
# Comunicações RFID para Identificação e Controlo de Acessos

Mestrado em Engenharia Eletrotécnica

Rui Miguel Baptista Peixoto

Leiria, novembro de 2021


# Comunicações RFID para Identificação e Controlo de Acessos

Mestrado em Engenharia Eletrotécnica

Rui Miguel Baptista Peixoto

Trabalho de Projeto realizado sob a orientação do Professor Doutor Hugo Miguel Cravo Gomes e do Professor Doutor Paulo Jorge Simões Coelho

Leiria, novembro de 2021

# Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionado o Autor e feita referência ao ciclo de estudos no âmbito do qual o mesmo foi realizado, a saber, Curso de Mestrado em Engenharia Eletrotécnica, no ano letivo 2020/2021, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

# Agradecimentos

A obtenção de grau académico acarreta só por si um conjunto de constrangimentos e dificuldades tanto ao nível académico, como a nível de gestão pessoal e familiar. Manter a persistência, a motivação e o foco são fundamentais para se caminhar em direção ao objetivo. Nesse sentido, não poderia deixar de agradecer aos meus orientadores, o Professor Doutor Hugo Miguel Cravo Gomes e Professor Doutor Paulo Jorge Simões Coelho pelos esclarecimentos, conselhos, troca de opiniões e sobretudo, pelo constante incentivo e motivação durante todo o desenvolvimento deste projeto.

Queria também agradecer à minha família pelo apoio incondicional e pela constante motivação em seguir caminhando na tentativa ser mais e melhor. A todos o meu sincero agradecimento.

# Resumo

A problemática da identificação de pessoas, não sendo um tema novo, está em constante desenvolvimento. A evolução tecnológica nas últimas duas décadas, em especial na área da eletrónica de microcontroladores, tem trazido diversas soluções, tanto ao nível dos métodos de identificação de pessoas utilizados, como ao nível das suas aplicações.

Este projeto contribui com o desenvolvimento de um dispositivo de identificação capaz de ser utilizado para registar a presença de estudantes em sala de aula. Foram utilizadas diversas tecnologias de identificação para permitir uma aproximação às necessidades e exigências de cada um dos seus utilizadores: docente e estudantes. Foram definidas duas áreas principais de intervenção: estudo e seleção das tecnologias de identificação a utilizar e formas de interface de utilizador.

Para as tecnologias de identificação pretendeu-se diversificar os métodos: para tecnologias de identificação por objetos identificadores utilizou-se o RFID e NFC; e para método de identificação por biometria utilizou-se a tecnologia de identificação por impressão digital.

Para a interface com o utilizador foi desenvolvida uma aplicação para *Smartphone* para introdução dos dados de estudantes e unidades curriculares. Foi também construído um interface gráfico no próprio dispositivo para visualização de todos os dados introduzidos e para navegação entre as diversas opções do sistema.

Para além disso, foram desenvolvidos recursos de *Hardware* para acomodar todas as ligações e dispositivos externos e desenvolvido todo o *Software* necessário à compatibilização o e interligação dos recursos.

**Palavras-chave:** Identificação de pessoas, RFID, NFC, biometria, impressão digital, portabilidade.

# Abstract

The issue of identifying people, although don't be a new topic, is in constant development. Technological evolution in the last two decades, especially in electronics and microcontroller areas, has brought several solutions, both in terms of the methods of identification of people used, and in terms of their applications.

This project contributes to the development of an identification device capable of being used to register the presence of students in the classroom. Different identification technologies were used to allow an approximation to the needs and requirements of teachers and students. Two main areas of intervention were defined: study and selection of identification technologies to be used and user interface formats.

For the identification technologies, it was intended to diversify the methods, using object identification based on RFID and NFC. For the biometric identification method, the fingerprint identification technology was used.

For the interface, an application for Smartphone was developed to enter the data of students and curricular units, together with the construction of a graphical interface on the device itself for viewing all the data entered and for navigating between the various system options. In addition, hardware resources were developed to accommodate all connections and external devices, and all the necessary software for the compatibility and interconnection of resources was developed.

**Keywords**: People identification, RFID. NFC, biometrics, fingerprint, portability.

# Índice

# Lista de Figuras

# Lista de tabelas

# Lista de siglas e acrónimos

| | |
|---|---|
| 2D | Duas dimensões |
| AC | Alternated Current |
| ADN | Ácido Desoxirribonucleico |
| AM | Amplitude Modulation |
| ANACOM | Autoridade Nacional de Comunicações |
| ASK | Amplitude Shift Keying |
| BASK | Binary Amplitude Shift Keying |
| BI | Bilhete de Identidade |
| BLE | Bluetooth LOW Energy |
| BR | Bluetooth Basic Rate |
| BT | Bluetooth |
| CC | Corrente Contínua |
| CI | Circuito Integrado |
| CDMA | Code Division Multiple Access |
| CSV | Comma Separated Values |
| DQPSK | Differential Quadrature Phase Shift Keying |
| EDR | Enhanced Data Rate |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EM | Eletromagnética |
| EPC | Eletronic Product Code |
| ESTG | Escola Superiror de Tecnologia e Gestão de Leiria |
| FHSS | Frequency-Hopping Spread Spectrum |
| FM | Frequency Modulation |
| GFSK | Gaussian Frequency Shift Keying |
| GPIO | General Purpose Input Output |
| HF | High Frequency |
| I2C | Inter-Integrated Circuit |
| IC | Integrated Circuit |
| ID | Identification - Código de Identificação |

