24 horas, com custos elevados. Alterando o sistema de controlo de acesso utilizado para estas unidades poderíamos reduzir os custos, permitindo melhorar as quotas e reduzir a margem existentes para a unidades hoteleiras.

1.3 Objetivo

Com o desenvolvimento de um sistema que permita ao cliente fazer a reserva remotamente e o check-in sem necessidade de recorrer à receção do hostel, proporciona a redução do número de horas de funcionamento da receção do hostel. Este sistema elimina o deslocamento que o proprietário terá de efetuar para entregar as chaves, aumentando deste modo o proveito obtido.

1.4 Metodologia

- Analisar as diferentes tecnologias de controlo de acessos utilizadas para definir as pessoas que tem autorização para aceder a um determinado local, e a partir destas desenvolver uma solução que permita revolucionar os mecanismos utilizados para aceder aos locais, nos hosteis e no arrendamento de apartamentos.

- Desenvolver um protótipo funcional, que possibilite a deslocação direta ao local para conseguir aceder ao mesmo, evitando a realização do check-in na receção ou necessidade de esperar pelas chaves do apartamento, estando o proprietário obrigado a se deslocar ao mesmo para as entregar. Com este sistema pretende-se reduzir o tempo de funcionamento da receção, evitar que o proprietário se desloque e reduzir os custos relativamente aos sistemas anteriormente utilizados.

- Acrescentar um novo sistema de controlo de acesso ao mercado que utiliza um método de troca de dados, bastante conhecido, mas pouco explorado para este tipo de função. Pretende-se demonstrar que esta tecnologia permite a criação de um sistema funcional, bastante acessível e que possibilita o acesso ao local através de um produto que pertence ao cliente.

1.5 Estrutura da dissertação

Esta dissertação está organizada em cinco capítulos, incluindo o atual capítulo (Introdução), e dois apêndices. De seguida é feita uma breve descrição do conteúdo dos diferentes capítulos, recorrendo à ordem em que se encontram apresentados no documento.

- **Estado de Arte**

  No capítulo 2, são apresentadas as diferentes etapas utilizadas no controlo de acessos, as diferentes tecnologias já desenvolvidas que permitem distinguir entre os indivíduos com ou sem permissão de acesso e as soluções mais utilizadas na área em análise desta dissertação, os hosteis e arrendamento de apartamentos.

- **Solução**

  No capítulo 3, é apresentado o conceito da solução proposta e as principais funções que terá de desempenhar para que o sistema de controlo de acesso permita uma boa interação entre cliente, proprietário e local a utilizar.

- **Implementação**

  No capítulo 4, apresentam-se os diferentes passos a seguir e os diferentes softwares utilizados na implementação do sistema de controlo de acessos baseado na solução proposta no capítulo 3. São também mostradas as diferente páginas que compõem o site que permite inscrever os clientes e o método a ser utilizado para que estes consigam aceder ao local, utilizando um código que receberam do sistema proposto.

- **Considerações Finais**

  No capítulo 5, são apresentadas as conclusões tiradas da análise geral realizada à solução apresentada e são propostos alguns trabalhos futuros que permitam ao produto evoluir e ser aplicado noutros sectores.

- **Apêndices**

  No apêndice A, apresenta-se o estudo realizado sobre a tecnologia RFID.

  No apêndice B, apresenta-se a forma de configurar a fechadura inteligente proposta nesta dissertação.

Capítulo 2

Estado de Arte

Este capítulo apresenta o estado de arte do controlo de acessos em que a dissertação se incide, bem como os conceitos básicos necessários à compreensão da matéria exposta nos capítulos seguintes. Inicialmente são apresentadas as etapas existentes no controlo de acessos (identificação, autenticação, autorização e auditoria) e os modelos utilizados, sendo depois apresentadas as diferentes tecnologias de controlo de acessos utilizadas atualmente.

2.1 Controlo de acessos

Controlo de acessos tem como objetivo verificar se um determinado utilizador tem autorização para aceder a dados, espaços ou objetos. Para conseguir a autorização o utilizador terá de pedir ao proprietário que lhe forneça o método para a realização do ato, deixando assim a sua informação com o proprietário permitindo que ele decida o nível de permissão a oferecer ao utente, sendo este nível verificado quando se tenta aceder ao que se pretende.

Com o controlo de acessos mantém-se um modelo de segurança pré-estabelecido, uma vez que o utilizador apenas conseguirá aceder a um lugar se obtiver permissão e passar pelos diferentes procedimentos que monitorizam os acessos, verificam a sua identidade e o seu pedido, decidindo se este pode ou não pode aceder ao local consoante a autorização que lhe foi atribuída. Deste modo é possível limitar as ações dos utilizadores, permitindo o acesso dependendo da vontade do proprietário ou negando o acesso não consentindo a utilizadores sem permissões.

2.1.1 Etapas de Controlo de Acessos

Nesta secção explicam-se os principais conceitos relativos a controlo de acessos, possibilitando uma melhor compreensão dos diferentes parâmetros que permitem a execução das funções impostas num sistema de controlo de acessos. As seguintes etapas apresentadas são fundamentais para que o processo de acesso seja realizado dentro das normas de segurança definidas, impedindo acessos ilegais a utilizadores não autorizados e permitindo acessos a utilizadores com permissões validadas para usarem o que pretendem com o consentimento do proprietário.

2.1.1.1 Identificação

A identificação consiste no fornecimento de informações relativas à identidade do utilizador ao sistema. Ao tentar aceder a um determinado conjunto de dados, a uma área ou a um determinado objeto o utente terá de se identificar, utilizando por exemplo o seu nome ou *username*, consoante o valor registado no sistema. Este valor não comprova a identidade do utilizador, uma vez que outros utilizadores podem obter a sua identificação e utilizá-la para aceder ilegalmente a um determinado serviço [2; 3].

2.1.1.2 Autenticação

A autenticação consiste na validação da identificação do utilizador. Esta completa o serviço de identificação recorrendo a um valor de segurança na obtenção de permissão, isto é, o utilizador para além de se ter de identificar terá de recorrer a uma palavra-chave, ou um código *Personal Identification Number* (PIN), ou à sua impressão digital que foi registada no sistema para confirmar a sua identidade. Deste modo tendo o *username* como método de identificação e uma palavra-chave como método de autenticação, o sistema irá verificar se ambos os métodos correspondem ao mesmo utilizador, se a avaliação for positiva o utilizador terá a permissão com o nível estabelecido, mas caso seja negativa significa a inexistência de autorização para aceder ao serviço pretendido [2; 3].

2.1.1.3 Autorização

A autorização determina que tipo de permissões um utilizador autenticado obteve quando foi registado no sistema de controlo de acessos. O nível de permissões de um utilizador depende do registo efetuado pelo proprietário do sistema, podendo este atribuir, alterar, suspender ou eliminar as autorizações concedidas aos diferentes utilizadores. Por exemplo, se um utilizador pretende aceder a uma base de dados, o responsável pode atribuir-lhe uma autorização para ver todos os documentos disponíveis, conceder-lhe uma permissão para apenas poder aceder a documentos até um certo tamanho ou não permitir que os documentos sejam vistos [2; 3].

2.1.1.4 Auditoria

A auditoria consiste na monitorização dos vários pedidos efetuados e atividades realizadas pelos diferentes utilizadores. Ao registar todas as ações desenroladas pelos vários utilizadores do sistema é possível verificar a existência de erros no sistema, tentativas de acesso ilegal, o serviço mais utilizado e caso apareça algum defeito nos serviços disponibilizados aos utilizadores permite verificar qual foi o último a recorrer ao serviço e descobrir o que aconteceu. Desta forma a auditoria funciona como mais um método de segurança para salvaguardar os vários serviços disponibilizados e permite avaliar o desempenho do sistema de controlo de acessos utilizado [2; 3].

2.2 Tecnologias de controlo de acessos

Nesta secção são apresentadas as principais tecnologias utilizadas no controlo de acessos para permitir a identificação de utilizadores que entram num determinado local. Estas tecnologias permitem a troca de informação entre o utilizador e o sistema de permissão de acesso ao local. O sistema processa e armazena a informação obtida pela tecnologia que identifica o utilizador de forma automática, e sem a necessidade de intervenção humana. Segue-se uma lista das tecnologias de troca de informação para controlo de acessos:

- Chaves e código numérico;
- Código de barras;
- RFID (*Radio-Frequency Identification*);
- NFC (*Near Field Communication*);
- Biometria;

2.2.1 Chaves metálicas e código numérico

A primeira tecnologia desenvolvida para controlar o acesso a um determinado lugar foi a chave metálica, como mostra a figura 2.1. Este mecanismo continua a ser muito utilizado, uma vez que é o método mais simples de controlo de acessos existente, e a evolução das chaves permitiu uma maior segurança ao dificultar a produção de cópias. O acesso através de uma chave mecânica é muita das vezes utilizado em conjunto com as outras tecnologias como método de prevenção.

Figura 2.1: Chaves metálicas.

Os dispositivos que utilizam código numérico como forma de acesso, consistem na atribuição de uma sequência numérica a uma pessoa. A pessoa digita o código que lhe corresponde no teclado (figura 2.2), o sistema procura na sua lista de acessos esse código e estando este na lista permite a entrada da pessoa. Estes dispositivos contém uma memória interna, que permite guardar os diferentes códigos de acessos criadas. Este método pode também ser usado em conjunto com os sistemas RFID, NFC, Biométricos, permitindo assim uma maior segurança no acesso.

Figura 2.2: Dispositivos de controlo de acesso através de código numérico[4].

2.2.2 Código de barras

Um código de barras é uma sequência de barras paralelas que apresentam largura e espaçamentos diferentes consoante a informação que pretendem transmitir, sendo apenas números ou um pequeno conjunto de caracteres relacionados com o objeto a que estão associados [5]. Os dados do código são obtidos recorrendo a um leitor de código de barras que ao incidir um feixe laser no código permite ao leitor decifrar os valores representados por cada barra e cada espaçamento. Estes valores identificam o objeto que contém o código e verificam se este tem permissão para poder aceder a um determinado recurso.

Os códigos de barras podem ser lineares ou uni-dimensionais (1D), o que corresponde a um conjunto de barras espaçadas entre si e de larguras variadas que apresentam os dados organizados horizontalmente da esquerda para a direita, ou podem ser bidimensionais (2D) que apresentam outros tipos de padrões geométricos (quadrados, retangulares, pontos, ...) e que permitem guardar muito mais informação, tanto na horizontal como na vertical, relativa ao produto em que se encontram colocados, podendo até fornecer 2.000 caracteres de dados [5; 6].

Este método de controlo de acessos é amplamente utilizado nos serviços de saúde e hospitalares para a identificação do paciente (para aceder aos dados do paciente, incluindo histórico médico, alergias a medicamentos, etc.) [5].

Figura 2.3: Exemplo de código de barras numa pulseira de identificação do paciente [5].

Os códigos de barras também podem ser usados para identificar objetos, pessoas, bagagem aérea, correspondência registada, correio expresso e encomendas [7]. Para permitir aos proprietários a identificação dos bilhetes duplicados ou fraudulentos com maior facilidade são utilizados bilhetes com código de barras que permitem entrar em arenas desportivas, cinemas, teatros, etc [5].

Figura 2.4: Torniquetes utilizados nos estádios permitem verificar a veracidade dos bilhetes comprados [8].

Nas secções seguintes apresentam-se alguns dos códigos de barras uni-dimensionais e bidimensionais mais utilizados.

2.2.2.1 Códigos de barras UPC e EAN-13

Os códigos de barras UPC(*Universal Product Code*) e EAN-13 (*European Article Number-13*) são códigos uni-dimensionais muito semelhantes, sendo que o primeiro apresenta 12 dígitos e é usado pelos Estados Unidos da América e pelo Canadá, enquanto que o segundo mostra 13 dígitos e é utilizado pelo continente europeu [9].

Códigos de barras UPC são compostos por doze dígitos, como mostra a figura 2.5. Os dígitos iniciais do código correspondem ao valor atribuído pela *General Specifications 1* (GS1) à empresa que fabrica o produto e a seguir aparece o número identificativo do produto. O último dígito do código de barras 1D é denominado de dígito de verificação (*check digit*) [10]. Este número é calculado a partir dos onze dígitos anteriores e permite ao scanner determinar se examinou o número corretamente ou não. O valor da empresa apresentado no código varia consoante a quantidade de produtos identificados na mesma, ou seja, quantos mais produtos estiverem identificados mais reduzido fica o valor apresentado no código [6; 11].

Figura 2.5: Códigos de barras UPC [5].

Códigos de barras EAN-13 (*European Article Number-13*) apresentam treze números, como apresentado na figura 2.6. Os três números iniciais representam origem do código ou a filial da GS1 onde este foi criado, os seguintes números correspondem à empresa e ao produto onde o código se encontra, sendo o último número, tal como no código UPC, o dígito de verificação (*check digit*) [10]. Assim como no caso anterior a quantidade de números utilizados no valor da empresa depende da necessidade de identificação dos produtos [12].

Figura 2.6: Códigos de barras EAN-13 [13].

2.2.2.2 *Portable Data File 417* (PDF417)

O *Portable Data File 417* é um código de barras bidimensional que permite armazenar até cerca de 1100 bytes de informação sobre um determinado objeto ou utilizador [9]. Desta forma para além de funcionar como identificação permite adicionar outro tipo de informações pertinentes sobre o produto, pode depois ser convertido num ficheiro de dados comprimido e portátil.

Figura 2.7: Exemplo do código PDF417 [14; 15].

2.2.2.3 *Data Matrix*

O código *Data Matrix* é um código de barras matriz bidimensional(2D) que consiste num padrão de pontos pretos e brancos, que permitem guardar dados relativos a um produto. Os códigos de maior volume permitem armazenar uma quantidade de dados até dois mil e trezentos caracteres alfanuméricos [16; 17]. Deste modo, tal como no código PDF417, pode-se inserir outro tipo de informação considerada importante no código, permitindo um melhor conhecimento do produto.

Figura 2.8: Código de barras 2D, denominado *Data Matrix* [16].

2.2.3 *Radio-Frequency Identification* (RFID)

A tecnologia RFID consiste na obtenção automática da informação sobre um produto a partir do seu identificador (*tags*, cartões), utilizando ondas eletromagnéticas de radiofrequência para transmissão de dados entre o leitor e o identificador. Neste tipo de controlo não existe a necessidade de contacto físico entre o leitor e a *tag*, podendo a distância entre ambos variar entre menor que um centímetro (pequeno alcance) e mais de um metro (longo alcance), dependo da composição dos elementos envolvidos na troca de dados [18; 19].

Esta tecnologia é composta por três elementos: *tags* ,leitor e software. O leitor RFID permite a leitura dos dados fornecidos pela etiqueta e verificar se esta obteve, ou não, permissão para aceder a um determinado lugar. As *tags* RFID funcionam como método de identificação do utilizador, estas podem ser de leitura e escrita ou apenas de leitura consoante a necessidade imposta. Num sistema onde existam *tags* de leitura e escrita, o leitor pode também permitir inserir dados nas diversas etiquetas que lê, tornando a identificação do produto/utilizador mais completa. O software RFID monitoriza, regista e coordena o sistema global de leitores existentes, permitindo assim um melhor controlo dos acessos dos diferentes utilizadores a todos os recursos disponíveis e protegidos. Este software pode disponibilizar uma interface para o operador permitindo um melhor funcionamento do sistema e uma constante atualização do método utilizado consoante a evolução dos vários utilizadores [19]. No Apêndice A utilizou-se um leitor que permite obter e alterar os dados que são inseridos nas *tags* que comunicam com ele.

Os dispositivos que recorrem à tecnologia RFID como meio de controlo de acessos consistem na atribuição de uma etiqueta ou cartão RFID a um utilizador, que ao passar o cartão pelo leitor, este obtém o número de série da etiqueta e verifica se esta tem permissão. Estes sistemas apresentam uma elevada memória permitindo guardar até milhares de números de séries.

Figura 2.9: Dispositivo de controlo de acessos por cartão RFID [20].

2.2.3.1 *Tags* RFID

As *tags* RFID (ou *transponders*) são compostas por um circuito eletrónico e uma antena que em colaboração com um mecanismo de armazenamento de dados, permitem guardar as informações sobre o utilizador e enviá-las para o leitor quando for necessário.

Figura 2.10: Exemplo de *tag* RFID [21].

As etiquetas RFID tomam diferentes formas de funcionamento, associadas a diferenças existentes nos componentes utilizados nas mesmas. Deste modo dividem-se em três categorias [19]:

- **Passivas**: Estas *tags* são as mais utilizadas devido a não conterem nenhuma fonte de energia interna. Ao aproximar a *tag* do leitor RFID, esta recebe as ondas eletromagnéticas e converte-as na energia necessária para permitir o envio da informação guardada. Este modo de funcionamento permite a criação de *tags* de forma mais barata e com maior durabilidade, mas com um alcance inferior aos outros tipos.

- **Semi-Passivas**: As semi-passivas possuem uma fonte de alimentação interna que serve apenas para fornecer energia ao circuito eletrónico que se encontra na *tag*, recorrendo, tal como as passivas, à energia obtida das ondas eletromagnéticas recebidas do leitor para enviar os dados que se encontram guardados. Estas *tags* permitem uma maior fiabilidade e um maior alcance que as passivas, devido a uma maior quantidade de energia disponível.

- **Ativas**: As *tags* ativas recorrem a uma bateria interna, fornecendo energia para o correto funcionamento do circuito eletrónico e para enviar os dados quando estes são requeridos pelo leitor. Uma vez que não dependem da energia convertida a partir das ondas enviadas pelo leitor, estas *tags* possuem um alcance superior às semi-passivas, sendo no entanto mais caras e apresentam um período de utilização inferior às anteriores, devido à vida finita da bateria integrada.

As *tags* RFID podem funcionar apenas no modo de leitura ou podem ter também o modo de escrita incluído no sistema operacional, sendo estas últimas as mais utilizadas, uma vez que estas permitem realizar as duas funções e caso não exista a necessidade da função de escrita, esta pode ser ignorada sendo utilizada apenas a função de leitura.

Todas as *tags* contêm um volume de dados que não podem ser alterados, correspondente ao número de identificação ou número de série. Aquelas que apresentam as funções de leitura e escrita, possuem uma área destinada à introdução de dados, permitindo adicionar ou alterar várias vezes as informações relativas ao utilizador, necessárias para a realização de um determinado serviço [22; 23].

2.2.3.2 Frequências RFID

Para permitir a transferência dos dados de uma etiqueta para um leitor, sem que exista contacto entre os dois dispositivos, utilizam-se ondas eletromagnéticas de radiofrequência entre eles com frequências iguais e com valores consoante os tipos de dados a serem transmitidos. Existem várias frequências utilizadas nestes sistemas, como os de baixa frequência (LF - Low Frequency), os de alta frequência (HF - High Frequency), os de ultra-alta-frequência (UHF - Ultra High Frequency) e as Micro-ondas (VUHF - Very Ultra High Frequency). Na tabela 2.1 apresentam-se os valores, o alcance, e as normas das frequências anteriormente referidas.

	LF	HF	UHF	VUHF
Valores Frequência	125KHz-134KHz	13.56 MHz	850MHz 930 MHz	2.45GHz-5.8 GHz
Distância	$<$ 31 cm	0,31 - 1 m	1 - 8 m	2 - 27 m
Normas	ISO 11784 ISO 11785 ISO 14224	ISO 14443 ISO 15693 ISO 18000-3	ISO 18000-6 EPC Gen2	ISO 18000-4 IEEE 802.11 IEEE 802.15.4

Tabela 2.1: Tabela de dados referentes às diferentes frequências utilizadas nos sistemas RFID [24].

2.2.3.3 Leitores RFID

Os leitores RFID, tal como as *tags*, têm uma antena incorporada que deve estar a funcionar com a mesma frequência. A antena do leitor serve para transmitir e receber os sinais rádio utilizados na interação com as *tags*. O leitor, normalmente, encontra-se conectado a um sistema central através de uma interface de rede (Rs-232, *Ethernet*, Wi-Fi ou *Bluetooth*), que obtém os dados das *tags* através de comandos executados pelo controlador inserido no leitor. O controlador define conforme o comando recebido qual a ação a ser executada pelo leitor e consequentemente o que enviar pela antena para obter uma resposta da *tag*.

2.2.4 *Near Field Communication* (NFC)

Near Field Communication (NFC), ou comunicação em campos próximos, corresponde ao método de troca de dados que permite a um dispositivo aceder aos dados disponibilizados por um smartphone ou um tablet, sem que exista contacto físico entre os dois aparelhos. Este tipo de comunicação permite ao utilizador evitar as diferentes etapas necessárias para a configuração de uma conexão, limitando-se a passar o seu aparelho perto de um dispositivo compatível com NFC para conseguir enviar as informações pretendidas [25]. As velocidades de transmissão de dados podem estar entre 106, 212 e 424 Kb/s (kilobits por segundo) e com uma frequência de 13.56 MHz [26; 27]. Estes valores permitem que os dispositivos se encontrem a uma distância máxima de 10 centímetros, possibilitando a transferência correta da informação entre eles [28].

Figura 2.11: Velocidade e distância máximas na comunicação NFC [28].

A tecnologia NFC apresenta dois modos de comunicação distintos [28]:

- **Passivo**: Neste modo apenas um dos aparelhos necessita de gerar o campo eletromagnético. O outro dispositivo ao passar pelo campo gerado, converte o mesmo na energia necessária para que este possa enviar os dados requisitados.
- **Ativo**: Neste caso, ambos os aparelhos geram o campo eletromagnético. Quando o dispositivo inicial se encontra a criar o campo, o dispositivo alvo não poderá ter um campo gerado. Ao se aperceber do campo do dispositivo inicial, o dispositivo alvo gera um campo onde será enviada a informação pedida, tendo o outro dispositivo parado de gerar o seu campo eletromagnético.

Em termos de modos operacionais, a tecnologia NFC apresenta três modos diferentes [28]:

- **Leitura e escrita**: Este modo operacional permite que o dispositivo inicial ao comunicar com o dispositivo alvo possa ler a sua identificação e receber outras informações que este tenha para disponibilizar. Por exemplo, ao passar o telemóvel por um panfleto com a tecnologia NFC, este envia para o telemóvel informações sobre o evento ou um site relacionado com ele.
- **Emulação de cartão**: Este modo permite ao dispositivo simular todas as funções que um determinado cartão inteligente possui. O dispositivo alvo recebe e envia os dados como se a troca de dados estivesse a ser efetuada por um cartão. Por exemplo, o telemóvel simula um cartão de crédito, permitindo assim a utilização deste para efetuar os pagamentos necessários.
- ***Peer-to-peer***: Este modo permite a troca de dados entre ambos os dispositivos, ou seja, o dispositivo inicial pode enviar e receber informações para o dispositivo alvo, e este também possibilita o envio e receção de dados do outro dispositivo. Por exemplo, ao tentar reproduzir um vídeo no telemóvel, pode transferir o que se está a ver no telemóvel para um tablet ou uma televisão, ficando os dois dispositivos a mostrar o vídeo.

O método de transmissão de dados NFC recorre a dois tipos de codificação, a codificação *Miller* e a codificação *Manchester*, que serão explicadas nas secções seguintes. Na tabela 2.2 apresentam-se as codificações utilizadas para cada velocidade de transferência de dados possível, e podemos verificar que a codificação *Manchester* é muito mais utilizada que a codificação *Miller* [29].

Taxa de dados (kbps)	**Dispositivos ativos**	**Dispositivos passivos**
106	*Modified Miller*, 100%, ASK	*Manchester*, 10%, ASK
212	*Manchester*, 10%, ASK	*Manchester*, 10%, ASK
424	*Manchester*, 10%, ASK	*Manchester*, 10%, ASK

Tabela 2.2: Tabela de codificação de dispositivos pela comunicação NFC (*ASK - amplitude shift keying*)[29].

Os dispositivos que utilizam NFC como meio de controlo de acessos permitem ao utilizador aceder ao local através de transferência de dados recorrendo ao telemóvel do utilizador. Tal como nos outros casos, os dados recebidos pelo dispositivo são verificados e caso estes se encontrem na memória do sistema o utilizador irá receber permissão.

Figura 2.12: Dispositivos de controlo de acesso por NFC [30].

2.2.4.1 Codificação *Manchester*

A codificação *Manchester* utilizada na tecnologia NFC divide-se em dois tipos de transições diferentes que podem ocorrer num período. O bit 0 corresponde à passagem de um valor baixo para um valor alto, sendo que o bit 1 corresponde à descida do valor alto para um valor baixo, tal como mostra a figura 2.13. Em certos casos existe a necessidade de realizar a transição a meio do período para se conseguir obter o bit pretendido, não contando a transição no centro como bit [29].

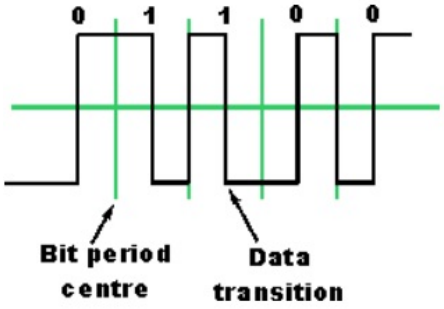

Figura 2.13: Codificação Manchester usada na transmissão de dados por NFC [29].

2.2.4.2 Codificação *Miller*

A codificação modificada *Miller* é uma codificação mais complexa que a de *Manchester*. Esta codificação divide o período em quatro segmentos de modo a determinar os bits utilizados neste tipo de codificação (bit 0 e 1) e que correspondem a cada período. O bit 1 corresponde a dois valores altos, seguido de um baixo e depois de alto novamente, como mostra a figura 2.14. O bit 0 apresenta duas configurações diferentes, uma delas é um conjunto de quatro valores altos e a outra começa com um valor baixo e três valores altos de seguida (figura 2.14) [29].

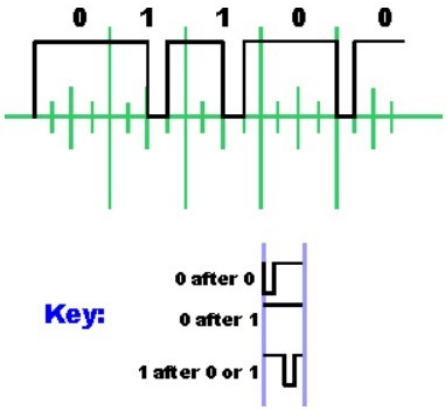

Figura 2.14: Codificação Miller utilizada na transmissão de dados por NFC [29].

2.2.5 Biometria

A biometria corresponde ao método que utiliza características físicas, como o rosto, impressões digitais, íris, veias, ou características comportamentais, como a voz, escrita ou o ritmo de digitação para permitir a troca de dados entre os dispositivos.

Tal como os sistemas anteriores os biométricos recorrem aos mesmos três passos utilizados para verificar se certo utilizador tem permissão para aceder a um determinado serviço [31]:

- **Inscrição**: Esta etapa corresponde a ação de registo das diferentes características que o utilizador vai usar ao tentar aceder a um determinado recurso. Assim utilizam-se sensores que permitem obter os traços pretendidos (impressão digital, íris, voz) e associa-se ao nome e a outros dados previamente obtidos sobre esse utilizador.

- **Armazenamento**: Nesta etapa pretende-se guardar as características do utilizador num computador ou numa base de dados, possibilitando assim uma maior organização dos dados recolhidos de cada utilizador que recorrer ao sistema. Para reduzir o espaço ocupado por imagens ou gravações, estas características são convertidas por um software em códigos ou gráficos que continuam a permitir diferenciar os diferentes utilizadores.

- **Comparação**: Nesta fase o sistema recorre ao dados armazenados para verificar se as características apresentadas pelo utilizador a usar o dispositivo se encontram na base de dados, e se correspondem sem que exista qualquer discordância com as informações existentes sobre o utilizador. No caso do software que analisa as características considerar que houve uma correspondência exata entre ambos os dados, o utilizador obterá a autorização para aceder ao serviço que pretendia.

Estes dispositivos disponibilizam um nível de segurança muito superior aos sistemas de controlo de acessos anterior, uma vez que é quase impossível copiar as características de um utilizador e utilizá-las ilegalmente. Na figura 2.15, mostram-se alguns exemplos de sistemas que utilizam este método de transmissão de dados.