| | |
|---|---|
| IoT | Internet of Things |
| IPLeiria | Instituto Politécnico de Leiria |
| ISM | Industrial, Scientific & Medical |
| LC | Circuito Bobine Condensador |
| LCD | Liquid Crystal Display |
| LF | Low frequency |
| Mbps | Mega bit por segundo |
| MEE | Mestrado em Engenharia Eletrotécnica |
| MISO | Master Input Slave Output |
| MOSI | Master Output Slave Input |
| NDEF | NFC Data Exchange Format |
| NFC | Near Fiel Communication |
| OOK | On-off Keying |
| QPSK | Quadrature Phase Shift Keying |
| RF | Radiofrequência |
| RFID | Radio-Frequency Identification |
| RTC | Real Time Clock |
| SCK | Clock |
| SD | Secure Digital |
| SEE | Sistemas Elétricos de Energia |
| SPI | Serial Peripheral Interface |
| SS | Slave Select |
| TDMA | Time Division Multiple Access |
| TP1 | Teórico-Prática Turno 1 |
| UART | Universal Asynchronous Receiver / Transmitter |
| UC | Unidade Curricular |
| UHF | Ultra High Frequency |
| W | Watt |
| Worm | Write once read many |
| WPAN | Wireless Personal Area Network |

# 1. Introdução

## 1.1. Considerações iniciais

São frequentes as expressões que dizem que o mundo em que habitamos, a sociedade para a qual contribuímos e a vida atual que vivemos é bem diferente das gerações anteriores. A constante necessidade de utilização dos meios de comunicação vulgarmente ao dispor de qualquer cidadão, o acesso à informação sobre o meio envolvente a toda a hora e em qualquer lugar, as digitalizações de toda a informação para cruzamento com diversas plataformas, têm criado focos de grande parte das evoluções tecnológicas presentes e certamente futuras.

A Internet das Coisas (do inglês *Internet of Things - IoT*) é exemplo dessa necessidade criada a partir da simbiose entre a internet e a eletrónica, responsáveis por grandes evoluções transformadoras da sociedade digital. Se, por um lado se tenta aumentar a velocidade e a qualidade das comunicações de forma a satisfazer a constante procura de mais informação, por outro lado, torna-se claro que a tecnologia digital faz cada vez mais parte do dia a dia das empresas, indústrias, serviços e, em regra geral, de todos os cidadãos. Por outras palavras, o que outrora funcionava independentemente e necessitava de constante monitorização local, passou a estar concentrado e monitorizado em tempo real através da interligação de aparelhos e/ou dispositivos outrora isolados ao mundo digital.

## 1.2. Motivação e objetivos gerais

O projeto "Comunicações RFID para Identificação e Controlo de Presenças" nasceu de uma necessidade observada na lecionação das aulas na Escola Superior de Tecnologia e Gestão (ESTG) do Politécnico de Leiria (IPLeiria), onde por regulamento, é necessário registar a presença dos estudantes em sala de aula. O objetivo será criar um método prático, de baixo custo e fácil utilização, que sirva de alternativa à forma atual de realizar o registo de presenças de estudantes em sala de aula. Antes do início da pandemia provocada pela doença do Covid-19, o registo de assiduidade era feito através da assinatura de um documento que circulava entre os estudantes. Dadas as recentes limitações impostas pelas Autoridades de Saúde, de modo a evitar possíveis propagações entre estudantes, será de relevância adicional que o procedimento de registo de assiduidades possa ser assegurado de modo mais seguro, sem contacto entre intervenientes.

O controlo da assiduidade dos alunos é, no seu geral, um fator de elevada importância para os serviços do IPLeiria, sendo também um elemento fundamental de admissão dos estudantes aos momentos de Avaliação Contínua/Periódica das unidades curriculares (UC). De acordo com o ponto 2 do artigo 53º do Regulamento Geral da Formação Graduada e Pós-Graduada no IPLeiria e Regimes Aplicáveis a Estudantes em Situações Especiais [25], os alunos inscritos pela primeira vez em uma UC necessitam de uma participação de 75% em aula ou em atividades de presença obrigatória para serem elegíveis para o momento de Avaliação Contínua/Periódica. Apesar da existência de um sistema de controlo através de acesso com cartão de identificação, nos principais laboratórios e em algumas salas especificas, este tem-se mostrado pouco eficaz e, sobretudo, apresentando algumas limitações onde se destacam a falta de manutenção e atualização do sistema instalado, a dificuldade na substituição de equipamentos danificados, entre outros.

Em virtude desta situação, ainda não foi possível aos docentes da ESTG-IPLeiria abandonarem os antigos registos em papel e a preocupação acrescida com livros de registos, grelhas de registo, controlo e preenchimento do número de aula, da data em que ocorre, com as assinaturas de estudantes, etc. Adicionalmente as questões pandémicas tornaram ainda mais premente a atualização dos procedimentos, sendo necessário recorrer à "tradicional" chamada oral para evitar de partilha do documento de registo de presenças entre os estudantes.

Em suma, a ideia principal do projeto surgiu da necessidade de colmatar algumas destas limitações e consistiu no desenvolvimento de um dispositivo eletrónico que realize esse registo de forma automática, retirando a necessidade do preenchimento prévio, controlo do preenchimento por parte dos alunos em cada aula, erros ou danos na folha de registo, entre outros. O dispositivo inclui diferentes tecnologias de identificação para que todos os estudantes possam ter um método ajustado a si. O dispositivo é portátil para que cada docente possa ter um exemplar e este possa ser utilizado facilmente em qualquer sala ou laboratório. A somar ao foco principal, juntou-se a necessidade de utilização de recursos de eletrónica comum e generalizada, com baixo custo de modo a criar um protótipo funcional e prático que pudesse servir de base para evolução futura.

## 1.3.História e dados estatísticos de sistemas de identificação

Para abordarmos o tema do registo e identificação de pessoas, teremos de recuar até aos tempos mais antigos, remontando à idade média onde a igreja católica tomou a iniciativa de criar registos do estado civil dos seus fiéis, nomeadamente, nascimentos, casamentos e falecimentos.

Em Portugal, foi já no século XIX, onde se percebeu os benefícios do registo de pessoas, pelo que se estendeu a toda a população, tendo mesmo sido redigido o primeiro decreto-lei em 16 de maio de 1832 [1]. Foi já no século XX, mais propriamente em 1914, que surge o aparecimento do primeiro Bilhete de Identidade (BI), documento este composto por informação detalhada e capaz de identificar um indivíduo. Para além do nome, fotografia, impressão digital, data de nascimento, filiação e altura, também continham informação da profissão, de traços distintivos da cor dos olhos, cabelo, barba ou pele e espaços para marcas físicas distintivas, tal como sinais. Toda esta informação conferia-lhe uma dimensão assinalável (Figura 1-1 [2][3]).

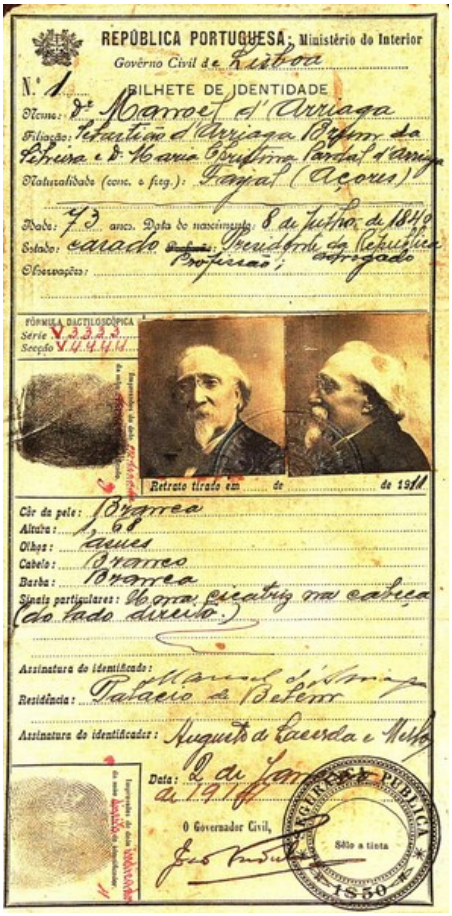

Figura 1-1: Primeiro Bilhete de Identidade Português (1914) [4].

Desde esse tempo, os documentos de identificação individual sofreram sucessivas evoluções até a criação da documentação da identificação pessoal que conhecemos atualmente, nomeadamente, registos de nascimento, cédulas militares, boletins de saúde, cartão do cidadão, cartas de condução, entre outros. Esta evolução verificou-se não só no tipo de informação a registar, como também na garantia da fidelidade do documento.

É neste último ponto que a tecnologia em geral e a eletrónica em particular têm tido um papel fundamental.

A utilização de leitores para introdução de um código alfanumérico ou leitores de cartões que emitem um sinal de radiofrequência (*Radio Frequency Identification* - RFID ou *Near Field Communication* - NFC), são já tecnologias maduras, mas continuam a sofrer evolução, tanto ao nível do desenvolvimento, como ao nível das aplicações. A autenticidade será sempre uma questão fundamental, aquando do desenvolvimento e utilização de sistemas de identificação. O grau de certeza de um dispositivo identificador de um indivíduo (p.ex. cartão de identificação) é reduzido pois este dispositivo pode ser passado de mão em mão se não contiver características únicas e intransmissíveis.

Atualmente tem-se apostado em sistemas de identificação biométricos, leitura de impressões digitais, reconhecimento de voz, leitura da retina, identificação facial, entre outros, como métodos de identificação únicos de indivíduos.