Figura 2.15: Dispositivos biométricos de controlo de acesso, à esquerda com leitor RFID e impressão digital e à direita com reconhecimento facial, impressão digital e RFID [32][33].

2.2.5.1 Reconhecimento facial

Os sistemas que utilizam reconhecimento facial recolhem imagens da face do utilizador recorrendo a uma câmara de filmar que permite obter dados como o comprimento do maxilar, o formato dos ossos da cara, distância entre os olhos, forma e dimensões do nariz, entre outras características faciais. Estes tipos de sistemas podem obter imagens em duas dimensões (2D) ou conseguir gerar imagens a três dimensões (3D), sendo que as segundas permitem obter um maior número de características tornando mais fiável e apurada a verificação de identidade do utilizador.

Nos sistemas que usam imagens a duas dimensões, podem haver dispositivos que pedem ao utilizador para realizar um movimento facial (expressar um sorriso ou piscar um olho), aumentando a precisão na verificação da sua identidade. Os dispositivos que obtém imagens a três dimensões têm de realizar um maior número de passos para verificar se o utilizador tem autorização ou não, sendo esses passos [34]:

- **Deteção**: Este passo corresponde à obtenção das imagens faciais do utilizador, recorrendo a uma câmara vídeo ou a imagens já existentes numa base de dados.
- **Alinhamento**: Neste passo as imagens obtidas vão ser analisadas e são determinados os dados como a posição, postura e tamanho da cabeça do utilizador, independentemente do ângulo em que esta se encontra nas imagens.
- **Medição**: As características que se pretendem determinar do utilizador são realizadas neste passo.
- **Representação**: Os valores obtidos no passo anterior são convertido num *template* ou modelo numérico que define as características do utilizador.

- **Comparação**: Nesta etapa realiza-se a correspondência do modelo criado com o modelo existente na base de dados. A tecnologia com imagens a três dimensões permite a partir do vídeo obter traços do utilizador e compará-los com uma fotografia existente, através de algoritmos.
- **Verificação**: Por fim, caso os dados existentes na base de dados correspondam exatamente aos valores obtidos nos passos anteriores, o utilizador obterá permissão para aceder ao serviço que pretende usufruir.

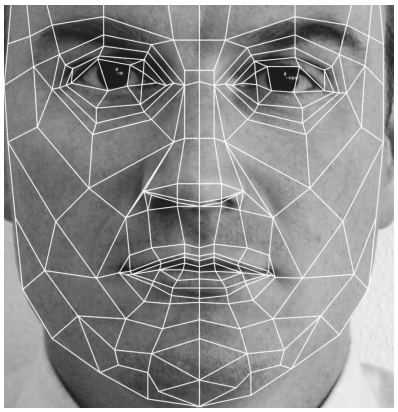

Figura 2.16: Tecnologia de reconhecimento facial (2D)[35].

2.2.5.2 Maneira de escrever

Os sistemas de análise à maneira de escrever do utilizador, examinam o ato de escrever deste. Recorrendo a uma vasta variedade de sensores incorporados em superfícies de escrita ou em canetas, podem-se analisar diferentes características utilizadas durante o processo de escrita de uma determinada palavra ou frase, tais como a pressão, direção, velocidade, ritmo ou ângulo que o utilizador normalmente usa a escrever.

O software deste sistema converte esses valores em gráficos, e consegue verificar as ligeiras alterações que o método de escrita utilizado por um determinado utilizador sofre ao longo do tempo, podendo assim atualizar a informação correspondente e permitir que o utilizador aceda aos serviços desejados [31].

Figura 2.17: Tablet com sistema de identificação por assinatura [31].

2.2.5.3 Geometria da mão e impressão digital

Estes sistemas têm como objetivo determinar a geometria da mão de um utilizador, medindo as características necessárias para a criação de um modelo numérico que permitirá identificar o utilizador. O sistema utiliza uma câmara e uma fonte de luz que incide na mão para recolher os dados: comprimento, largura, espessura ou curvatura dos dedos e da mão. Ao criar uma imagem tridimensional da mão, esta converte-se num modelo numérico, que será comparado com o outro guardado na base de dados para que o utilizador consiga obter autorização.

Este sistema permite um fácil controlo de acesso, uma vez que é simples e não invasivo, onde o utilizador tem de colocar a mão numa superfície com pinos que delimitam o lugar a colocar a mão permitindo uma melhor precisão na captura da imagem. Este sistema é dos menos seguros nos sistemas biométricos, pois a geometria da mão não é exclusiva para cada utilizador e pode ser recriada [31].

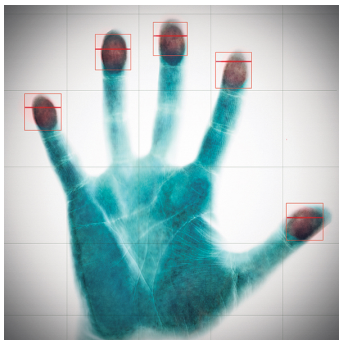

Figura 2.18: Geometria da mão e dedos [36].

A impressão digital consiste nos diferentes padrões existentes nas pontas dos dedos, que para cada utilizador se combinam de uma maneira diferente, não existindo dois utilizadores com a mesma impressão digital. Os diferentes padrões existentes causados pela elevação da pele (ou papila) podem apresentar interseções, centros, bifurcações, ilhas deltas, poros ou fins de linhas como mostra a figura 2.19. São estas características que permitem distinguir as diferentes impressões e determinar com exatidão a identidade do utilizador. Estes sistemas pode utilizar a impressão digital de apenas um dos dedos ou até utilizar todos os dedos de uma mão.

Figura 2.19: Impressão digital [37].

2.2.5.4 Geometria das veias

Um sistema para obtenção da geometria das veias de um utilizador consiste em tirar uma fotografia digital do dedo, palma, pulso ou dorso da mão que se encontra no campo de visão do scanner, utilizando uma câmara com luz infravermelha. O uso da luz infravermelha permite distinguir as veias devido à existência de hemoglobina no sangue que absorve a luz, tornando as veias pretas e deixando o resto do corpo num tom mais claro. Tal como nos outros tipos de biometria, a configuração das veias do utilizador será convertida por um software num modelo que depois pode ser comparado com os dados já existentes [31].

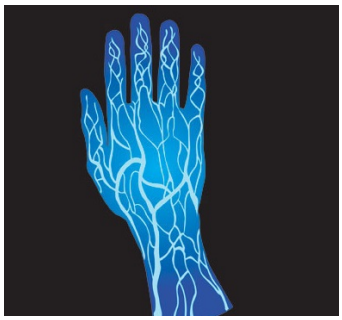

Figura 2.20: Estes scanners utilizam luz infravermelha para revelar o padrão das veias de uma pessoa [31].

2.2.5.5 Scan da íris

Os sistemas de reconhecimento da íris consistem num dispositivo com ou a interagir com um computador que possui um software de visão, que permite obter apenas a íris de uma fotografia tirada ao olho do utilizador. Para conseguir uma imagem de alta qualidade este sistema recorre a câmaras que utilizam luz infravermelha e visível, sendo que a luz infravermelha possibilita ao software uma melhor separação entre a íris e a pupila, pois a pupila torna-se muito preta.

Alguns destes sistemas necessitam que o utilizador se posicione corretamente, podendo estes ajudá-lo a colocar-se no lugar certo, para que possibilite ao scanner analisar a íris e convertê-la num código, para que depois se verifique se já existe algum registo igual ao agora obtido, permitindo o acesso ao utilizador caso haja equivalência [31].

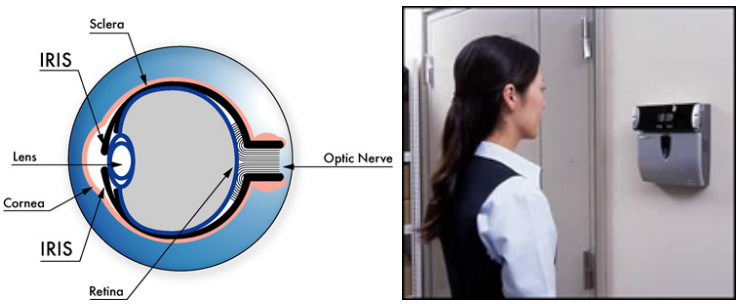

Figura 2.21: Anatomia do olho (à esquerda) e exemplo de scanner da iris (à direita) [31].

2.2.5.6 Comandos de voz

Nos sistemas de reconhecimento de voz são analisadas as diferentes características ligadas à voz de um utilizador, como o sotaque, timbre, rapidez e volume utilizados. Para que o sistema consiga adquirir a informação necessário para criar um gráfico ou espectograma de som, o utilizador deve dizer umas palavras ou frases exatas consoante o que for pedido pelo dispositivo. O gráfico criado apresenta a frequência do som no eixo vertical e o tempo na horizontal, sobrepondo os valores obtidos aos valores relativos ao mesmo utilizador que se encontram guardados numa base de dados, e verificando se ambos os valores são iguais, recebendo o utilizador autorização para aceder ao que pretende [31].

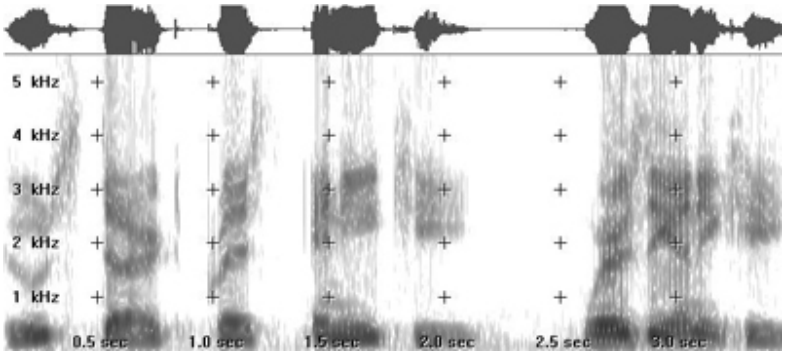

Figura 2.22: Sistemas de reconhecimento de voz usam espectrogramas para representar vozes humanas [31].

2.3 *Wireless Fidelity* (Wi-Fi)

A tecnologia *Wireless Fidelity* consiste na transmissão de dados via radio frequência entre o *router* e os dispositivos sem fios que estiverem ligados a este. O *router* recebe os dados da Internet uma vez que se encontra ligado ao fornecedor por um cabo *Ethernet* ou fibra ótica. Ele é um ponto de acesso (AP) que permite aos dispositivos que se conectarem receber os dados que pretendem visualizar da Internet, recebendo-os através dos sinais radio enviados a partir da antena do *router* [38].

Figura 2.23: Um *router* sem fios utiliza a(s) sua(s) antena(s) para enviar sinais para os dispositivos sem fios e um fio para enviar e receber informações da Internet. [38].

Hoje em dia, existem diversos espaços públicos com uma rede Wi-Fi disponível permitindo que uma grande variedade de utilizadores possa aceder à Internet onde se encontrem, estes lugares são denominados *hotspots* [39]. Nas redes Wi-Fi os dados podem ser acedidos sem que exista qualquer tipo de segurança bastando ao utilizador conectar-se com a rede, ou pode ser requisitado o nome do utilizador e uma palavra-chave ou apenas a palavra-chave (WPA2-*Enterprise* ou WPA2-Pessoal, respetivamente) ao se tentar ligar à rede Wi-Fi.

Os sistemas de controlo de acesso não recorrem, por enquanto, muito à tecnologia Wi-Fi para troca de informações, sendo por isso muito limitado o número de soluções que existem no mercado. Ao utilizar este meio de troca de dados nos sistemas de controlo, pode-se desenvolver um produto inovador que permite ao cliente efetuar o pedido de inscrição e aceder ao espaço remotamente.

2.3.0.7 Normas Wi-Fi

As normas utilizadas pela tecnologia Wi-Fi pertencem à família da norma 802.11 e de seguida enumero as principais:

- **802.11 (1997, revisto em 2007)**: Esta é a norma original e apresentava a capacidade de transmissão de dados com uma velocidade entre 1 e 2 megabits por segundo numa frequência de cerca de 2,4 GHz [39; 40; 41].
- **802.11a (1999)**: Esta norma é uma extensão da norma inicial e fornecia até 54 megabits de dados por segundo numa faixa de 5 GHz. Para reduzir as interferências existentes na norma anterior esta utiliza um método de codificação de multiplicação por divisão de frequência ortogonal (OFDM) [38; 41].
- **802.11b (1999)**: Esta norma é também uma extensão da norma inicial, apresentando a mesma faixa de frequência (2,4 GHz) mas uma velocidade máxima de envio de dados de 11 megabits por segundo. Estes valores permitiram à tecnologia Wi-Fi a execução de funcionalidades ao mesmo nível que os cabos *Ethernet* [39; 40; 41].
- **802.11g (2003)**: Esta norma manteve a mesma frequência que as normas 802.11 e 802.11b, aumentando a velocidade de transmissão para 54 megabits por segundo, devido ao uso da codificação da norma 802.11a [38; 41].
- **802.11i (2004)**: Esta norma, também denominada WPA2, consiste nas especificações definidas para a segurança de uma rede Wi-Fi, recorrendo à técnica de criptografia AES, permitindo uma transmissão de dados eficiente e segura [39; 42].
- **802.11n (2009)**: Esta norma é compatível com as anteriores e permite a existência de até quatro canais. A frequência utilizada continua a ser na gama dos 2,4 GHz, sendo possível enviar no máximo 150 megabits por segundo em cada canal, ou seja, 600 nos quatro canais. Os *routers*, normalmente, apenas possuem entre dois ou três canais para a transmissão de dados [38; 40; 41].
- **802.11ac (2013)**: Esta norma é a mais recente e apresenta uma faixa de 5 GHz, permitindo uma velocidade máxima de 450 megabits por segundo em cada canal [38; 40].

2.4 Soluções existentes

As soluções utilizadas para o controlo de acessos no aluguer de apartamentos e em hosteis são, normalmente, as chaves metálicas e os cartões RFID, obrigando o cliente a se dirigir a um determinado local (receção no caso dos hosteis) para obter o mecanismo que lhe permite aceder ao espaço reservado.

Nos hosteis, os clientes efetuam a reserva para um determinado período a partir de uma agência turística ou de um site que serve para efetuar o pedido de aluguer, recebendo assim que estiverem inscritos a confirmação e efetuando depois o pagamento da estadia. Na data inicial escolhida a pessoa tem de se deslocar à receção para conseguir o cartão ou chave para poder aceder ao espaço reservado, sendo que caso existam outros utilizadores que tenham o mesmo espaço reservado estes necessitam também de uma cópia do mecanismo de acesso. Com o processo desenvolvido nestes moldes o cliente está dependente da pessoa que se encontra na receção para poder entrar no quarto que reservou.

Em alguns casos, a pessoa tem de deixar a chave na receção sempre que se quiser deslocar a algum local turístico existente ou decidir ir comer num determinado restaurante na localidade que escolheu como destino, tendo que requisitar as mesmas no momento em que regressa ao hostel para descansar.

No arrendamento de apartamentos, o cliente pode recorrer aos mesmos serviços de reserva utilizados no caso dos hosteis, sendo o processo de inscrição e pagamento semelhante. No inicio do período selecionado para habitação, a pessoa dirige-se ao local escolhido para receber, normalmente, as chaves do apartamento entregues pelo proprietário, obrigando este a deslocar-se desde o local onde mora até ali para que o cliente possa aceder ao espaço. Tal como no caso dos hosteis, a pessoa está dependente do proprietário, podendo este atrasar-se e criar um período de espera desagradável para a pessoa que pretende colocar os seus bens no apartamento o mais cedo possível.

Neste caso, o proprietário apesar de lucrar com o arrendamento do apartamento, tem alguns custos adicionais ao ter de se deslocar, sendo obrigado a gastar combustível e aumentando o desgaste que o veículo possa apresentar, quer seja nos pneus ou nos componentes mecânicos que o constituem. O cliente no fim do seu período de aluguer deve deixar as chaves no apartamento antes de sair para serem depois entregues ao próximo inquilino, ou o proprietário terá de se deslocar outra vez para as ir buscar.

No mercado atual existem poucas soluções que permitam ao cliente inscrever-se e poder deslocar-se diretamente ao espaço reservado sem ter de pedir algum mecanismo de acesso ao mesmo. Uma das soluções que mais se aproxima da realização dos objetivos pretendidos é o ZigLock Hotel (figura 2.24), criado pela empresa ACURA Global em parceria com a RWTECH. Este sistema é de fácil instalação, uma vez que todos os pontos comunicam sem fios (Zigbee) com a unidade central da unidade hoteleira. O cliente após efetuar a reserva, apenas terá de registar a sua impressão digital na receção, ficando esta guardada na unidade e permitindo ao cliente aceder ao espaço diretamente quando pretender efetuar uma nova reserva. As informações do cliente são enviadas para o sistema utilizado, permitindo ao cliente entrar e guardar alguns bens no cofre existente no espaço, sendo utilizado o mesmo sistema para se conseguir aceder ao conteúdo do cofre [43].

Uma vez que é utilizada a biometria como método de acesso, esta solução é prática e segura, devendo o seu custo ser mais elevado relativamente aos sistemas atualmente utilizados.

Figura 2.24: ZigLock Hotel. [43].

A outra solução é o Oracode 660 criado pela empresa Kaba e é apresentada na figura 2.25. Tal como o sistema ZigLock, este também é de fácil utilização e não necessita de fios para a sua programação. O sistema central da unidade hoteleira atribui um código de seis cifras, definido para um determinado período de tempo, ao cliente que terá de introduzi-lo no teclado da fechadura [44]. Caso este código seja enviado para o cliente quando este efetuar a sua reserva ou pagamento, ele tem a possibilidade de aceder ao espaço diretamente, sem ter de se deslocar à receção.

O sistema é inicialmente programado utilizando um dispositivo portátil de infravermelhos, sendo os códigos depois introduzidos através de um site desenvolvido para esse efeito. O código pode ser alterado consoante a vontade do cliente [45].

Figura 2.25: Oracode 660. [44].

A existência de um sistema que permite evitar a receção do hostel ou o deslocamento do proprietário ao apartamento (também benéfico para o proprietário), aumentava a autonomia do cliente permitindo a este ter um maior controlo do mecanismo de acesso ao espaço, recorrendo à receção e ao proprietário apenas em situações que existam dúvidas sobre determinado aspeto do espaço, sobre percursos a realizar para atingir um determinado local ou sobre informações relativas a zonas com determinadas atividades existentes dentro e perto da localidade onde se encontram, como parques aquáticos, zoológicos, atividades desportivas, monumentos ou passeios turísticos.

Sendo hoje em dia um dos principais objetivos do marketing turístico inovar e agradar o cliente, a criação de um sistema que permitisse o acesso direto ao espaço ou apartamento, sem ter de depender de terceiros seria uma forma de modernizar os sistemas de controlo de acessos já existentes, facilitando a vida a todas as partes envolvidas.

Capítulo 3

Solução

Neste capítulo pretende-se dar a conhecer a solução proposta e as etapas seguidas na criação desta, sendo também mencionados os objetivos que se pretendem cumprir. Inicialmente descrevem-se os diferentes critérios utilizados na definição da solução, sendo de seguida explicados os diferentes passos utilizados na criação desta.

3.1 Requisitos

Na criação de um sistema de controlo de acessos têm de se respeitar algumas condições para que este funcione corretamente, e permita que tanto o proprietário como o cliente consigam aceder ao espaço requisitado de forma segura.

Uma das condições a ser tratada é a identificação dos diversos clientes que pretendem utilizar o local. A forma de resolver esta condição consiste em pedir determinadas informações ao cliente durante a fase de inscrição.

Outra circunstância a considerar é a autenticidade do cliente quando este tenta aceder ao espaço, sendo este fator que autoriza ou nega o acesso. Para solucionar esta questão utilizam-se palavras-chave que juntamente com a identificação permitem verificar a veracidade dos dados introduzidos pelo cliente para obter autorização para aceder ao espaço requisitado.

A última condição a ter em consideração é a realização de uma auditoria, permitindo assim ao proprietário saber que cliente se encontra a usufruir do local fornecido numa determinada altura do ano.

Na resolução destas condições aparecem duas entidades, o proprietário e o cliente, que em conjunto permitem criar uma solução que pretende agradar a ambos. O proprietário tem de gerir o espaço que pretende alugar, de modo a cativar os diferentes clientes que estejam interessados em efetuar uma reserva. O cliente tem de fazer um pedido de inscrição para conseguir obter o mecanismo de acesso ao espaço que o proprietário lhe irá fornecer.

Nas secções seguintes apresentam-se os cinco diferentes serviços necessários para resolver as condições anteriores e obter a solução proposta, estando estas ilustradas e numeradas na figura 3.1.

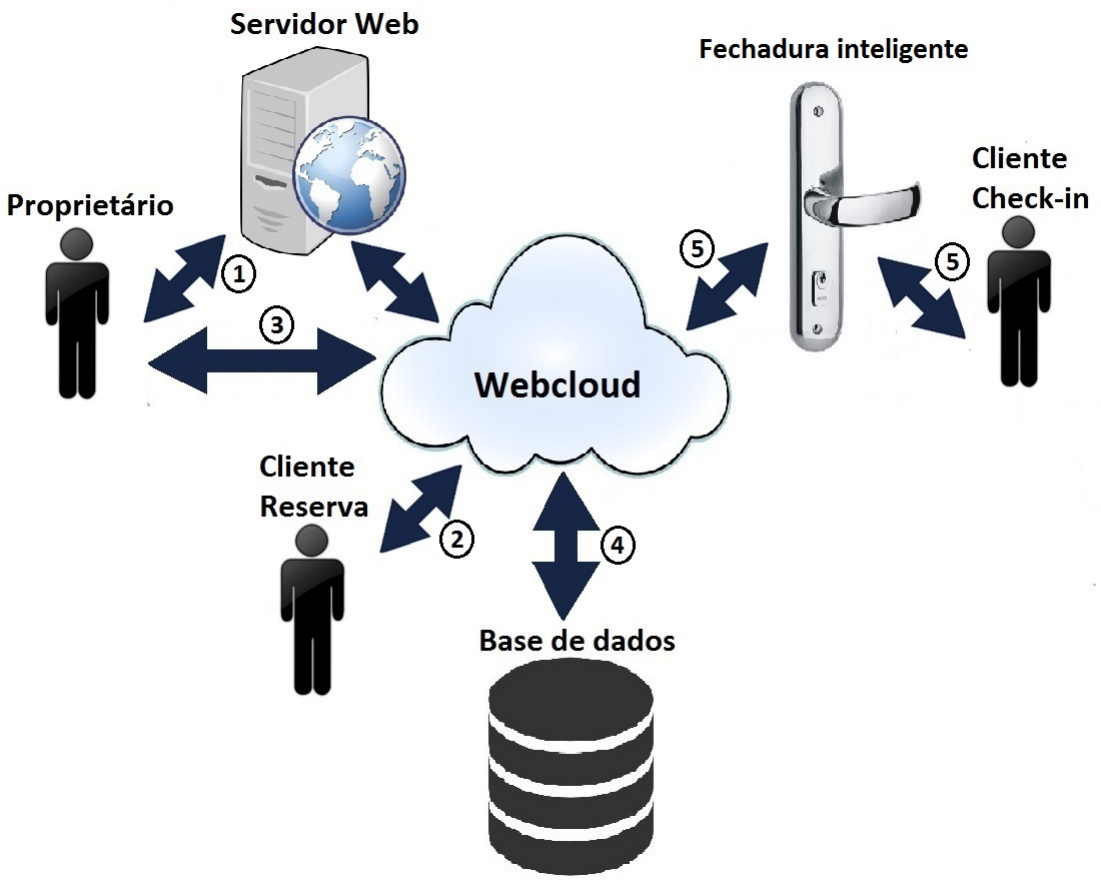

Figura 3.1: Esquema representativo da solução proposta.

3.2 Serviço 1 - Divulgação do espaço

Este serviço permite que o proprietário divulgue o espaço a potenciais clientes que pretendam usufruir do mesmo. Para que este serviço seja o mais acessível e simplificado possível recorre-se à Internet, utilizando o site do espaço, para dar a conhecer imagens do espaço, a sua localização e coordenadas num mapa e os valores praticados para os diferentes períodos do ano.

3.3 Serviço 2 - Pedido de inscrição, efetuado remotamente pelo cliente

Este serviço permite ao cliente reservar remotamente o espaço. O site permite ao cliente verificar em que datas o espaço se encontra disponível ou aquelas em que está reservado. O pedido de reserva pode ser efetuado a partir do site, tendo o cliente de preencher alguns parâmetros pedidos, como o seu primeiro e último nomes, o período desejado para aluguer (data inicial e final), número de telefone e email. Após introduzidos os dados estes serão enviados para serem verificados pelo proprietário.

3.4 Serviço 3 - Confirmação da inscrição, realizada remotamente pelo gestor

O objetivo de terceiro serviço é a confirmação da reserva do cliente e o consequente fornecimento da autorização (código) necessária para este aceder ao espaço que reservou.

O proprietário ao receber as informações necessárias do cliente, utiliza-as para fazer a inscrição do mesmo recorrendo ao site. Ao ser inscrito é atribuído um código de acesso ao cliente e é enviada uma mensagem com o código e os dados necessários para efetuar o pagamento do aluguer do espaço. O pagamento pode ser também efetuado no site, tendo o cliente de utilizar os dados recebidos, caso contrário sua inscrição será cancelada e o código de acesso recebido anulado.

3.5 Serviço 4 - Registo das reservas

Nesta secção pretende-se arranjar uma maneira de guardar todos os dados que durante o processo de inscrição são solicitados ao cliente e utilizá-los na identificação e autenticação do mesmo quando este tentar aceder fisicamente ao espaço que reservou.

Um método aceitável para guardar a informação consiste na criação de uma base de dados, que permita organizar a informação da maneira que o operador achar mais percetível, podendo este inserir dados sobre o cliente, alterar os dados sempre que necessária a sua atualização ou eliminar o cliente da base de dados caso este cancele a sua reserva. Os dados recolhidos são depois organizados numa tabela com as seguintes informações por coluna: um valor de identificação do cliente, o primeiro e último nome, a data inicial e final escolhidas para reservar o espaço (representado por ano-mês-dia), o email, o número de telefone e o código de acesso a ser atribuído para conseguir ter permissão para aceder ao espaço, como na tabela 3.1.

ID	**Primeiro Nome**	**Último Nome**	**Inicio Aluguer**	**Fim Aluguer**	**Código**	**Email**	**Telefone**
1	David	Cardoso	a-m-d	a-m-d	******	..@ua.pt	96...

Tabela 3.1: Exemplo da tabela da base de dados .

Esta base de dados permite a auditoria, uma vez que permite guardar uma lista com os vários clientes que usufruíram do espaço a que corresponde esta base. Com esta lista o proprietário pode analisar as diferentes datas que os clientes escolheram para usufruir do espaço, e verificar em que período houve uma maior afluência, determinar a média dos dias reservados por cliente e avaliar os preços impostos, alterando estes consoante a análise realizada.

3.6 Serviço 5 - *Check-in* realizado pelo cliente

Nesta fase o cliente tem um código de acesso ao espaço desejado que recebeu ao ter-se inscrito e ter efetuado o pagamento do período de aluguer que escolheu.

Desta forma o cliente torna-se mais autónomo, podendo dirigir-se diretamente ao espaço sem ter de depender de terceiros para conseguir aceder ao local reservado. Consegue-se também reduzir os custos de receção, nomeadamente custos de mão-de-obra. Permite ainda, no caso do arredamento de apartamentos, evitar a deslocação do proprietário para entrega do mecanismo, tendo o cliente apenas de introduzir o código que lhe foi fornecido para conseguir aceder ao local.

Capítulo 4

Implementação

Neste capítulo pretende-se dar a conhecer a implementação realizada da solução e os seus diferentes componentes. São especificados os diferentes métodos utilizados para a realização dos diferentes componentes e as suas funções, e também serão apresentados os processos interativos desenvolvidos para a comunicação entre o cliente e o proprietário, e entre o cliente e o sistema de acesso ao espaço.