## 1.4. Estrutura do Relatório

O relatório está distribuído por 6 capítulos e organizado da seguinte forma:

- "Introdução", onde são apresentadas as principais motivações do projeto bem como a área científica de estudo, objetivos gerais, aplicações e uma breve integração histórica acerca da necessidade e benefício do registo de pessoas.
- "Estudo de Tecnologias Existentes", onde são analisadas algumas soluções e aplicações de sistemas de identificação utilizados na generalidade das aplicações atuais.
- "Desenvolvimento e Implementação", onde são detalhados os principais requisitos físicos (hardware) necessário para o desenvolvimento do protótipo demonstrativo do presente projeto.
- "Software", focalizado nos diversos recursos de software necessários para a implementação do protótipo, detalhando e identificando informações importantes no modo de utilização do protótipo.
- "Testes de funcionamento", onde são apresentados os resultados obtidos em testes de funcionamento, validando os principais objetivos alcançados e identificando as principais limitações. São analisados aspetos tais como a introdução de dados de estudantes e de unidades curriculares no sistema, identificação de estudantes em aula, entre outros.
- Por fim as "Conclusões ", destinadas à análise/resumo do trabalho desenvolvido e à realização de considerações/conclusões finais, bem como identificar algumas possibilidades de evolução futura para o projeto.

# 2. Estudo de Tecnologias Existentes

No presente capítulo são apresentadas algumas das tecnologias de mercado mais utilizadas em sistemas de identificação de pessoas, enunciando-se de forma prática e concisa os conteúdos técnico-científicos mais relevantes ao seu estudo, que servem de fundamento base à realização do protótipo desenvolvido no âmbito deste projeto.

Não é intuito deste relatório, o estudo exaustivo de qualquer das formas de identificação, mas sim dar ênfase às funcionalidades pretendidas e focar os recursos materiais necessários para a sua realização.

Serão abordadas as principais características dos sistemas de deteção / identificação / comunicação por RFID, por NFC, por *Bluetooth* e por deteção biométrica (impressão digital).

## 2.1. Tecnologias utilizadas em métodos de identificação

### 2.1.1. RFID

O método de identificação por RFID, baseia-se no uso de ondas eletromagnéticas (radiofrequência) para identificar indivíduos, animais, objetos, mercadorias, veículos, entre outros. Cada individuo/objeto terá um identificador único que ao ser lido pelo sistema o identifica e recolhe informação útil a essa identificação.

Um sistema RFID genérico é um sistema relativamente simples, constituído por dispositivos leitores (também designados por *Readers* ou interrogadores), por dispositivos identificadores (*tags* ou *transponders*) e por *software*, responsável pela gestão de armazenamento e tratamento de dados.

Um sistema RFID pode conter um ou mais *Readers* (estáticos ou móveis), diversas *tags* anexadas a indivíduos ou objetos tais como cartões, paletes, caixas, garrafas, cartazes, entre outros. O diagrama de blocos típico de um sistema RFID pode ser observado na Figura 2-1.

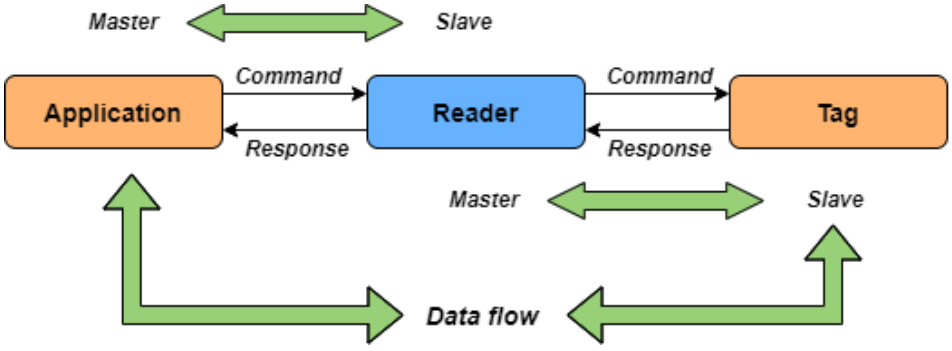


Figura 2-1: Diagrama de blocos do sistema RFID [5].

No seu funcionamento mais básico, o leitor comunica com as *tags* que estão ao seu alcance e recolhe as informações sobre os objetos a que estão anexadas. As informações recebidas são depois geridas por *software* e base de dados associados ao sistema. Sendo um sistema bastante versátil e de custo acessível para a maioria das empresas, este sistema de identificação está a ganhar cada vez mais popularidade em todos os setores de atividade [6][7][8]. Pode observar-se na imagem da Figura 2-2, a configuração básica de um sistema de identificação por RFID, composto por módulo de tratamento de dados, leitor e cartão.