4.1 Metodologia

Inicialmente foram desenvolvidas algumas páginas web, recorrendo às linguagens PHP, HTML e JavaScript, para permitir ao proprietário expor o seu espaço na Internet, através de imagens, a sua localização e os preços durante as diferentes épocas do ano. Para conseguirem ser visualizadas pelos diferentes clientes possíveis, estas páginas foram enviadas para um servidor Web denominado GearHost, que permite que estas sejam acessíveis em qualquer lugar onde exista Internet.

Acedendo ao *site* desenvolvido, o cliente tem a possibilidade de avaliar as condições do espaço através das imagens que o proprietário disponibilizou, verificar a posição a que este se encontra de determinados pontos turísticos que possa querer visitar e analisar o preço da estadia, decidindo se está ou não interessado em efetuar a reserva do espaço.

De modo a possibilitar ao cliente a oportunidade de reservar o espaço durante um período que deseja, este terá de efetuar um pedido de reserva através de uma das páginas desenvolvidas, onde são pedidos alguns dados para identificação do cliente. O cliente possui também uma página à sua disposição onde consegue verificar em que períodos o espaço se encontra ocupado ou disponível, podendo realizar a sua reserva com base nessa informação. Após a inserção dos dados requeridos, estes são enviados por email para o proprietário os poder verificar.

Ao receber o email com os dados do cliente, o proprietário verifica e compara os dados inscritos com os recebidos na mensagem, de modo a verificar se houve alterações efetuadas após a sua reserva. Caso sejam confirmados, os dados serão inseridos numa tabela de clientes, a partir de uma página de confirmação apenas acessível ao proprietário.

A tabela de clientes foi desenvolvida utilizando a base de dados MySQL, que permite adicionar e eliminar clientes e configurar os seus dados consoante a necessidade de atualizar as informações que os identificam. Para permitir a verificação dos dados dos clientes com as reservas confirmadas, estes são apresentados numa página destinada ao proprietário.

Na fechadura inteligente foi escolhido o módulo ESP8266 como interface de comunicação Wi-Fi com o cliente e com a base de dados do sistema proposto. Um sistema que recorria à tecnologia RFID foi também analisado (ver Apêndice A), sendo escolhida a solução proposta baseada no módulo, uma vez que permite uma maior autonomia do cliente e utiliza uma tecnologia inovadora nos sistemas de controlo de acessos. Outra desvantagem é a necessidade do cliente ter previamente de obter um cartão RFID programado e fornecido numa receção, enquanto que com a solução proposta não existe essa necessidade.

O sistema desenvolvido possibilita ao cliente aceder ao espaço recorrendo à autorização que recebeu do proprietário quando se inscreveu. Sendo a autorização um código de acesso, este terá de ser inserido no sistema para que seja verificada a veracidade da identidade do cliente que pretende aceder ao espaço.

A fechadura inteligente cria uma rede Wi-Fi que permite ao cliente introduzir o código de acesso do espaço, recorrendo a um telemóvel, tablet ou computadores.

Os dispositivos que permitem aceder ao espaço encontram-se a ter um aumento de popularidade, tendo os clientes, na sua grande maioria, pelo menos um deles ao seu dispor, sendo o telemóvel o mais importante e o mais adequado para a realização desta função, sendo um dispositivo mais móvel e compacto que normalmente se encontra guardado num bolso.

No mercado atual, estes dispositivos apresentam, quase todos, um software que permite conectarem-se a uma rede Wi-Fi, permitindo ao cliente utilizar um dispositivo pessoal para entrar no espaço, substituindo os cartões e chaves que teriam de requisitar.

A fechadura inteligente comunica com a base de dados recorrendo à tecnologia Wi-Fi para validar o código introduzido pelo cliente. Uma vez que para cada cliente o código de acesso varia, outros não conseguem aceder ao espaço numa data que não esteja inserida no intervalo reservado.

A figura 4.1 representa as diferentes fases do processo de arrendamento, os diversos componentes constituintes deste sistema e as várias trocas de dados que ocorrem para que seja autorizado o acesso a um determinado espaço.

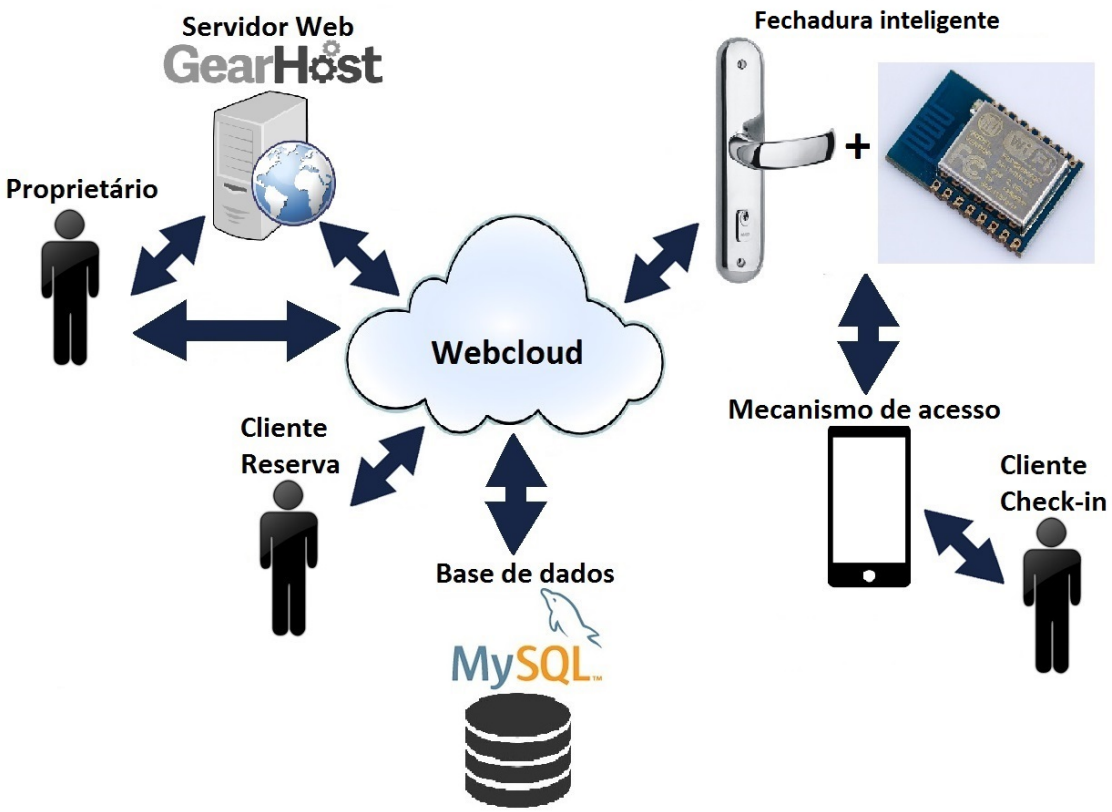

Figura 4.1: Esquema da implementação da solução.

4.2 Apresentação do *site* desenvolvido

Nesta secção apresentam-se as diferentes páginas desenvolvidas que compõem o *site* do espaço a alugar. Serão explicadas as diferentes funções que cada uma delas possui para possibilitar o bom funcionamento do sistema de controlo de acessos.

No *site*, tanto o proprietário como o cliente, tem disponíveis páginas com informações sobre o espaço e por onde conseguem tratar dos detalhes de aluguer do mesmo, embora o cliente não tenha permissão para visualizar as páginas destinadas ao proprietário.

Ao colocar o endereço da referência [46] num motor de busca da Internet, encontra-se a página inicial do site, como mostra a figura 4.2. Nesta página existe uma divisão entre as páginas acessíveis ao proprietário e as páginas disponíveis para o cliente.

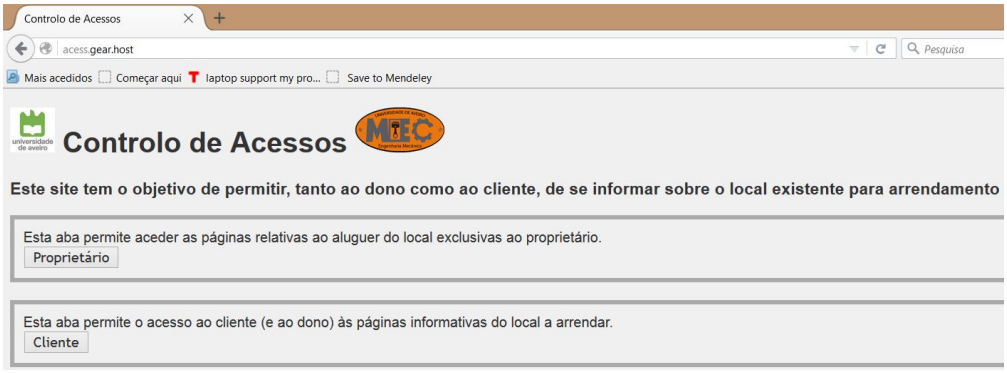

Figura 4.2: Página inicial do *site* do local.

Ao pressionar os botões "Proprietário" e "Cliente" consegue-se observar o conteúdo existente nas diferentes abas, como mostra a figura 4.3. Verifica-se que para a área do proprietário existe a necessidade de introduzir o nome do utilizador e a palavra-chave definidas e apenas conhecidas pelo próprio, não permitindo ao cliente aceder as estas páginas.

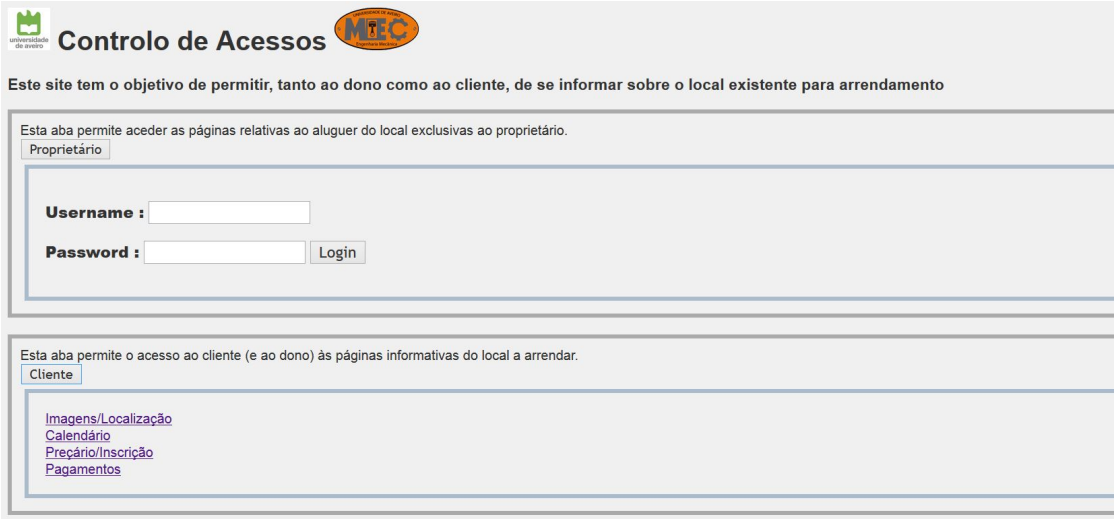

Figura 4.3: Página inicial com as áreas do cliente e do proprietário visíveis.

Na aba do cliente apresentam-se referências correspondentes às diferentes páginas disponíveis para este conseguir avaliar o espaço, como mostra a figura 4.3. As páginas acessíveis ao cliente são:

- Imagens e localização;
- Calendário de ocupação;
- Preços e método de inscrição;
- Forma de pagamento;

Na área do cliente para permitir uma simples navegação entre as diferentes páginas, foram criados separadores, como mostra a figura 4.4. Estes separadores encontram-se em todas as páginas destinadas ao cliente e permitem ao cliente navegar pelas diferentes páginas ao pressionarem a referência que pretendem abrir. A página em que o cliente se encontra fica assinalada a amarelo, como se pode verificar na figura.

Figura 4.4: Separadores das páginas para os clientes.

A primeira referência ("Imagens/Localização") corresponde a uma página onde existem imagens do local a alugar e a sua localização no mapa, deste modo a pessoa pode visualizar as diferentes divisões da residência, ficar com uma ideia de como a sua estadia poderá vir a ser e verificar se se encontra perto dos locais turísticos que tinham em mente visitar para esse período de férias.

Após o cliente aceder à página, esta encontra as imagens escolhidas do local na Internet e coloca-as na ordem estabelecida para a sua amostragem. O mapa com a localização é obtido recorrendo à função *GoogleMaps*, tendo de se colocar as coordenadas do local para que o mapa apresente automaticamente a sua posição correta.

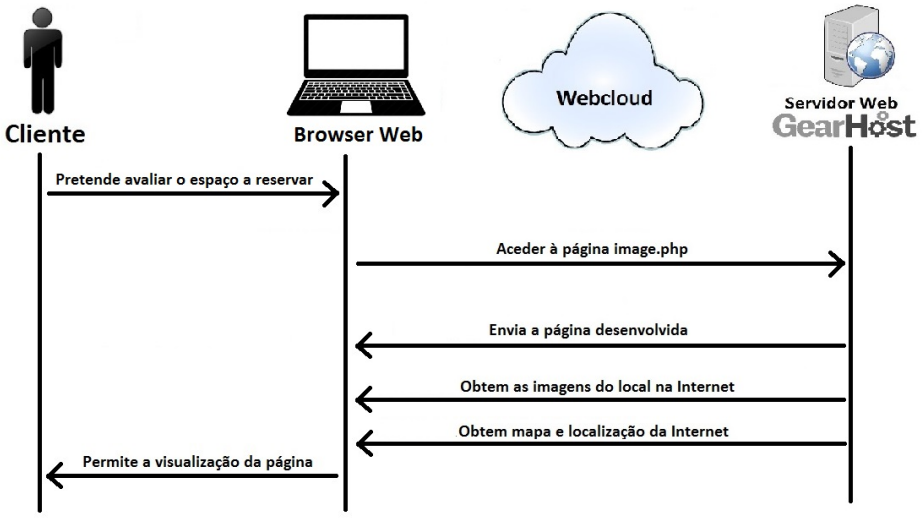

Figura 4.5: Etapas executadas ao aceder à página com as imagens e localização do local.

A figura 4.6 mostra a parte onde o cliente pode observar as imagens disponibilizadas, para isso tem de alterar o número da caixa e deslocar o rato para cima da imagem, permitindo assim a sua atualização.

Figura 4.6: Parte de visualização de imagens do local a alugar.

Na figura 4.7 apresenta-se o método de localização utilizado, permitindo ao cliente verificar onde se encontra o espaço e como se pode dirigir ao mesmo.

Figura 4.7: Parte da localização do local a alugar.

Outra página destinada ao cliente consiste num calendário com informação sobre a ocupação do local a alugar. Esta página interage com a base de dados, uma vez que requer os períodos reservados e por confirmar dos diferentes clientes. Estes períodos são obtidos das tabelas criadas para de seguida serem analisadas as datas inicial e final escolhidas pelos clientes e determinar os dias incluídos em cada um deles, sendo estes depois apresentados no calendário com cores diferentes dos dias disponíveis. Deste modo, o cliente ao visitar esta página verifica se existe a possibilidade de efetuar uma reserva para a altura do ano que tinha em mente, podendo inscrever-se com bastante antecedência.

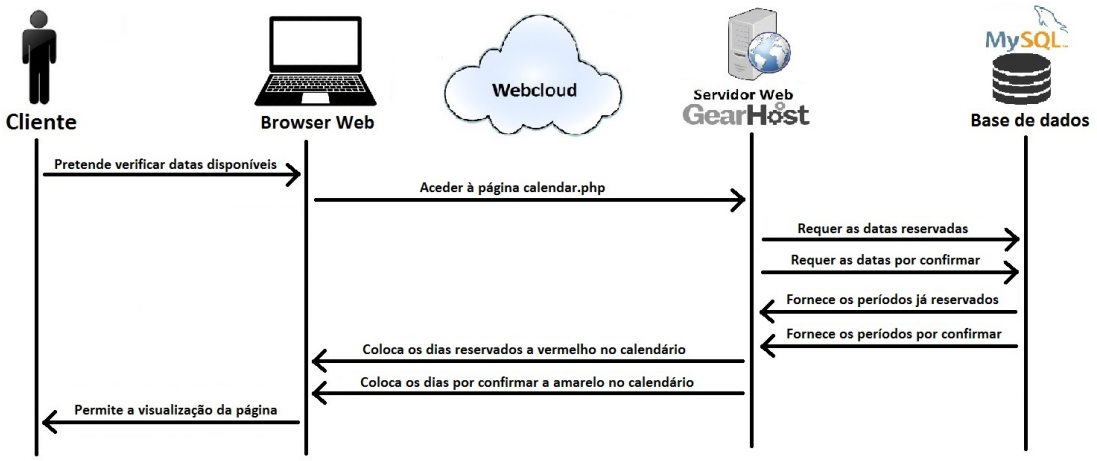

Figura 4.8: Etapas executadas ao aceder à página com o calendário ocupacional.

Este calendário permite navegar pelos doze meses de cada ano e verificar se os dias de cada mês se encontram ocupados ou livres, recorrendo aos botões "Prev" e "Next" para voltar ao mês anterior ou avançar para o mês seguinte, respetivamente.

Como se pode verificar na figura 4.9, os dias encontram-se a cores diferentes, tendo cada uma o seguinte significado:

- Dias verdes - São dias sem nenhum registo efetuado, existindo a possibilidade de efetuar uma inscrição nesses períodos.
- Dias amarelos - São dias que se encontram incluídos numa inscrição efetuada por um cliente e esta se encontra à espera da confirmação do proprietário. Após a confirmação estes dias passam a vermelho.
- Dias vermelhos - São dias onde a inscrição efetuada pelo cliente já foi confirmada, estando estes dias reservados e impedidos de ser usados numa futura inscrição;

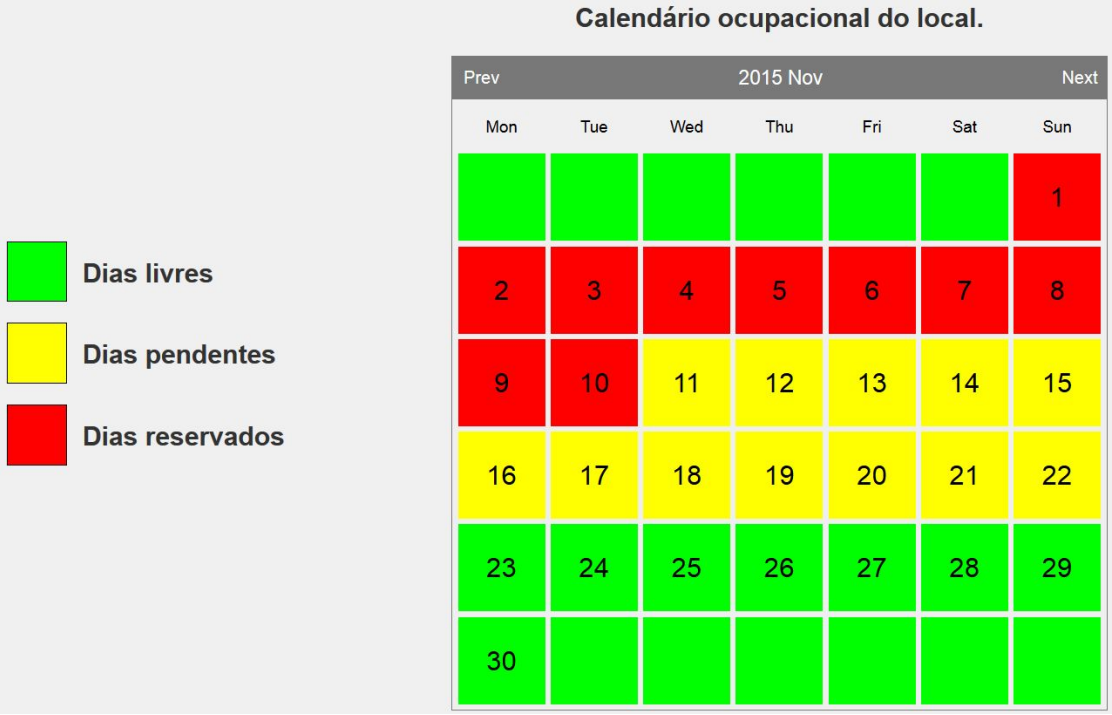

Figura 4.9: Calendário de ocupação da residência a alugar.

Na página "Preçário/Inscrição" são apresentados os preços para as diferentes épocas do ano e um formulário que permite ao cliente enviar o pedido de inscrição para um determinado período ao proprietário, caso esteja interessado. Esta página também comunica com as tabelas existentes na base de dados, de modo a conseguir verificar as datas utilizadas no pedido de inscrição do cliente e a guardar os dados do cliente que efetua o pedido. Após efetuado o pedido o cliente deverá enviar um email a confirmar as informações introduzidas ao proprietário.

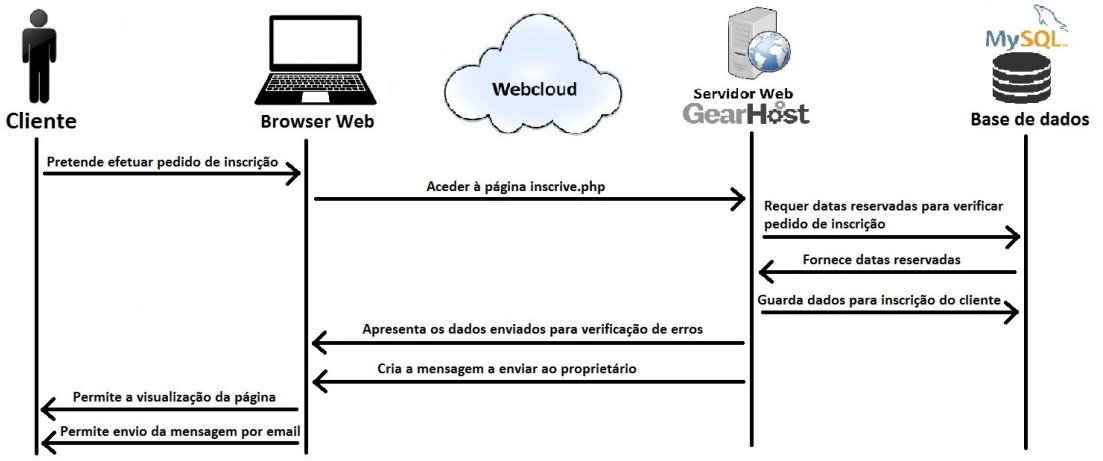

Figura 4.10: Etapas executadas ao aceder à página onde se efetua a inscrição.

A figura 4.11 mostra o conteúdo da página que permite verificar os valores praticados nas diferentes épocas e o formulário para a realização do pedido de inscrição.

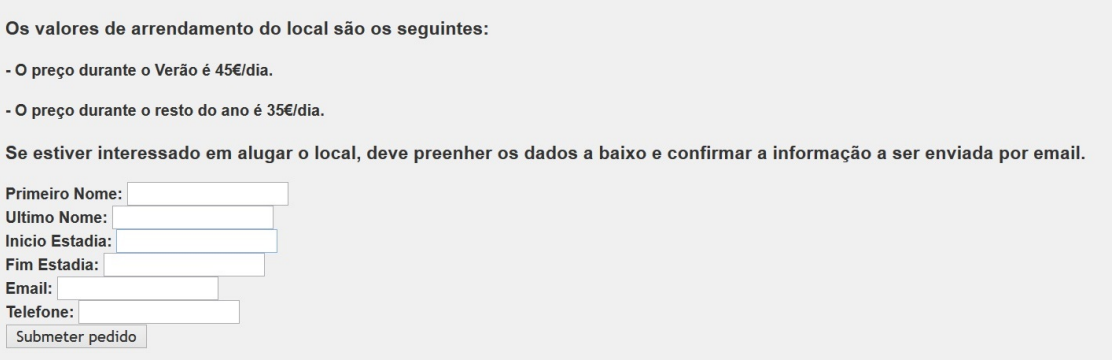

Figura 4.11: Página de pedido de aluguer.

Na realização do pedido o cliente tem de preencher todos os parâmetros do formulário, como o primeiro e último nome, o período de estadia, o número de telefone e o correio eletrónico para receber a resposta. Se existir algum campo que não se encontre preenchido, será pedido que se preencham os espaços que ficaram em brancos ao submeter o pedido anterior, como mostra a figura 4.12.

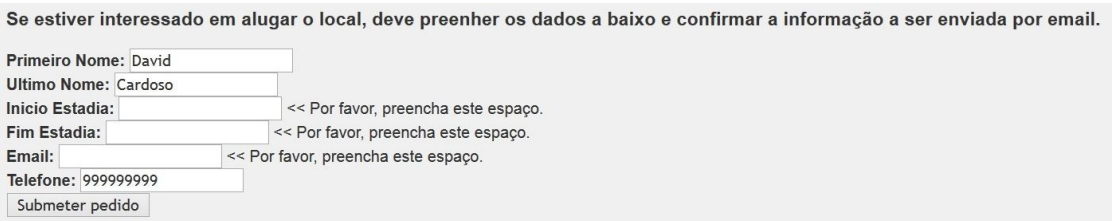

Figura 4.12: Página de pedido de aluguer, todos os campos devem ser preenchidos.

Quando todos os campos se encontrem preenchidos, será verificado se os valores inseridos no inicio e fim da estadia não se encontram já reservados por outros clientes. Caso o período escolhido já se encontre reservado, é pedido que verifique o calendário e altere os valores, como mostra a figura 4.13.

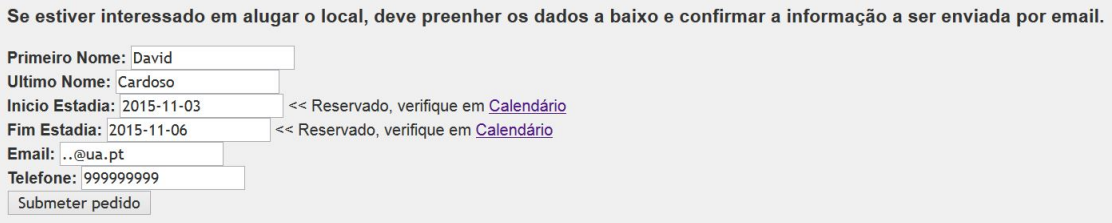

Figura 4.13: Página de pedido de aluguer, verificação do período escolhido.

Após a submissão dos dados, estes são enviados para a base de dados para que o proprietário possa confirmar o pedido (aparecendo a amarelo o periodo escolhido, como se pode verificar na figura 4.9) e são apresentados ao cliente para que os possa verificar e detetar se existe algum engano nos vários parâmetros preenchidos. Caso o cliente se tenha enganado, pode corrigir os dados realizando novamente a inscrição ou alterando-os no email que irá ser enviado ao proprietário ao pressionar o botão "Enviar Mensagem", como apresenta a figura 4.14.

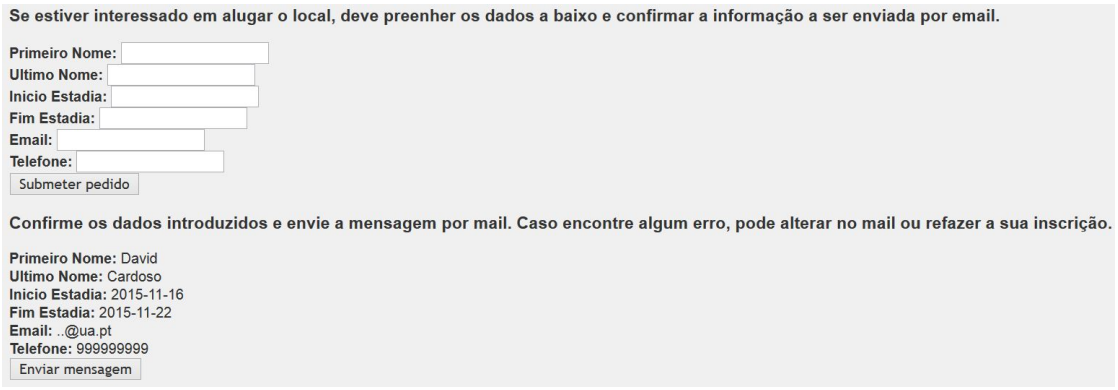

Figura 4.14: Página de pedido de aluguer, confirmação dos dados.

Depois de pressionar o botão "Enviar Mensagem", a página procura o programa utilizado pelo cliente para troca de emails e cria um novo email com uma mensagem já pré-definida, como mostra o exemplo da figura 4.15 onde é utilizado o *Microsoft Outlook*. Ao utilizar o programa, o cliente tem a possibilidade de alterar o conteúdo da mensagem, decidindo qual a estrutura a utilizar consoante o método de escrita a que está mais habituado.

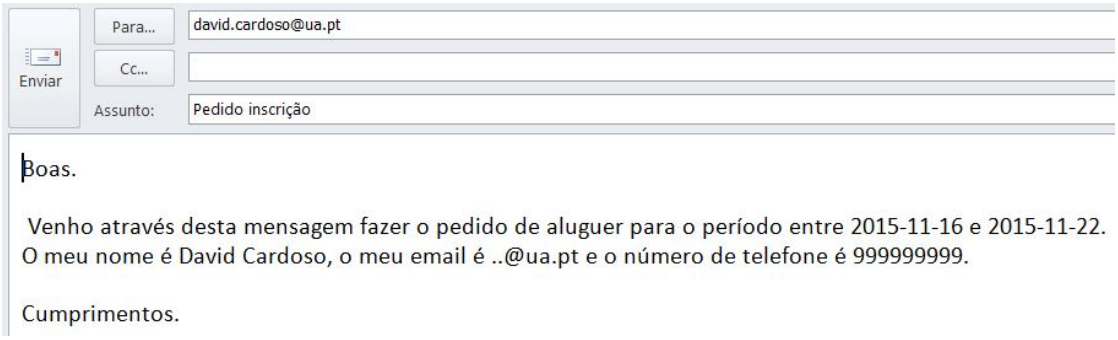

Figura 4.15: Mensagem com o pedido de inscrição a ser enviada ao proprietário.

A última página ("Pagamentos") servirá para o cliente efetuar o pagamento do período de ocupação do local através do *site*. Este será realizado após o proprietário ter confirmado o pedido de inscrição e enviar uma resposta ao cliente com o número de identificação e a palavra-chave que lhe foram atribuídos. Estes dados serão confirmados através da verificação da veracidade dos mesmos na base de dados.

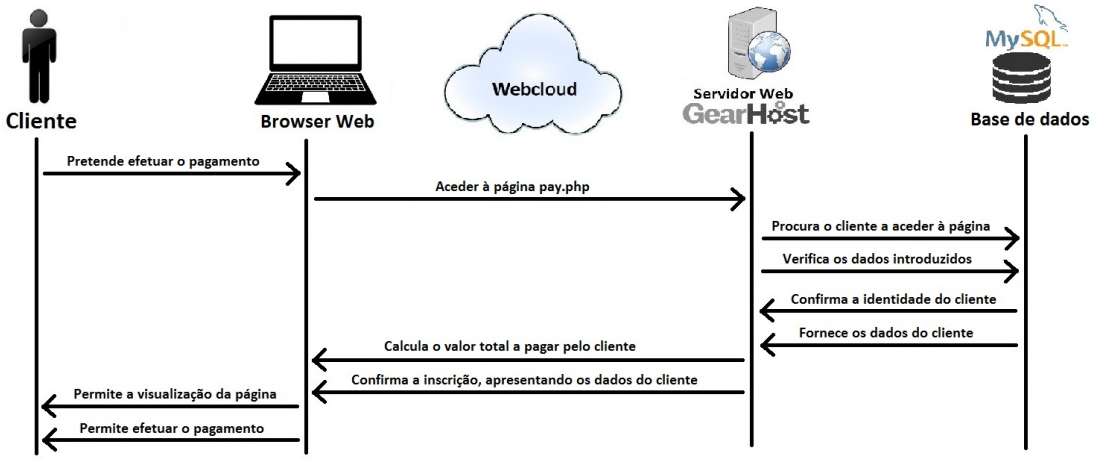

Figura 4.16: Etapas executadas ao aceder à página de pagamento.

Na figura 4.17 apresentam-se os campos a preencher pelo cliente, de modo a permitir que este verifique a sua inscrição e realize o pagamento.

Figura 4.17: Página inicial de pagamento do aluguer.

Após introduzir os dados nos respetivos campos e pressionando o botão "Entrar", vai aparecer uma tabela com os dados da inscrição confirmada e uma mensagem com o período reservado e o valor a pagar, permitindo ao cliente confirmar ambos os dados.

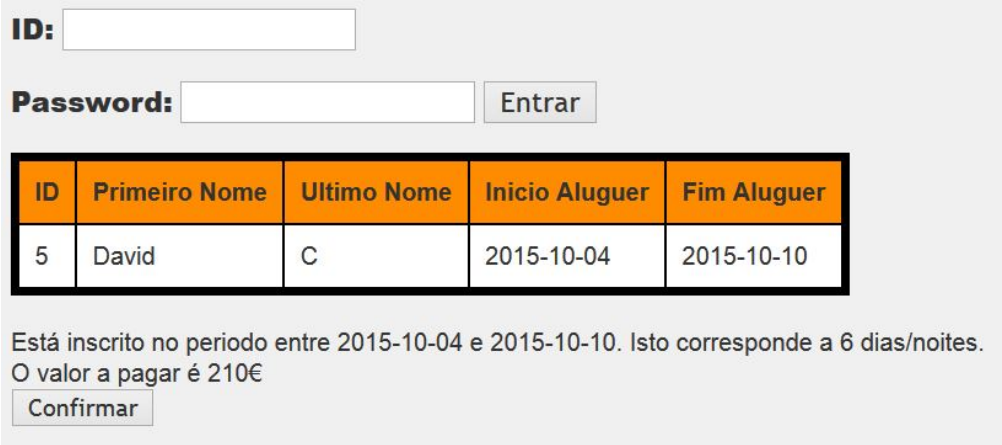

Figura 4.18: Página de pagamento do aluguer, verificação dos dados da inscrição.

Ao confirmar as informações o cliente será redirecionado a uma página onde irá ser realizada a transferência bancária entre o cliente e o proprietário (figura 4.19). Esta vai ocorrer utilizando o sistema *Paypal* que permite a transferência de dinheiro entre ambos usando endereços de email. O cliente pode também optar por outro método de pagamento tendo este de ser aceite e combinado com o proprietário do local a ser alugado.

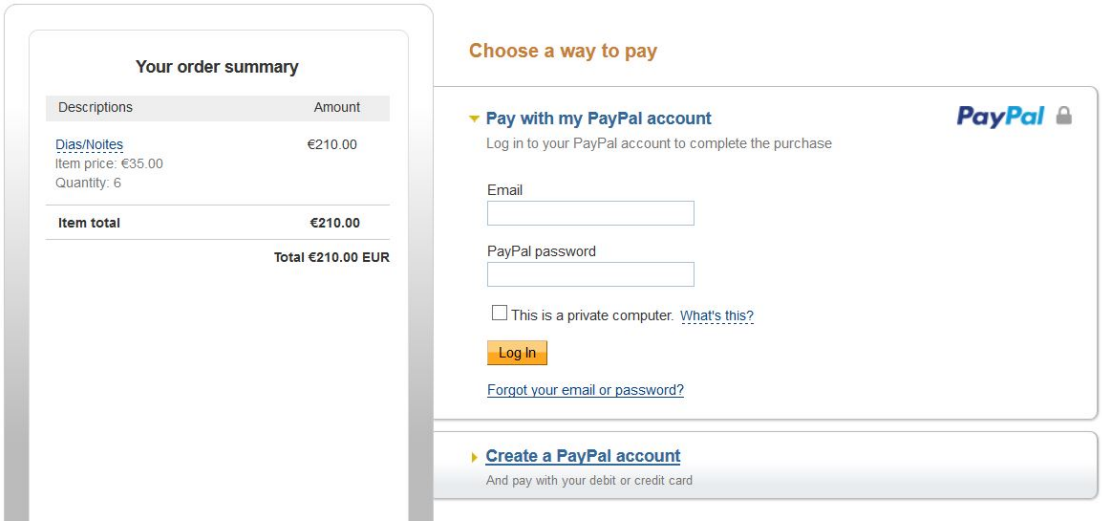

Figura 4.19: Página de pagamento do PayPal.

As páginas destinadas ao proprietário do local, servem para este conseguir confirmar os pedidos de inscrição dos novos clientes e verificar a quantidade de clientes que usufruíram do local. Para conseguir visualizar o conteúdo que estas possuem, o proprietário terá de colocar os valores definidos para o *username* e a *password*. Caso se engane aparecerá a mensagem da figura 4.20, que permite voltar à página inicial e tentar preencher novamente os campos necessários.

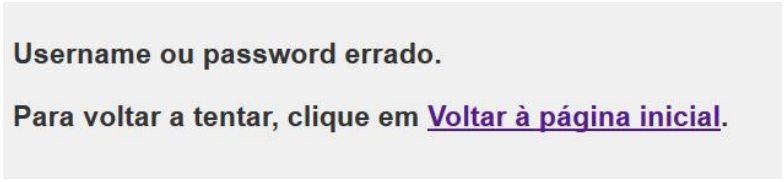

Figura 4.20: Mensagem apresentada após colocar um valor errado num dos campos pedidos.

Tal como nas páginas destinadas ao cliente, para facilitar a navegação entre as páginas foi criado um separador, sendo assinalada a amarelo a página em que se encontra.

Figura 4.21: Separadores das páginas para o proprietário do local.

Uma das páginas acessíveis ao proprietário permite, após receber o pedido de inscrição dos clientes, confirmar os dados e adicioná-los às tabelas da base de dados. Os dados a serem confirmados são os enviados durante o processo de inscrição efetuado pelo cliente na página destinada a esse efeito, e que foram guardados numa tabela da base de dados.

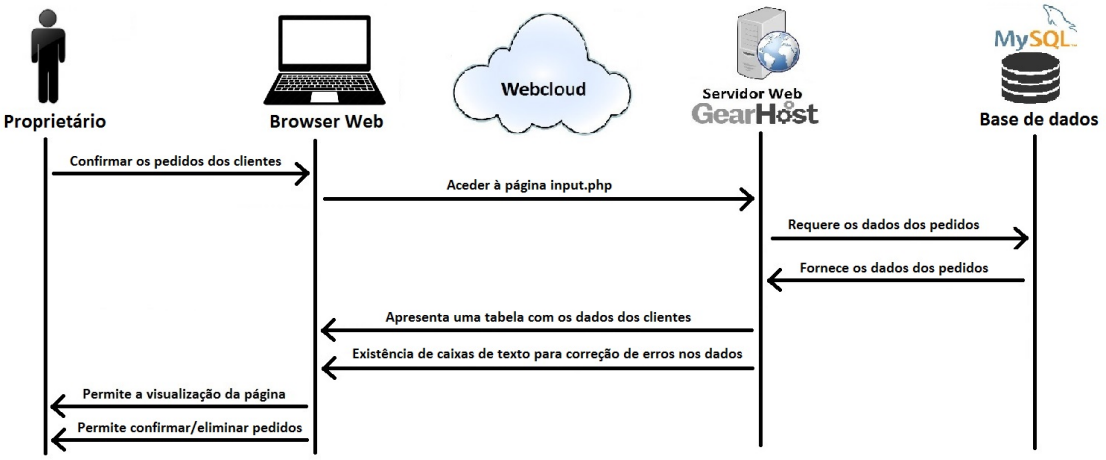

Figura 4.22: Etapas executadas ao aceder à página de confirmação de inscrições.

Para confirmar o pedido de inscrição e registar o cliente, de modo a permitir que este tenha acesso ao local, utiliza-se a página "Registar Cliente" onde existe uma tabela com todos os dados recebidos do processo de inscrição, tal como apresentado na figura 4.23. Antes de se confirmar a inscrição verifica-se todos os valores, comparando-os com os recebidos no email enviado pelo cliente e conferindo se estes são iguais ou se o cliente decidiu alterar algum dos dados após efetuar a inscrição. O botão "Confirm" serve para confirmar a inscrição quando pressionado, sendo que o botão "Delete" serve para eliminar algum pedido de inscrição repetido por engano ou que tenha desistido após efetuar o pedido.

Para inscrever um cliente tem de se verificar todos os dados da tabela em baixo.

Pedidos de inscrição

ID	Primeiro Nome	Ultimo Nome	Inicio Aluguer	Fim Aluguer	Email	Telefone	Confirmar	Eliminar
1	António	Pereira	2015-11-11	2015-11-15	..@ua.pt	999999999	Confirm	Delete
3	David	Cardoso	2015-11-16	2015-11-22	..@ua.pt	999999999	Confirm	Delete

Figura 4.23: Página de registo de novos clientes pelo proprietário.

Após confirmado o pedido de inscrição, as informações referentes a esse cliente são eliminadas da tabela e ao serem enviados os dados para as outras tabelas de registo, é lhe atribuído automaticamente um número de identificação e um código de acesso, permitindo ao cliente efetuar o pagamento na página já referida e conseguir aceder ao local que reservou. Assim como acontece no pedido de inscrição, os dados são apresentados ao proprietário para serem verificados e enviados por email ao cliente.

A figura 4.24 demonstra o processo de registo do cliente "David", podendo-se verificar que a linha da tabela onde os seus dados se encontravam foi eliminada e os seus dados foram apresentados ao proprietário para envio, já com o código de acesso que lhe foi atribuído. Nesta fase o período escolhido pelo cliente já se encontra a vermelho no calendário ocupacional, impedindo que sejam realizados pedidos para esta altura.

Figura 4.24: Página de registo de novos clientes pelo proprietário, todos os campos devem ser preenchidos.

Depois de pressionar o botão "Enviar Mensagem", um novo email com uma mensagem já pré-definida é criado, como mostra o exemplo da figura 4.25. Na mensagem a ser enviada ao cliente, são confirmados os dados recebidos e é explicado o método para efetuar o pagamento e para conseguir aceder ao local que reservou. A forma de pagamento também pode ser negociada, tendo o cliente de entrar em contacto com o proprietário, com se indica no email.

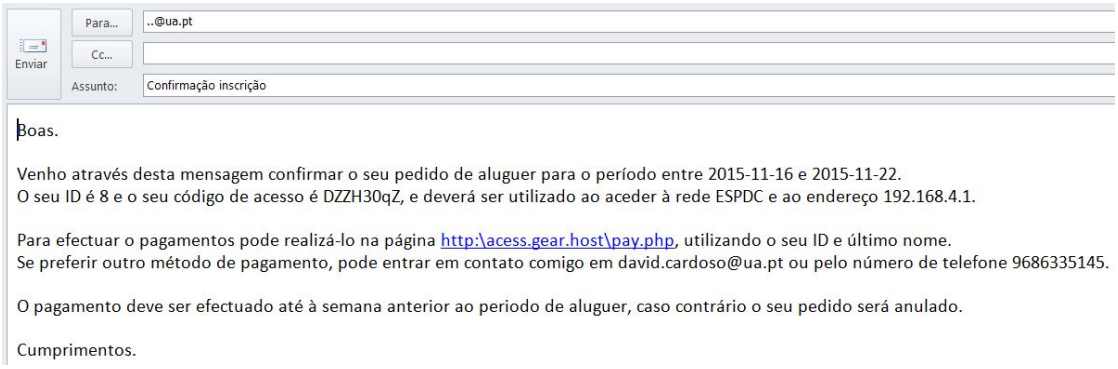

Figura 4.25: Mensagem com a confirmação da inscrição a ser enviada ao cliente.

A outra página destinada ao proprietário permite visualizar a lista de clientes que reservaram o local ao longo do ano. A base de dados que recebe as informações do cliente após confirmada a sua inscrição deve ser normalizada para que esta seja mais fácil de gerir e evitar problemas futuros. Na realização da normalização recorre-se ao método do Diagrama de Dependências Funcionais (DDF) permitindo organizar os diferentes parâmetros da relação universal em sub relações normalizadas [47].

Na figura 4.26 está representada a relação universal "R" entre os vários dados que o cliente fornece quando efetua a inscrição e os dados que lhe são atribuídos após a sua confirmação. Para que a relação "R" se encontre normalizada esta tem de se apresentar na Forma Normal de Boyce Codd (FNBC), ou seja, todos os determinantes devem ser chaves candidatas desta mesma relação[47]. Como se pode verificar na figura, existem mais determinantes que chaves candidatas, sendo por isso necessário decompor a relação "R".

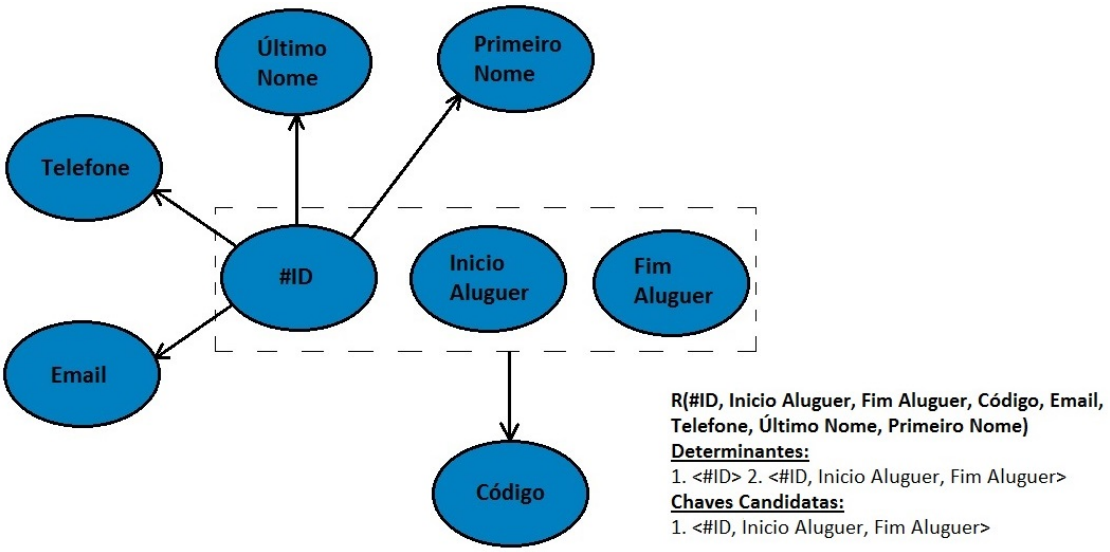

Figura 4.26: Diagrama da relação universal dos diferentes dados recolhidos.

Na relação universal verifica-se que um dos determinantes compreende unicamente o valor "#ID". A primeira sub relação (R1) consiste nas dependências funcionais existentes entre esse atributo e os outros, pois para cada "#ID" existe "um e apenas um" "Email", "Telefone", "Último Nome" e "Primeiro Nome". Deste modo o número de identificação ("#ID") de um cliente encontra-se exclusivamente associado aos dados deste, permitindo assim identificá-lo e verificar dados pessoais que ele forneceu no pedido de inscrição.

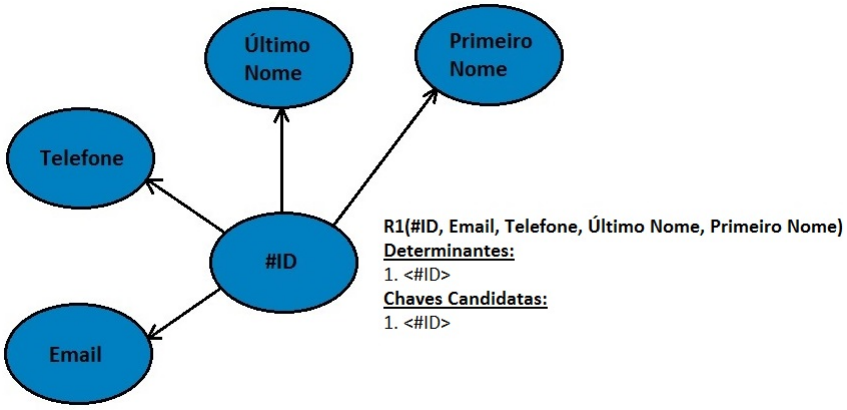

Figura 4.27: Diagrama da primeira sub relação dos diferentes dados recolhidos.

A segunda sub relação (R2) consiste na dependência funcional existente entre o segundo determinante da relação universal e o parâmetro ainda não utilizado. Nesta relação pode-se afirmar que cada "#ID" num período entre "Inicio Aluguer" e "Fim Aluguer" apresenta "um e só um" "Código". Desta forma o número de identificação ("#ID") e as datas escolhidas para o "Inicio Aluguer" e "Fim Aluguer", permitem ao cliente utilizar o seu código de acesso apenas nesse intervalo. O número de identificação permite também associar estes dados de acesso aos dados pessoais do cliente.

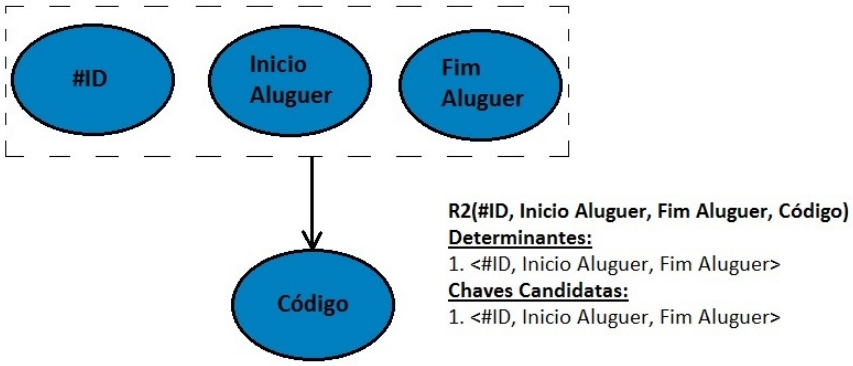

Figura 4.28: Diagrama da segunda sub relação dos diferentes dados recolhidos.

Concluído o processo de normalização verifica-se que é necessário criar duas tabelas normalizadas para permitir uma melhor gestão da base de dados, uma tabela correspondente à sub relação "R1" com os dados pessoais do cliente e outra correspondente à sub relação "R2" com os dados de acesso do cliente. Para facilitar a visualização dos diversos clientes que reservaram o local ao longo do ano na página, esta recorre a estas tabelas para criar uma lista com todas as informações dos clientes em função do seu número de identificação, apresentando todos os valores apenas numa tabela em vez de se criarem duas tabelas distintas.

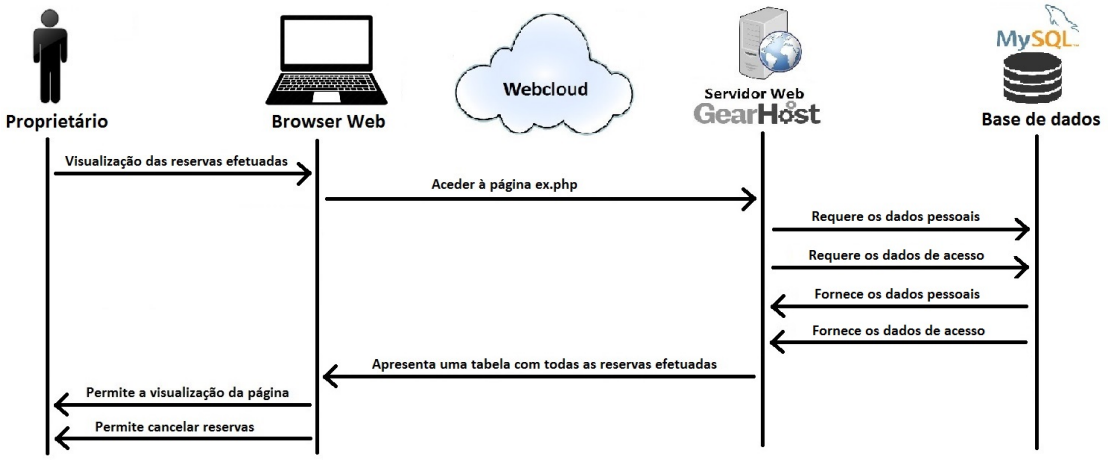

Figura 4.29: Etapas executadas ao aceder à página com a tabela dos clientes.

Na figura 4.30 mostra-se o produto resultante da união das duas tabelas de dados, permitindo assim ao proprietário verificar a afluência de pessoas a frequentar o local. Esta página também permite eliminar clientes das duas tabelas da base de dados caso este queira cancelar a reserva efetuada ou não pague a estadia a tempo, tendo para isso de colocar o seu número de identificação no campo indicado e pressionar o botão "Delete".

Para eliminar uma linha(cliente) da tabela anterior temos de escrever o ID pretendido em baixo.

ID:

Delete

Tabela de clientes

ID	Primeiro Nome	Ultimo Nome	Inicio Aluguer	Fim Aluguer	Codigo	Email	Telefone
1	David	Cardoso	2015-07-31	2015-08-07	123456789	david.cardoso@ua.pt	968635145
4	Client1	C	2015-09-30	2015-10-03	TX8wjARJ	jps@ua.pt	99999999
6	David	C	2015-10-26	2015-11-01	rtcHCfxk	..@ua.pt	999999999
7	David	Card	2015-11-02	2015-11-10	iUGIHU72	@ua.pt	123456789
8	David	Cardoso	2015-11-16	2015-11-22	DZZH30qZ	..@ua.pt	999999999

Figura 4.30: Página com a tabela de clientes que reservaram o local.

4.3 Apresentação do sistema de controlo de acesso desenvolvido

O sistema que foi desenvolvido consiste na inclusão do módulo ESP8266 no circuito de uma fechadura elétrica, de modo a permitir o acesso apenas aos clientes que forem inscritos pelo proprietário através do *site*.

Para o correto funcionamento do sistema deve-se escolher o método de codificação a ser utilizado no processo de programação e atualizar o software do mesmo. Depois da atualização, utilizando o programa adequado é enviado o código desenvolvido para o módulo, permitindo bloquear o acesso a cliente que não tenha a palavra-chave certa para esse dia. No apêndice B encontram-se explicadas as diferentes etapas a ser usadas na programação do módulo e exemplos de código a enviar.

O cliente para conseguir aceder ao local terá de aceder a duas páginas criadas no módulo, uma para inserir o código e outra para voltar a bloquear o acesso. O módulo para verificar se o código inserido é o correto, necessita de se conectar a um rede Wi-Fi para permitir que este consiga aceder à base de dados onde o código se encontra guardado e compará-lo ao inserido pelo cliente. O módulo gera uma rede Wi-Fi, que possibilita ao cliente ao se conectar a esta aceder às páginas de acesso criadas pelo módulo. O cliente pode aceder à rede utilizando um computador, um tablet ou um telemóvel, desde que o dispositivo possua a função que permita utilizar a tecnologia Wi-Fi.

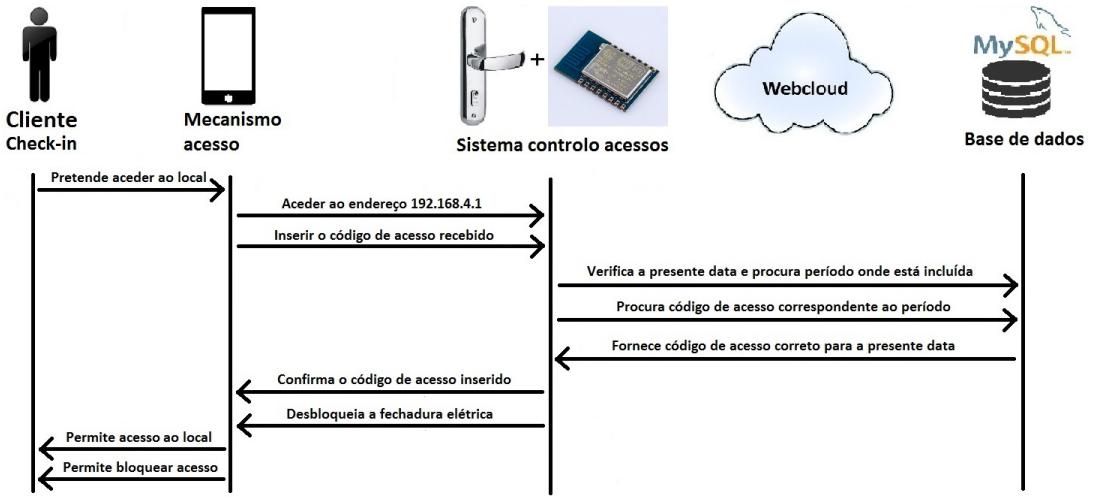

Figura 4.31: Etapas executadas para o cliente conseguir aceder ao local.