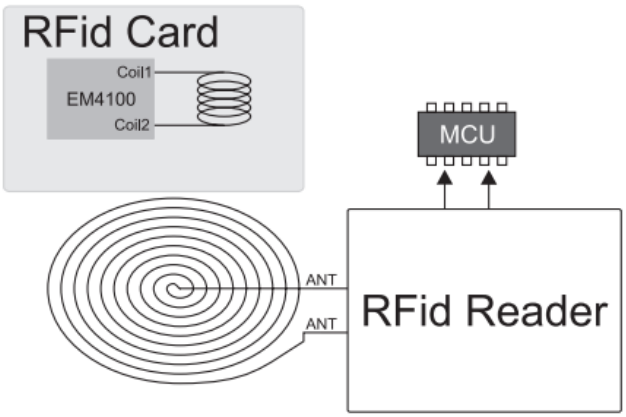


Figura 2-2: Configuração básica de um sistema RFID.

Como já referido anteriormente, os componentes principais de um sistema RFID são:

- ***Tag (Transponder):*** Etiqueta identificadora que é anexada ao objeto/pessoa que se quer identificar/monitorizar. Tem a possibilidade de armazenar a informação, sendo que cada *tag* RFID contém um circuito integrado (CI) e uma antena encapsulada no interior de embalagens adequadas.
- ***Leitor (Reader):*** Pode considerar-se o módulo central do sistema RFID. É responsável pelo envio e recolha dos sinais RF que recolhem as informações armazenadas nas *tag* no seu raio de ação. Para além do envio dos sinais RF e relógio de sincronização, o leitor de RFID tem ainda o papel de gestor de protocolos de anti-colisão entre as *tags*, gestão do nível potência dos sinais RF emitidos entre outras operações necessárias ao correto funcionamento do sistema. Associado ao leitor pode estar uma ou mais antenas RF que transmitem e recebem as ondas eletromagnéticas que transportam a informação do leitor para a *tag* e vice-versa.
- ***Sistema de tratamento e armazenamento de dados:*** Faz a gestão e tratamento dos dados recebidos e das operações tanto do leitor como da *tag*.

Os sistemas RFID podem ser classificados das seguintes formas [9]:

**A. Princípio da Comunicação**

Os sistemas RFID podem comunicar entre si utilizando um acoplamento magnético ou eletromagnético. A diferença entre os dois reside no seu campo de operação, isto é, campo próximo *(Near-Field* com distâncias aproximadamente até 15cm) para um acoplamento magnético ou campo distante *(Far-Field* com distâncias que podem ir até 100m*)* para acoplamento eletromagnético [10]. O campo distante tem maior alcance de leitura em comparação com sistemas de campo próximo, no entanto, não podemos deixar de considerar que as frequências de operação que também influenciam esta mesma distância de operação, como veremos mais à frente.

**1) Sistemas acoplados magneticamente:** São sistemas magnéticos ou indutivos que operam passivamente em bandas de baixa frequência (*Low frequency* - LF) e alta frequência (*High Frequency* - HF). Baseiam o funcionamento no princípio de indução magnética de Faraday [10], em que uma corrente que flui através da bobina produz um campo magnético em torno dela. Para esta tipo de aplicação em particular, o campo magnético gerado induz na bobine de uma *tag* próxima uma corrente. A Figura 2-3, mostra um leitor que gera um campo magnético variante no tempo, o qual induz uma tensão alternada (AC) na *tag*. A tensão AC é retificada para uma tensão contínua (CC) para alimentar o CI da *tag*. Tanto a bobine da antena do leitor como da *tag* são circuitos indutivos-capacitivos (LC), maximizando a transferência de energia do leitor para a *tag* quando sincronizada com a frequência correta.

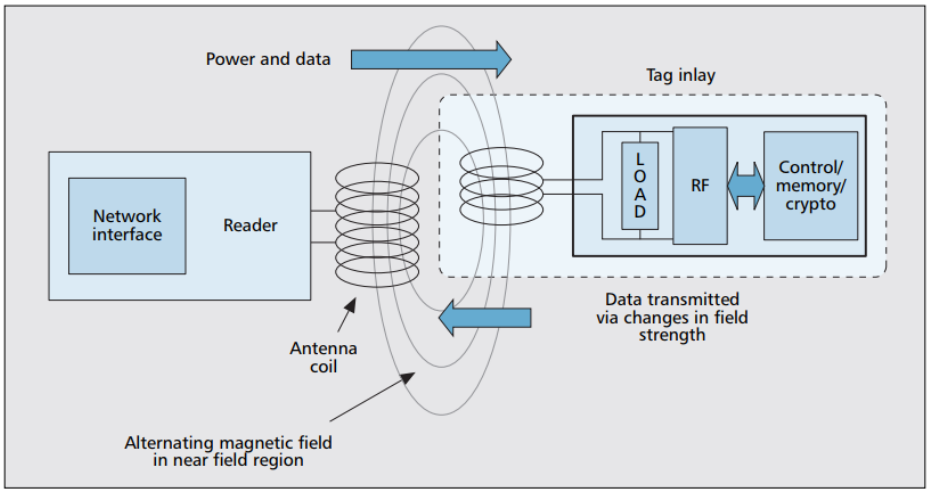


Figura 2-3: Acoplamento indutivo [10].