O dispositivo mais apropriado para aceder ao local é o telemóvel, uma vez que este é o mais pequeno e leve, permitindo conectar-se à rede disponibilizada pelo módulo. Deste modo o cliente consegue ter a autonomia necessária para não ter de requisitar na receção um cartão ou a chave.

Para uma melhor demonstração dos passos que o cliente deve seguir para aceder ao local utiliza-se um computador, pois permite obter imagens com melhor qualidade. Para aceder à rede criada pelo módulo, deve-se procurar uma denominada "ESPDC" (figura 4.32) e inserir a palavra-chave definida. A rede do módulo pode também ser livre, ou seja, sem palavra-chave, sendo isto definido consoante a vontade do proprietário do local.

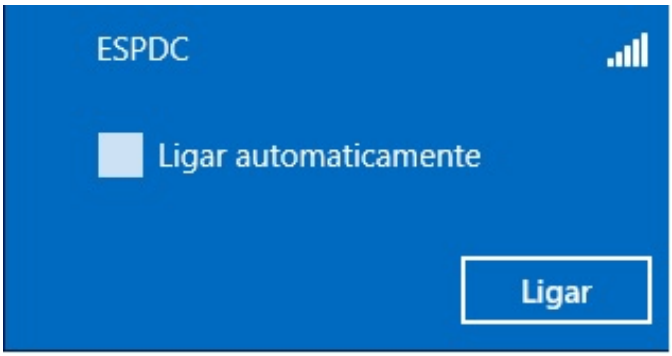

Figura 4.32: Rede Wi-Fi do modo, visualizada num computador.

Após se aceder à rede que o módulo disponibiliza pode-se aceder à primeira página web criada no módulo ESP8266 ao colocar o endereço IP do módulo (192.168.4.1) no endereço de um navegador de Internet, neste caso utilizou-se o Opera pois apresenta uma velocidade superior ao Mozilla Firefox. A figura 4.33 apresenta a página inicial onde o cliente tem de colocar o seu código de acesso para poder aceder ao local alugado.

Figura 4.33: Página inicial do módulo ESP8266, ao colocar 192.168.4.1 no endereço.

Na figura 4.34 apresenta-se a mensagem criada para quando cliente se enganou a introduzir o código de acesso, permitindo que este volte a tentar.

Figura 4.34: Mensagem apresentada ao colocar o código errado.

Caso o código introduzido esteja correto, a fechadura será ativada e permite o acesso ao local durante quinze segundos. Após este intervalo de tempo a fechadura bloqueia novamente, aparecendo a página apresentada na figura 4.35 que permite, pressionado o primeiro botão, ativar a fechadura novamente caso seja necessário ou bloquear o acesso ao pressionar o botão "Sair", anulando o código inserindo e redirecionando para a página inicial.

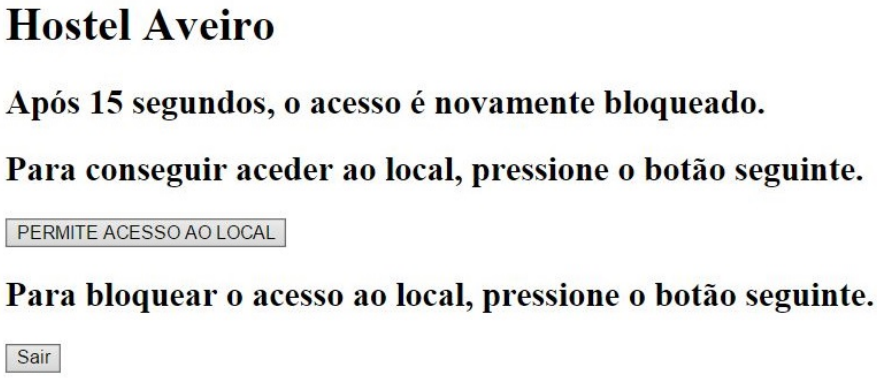

Figura 4.35: Segunda página criada, acesso permitido após colocar o código correto.

Capítulo 5

Considerações Finais

5.1 Conclusões

O trabalho realizado consistiu na pesquisa de uma maneira de melhorar o sistema utilizado nos hosteis e arrendamento de apartamentos, permitindo a redução de custos, removendo a necessidade de o proprietário se deslocar ao apartamento para entregar as chaves e reduzir o tempo de funcionamento da receção, uma vez que o cliente não necessita de se deslocar a esta para efetuar o *check-in*.

Durante a fase de pesquisa verificou-se que existem diversas tecnologias a serem utilizadas para diferentes propósitos, que poderiam ser adaptadas a um sistema de controlo de acesso de um determinado espaço. O mecanismo mais usado é a chave sendo por isso necessário replicar a mesma para permitir a entrada de diversas pessoas ou o cliente terá de receber a chave ao fazer o *check-in* e entrega-la ao fazer o *check-out* para esta estar disponível para o cliente seguinte. Os cartões magnéticos ou *tags* RFID apresentam o mesmo problema das chaves e tornam-se mais caros, uma vez que se tem de introduzir o leitor na entrada do espaço a aceder. Existem também uns sistemas mais complexos que permitem uma maior segurança ao serem introduzidas certas caraterísticas físicas do cliente na sua identificação, permitindo uma segurança muito mais elevado relativamente aos outros mecanismos mas são também muito mais caros e não existe a necessidade deste tipo de identificação no arrendamento de apartamentos ou hosteis.

Para remover a necessidade de se deslocar à receção ou esperar pelo proprietário para receber o mecanismo de acesso, foi desenvolvido um sistema que utiliza a tecnologia Wi-Fi para a troca de dados entre o cliente e a fechadura. A fechadura permite aceder ao espaço reservado após ser introduzido um código de acesso através de um dispositivo pessoal como o telemóvel ou tablet, podendo o cliente deslocar-se diretamente ao espaço sem ter de passar pela receção. Para o cliente conseguir obter o código terá de se inscrever no site desenvolvido e esperar que o proprietário confirme a sua inscrição. Só depois de receber o código é que o cliente se pode deslocar ao espaço e introduzir este nas páginas criadas no módulo ESP8266 que foi integrado no sistema desenvolvido, este verifica se o código corresponde ao período correto e poderá autorizar o acesso ao espaço que reservou.

O sistema desenvolvido permitiu cumprir os objetivos do trabalho, uma vez que com este sistema o cliente não depende de terceiros para conseguir aceder ao espaço, tendo apenas de efetuar a reserva a partir do site. Outro dos objetivos consistia na redução de custos nos hosteis e no arrendamento de apartamentos, tendo este também sido realizado porque este sistema permite a redução da carga horário da receção dos hosteis e a redução

do consumo de combustível e tempo utilizado pelo proprietário ao ter de se deslocar ao espaço para entregar as chaves no caso dos apartamentos. Sendo o módulo relativamente barato permite também reduzir os custos em comparação com os sistemas com leitores de *tags* RFID ou cartões magnéticos.

Por fim, realçar que o desenvolvimento deste sistema e a sua implementação permitiu adquirir novos conhecimentos em áreas onde estes praticamente não existiam, e aprofundar aqueles que já haviam com ideias mais definidas.

5.2 Trabalhos Futuros

Durante o desenvolvimento do sistema de controlo de acessos apresentado, foram surgindo algumas ideias que devido à falta de tempo não conseguiram ser aplicadas nesta dissertação, ficando aqui algumas delas para serem analisadas e aplicadas em trabalhos futuros:

- Integração do sistema desenvolvido com o o site Booking, permitindo ao cliente efetuar a reserva e obter o código de acesso ao fazer o registo no site. Para obter o código este terá de ser gerado e introduzido numa base de dados, podendo esta estar incluída no site ou, caso o proprietário não pretenda disponibilizar os códigos, ser uma base de dados pessoal criada e apenas acessível por determinadas entidades.

- Desenvolvimento de uma página que permita verificar se o cliente efetuou o pagamento e que tenha integrado um software que permita gerar a fatura automaticamente. Deste modo, o código de acesso poderia ser apenas gerado e enviado após a confirmação do pagamento efetuado, e o cliente ficaria com a possibilidade de ter uma fatura comprovativa do pagamento em formato digital e em papel.

- Adaptar o sistema desenvolvido a unidades hoteleiras, substituindo os cartões magnéticos como mecanismo de acesso. Devido à elevada quantidade de quartos, o site desenvolvido tornar-se-ia muito pesado e confuso para efetuar os registos, no entanto, pode-se utilizar os módulos para permitir aos clientes acederem aos quartos que reservaram. Utilizando uma página que permita definir o código de acesso em cada quarto, não existe a necessidade de programar os cartões e o cliente não precisa de deixar o cartão na receção sempre que pretender ir dar uma volta, podendo utilizar o telemóvel para introduzir o código e aceder ao seu quarto.

- Implementação de um mecanismo de segurança na rede Wi-Fi criada pelo módulo, de modo a permitir uma maior proteção do espaço disponibilizado pelo proprietário e uma interação mais fiável entre o cliente e a fechadura inteligente.

Bibliografia

[1] [autor desconhecido] - Turismo de Portugal, I.P. - Quadros estatísticos [on-line]. Citado em 2015-10-27. Disponível em: <http://www.turismodeportugal.pt/Portugu%C3%AAs/ProTurismo/estat%C3%ADsticas/quadrosestatisticos/Pages/Quadrosestat%C3%ADsticos.aspx>

[2] MOREIRA, Pedro Alexandre - Gestão de Controlo de Acessos. Porto: Faculdade de Engenharia da Universidade do Porto, 2008. Dissertação de Mestrado em Engenharia Eletrotécnica e de Computadores.

[3] CARDOSO, César Filipe Duarte - Controlo de Acessos. Aveiro: Departamento de Engenharia Mecânica da Universidade de Aveiro, 2013. Dissertação de Mestrado em Engenharia Mecânica.

[4] [autor desconhecido] - ID KEY 2 | Idonic Access [on-line]. Citado em 2015-10-14. Disponível em: <http://www.controlo-acessos.com.pt/?attachment_id=516>

[5] [autor desconhecido] - Barcode [on-line]. Citado em 2015-10-14. Disponível em: <http://en.wikipedia.org/wiki/Barcode>.

[6] [autor desconhecido] - Barcoding Frequently Asked Questions (FAQ) [on-line]. Citado em 2015-10-14. Disponível em: <http://www.barcodesinc.com/faq/>

[7] GS1. The GS1 Traceabilitty Standard: What you need to know. GS1, 2007.

[8] [autor desconhecido] - Controlo de acessos [on-line]. Citado em 2015-10-14. Disponível em: <http://www.tecnicontrol.pt/pt/wiki/item.html?id=52-controlo-de-acessos>

[9] [autor desconhecido] - Barcode FAQ Bar Code Frequently Asked Questions [on-line]. Citado em 2015-10-14. Disponível em: <http://www.azalea.com/barcode-faq/>

[10] GS1. GS1 Identifcation Key Series GTIN (Global Trade Item Number). GS1, June 2009.

[11] BRAIN, Marshall - How UPC Bar Codes Work - HowStuffWorks. Citado em 2015-10-14. Disponível em: < http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/upc.htm>

[12] [autor desconhecido] - EAN-13 - Wikipédia, a enciclopédia livre [on-line]. Citado em 2015-10-14. Disponível em: <http://pt.wikipedia.org/wiki/EAN-13>

[13] [autor desconhecido] - International Article Number (EAN) - Wikipedia, the free encyclopedia [on-line]. Citado em 2015-10-14. Disponível em: <https://en.wikipedia.org/wiki/International_Article_Number_%28EAN%29>

[14] [autor desconhecido] - PDF417 [on-line]. Citado em 2015-10-14. Disponível em: <http://en.wikipedia.org/wiki/PDF417>

[15] ISO/IEC 15438:2006(E) - Information technology ? Automatic identification and data capture techniques ? PDF417 bar code symbology specification. INTERNATIONAL STANDARD, Second edition 2006-06-01.

[16] [autor desconhecido] - Data Matrix [on-line]. Citado em 2015-10-14. Disponível em: <http://en.wikipedia.org/wiki/Data_Matrix>

[17] GS1. GS1 DataMatrix Guideline. Overview and technical introduction to the use of GS1 DataMatrix. GS1, July 2015.

[18] [autor desconhecido] - Identificação por radiofrequência [on-line]. Citado em 2015-10-14. Disponível em: <http://pt.wikipedia.org/wiki/Identifica%C3%A7%C3%A3o_por_radiofrequ%C3%AAncia>

[19] POOLE, Ian - What is RFID | Radio Frequency Identification [on-line]. Citado em 2015-10-14. Disponível em: <http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/technology-tutorial-basics.php>

[20] [autor desconhecido] - ProxNC A60-Proximidade RFID [on-line]. Citado em 2015-10-14. Disponível em: <http://www.ncontrol.com.pt/produtos/controlo-de-acessos/proxnc-100-proximidade-rfid-62-68-74-detail.html>

[21] [autor desconhecido] - RFID Labelling Solutions | CSols Ltd. [on-line]. Citado em 2015-10-14. Disponível em: <http://www.csols.com/wordpress/tag/rfid-labelling-solutions/>

[22] VIOLINO, Bob - A Summary of RFID Standards RFID Journal [on-line]. Disponível em: <http://www.rfidjournal.com/articles/view?1335/>.

[23] POOLE, Ian - RFID Standards - details of the RFID standards including the ISO RFID standards (inc ISO 18000) and EPCglobal standards used to specify and standardise RFID systems and elements. [on-line]. Disponível em: <http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/iso-epcglobal-iec-standards.php>

[24] WOMACK, Elizabeth - RFID - Saving the World One Tag at a Time [on-line]. Citado em 2015-10-14. Disponível em: <http://telaeris.com/2012/01/rfid-saving-the-world-one-tag-at-a-time/>

[25] [autor desconhecido] - About Near Field Communication [on-line]. Citado em 2015-10-14. Disponível em: <http://www.nearfieldcommunication.org/about-nfc.html>

[26] ISO/IEC FCD 14443-1 - Identification cards ? Contactless integrated circuit(s) cards ? Proximity cards ? Part 1: Physical characteristics. INTERNATIONAL STANDARD 1997.

[27] ISO/IEC 14443-2:2001(E) - Identification cards ? Contactless integrated circuit(s) cards ? Proximity cards ? Part 2: Radio frequency power and signal interface. INTERNATIONAL STANDARD, First edition 2001-07-01.

[28] ALECRIM, Emerson - O que é NFC (Near Field Communication)? [on-line]. Citado em 2015-10-14. Disponível em: <http://www.infowester.com/nfc.php>

[29] POOLE, Ian - NFC Modulation & RF Signal [on-line]. Citado em 2015-10-14. Disponível em: <http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-modulation-rf-signal-interface.php>

[30] [autor desconhecido] - Terminal RFID de controlo de acessos NFC (Near Field Communication) - Kimaldi [on-line]. Citado em 2015-10-14. Disponível em: <http://www.kimaldi.com/kimaldi_por/produtos/controlo_de_acessos/sistemas_off_line/terminal_rfid_de_controlo_de_acessos_nfc_near_field_communication>

[31] WILSON, Tracy V. - "How Biometrics Works" 11 Novembro 2005. HowStuffWorks.com [on-line]. Citado em 2015-10-14. Disponível em: <http://science.howstuffworks.com/biometrics.htm>

[32] [autor desconhecido] - BioNC A30 - Impressão Digital [on-line]. Citado em 2015-10-14. Disponível em: <http://www.ncontrol.com.pt/produtos/controlo-de-acessos/bionc-a90-impress%C3%A3o-digital-71-detail.html>

[33] [autor desconhecido] - FaceNC A400 - Leitura de Face [on-line]. Citado em 2015-10-14. Disponível em: <http://www.ncontrol.com.pt/produtos/controlo-de-ponto/facenc-a400-leitura-de-face-detail.html>

[34] BONSOR, Kevin; JOHNSON, Ryan - How Facial Recognition Systems Work - HowStuffWorks [on-line]. Citado em 2015-10-14. Disponível em: <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>

[35] [autor desconhecido] - Wavestore | Identify, track and compare individuals [on-line]. Citado em 2015-10-14. Disponível em: <http://www.wavestore.com/technologies/analytics/facial-recognition>

[36] CALDWELL, Tracey - Safety in the palm of your hand - Business Technology [on-line]. Citado em 2015-10-14. Disponível em: <http://business-technology.co.uk/2012/04/safety-in-the-palm-of-your-hand/>

[37] PEREIRA, João de Freitas - IMPRESSÃO DIGITAL - JOÃO DE FREITAS PEREIRA - BELO HORIZONTE [on-line]. Citado em 2015-10-14. Disponível em: <http://www.joaodefreitas.com.br/impressao-digital.htm>

[38] BRAIN, Marshall; JOHNSON, Bernadette; WILSON, Tracy V. - How WiFi Works - HowStuffWorks [on-line]. Citado em 2015-10-20. Disponível em: <http://computer.howstuffworks.com/wireless-network.htm>

[39] [autor desconhecido] - What is Wi-Fi ? [on-line]. Citado em 2015-10-20. Disponível em: <http://www.tutorialspoint.com/wi-fi/what_is_wifi.htm>

[40] BEAL, Vangie - What is 802.11 Wireless LAN Standards? Webopedia Definition [on-line]. Citado em 2015-10-20. Disponível em: <http://www.webopedia.com/TERM/8/802_11.html>

[41] SMITH, Matt - Understanding The Common WiFi Standards [Technology Explained] [on-line]. Citado em 2015-10-20. Disponível em: <http://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/>

[42] ALECRIM, Emerson - O que é Wi-Fi (IEEE 802.11)? [on-line]. Citado em 2015-12-14. Disponível em: <http://www.infowester.com/wifi.php>

[43] [autor desconhecido] - ZigLock Hotel - Sistema de acesso para hotéis por biometria e comunicação sem fio [on-line]. Citado em 2015-10-20. Disponível em: <http://www.acura.com.br/case-rwtech2.php>

[44] [autor desconhecido] - Kaba fechaduras para hotéis [on-line]. Citado em 2015-06-29. Disponível em: <http://www.kaba.pt/produtos-e-solucoes/50838/fechaduras-de-hotel.html>

[45] Kaba Lodging Systems® - The Oracode Solution - Access Control for Rental Properties. Citado em 2015-10-20. Disponível em: <www.kabalodging.com/oracode>

[46] CARDOSO, David - Controlo de Acessos. Disponível em: http://acess.gear.host/

[47] SANTOS, José P. - Capítulo 12: Base de Dados. Aveiro: Universidade de Aveiro - Informática Industrial(2010/2011).

[48] [autor desconhecido] - Radio-frequency identification - Wikipedia, the free encyclopedia [on-line]. Citado em 2015-06-29. Disponível em: <http://en.wikipedia.org/wiki/Radio-frequency_identification#Tags>

[49] [autor desconhecido] - SM130 [on-line]. Citado em 2015-06-29. Disponível em: <http://www.sonmicro.com/en/index.php?option=com_content&view=article&id=57&Itemid=70>

[50] [autor desconhecido] - 13.56 MHz RFID MIFARE - SUPPORT [on-line]. Citado em 2015-06-29. Disponível em: <http://www.sonmicro.com/en/index.php?option=com_content&view=article&id=61&Itemid=74>

[51] [autor desconhecido] - Código para programação do módulo ESP8266 com comandos AT [on-line]. Citado em 2015-06-29. Disponível em: <http://www.joostaanen.com/RFID/SM130/Firmware/i2c_28_b1.rme>

[52] [autor desconhecido] - Ascii Table - ASCII character codes and html, octal, hex and decimal chart conversion [on-line]. Citado em 2015-06-29. Disponível em: <http://www.asciitable.com/>

[53] [autor desconhecido] - ESP8266 Firmware and SDK [on-line]. Citado em 2015-09-28. Disponível em: <http://www.electrodragon.com/w/ESP8266_Firmware#Customized_AT-thinker_Firmware>

[54] [autor desconhecido] - NodeMCU API Instruction [on-line]. Citado em 2015-09-28. Disponível em: <https://github.com/nodemcu/nodemcu-firmware/wiki/nodemcu_api_en>

[55] [autor desconhecido] - NodeMCU Docs | node module [on-line]. Citado em 2015-09-28. Disponível em: <http://www.nodemcu.com/docs/node-module/>

[56] [autor desconhecido] - Arduino - Software [on-line]. Citado em 2015-09-28. Disponível em: <https://www.arduino.cc/en/Main/Software>

[57] [autor desconhecido] - Pacotes de dados para programação do módulo ESP8266 com Arduino IDE [on-line]. Citado em 2015-09-28. Disponível em: <http://arduino.esp8266.com/stable/package_esp8266com_index.json>

[58] [autor desconhecido] - ESP8266 Arduino Core [on-line]. Citado em 2015-09-28. Disponível em: <http://arduino.esp8266.com/versions/1.6.5-947-g39819f0/doc/reference.html>

Apêndices

Apêndice A

Trabalho RFID

Neste apêndice apresenta-se o trabalho realizado com a tecnologia RFID e explica-se o funcionamento de programa SMRFID Mifare v1.2 e os diferentes passos a seguir para se conseguir ler as diferentes *tags* com o mesmo.

A.1 RFID

Tal como explicado na secção 2.2.3 do capítulo 2, a identificação por radiofrequência consiste na transferência de dados entre um leitor e uma etiqueta através de campos eletromagnéticos, onde a etiqueta serve para identificar o objeto ou pessoa e o leitor permite a verificação da identidade introduzida nessa etiqueta e atualizar as informações que ela contem. Este processo não necessita de fios, permitindo ao leitor obter as informações pretendidas mesmo que a etiqueta não esteja no seu campo de visão ou se encontre a alguma distância. Existem etiquetas que recebem energia por indução eletromagnética a partir dos campos magnéticos do leitor, e outras que possuem uma fonte de energia interna, permitindo um maior alcance. As *tags* utilizadas podem ser de escrita e leitura ou apenas de leitura, ou seja, elas podem permitir introduzir mais informação durante etapas que realizam ou apenas servir para identificar o produto em cada etapa [48].

Figura A.1: Exemplos de *tags*.

A.2 Configuração Eletrónica

Para a leitura das etiquetas RFID vamos utilizar o módulo SM130 (figura A.2) a comunicar com o programa SMRFID Mifare v1.2 no computador através de comunicação Rs232, realizada por um conversor USB para Rs232.

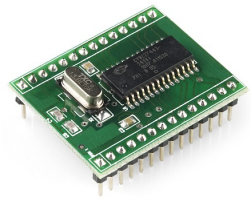

Figura A.2: Módulo SM130.

De modo a permitir a utilização de uma fonte de alimentação de 5V, recorre a um conversor de nível MAX232, isto transforma os sinais RX, TX, CTX e RTS de uma porta serial em sinais adequados para uso em circuitos microprocessados. A figura A.3 mostra as ligações necessárias para o correto funcionamento do MAX232.

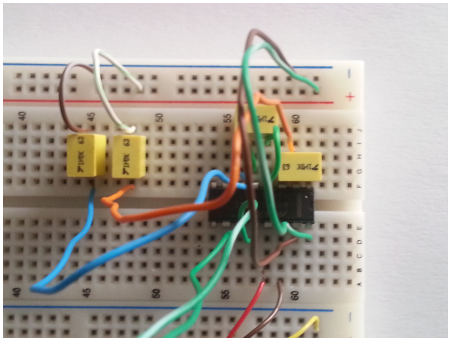

Figura A.3: Ligações Max232.

O cabo DB9 macho (cabo esquerdo da figura A.4) encontra-se ligado ao computador, estando o cabo DB9 fêmea encaixado no DB9 macho, como mostra a figura A.4, e ao MAX232.

Figura A.4: Ligação macho-fêmea DB9.

O módulo SM130 é um DIP (*dual in-line package*) de 28 pinos compacto que inclui todos os componentes necessário para um Leitor/Programador 13,56 MHz RFID Mifare com exceção de uma antena PCB [49]. A figura A.5 apresenta as ligações efetuadas no módulo.

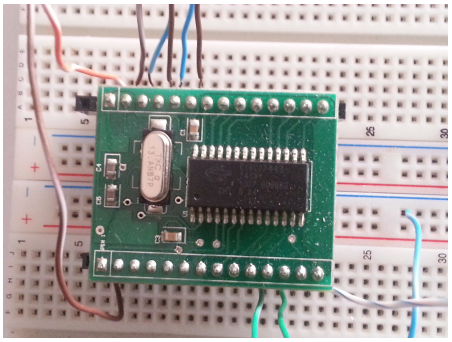

Figura A.5: Ligações do módulo SM130.

Na figura A.6 temos o esquema elétrico correspondente a todas as ligações efetuadas entre o MAX232 e o módulo SM130. Com esta configuração podemos instalar o *firmware* necessário e aceder ao módulo através do programa SMRFID Mifare v1.2.

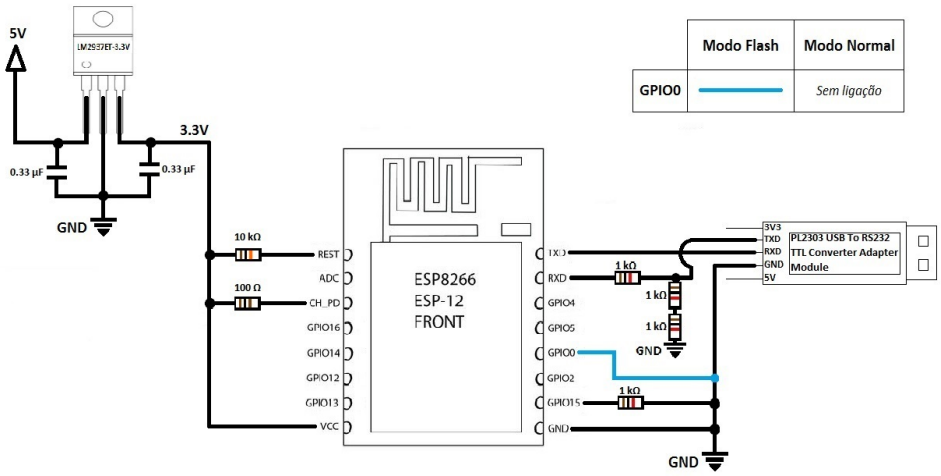

Figura A.6: Esquema elétrico das ligações do módulo SM130 e MAX232.

Para o módulo conseguir aceder aos dados das *tags* temos de lhe ligar uma antena PCB, tal como mostra a figura A.7.

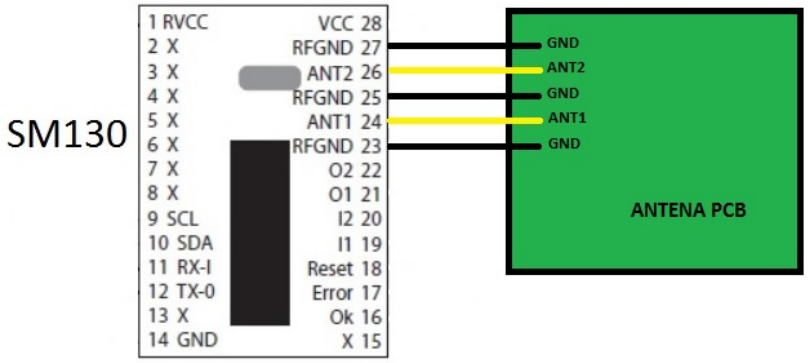

Figura A.7: Esquema da ligação entre o módulo e a antena.

Mantendo as restantes ligações, ligamos o módulo SM130 à antena incorporada no SparkFun RFID Evaluation Shield - 13.56MHz. Na figura A.8 estão as ligações efetuadas para permitir a leitura dos dados existentes nas etiquetas RFID.