Uma vez alimentadas as *tags*, a comunicação entre o leitor e a *tag* (e vice-versa) inicia- se através de uma modulação em amplitude (AM) ou em frequência (FM). O leitor modula a

amplitude do campo magnético de acordo com a informação digital ou o sinal de banda base a ser transmitido à *tag*. A *tag* transmite o seu código de identificação (ID) ligando e desligando a sua resistência de carga de acordo com o seu ID, um fenómeno referido como modulação de carga. O leitor identifica estas variações e desmodula o ID transmitido [11]. Alguns exemplos de formatos de *tags* são mostrados na Figura 2-5.

O limite entre as regiões do campo próximo e do campo distante é inversamente proporcional à frequência e aproximadamente igual a $c/2\pi f$, onde $c$ é a velocidade da luz. Por conseguinte, são utilizadas apenas as frequências mais baixas nas *tags* de acoplamento de campo próximo. As *tags* mais comuns operam a 125 kHz (LF) e 13,56 MHz (HF). O valor do campo magnético diminui na região do campo distante. Outra desvantagem é a baixa largura de banda e, portanto, a baixa taxa de transferência de dados [5].

**2) Sistemas acoplados electromagneticamente:** são sistemas também chamados sistemas de *Backscattering*, que operam nas bandas de ultra alta frequência (*Ultra High Frequency* - UHF) e nas micro-ondas. Conforme se apresenta na Figura 2-4, o dipolo da antena do leitor envia uma onda eletromagnética (EM) contendo energia AC para as *tags* [11], resultando numa diferença de potencial no dipolo da antena das *tags*, alimentando assim o seu CI [12]. A comunicação de uma *tag* com o leitor é então conseguida variando a amplitude ou a frequência das ondas EM refletidas pela antena de *tag* de acordo com os dados digitais a serem transmitidos.

Os sistemas de *Backscattering* como atuam em cenários de campo distante apresentam problemas que não existem nos sistemas HF ou LF. Problemas com a absorção de sinal ou reflexão do campo do leitor devido a objetos são as mais comuns. As reflexões podem causar interferência ou mesmo cancelamento dos sinais principais.

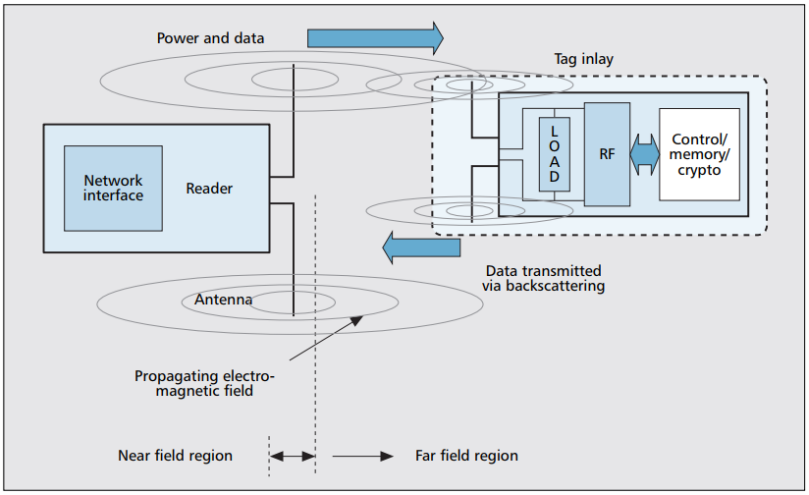


Figura 2-4: Acoplamento Eletromagnético (*Backscatterring*) [5].

O acoplamento de campo distante *(Far-Field)* é bastante utilizado em sistemas RFID de longo alcance e, em contraste com o campo próximo *(Near-Field)*, não existe limite de alcance para RFID de campo distante. A vantagem de uma *tag* de campo distante *(Far-Field)* que opera em alta frequência é que a antena pode ser de pequena dimensão, levando a baixos custos de fabricação e montagem. Com CI's inovadores, combinados com os avanços na tecnologia de silício, permitiram criar *tags* passivas de campo distante *(Far-Field)*, que consomem apenas alguns microwatts.

As *tags* de campos distantes *(Far-Field)* geralmente operam na faixa UHF (860-960 MHz) ou na banda de micro-ondas a 2,45 GHz. Vários formatos e formas de antena são usados para *tags* de campo distante *(Far-Field)* para atender aos requisitos das mais variadas aplicações (Figura 2-5).

Figura 2-5: Tipos de *tags* passivas [13].

**B. Frequência de funcionamento**

Os sistemas RFID operam em diferentes bandas de frequências que podem ir de 100 kHz a 5.8 GHz. No entanto só utilizam as de frequência Industrial, Científica e Médica (ISM), que tem como característica fundamental o facto de não carecer de licenciamento e por consequência, custos de aquisição. No entanto, a utilização destas frequências, necessita de obedecer às regras impostas pela Autoridade Nacional de Comunicações dos diferentes países.

A Figura 2-6 apresenta a organização do espectro eletromagnético com particular ênfase para as ondas de rádio onde podemos observar o posicionamento das bandas de frequências utilizadas nos sistemas de RFID, as bandas de LF, HF e UHF.