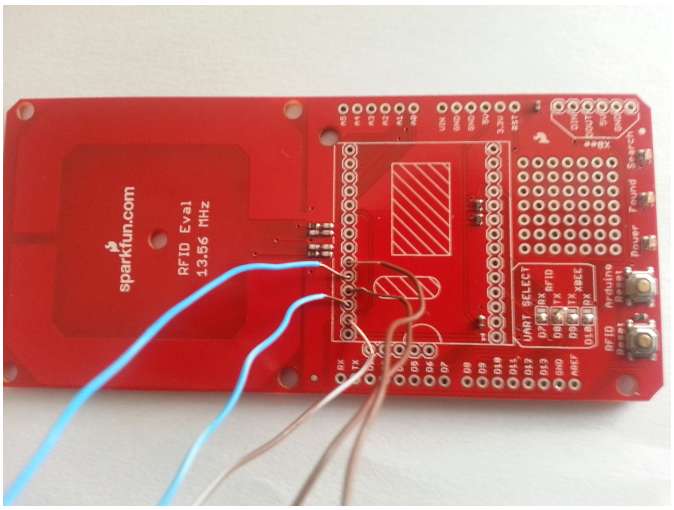

Figura A.8: Ligações efetuadas com a antena.

A.3 Leitura das *tags*

A.3.1 Passo 1 - Atualização do firmware

Para comunicar com o módulo, recorreu-se a dois programas disponibilizados pela Son-Micro [50] , o SMRFID Mifare v1.2 e o SMRFID_FU. Após a descarga do firmware de atualização da comunicação I2C do módulo de [51], utilizamos o programa SMRFID_FU para atualizar o SM130, tal como mostra a figura A.9. Deve-se verificar se a porta é a correta (COM4 no meu caso) e definir o valor do BaudRate como 19200 bps.

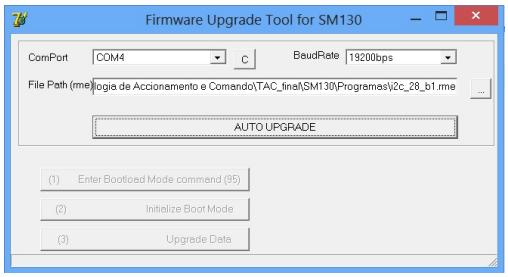

Figura A.9: 1º Passo - Programa de atualização do firmware (SMRFID_FU).

A.3.2 Passo 2 - Configurações iniciais

Após a atualização do firmware, podemos utilizar o programa SMRFID Mifare v1.2 para interagir com o módulo.

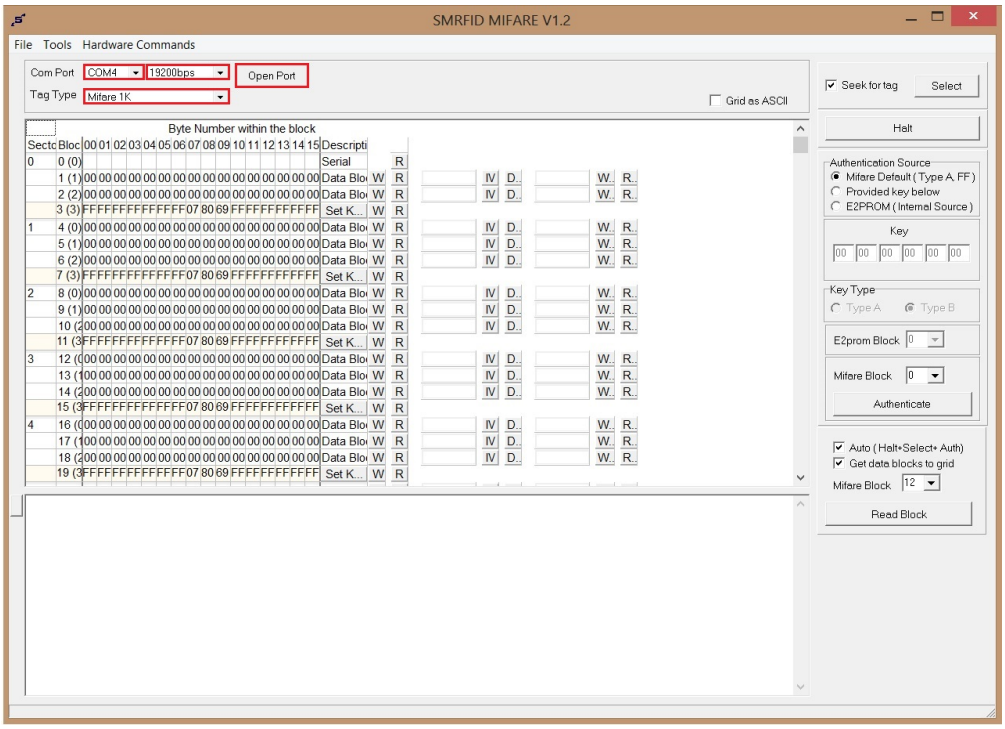

Figura A.10: 2º Passo - Configurações iniciais.

Inicialmente temos de configurar a porta série (COM4), o BaudRate (19200bps) e o tipo de *tag* (Mifare 1K), partes assinaladas na figura A.10. Após a configuração dos parâmetros anteriores, pressionamos o botão "Open Port", devendo este mudar para "Close Port" caso consiga comunicar com o módulo.

A.3.3 Passo 3 - SM130 Address

Após as configurações iniciais, efetua-se a procura do endereço Slave do módulo, utilizando o menu "Hardware Commands" e seleccionando o "Read I2C Address", como mostra a figura A.11. Se o valor enviado pelo módulo for 0x42 (valor default), podemos passar ao passo seguinte, caso contrário devemos seleccionar o "Set I2C Address" do menu anterior, e definir o endereço com o valor default.

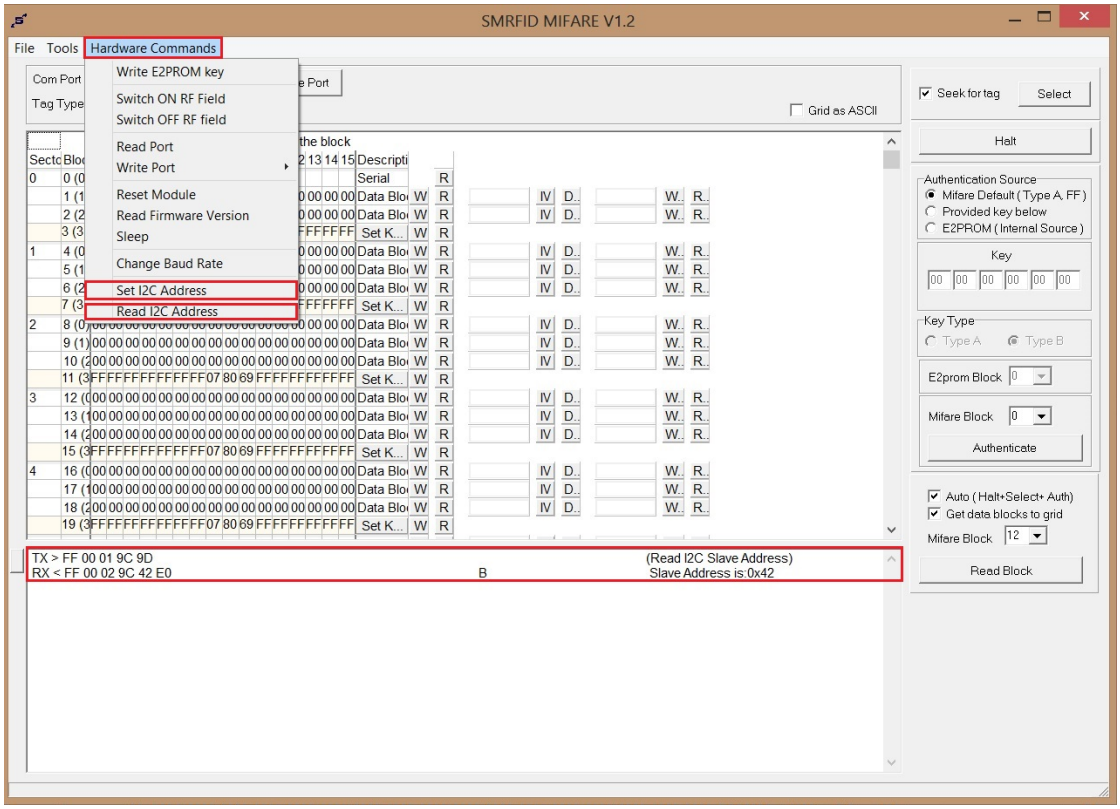

Figura A.11: 3º Passo - Endereço I2C do módulo.

Na figura A.11 temos os comandos enviados e a resposta recebida na caixa assinalada a vermelho. O comando para ler o endereço é "01 9C 9D", onde:

- 01 é o comprimento da mensagem a enviar;
- 9C é o comando de leitura do endereço;
- 9D é o checksum (01+9C = 9D);

A resposta recebida foi "02 9C 42 E0" onde:

- 02 é o comprimento da mensagem recebida;
- 9C é o comando de leitura do endereço;
- 42 é o endereço Slave do módulo (0x42);
- E0 é o checksum (02+9C+42 = E0);

A.3.4 Passo 4 - Selecionar *tag*

Depois da configuração do endereço Slave do módulo SM130, vamos selecionar a etiqueta que pretendemos alterar ou ler. Para este efeito recorremos ao botão "Select" assinalado na figura A.12. Ao pressionar o botão este envia o comando para o módulo, ficando o módulo à espera que se passe uma *tag* pela antena utilizada. Assim que a etiqueta é detetada o módulo envia uma resposta com as informações da etiqueta.

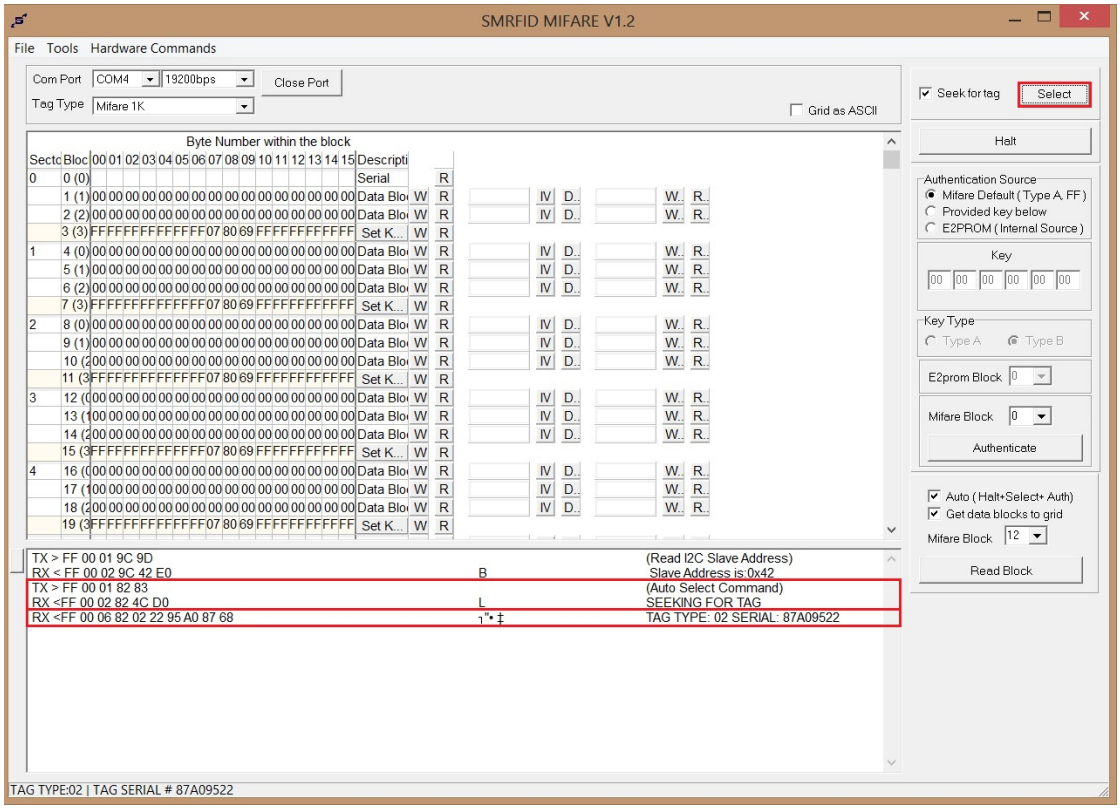

Figura A.12: 4º Passo - Seleção de uma *tag*.

Na figura A.12 apresentam-se os comandos enviados e as respostas recebidas do módulo nas caixas assinaladas a vermelho. O comando para selecionar a *tag* é "01 82 83", onde:

- 01 é o comprimento da mensagem a enviar;
- 82 é o comando de procura da *tag*;
- 83 é o checksum (01+82 = 83);

A primeira resposta recebida significa que o módulo SM130 se encontra à procura de uma etiqueta ("SEEKING FOR TAG" como mostra a figura A.12). Os valores apresentados foram "02 82 4C D0" onde:

- 02 é o comprimento da mensagem recebida;
- 82 é o comando de procura da *tag*;
- 4C significa que o comando anterior está a ser efetuado;
- D0 é o checksum (02+82+4C = D0);

A segunda resposta corresponde às informações recolhidas da etiqueta pelo módulo. Os valores da resposta foram "06 82 02 22 95 A0 87 68" onde:

- 06 é o comprimento da mensagem recebida;
- 82 é o comando de procura da *tag*;
- 02 é o tipo de *tag* encontrada (02 - Mifare Standard 1K);
- 22 é o último elemento do número de série da *tag* encontrada;
- 95 é o penúltimo elemento do número de série da *tag* encontrada;
- A0 é o segundo elemento do número de série da *tag* encontrada;
- 87 é o primeiro elemento do número de série da *tag* encontrada;
- 68 é o checksum (06+82+02+22+95+A0+87 = 268);

Como podemos verificar na figura A.12 a etiqueta encontrada é do tipo 1K e tem o número de série 87 A0 95 22.

A.3.5 Passo 5 - Autenticar a *tag*

Após selecionar a *tag* temos de realizar a autenticação da mesma. Para concretizar este passo podemos recorrer ao botão "Authenticate" assinalado na figura A.13, sendo enviado para o módulo o comando e a chave de autenticação da etiqueta selecionada. Após o módulo receber a chave e caso esta seja a correta, este envia uma mensagem de confirmação da autenticação.

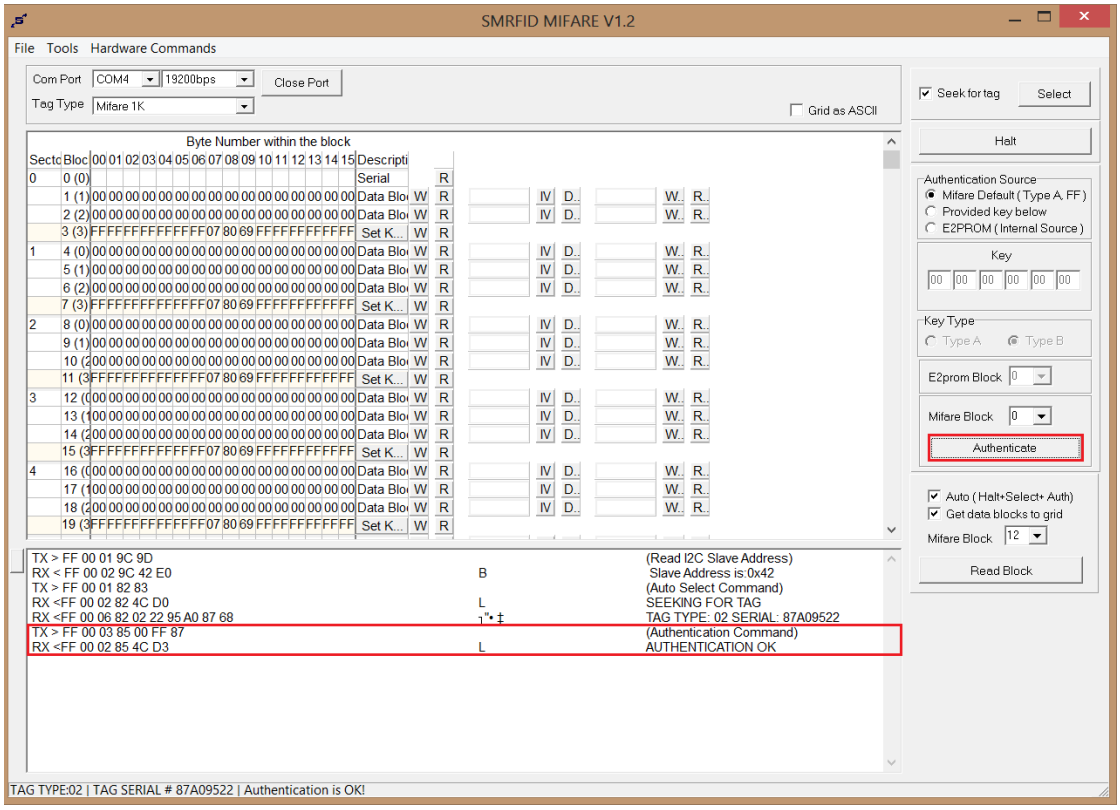

Figura A.13: 5º Passo - Autenticação da *tag*.

Na figura A.13 apresenta-se o comando enviado e a resposta recebida do módulo na caixa assinalada a vermelho. O comando para autenticar a *tag* é "03 85 00 FF 87", onde:

- 03 é o comprimento da mensagem a enviar;
- 85 é o comando de autenticação da *tag* ;
- 00 é a primeira parte da chave de autenticação ;
- FF é a segunda parte da chave de autenticação;
- 87 é o checksum (03+85+00+FF = 1$\underline{87}$);

A resposta recebida significa que o módulo SM130 conseguiu realizar a autenticação corretamente ("AUTHENTICATION OK" como mostra a figura A.13). Os valores apresentados foram "02 85 4C D3" onde:

- 02 é o comprimento da mensagem recebida;
- 85 é o comando de procura da *tag*;
- 4C significa que o comando anterior foi efetuado com sucesso;
- D3 é o checksum (02+85+4C = D3);

A.3.6 Passo 6 - Leitura de um Bloco

Depois de fazer a autenticação da etiqueta podemos ler as informações disponíveis na mesma. Para ler um bloco da *tag* recorremos ao botão "Read Block" e mantemos o visto na checkbox assinalada na figura A.14, deste modo o módulo é pausado, procura uma etiqueta e autentica o bloco a ler da etiqueta antes de enviar o comando de leitura para o módulo. O módulo depois de receber o comando envia uma resposta com o conteúdo do bloco pretendido.

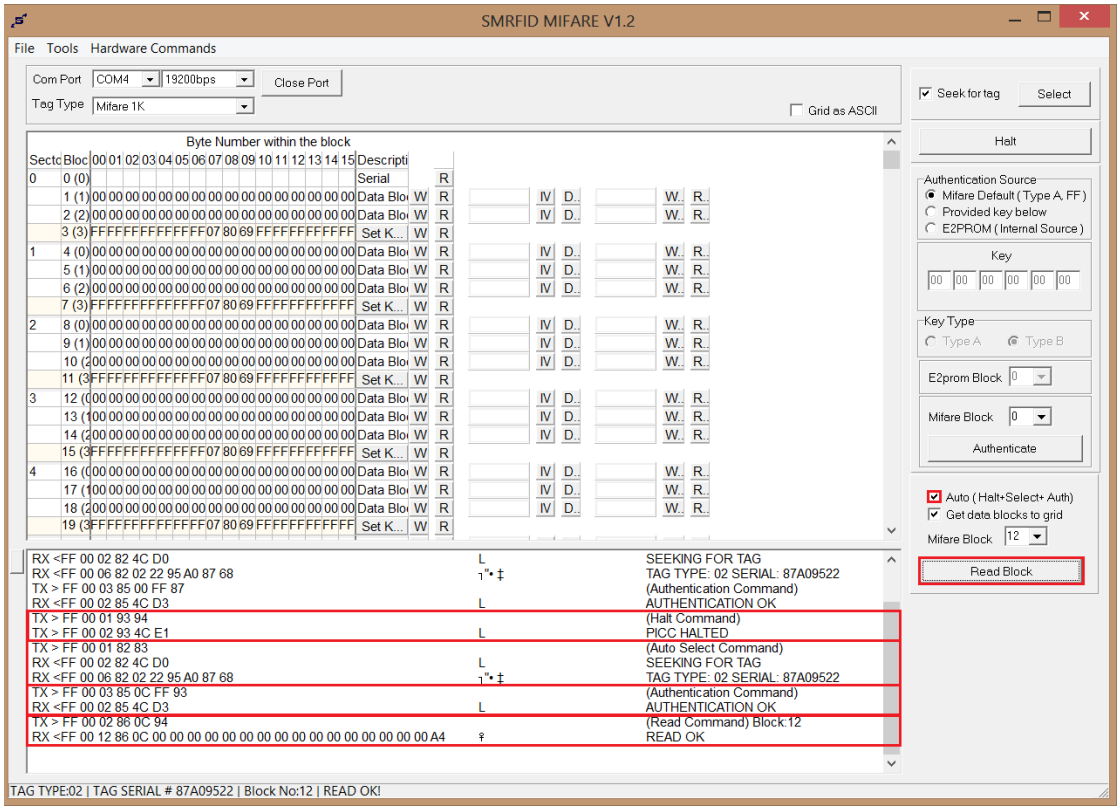

Figura A.14: 6º Passo - Leitura de um bloco da *tag*.

Na figura A.14 apresenta-se os diferentes comandos enviados para a leitura do bloco 12 e as resposta recebidas do módulo nas caixas assinaladas a vermelho. O comando para pausar o módulo é "01 93 94", onde:

- 01 é o comprimento da mensagem a enviar;
- 93 é o comando para pausar o módulo;
- 94 é o checksum (01+93 = 94);

A resposta recebida significa que o módulo SM130 se encontra parado ("PICC HALTED" como mostra a figura A.14). Os valores apresentados foram "02 93 4C E1" onde:

- 02 é o comprimento da mensagem recebida;
- 93 é o comando para pausar o módulo;
- 4C significa que o comando anterior foi efetuado com sucesso;
- E1 é o checksum (02+93+4C = E1);

Os comandos de seleção de *tag* e de autenticação de bloco são enviados como foram descritos anteriormente nos passos 4 e 5, respetivamente.

O comando para ler o bloco 12 da *tag* selecionada é "02 86 0C 94", onde:

- 02 é o comprimento da mensagem a enviar;
- 86 é o comando de leitura de um bloco;
- 0C é o número do bloco a ler (0C corresponde ao bloco 12);
- 94 é o checksum (02+86+0C = 94);

A resposta recebida significa que o módulo SM130 conseguiu realizar a leitura corretamente ("READ OK" como mostra a figura A.14), e envia os dados do bloco pretendido. Os valores apresentados foram "12 86 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A4" onde:

- 12 é o comprimento da mensagem recebida;
- 86 é o comando de leitura de um bloco;
- 0C é o número do bloco a ler (0C corresponde ao bloco 12);
- 16*00 são os 16 bytes de informação existentes no bloco, neste caso o bloco encontra-se vazio;
- A4 é o checksum (12+86+0C+16*00 = A4);

Caso os blocos apresentem dados, ou seja, valores diferentes de 0x00 (em hexadecimal), podemos convertê-los para ASCII utilizando a checkbox assinalada a vermelho na figura A.15. Assim na figura apresento os valores escritos nos blocos 4, 5 e 6 da *tag*, assinalados na mesma a vermelho. Na caixa de comandos podemos verificar os diferentes comandos efetuados e as respostas enviadas pelo módulo para se obterem os dados apresentados.

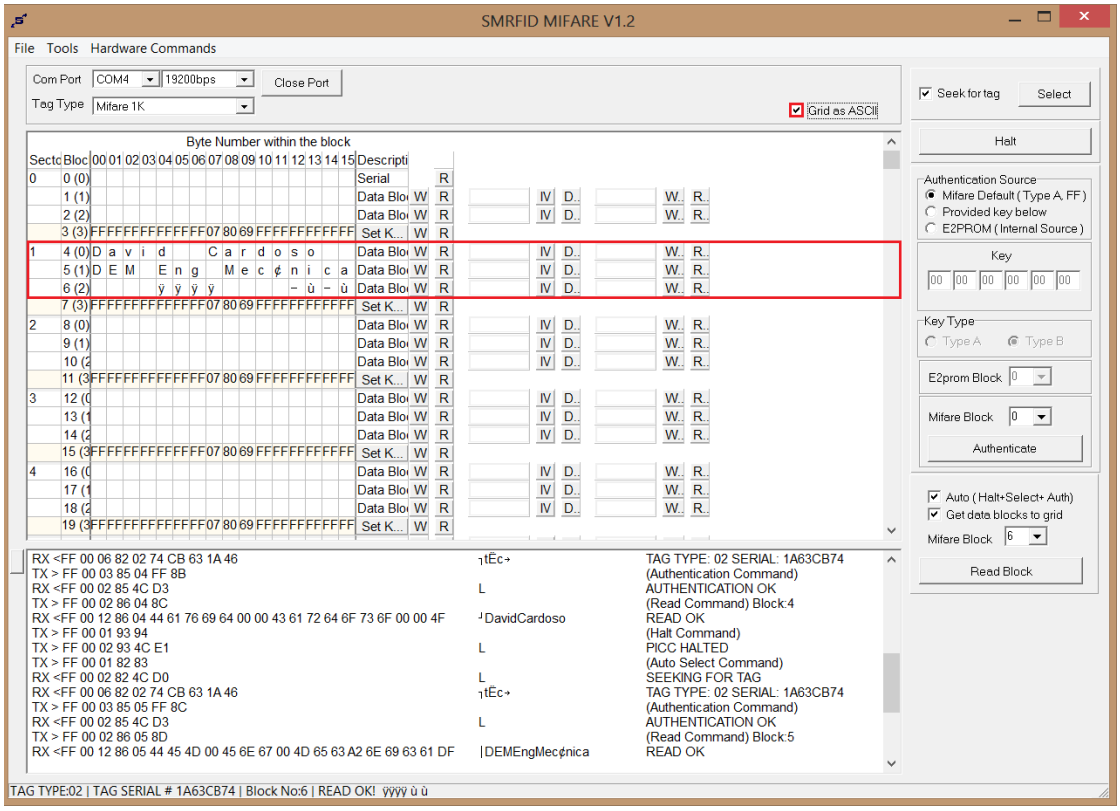

Figura A.15: 6º Passo - Conversão dos dados em ASCII.

Na figura seguinte apresento a tabela de conversão ASCII de modo a permitir perceber a conversão dos valores na caixa de comandos.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Figura A.16: Tabela de conversão ASCII[52].

A.3.7 Passo 7 - Escrever num Bloco

O programa também permite escrever dados nos blocos da *tag* selecionada. Para escrever num bloco da *tag* recorremos ao botão "W" localizado ao lado dos dados no bloco assinalado na figura A.17, deste modo o módulo é pausado, procura uma etiqueta e autentica o bloco a ler da etiqueta antes de enviar o comando de leitura para o módulo. O módulo depois de receber o comando envia uma resposta com o conteúdo enviado para o bloco pretendido.

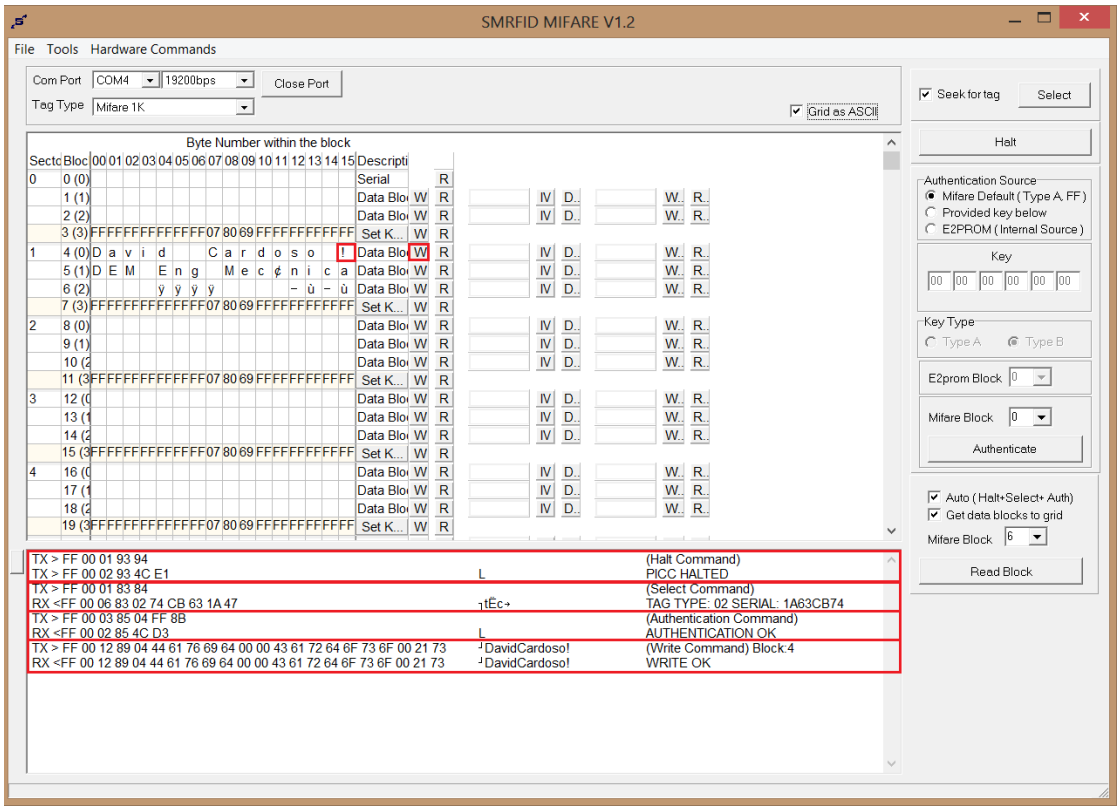

Figura A.17: 7º Passo - Escrita num bloco da *tag*.

Na figura A.17 apresentam-se os diferentes comandos enviados para a escrita do bloco 4 e a resposta recebida do módulo nas caixas assinaladas a vermelho. Após a alteração dos dados do bloco, neste caso acrescentar um "!" no fim do bloco como mostra a figura, pressiona-se o botão. Este depois segue as mesmas etapas descritas no passo anterior, onde pausa o módulo, seleciona a *tag* e autentifica o bloco a escrever antes de enviar o comando para o módulo.

O comando para escrever no bloco 4 da *tag* selecionada é "12 89 04 44 61 76 69 64 00 00 43 61 72 64 6F 73 6F 00 21 73", onde:

- 12 é o comprimento da mensagem a enviar;
- 89 é o comando de escrita de um bloco;
- 04 é o número do bloco a ler;
- 44 é o primeiro byte do bloco 4, com o valor "D";
- 61 é o segundo byte do bloco 4, com o valor "a";
- 76 é o terceiro byte do bloco 4, com o valor "v";
- 69 é o quarto byte do bloco 4, com o valor "i";
- 64 é o quinto byte do bloco 4, com o valor "d";
- 00 é o sexto byte do bloco 4, sem dados;
- 00 é o sétimo byte do bloco 4, sem dados;
- 43 é o oitavo byte do bloco, com o valor "C";
- 61 é o nono byte do bloco, com o valor "a";
- 72 é o décimo byte do bloco, com o valor "r";
- 64 é o décimo primeiro byte do bloco, com o valor "d";
- 6F é o décimo segundo byte do bloco, com o valor "o";
- 73 é o décimo terceiro byte do bloco, com o valor "s";
- 6F é o décimo quarto byte do bloco, com o valor "o";
- 00 é o penúltimo byte do bloco, sem dados;
- 21 é o último byte do bloco, com o valor "!";
- 73 é o checksum (12+89+04+44+61+76+69+64+00+00+43+61+72+64+6F+73+6F+00+21 = 5$\underline{73}$);

A resposta recebida significa que o módulo SM130 conseguiu realizar a escrita corretamente ("WRITE OK" como mostra a figura A.17). Os valores apresentados foram "12 89 04 44 61 76 69 64 00 00 43 61 72 64 6F 73 6F 00 21 73", que são iguais aos valores do comando de leitura.

Apêndice B

Módulo ESP8266

ESP8266 apresenta uma solução completa e independente de rede Wi-Fi, a um preço bastante acessível (entre 3 a 5 euros, dependendo do modelo escolhido).

O módulo ESP8266 possibilita a utilização da rede Wi-Fi como método de comunicação entre dispositivos, sendo isto para recolha ou envio de dados de um dispositivo para outro.

Este módulo apresenta diferentes funções desenvolvidas em diferentes métodos de programação (comandos AT, NodeMCU ou Arduino), que permite que este seja integrado com sensores ou dispositivos específicos a outras aplicações através das saídas GPIOs existentes no módulo (número de GPIOs variam consoante o módulo escolhido).

Com este dispositivo podemos criar uma rede Wi-Fi nova no ESP8266, que apenas irá permitir a comunicação entre o módulo e os dispositivos que acederem à sua rede, ou aceder através deste a uma rede já existente, permitindo a comunicação deste com os outros utilizando essa rede. Neste último caso também é possível recolher uma determinada informação pretendida de alguma página web.

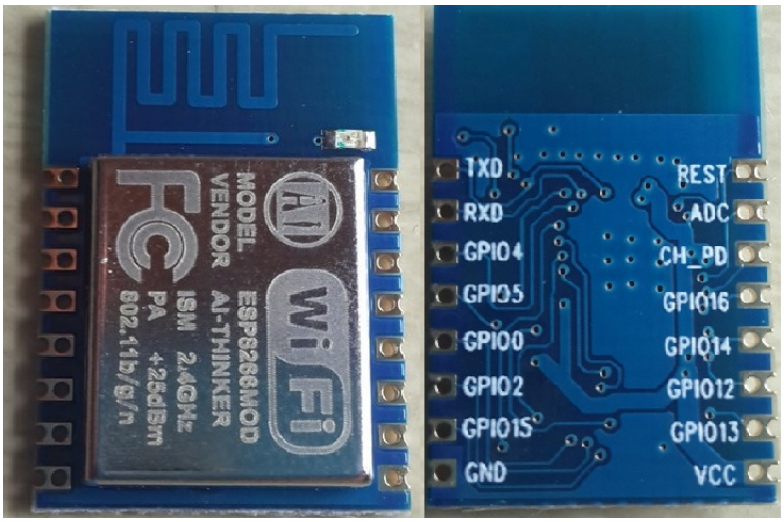

Figura B.1: Módulo ESP8266.

B.1 Ligações elétricas

O módulo ESP8266 funciona com uma voltagem de 3,3 Volts, caso não seja possível aplicar este valor diretamente temos de recorrer a um regulador de voltagem tal como mostra a figura B.2. Neste caso recorremos ao regulador LM2937ET-3.3V.

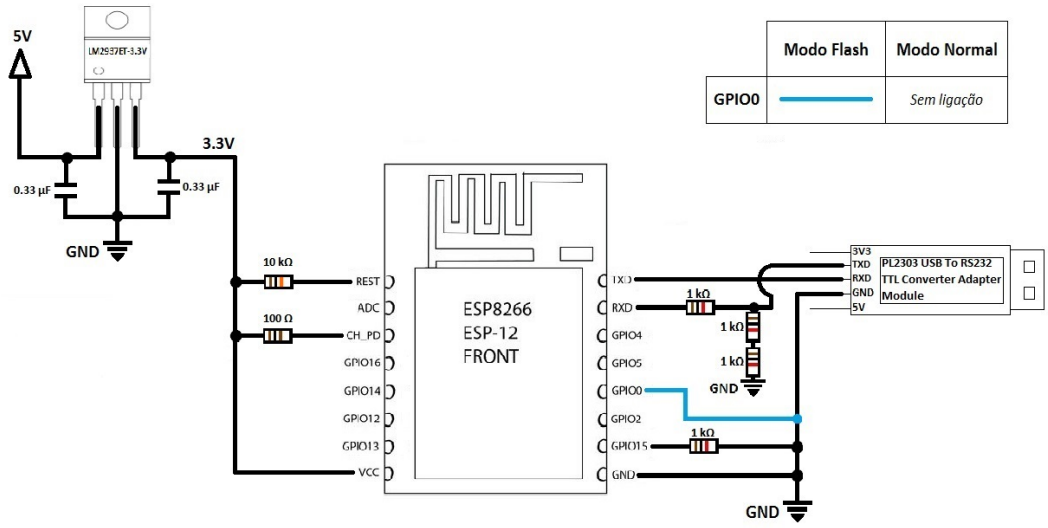

Figura B.2: Ligações do módulo ESP8266.

Na figura B.2 temos as ligações efetuadas para o correto funcionamento do módulo. Assim temos de ligar os pinos RST (com resistência de 10 kΩ), CH_PD (com resistência de 100 Ω) e VCC aos 3,3 Volts obtidos pelo regulador dos 5 Volts inicialmente fornecidos. Os pinos GPIO15 (com resistência de 1 kΩ), GND e GPIO0 ligam-se à terra, sendo que o pino GPIO0 apenas deve estar ligado quando se pretende programar o módulo (modo flash), em modo de funcionamento (modo normal) este pino deve-se encontrar sem ligações efetuadas.

De modo a programar o módulo utiliza-se um conversor USB para Rs232, o qual se liga aos pinos TXD e RXD. O pino RXD encontra ligado a três resistências antes e se ligar ao conversor para transformar os 5 Volts do conversor nos 3,3 Volts que o módulo consegue receber.

Mantendo as ligações efetuadas anteriormente, e ligando LEDs como mostra a figura B.3 podemos ativar os respetivos pinos (acendendo os LEDs) a partir dos diferentes códigos programados no módulo.

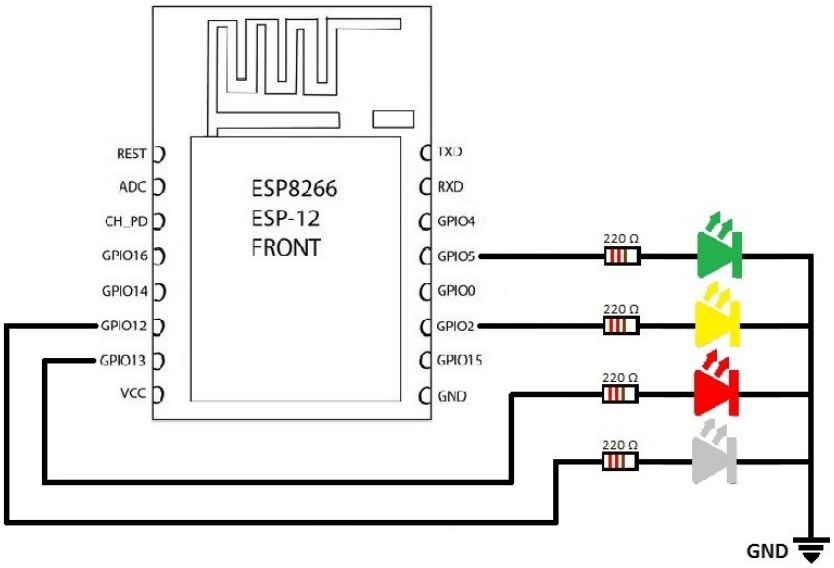

Figura B.3: Ligações dos LEDs ao módulo ESP8266.

Na figura B.4 apresento o programa *ESP8266 Flasher*, que permite enviar o ficheiro ".bin" para o módulo. Este ficheiro consiste no tipo de *firmware* e codificação que este irá utilizar, ou seja, Código Lua ou comandos AT. No caso da figura seguinte o ficheiro corresponde ao sistema de codificação baseada em comandos AT.

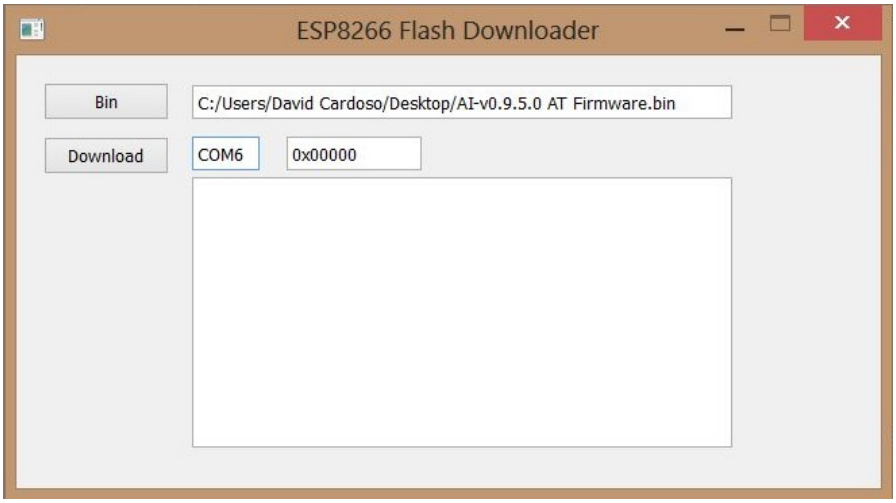

Figura B.4: Software para programar o módulo ESP8266.

Para conseguir "flashar" o módulo é necessário inicialmente verificar se as ligações estão corretamente efetuadas, como mostra a figura B.2, tendo o pino GPIO0 ligado à terra (modo flash).

Depois de verificadas as ligações, utilizando o programa anterior temos de encontrar o ficheiro ".bin" no nosso computador (no meu caso funcionou melhor com o ficheiro no ambiente de trabalho) após pressionar o botão "Bin". O ficheiro utilizado no exemplo encontra-se em [53].

Após encontrado o ficheiro devemos alterar o valor da porta de comunicação, no meu caso é COM6. De seguida podemos iniciar a programação do módulo ESP8266 ao carregar no botão "Download".

As figuras B.5 e B.6 mostram o início e fim da programação do módulo. Depois de programar o módulo deve-se remover a voltagem do módulo e a ligação do pino GPIO0. Reiniciando o módulo deve ser possível através de um terminal com COM6 e 9600 de *baudrate* enviar o comando "AT" e obter a resposta "OK".

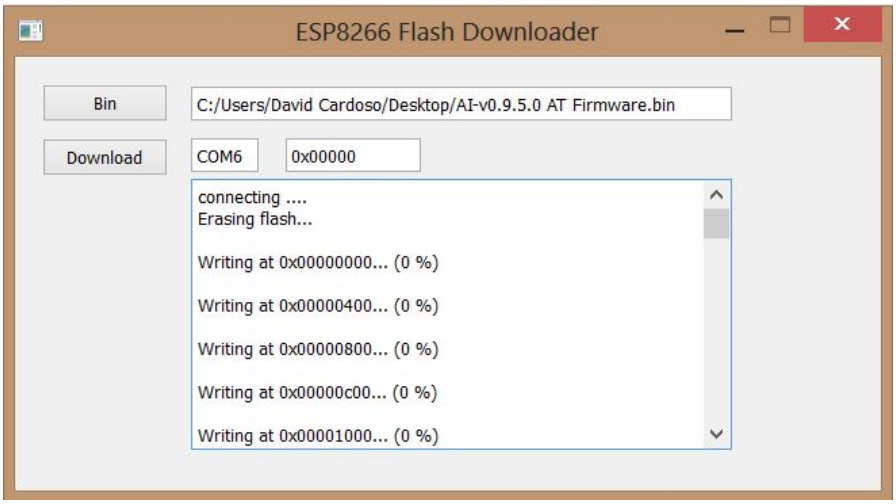

Figura B.5: Início da programação.

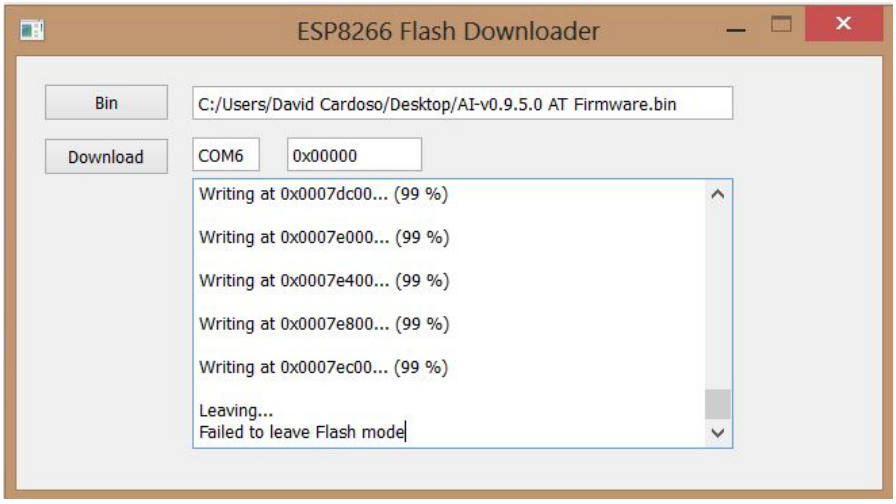

Figura B.6: Fim da programação.

B.2 Programação NodeMCU

A programação NodeMCU consiste no desenvolvimento de códigos para a realização de diferentes funções (como ativar ou desativar pinos, colocar o módulo em modo *Stand Alone* ou em modo *Acess Point*, criação de servidores, ...), recorrendo ao tipo de codificação LUA.

A figura B.7 apresenta o programa utilizado para programar o módulo com o NodeMCU.

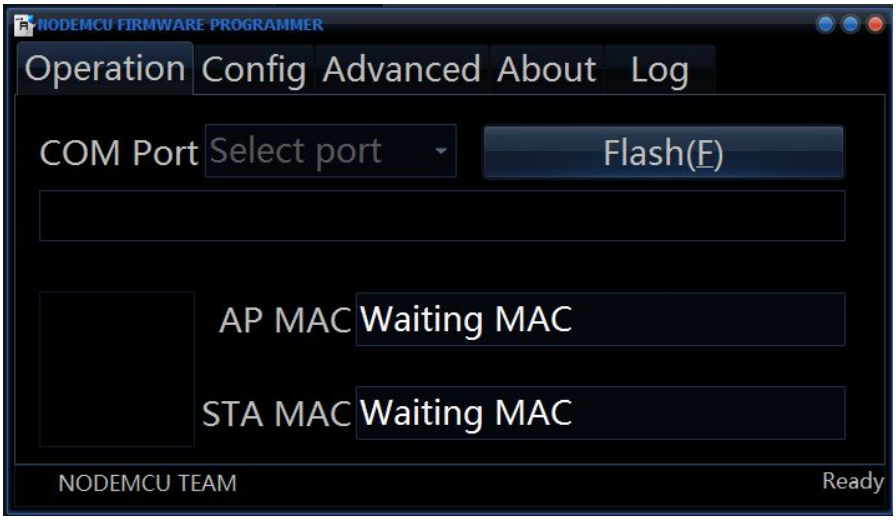

Figura B.7: Software para programar o módulo ESP8266 com o NodeMCU.

Para iniciar a configuração do módulo temos de ir a aba "Config", como mostra a figura B.8, e tal como no programa anterior temos de selecionar o ficheiro ".bin" a utilizar.

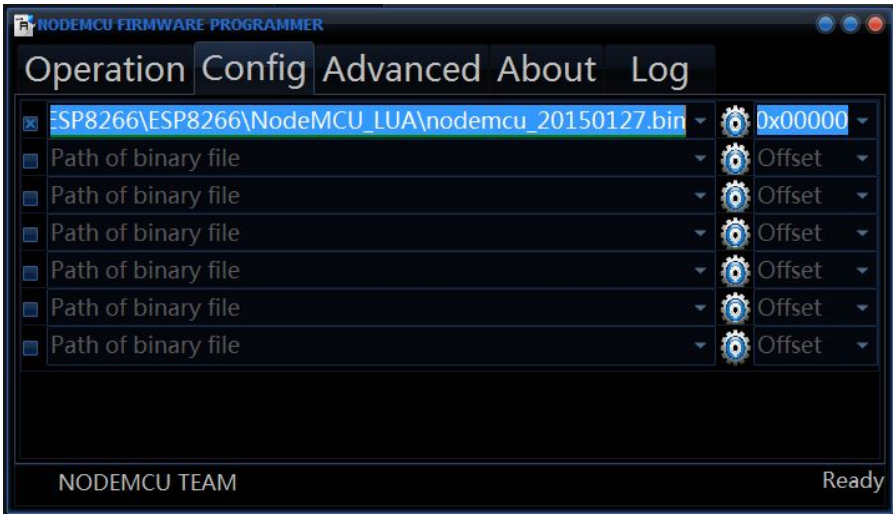

Figura B.8: Aba onde se seleciona o ficheiro ".bin".

Na aba "Advanced" (figura B.9) devemos selecionar o valor 9600 para a configuração do *Baudrate*, podendo o resto dos valores ser os inicialmente definidos.

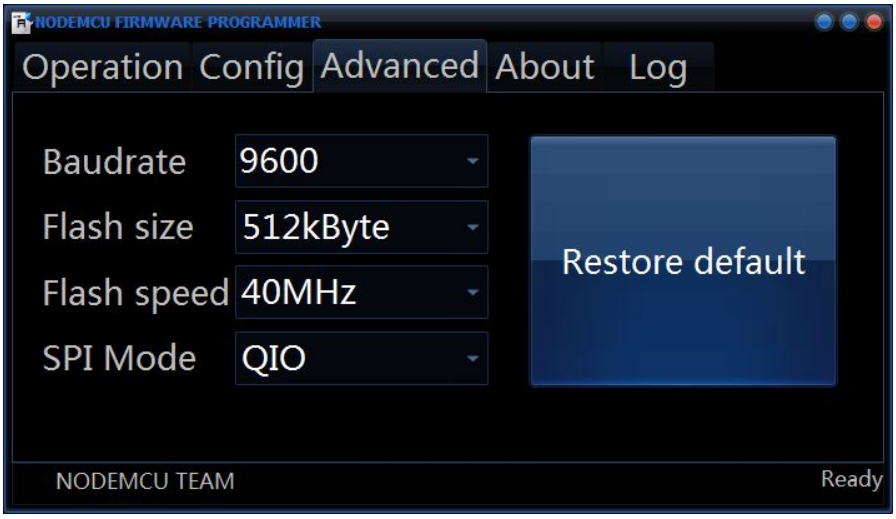

Figura B.9: Aba de configuração da porta de comunicação.

Para iniciar a programação do módulo temos de verificar as ligações efetuadas e ligar o pino GPIO0 à terra.

De seguida temos de selecionar a porta de comunicação que comunica com o módulo ESP8266, tal como antes, a porta utilizada é a COM6.

Após selecionada a porta pode-se começar a atualizar o software do módulo pressionando o botão "Flash(F)". Ao premir o botão este passa a "Stop(S)" e caso as configurações e ligações se encontrem corretas aparecem os valores de "AP MAC", "STA MAC" e o código de barras, tal como mostra a figura B.10.

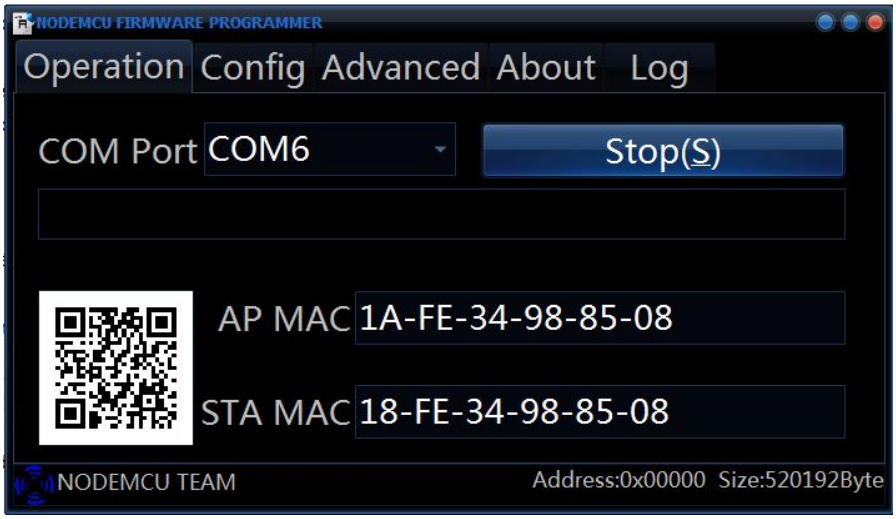

Figura B.10: Início da programação com o NodeMCU.

A figura B.11 mostra o fim da programação do módulo.

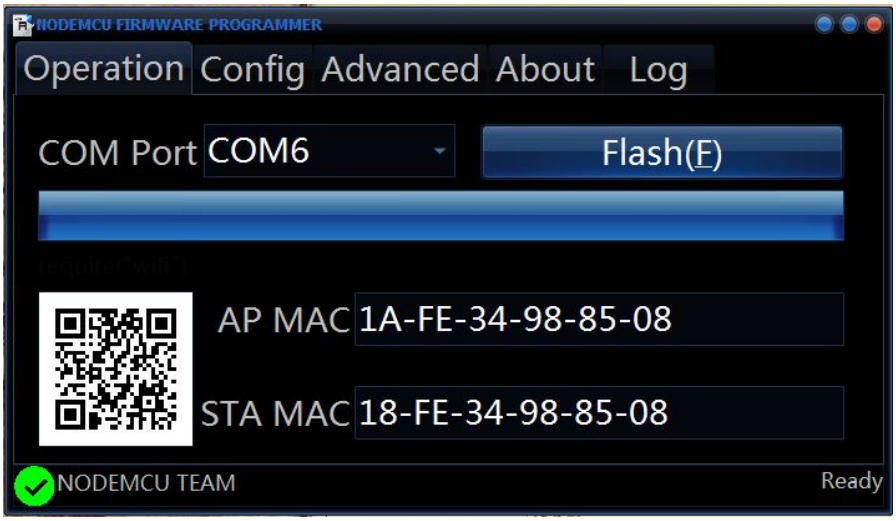

Figura B.11: Fim da programação com o NodeMCU.

Após retirar o GPIO0 da ligação com a terra, para enviar o código desenvolvido para o ESP8266 podemos recorrer ao Esptool ou ao Lua Uploader. Na figura B.12 mostra a área de desenvolvimento de código do Lua Uploader e as configurações alteradas da porta (COM6) e do baudrate (9600).

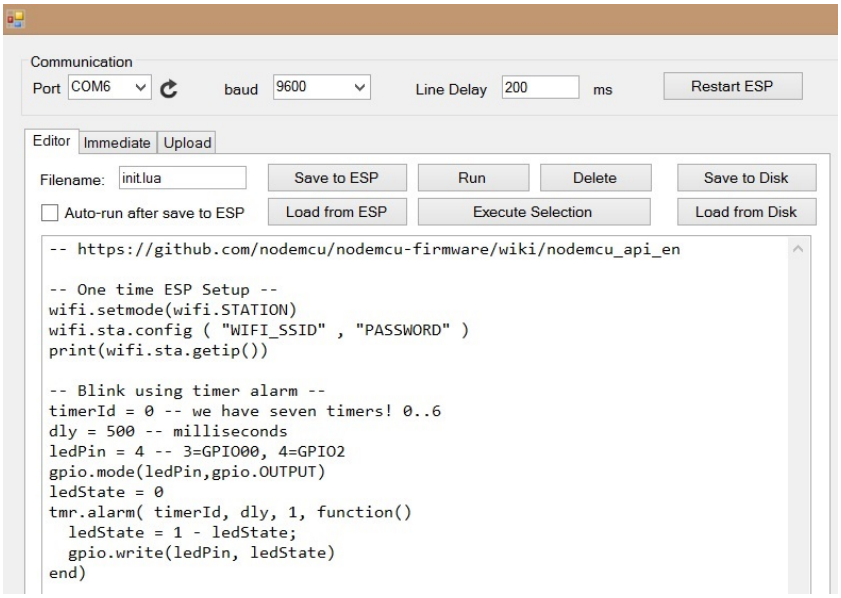

Figura B.12: Área de desenvolvimento de código.

O botão "Restart ESP" envia para o módulo o comando "node.restart", reiniciando o mesmo. Ao reiniciar, o módulo começa a funcionar com o código criado no ficheiro "init.lua" existente no mesmo.

Na aba "Editor" temos vários botões que significam:

- "Save to ESP" - Este botão quando pressionado envia o código desenvolvido na área em baixo e guarda-o no módulo com o nome que aparece em "Filename:";
- "Load from ESP" - Este botão permite obter o código criado com o nome colocado em "Filename:" do módulo, caso este já exista;
- "Run" - Este botão utiliza a função dofile() para executar o código cujo nome se encontra em "Filename:";
- "Delete" - Este botão utiliza a função file.remove() para eliminar o código no módulo cujo nome se encontra em "Filename:";
- "Execute Selection" - Este botão executa o código que estiver selecionado na área em baixo;
- "Save to Disk" - Este botão guarda o código desenvolvido na área em baixo no computador, podendo alterar o nome deste;
- "Load from Disk" - Este botão permite procurar um código desenvolvido e guardado no computador e mostra o mesmo na área em baixo;

Na aba "Immediate" (figura B.13) podemos colocar alguns comandos e este serão enviados para o módulo ao pressionar o botão "Execute".

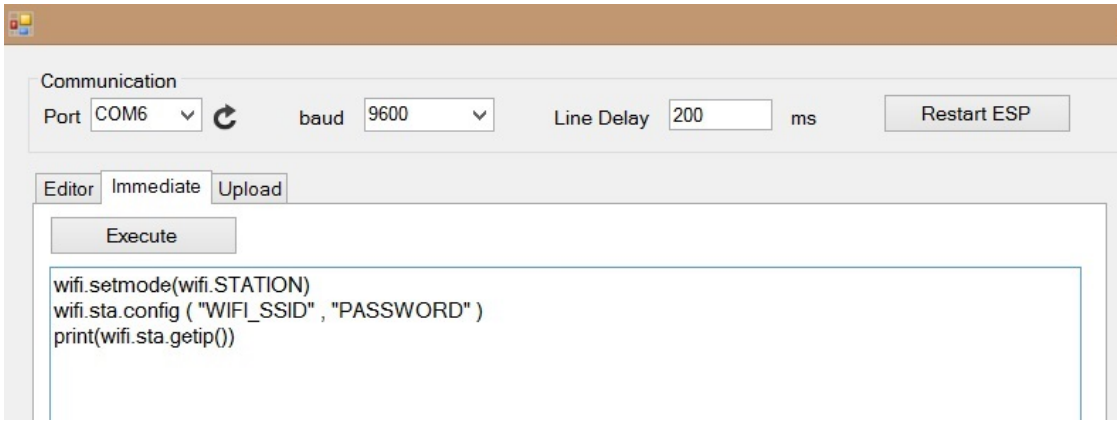

Figura B.13: Área de envio de comandos.

Os comandos ou códigos enviados para o módulo ESP8266 aparecem inicialmente com "SENT:" antes dos mesmos, como mostra a figura B.14.

Os comandos enviados são depois executados, aparecendo no terminal disponível no programa utilizado. Neste terminal também aparecem as respostas enviadas pelo módulo. No caso mostrado na figura B.14 a resposta foi "nil"(nulo), uma vez que não existe uma rede WiFi de nome "WIFI_SSID" e palavra-chave "PASSWORD".

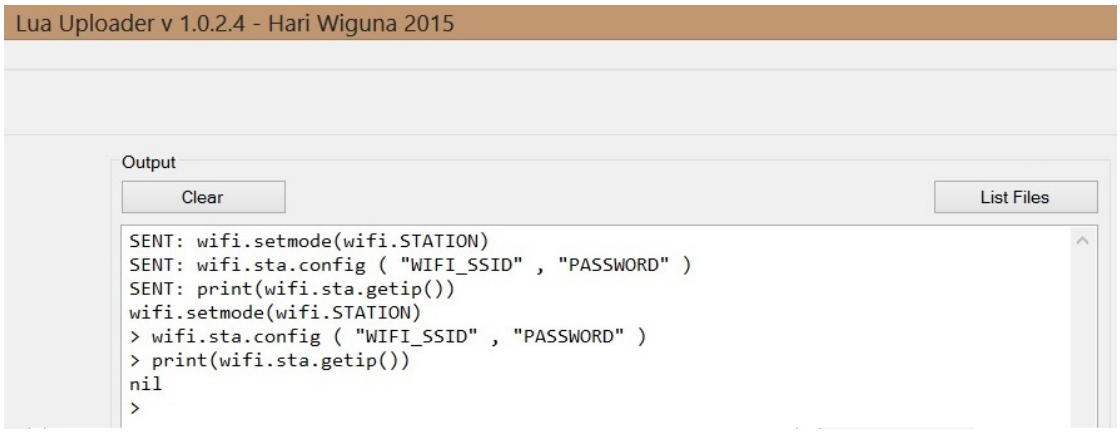

Figura B.14: Terminal incorporado no programa.

De seguida vou apresentar alguns exemplos de códigos que podem ser enviados para o módulo e as respetivas funções.

No exemplo seguinte apresento o código que define o módulo com o modo *Acess Point*. A primeira linha define o modo, a segunda define as configurações como o nome e palavra-chave da rede do módulo, a terceira guarda o ip do módulo na variável "ip" e a última linha envia o ip para o terminal do programa.

```
1 wifi.setmode(wifi.SOFTAP);
2 wifi.ap.config({ssid="test",pwd="12345678"});
3 ip = wifi.ap.getip();
4 print (ip);
```

Listing B.1: Configuração AP.

Neste exemplo o código define o modo *Stand Alone* do módulo. A primeira linha define o modo, a segunda define o nome e palavra-chave da rede wireless à qual o módulo se vai conectar e a última linha envia o ip obtido a partir da função no interior de "print".

```
1 wifi.setmode(wifi.STATION)
2 wifi.sta.config("myssid","mypassword")
3 print(wifi.sta.getip())
```

Listing B.2: Configuração STA.

O exemplo seguinte mostra um código que permite ativar e desativar um dos pinos do módulo continuamente, caso as ligações da figura B.3 estejam feitas corretamente um LED irá acender e apagar continuamente.

Na parte das configurações temos a atribuição de valores às variáveis locais "pin", "value" e "duration". A função criada altera o estado do pino, caso este esteja ativo (HIGH) passa a desativo (LOW) e vice-versa. De seguida definimos o pino como saída e o estado do mesmo. Na última linha temos o comando que permite executar a função criada a cada segundo, uma vez que o valor na variável "duration" corresponde a 1000 ms, ou seja, a 1 segundo.

```
-- Configurações
local pin = 4
local value = gpio.LOW
local duration = 1000

-- Função criada
function toggleLED ()
    if value == gpio.LOW then
        value = gpio.HIGH
    else
        value = gpio.LOW
    end
  tmr.delay(1000000)
  gpio.write(pin, value)
end

-- Definições do pino utilizado
gpio.mode(pin, gpio.OUTPUT)
gpio.write(pin, value)

-- Repete continuamente a função criada
tmr.alarm(0, duration, 1, toggleLED)
```

Listing B.3: Código para piscar um LED.

Com o código seguinte é possível criar uma página web no módulo, podendo ser desenvolvida uma página que permita alterar o estado dos pinos pressionando botões criados. A primeira linha serve para criar o servidor, na segunda a função faz o módulo esperar por uma resposta na porta 80, a terceira linha permite ao módulo verificar a resposta recebida. Na quarta linha temos a mensagem que irá ser enviada para a página guardada na variável "buf". As linhas seguintes servem para enviar os dados do servidor, fechar o servidor, limpar os dados desnecessários e terminar as funções srv: e conn:, respetivamente.

```
srv=net.createServer(net.TCP)
srv:listen(80,function(conn)
    conn:on("receive", function(client,request)
        buf = "<h1> Hello, NodeMcu.</h1>";
        client:send(buf);
        client:close();
        collectgarbage();
    end)
end))
```

Listing B.4: Código para criação de um servidor.

Mantendo o código que define o modo do módulo como *Acess Point* e adicionando o código anterior, podemos aceder á rede "test" do módulo. Após aceder à rede do módulo, ao introduzir o ip 192.168.4.1 no endereço de um motor de busca obtemos a mensagem apresentada na figura B.15.

Hello, NodeMcu.

Figura B.15: Mensagem que aparece no endereço 192.168.4.1 de um motor de busca.

Nas páginas [54] e [55] encontramos as diferentes funções disponíveis para a codificação LUA do módulo ESP8266.

B.3 Programação via Arduino IDE

A programação via Arduino consiste no desenvolvimento de códigos para a realização de diferentes funções, tal como na programação NodeMCU, recorrendo a uma linguagem de codificação padrão utilizada no programa Arduino (semelhante a C/C++).

Para iniciar a programação temos de descarregar o software gratuitamente da página em [56].

Após instalar o programa Arduino temos de ir ás preferências do mesmo, de modo a se poder atualizar as ferramentas e permitir a comunicação com o módulo ESP8266, tal como mostra a figura B.16.

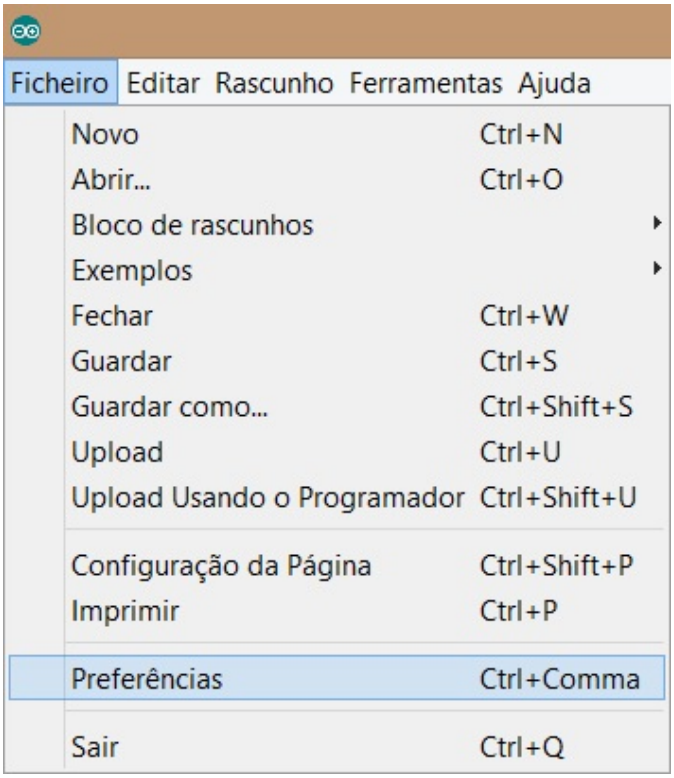

Figura B.16: Como chegar às preferências do Arduino.

Ao abrir as "Preferências" do programa, vamos procurar o espaço que se encontra a seguir a "Aditional Boards Manager URLs:" (apenas a partir do Arduino 1.6.4 é que esta opção existe) e coloca-se o endereço [57], tal como apresentado na figuraB.17.

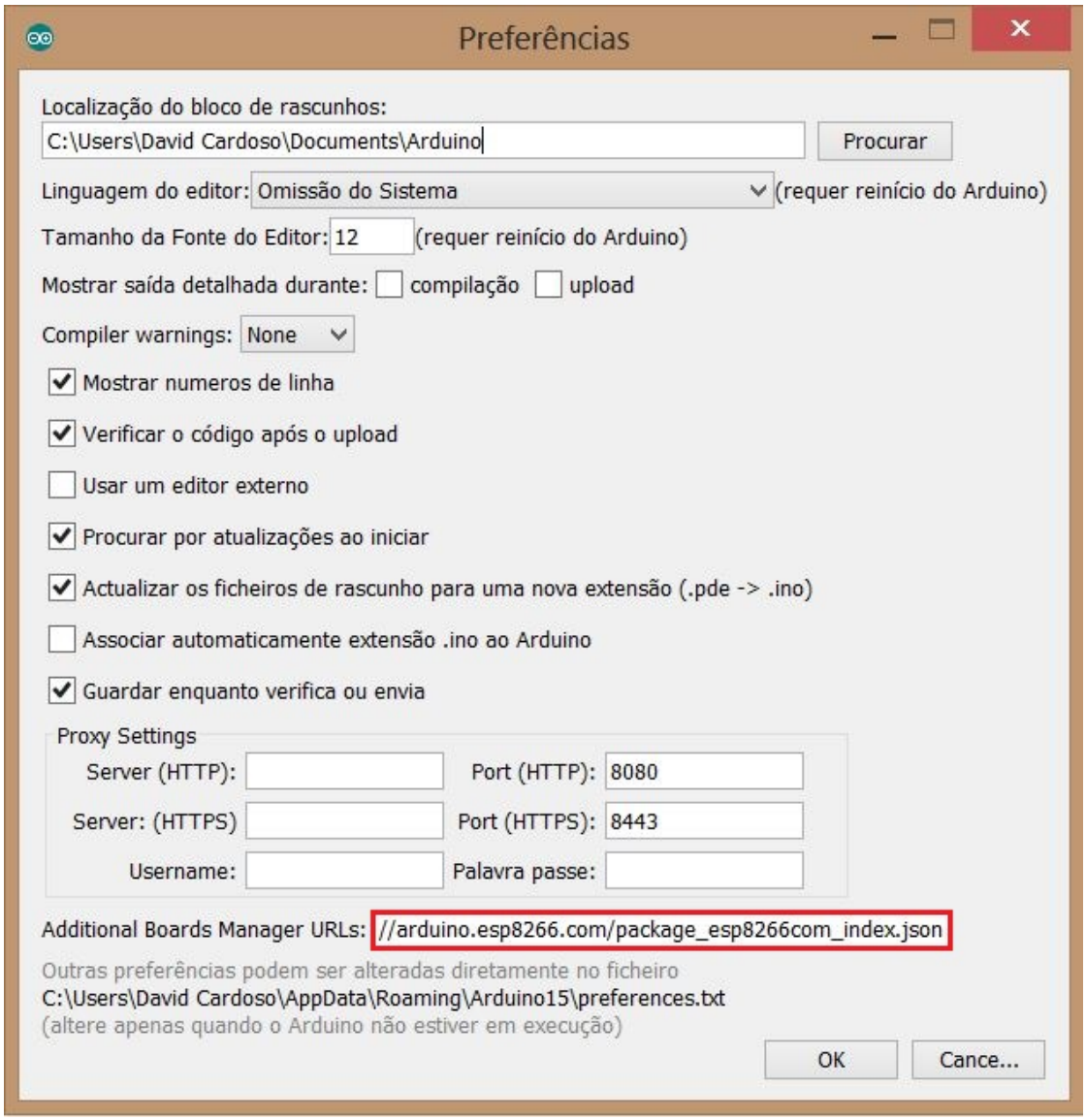

Figura B.17: Preferências do Arduino.

Depois de concluída a atualização, podemos ir às "Ferramentas" e selecionar o tipo de placa que vamos utilizar, no nosso caso vamos escolher "Generic ESP8266 Module", como podemos ver na figura B.18. No caso de erro pode-se ir a "Boards Manager..." e de seguida selecionar "esp8266" e clicar no botão Instalar.

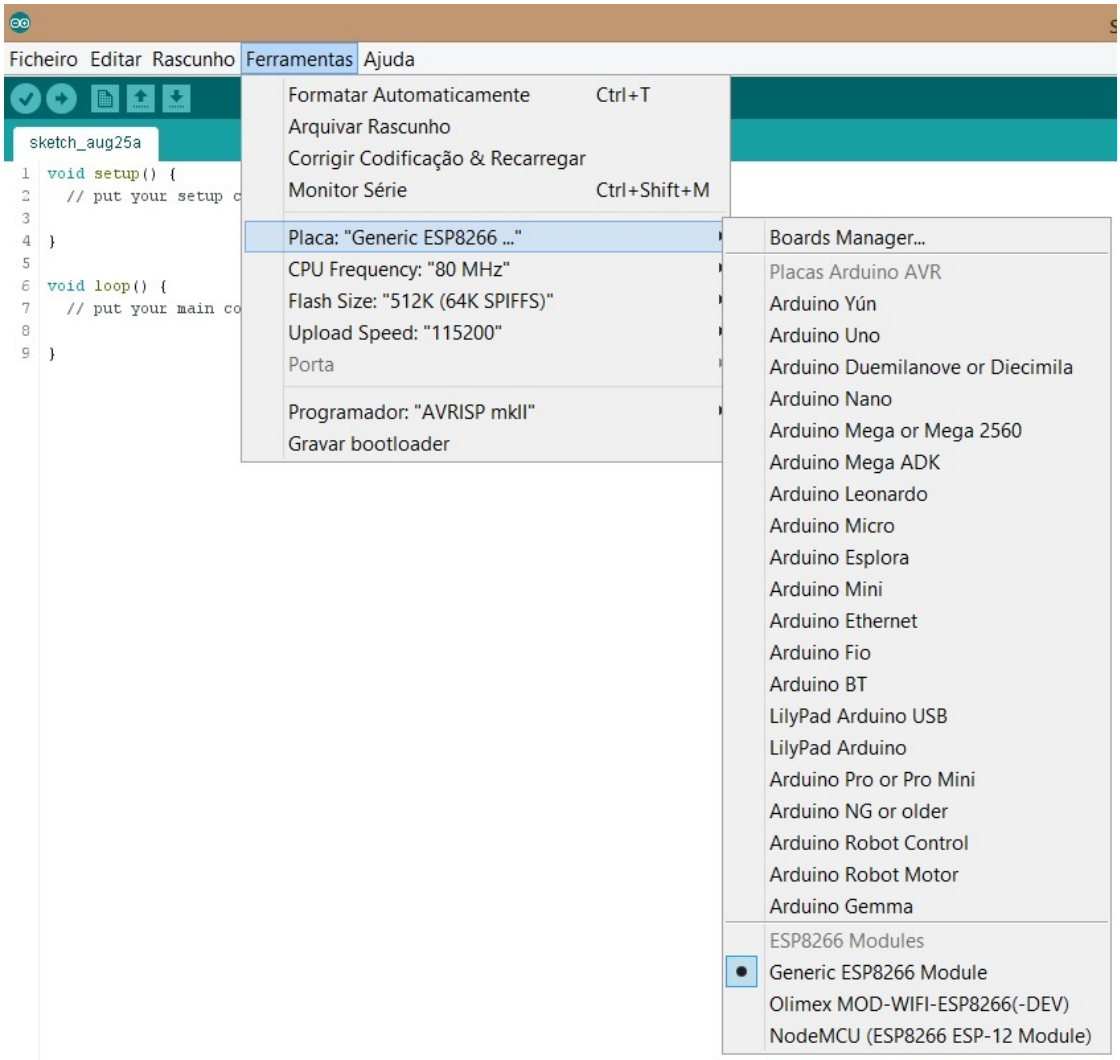

Figura B.18: Configuração da placa.

Quando selecionada a placa "Generic ESP8266 Module", o menu "Ferramentas" apresenta outras dados que anteriormente não apareciam como o CPU Frequency, Flash Size e Upload Speed. Estes valores não precisam de alterações podendo ficar como inicialmente definidos. Em algumas atualizações, existe a necessidade de selecionar o "esptool" na aba "Programador". Neste caso o "esptool" não aparece podendo ficar o que se encontra inicialmente. No menu "Ferramentas" (apresentado na figura B.19) também é importante selecionar a porta de comunicação correta quando se pretende enviar ou receber dados do módulo ESP8266.

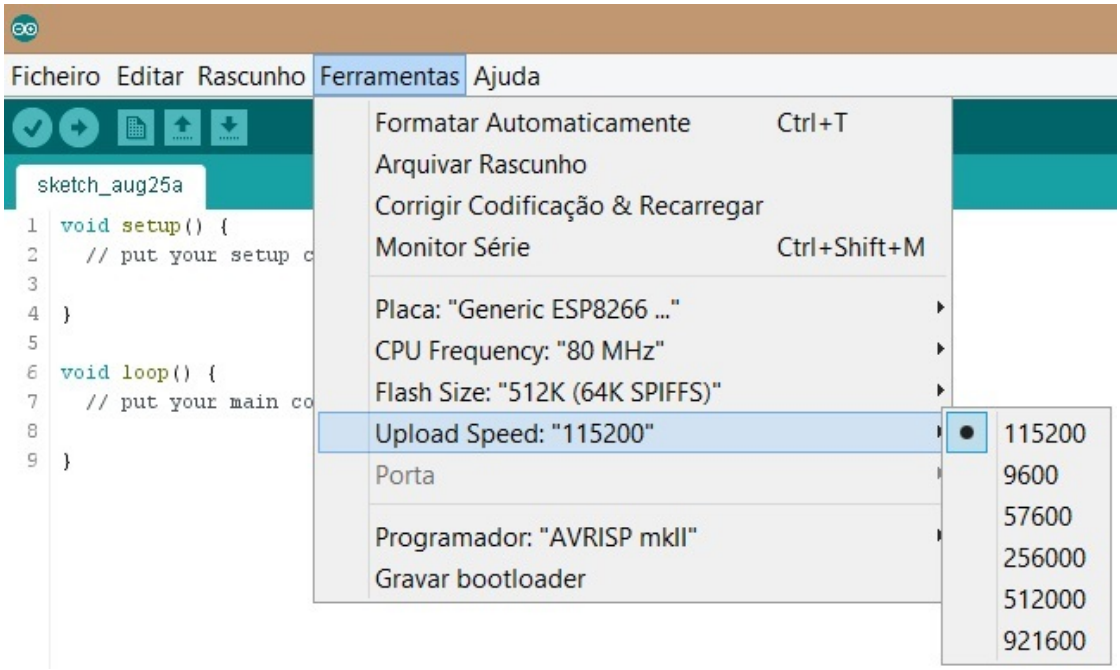

Figura B.19: Configuração da velocidade de envio.

Para conseguir enviar o código desenvolvido para o módulo é necessário inicialmente verificar se as ligações estão corretamente efetuadas, como mostra a figura B.2, tendo o pino GPIO0 ligado à terra (modo flash). Caso as ligações estejam efetuadas, temos de pressionar a seta assinalada a vermelho na figura B.20. Ao premir o botão, este irá verificar se existem erros no código e de seguida, caso não hajam erros, envia-o para o módulo apresentando as mensagens a laranja que se encontram no ecrã preto da figura seguinte.

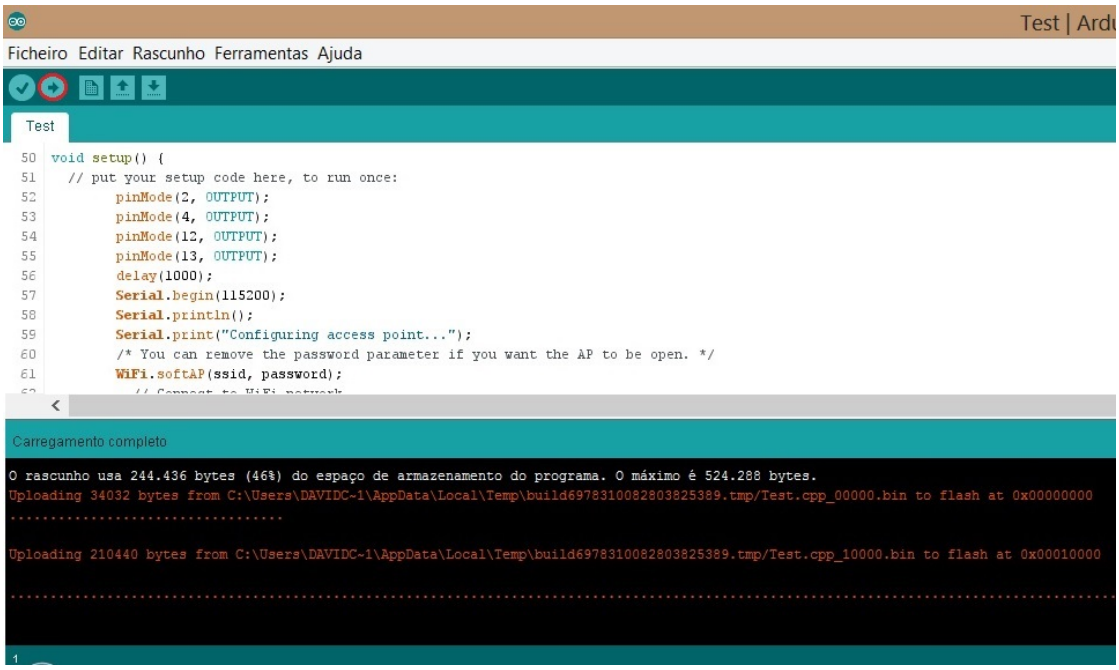

Figura B.20: Envio do código para o módulo.

De seguida vou apresentar alguns exemplos de códigos que podem ser enviados para o módulo e as respetivas funções. Os códigos seguintes correspondem a funções semelhantes às explicadas na parte da programação NodeMCU, mas agora desenvolvidas em Arduino.

O código a seguir apresentado corresponde às livrarias utilizadas pelo Arduino para a comunicação com o módulo ESP8266 e interação com a rede Wi-Fi. Estas livrarias devem aparecer no inicio de todos os códigos a enviar para o módulo.

```
#include <ESP8266WiFi.h>
#include <WiFiClient.h>
#include <ESP8266WebServer.h>
```

Listing B.5: Livrarias utilizadas para codificação do módulo ESP8266.

No exemplo seguinte apresento o código que define o módulo com o modo *Acess Point*. As primeiras duas linhas apresentam duas variáveis onde se guardam o nome e palavra-chave da rede do módulo, a terceira linha define o modo e a rede, a quarta guarda o ip do módulo na variável "myIP" e as últimas duas linhas enviam uma mensagem e o ip para o terminal do Arduino.

```
const char *ssid = "test";
const char *password = "12345678";
WiFi.softAP(ssid, password);
IPAddress myIP = WiFi.softAPIP();
Serial.print("AP IP address: ");
Serial.println(myIP);
```

Listing B.6: Configuração AP.

Neste exemplo o código define o modo *Stand Alone* do módulo. As primeiras duas linhas apresentam duas variáveis onde se guardam o nome e palavra-chave da rede wireless à qual o módulo se vai conectar , a terceira linha define o modo e liga-se à rede e as últimas

duas linhas enviam uma mensagem e o ip obtido para o terminal do Arduino a partir da função no interior de "Serial.print".

```
const char *router = "myssid";
const char *pass = "mypassword";
WiFi.begin(router, pass);
Serial.print("IP address: ");
Serial.println(WiFi.localIP());
```

Listing B.7: Configuração STA.

O exemplo seguinte mostra um código que permite ativar e desativar um dos pinos do módulo continuamente, caso as ligações da figura B.3 estejam feitas corretamente, um LED irá acender e apagar continuamente.

A função criada altera o estado do pino, este passa ao estado ativo (HIGH) ficando 1 segundo (1000 ms) nesse estado, passando de seguida para o estado desativo (LOW) durante 1 segundo. Na parte das configurações (função "setup") temos a definição do pino como saída. Na função "loop" temos a função criada a ser executada, ou seja, pino ativo durante 1 segundo e desativo por outro segundo e assim repetidamente.

```
// Função criada
void toggleLED() {
  digitalWrite(2, HIGH);
  delay(1000);
  digitalWrite(2, LOW);
  delay(1000);
}

void setup() {
  // Definições do pino utilizado
  pinMode(2, OUTPUT);
}

void loop() {
  // Repete continuamente a função criada
  toggleLED();
}
```

Listing B.8: Código para piscar um LED.

Com o código seguinte é possível criar uma página web no módulo, podendo ser desenvolvida uma página que permita alterar o estado dos pinos pressionando botões criados. A primeira linha serve para criar o servidor na porta 80. Na função "Setup" temos a definição das informações a enviar para a página criada. A primeira linha significa que caso seja o endereço inicial (192.168.4.1) irá ser enviado para a página o código com a mensagem "<h1> Hello, NodeMcu.</h1>". A ultima linha nesta função inicia o servidor criado anteriormente. Na função "loop" temos a página a ser atualizada continuamente devido à função "handleClient".

```
ESP8266WebServer server(80);

void setup() {
  server.on("/", [](){
  server.send(200, "text/html", "<h1> Hello , NodeMcu.</h1>");
  }
  server.begin();
}

void loop() {
  server.handleClient();
}
```

Listing B.9: Código para criação de um servidor.

Tal como na programação NodeMCU, mantendo o código que define o modo do módulo como *Acess Point* na função "setup" e adicionando o código anterior, podemos aceder á rede "test" do módulo. Após aceder à rede do módulo, ao introduzir o ip 192.168.4.1 no endereço de um motor de busca obtemos a mensagem apresentada na figura B.15.

Na página [58] encontramos as diferentes funções disponíveis para a codificação via Arduino do módulo ESP8266.