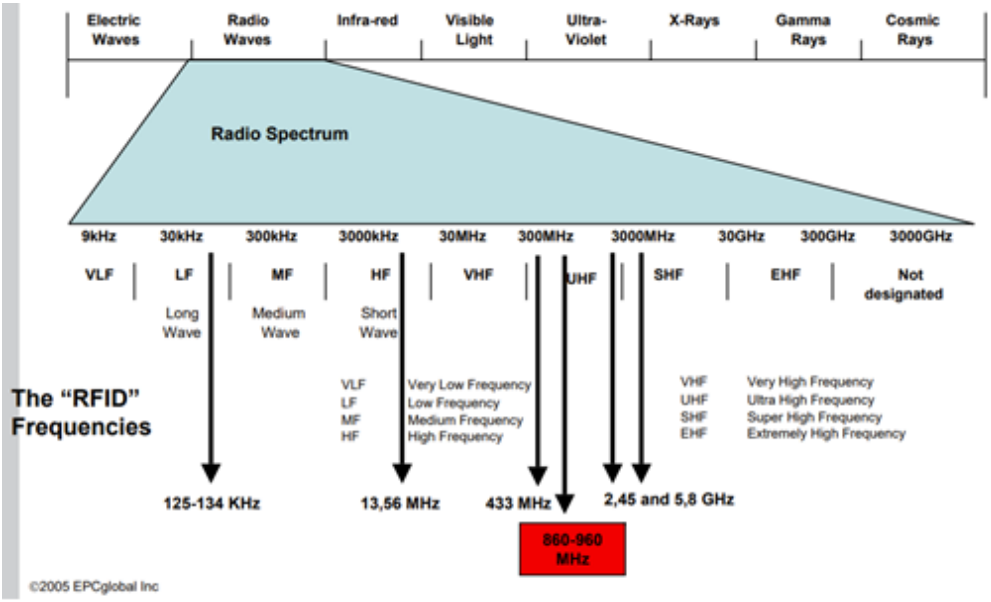


Figura 2-6: Espectro Eletromagnético [14].

Relativamente ao acoplamento magnético ou indutivo utilizado em sistemas de campo próximo, são utilizadas as bandas LF que se situam entre os 125-134kHz e como solução de HF é utilizada a banda de 13,56MHz. Já para os sistemas de acoplamento eletromagnético ou de *Backscatterring*, como abordado, utilizam as bandas de UHF, com as frequências de 433MHz, a banda entre 860-960MHz e 2.4GHz.

### C. Tipos de *tag*

As *tags* são o elemento básico de um sistema RFID. Uma *tag* consiste num CI e elementos de acoplamento, mas já estão a ser desenvolvidas *tags* RFID sem CI (*Chipless tags*) e prometem economias de custos significativas, uma vez que podem ser impressas diretamente na maioria dos produtos [11].

Existem três tipos de *tags*: passiva, ativa e semi-passiva [12]. As *tags* passivas têm capacidade computacional limitada, nenhuma capacidade de detetar o canal de comunicação, detetar colisões e comunicar-se entre si. As *tags* semi-passivas são semelhantes às *tags* passivas, mas têm a vantagem de ter uma fonte de alimentação que pode ser utilizada para alimentar o seu CI. As *tags* ativas têm carga própria e são consequentemente mais caras quando comparadas com as demais e podem detetar o canal de comunicação e detetar colisões. A Tabela 2-1 que resume os vários tipos de *tags*, envolvendo os diferentes sistemas de acoplamento de sistemas RFID abordados [12].

Tabela 2-1: Tipos de *Tags* de RFID.

| **Tipos de Tags de RFID** | | | | |
|---|---|---|---|---|
| **Critério** | LF | HF | UHF | Micro-ondas |
| **Frequência** | < 135 kHz | 13,56 MHz | 860 – 960 MHz | 2,45 GHz |
| **Acoplamento** | Indutivo | | *Backscattering* | |
| **Características da *tag*** | Passiva | | Passiva, Semi-passiva e Ativa | Ativa e Passiva |
| **Limites de comunicação** | Near-field | | Far-Field | |
| **Standards** | ISO 18000-2 | ISO 18000-3, AutoID Class 1 | ISO 18000-6, AutoID Class 0, AutoID Class 1, | ISO 18000-4 |
| **Taxa de transferência de dados** | < 10 kbits/s | < 100 kbits/s | < 100 kbits/s | < 200 kbits/s |
| **Aplicações típicas** | Marcação de animais, controlo de acessos, identificação de veículos, controlo de contentores | Controlo de acessos, smartcards, marcação de bens, bilheteiras, marcação de documentos, controlo de bagagem, bibliotecas | Controlo de bagagem, cobrança de portagens, gestão de cadeias de abastecimento | Cobrança de portagens, controlo de bens a tempo real, controlo de linhas de produção |
| **Nº de tags lidas por segundo** | Menor | ⟷ | | Maior |
| **Consumo de potência da tag** | Menor | ⟷ | | Maior |
| **Largura de banda** | Menor | ⟷ | | Maior |

**Classes das *TAGS*:**

As *tags* são ainda divididas em diversas classes consoante a sua capacidade. A *EPCglobal* [15], entidade pertencente à GS1 e responsável por desenvolver os *standards* para o código de produto eletrónico (EPC) que suporte a tecnologia RFID, definiu seis classificações para *tags* RFID (0 a 5). A descrição geral da funcionalidade que cada classe é [16]:

**Classe 0:** fornece a capacidade passiva básica de RF. A classe 0 é programada de fábrica.
**Classe 1:** também fornece a capacidade passiva básica, mas as *tags* são programáveis pelo utilizador *(WORM – Write Once Read Many).*
**Classe 2:** Tem uma funcionalidade adicional, que inclui criptografia e memória RF de leitura e gravação.
**Classe 3:** Baterias *on-board* para alimentar o circuito lógico. Fornece comunicações de longo alcance e banda larga. Permite escrita e leitura com sensores acoplados, capaz de guardar parâmetros de temperatura, pressão, movimento, etc. Podem ser semi-passivas ou ativas.
**Classe 4:** Permite comunicações *peer-to-peer* e também pode incluir sensores adicionais às *tags,* sendo consideradas ativas.
**Classe 5:** As *tags* Classe 5 possuem energia suficiente para ativar outras *tags* e podem ser efetivamente classificadas como leitor.

As *tags* passivas, sem fonte de energia própria (utilizam energia fornecida pela onda de RF criada pelo leitor) estão inseridas nas classes 0 a 2. As classes 3 e 4 são *tags* ativas, que possuem uma fonte de energia interna, que fornece a energia necessária para o funcionamento da *tag* ao longo de um período de tempo. A classe 5 é reservada para *tags* ativas que podem ler dados de outras *tags*.

**Modulação de Sinais RFID**

Para se estabelecer uma comunicação em sistemas RFID, os dados são enviados através de uma onda RF utilizando um processo de modulação. Neste processo, os dados enviados na comunicação ("1"s e"0"s lógicos) são modelados com a onda portadora. Geralmente a frequência do sinal de dados é inferior à frequência da portadora e tem como função permitir a sincronização do leitor com a *tag*.

Para se compreender este processo de modulação, consideremos um sistema de acoplamento eletromagnético, com frequência de portadora na banda UHF, sendo que a frequência de dados terá um valor bastante inferior [17]. A Figura 2-7 apresenta de forma gráfica os sinais descritos.

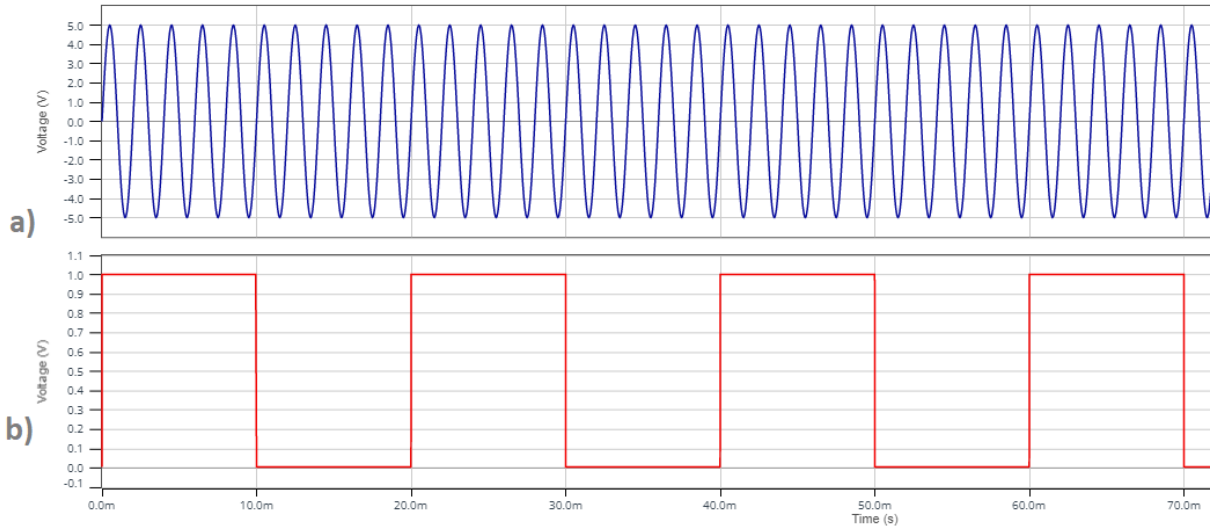


Figura 2-7: a) Sinal de portadora UHF b) Sinal de dados a transmitir.

Observando a Figura 2-7, verificamos que, tal como descrito, a frequência do sinal da portadora é bastante superior à frequência doi sinal de dados. Já relativamente aos bits de dados, estes encontram-se a "0" e "1" lógicos, valores que se pretende modular e enviar.

Os dois principais tipos de modulação deste tipo de sistemas são: Modelação por Amplitude (AM) e Modelação por Frequência (FM). A AM, mais precisamente *Amplitude Shift-Keying* (ASK), funciona utilizando o próprio fluxo de dados para variar a amplitude da portadora, neste caso a potência do sinal transmitido. Na Figura 2-8 apresenta-se um exemplo de modelação AM para o referido sinal.

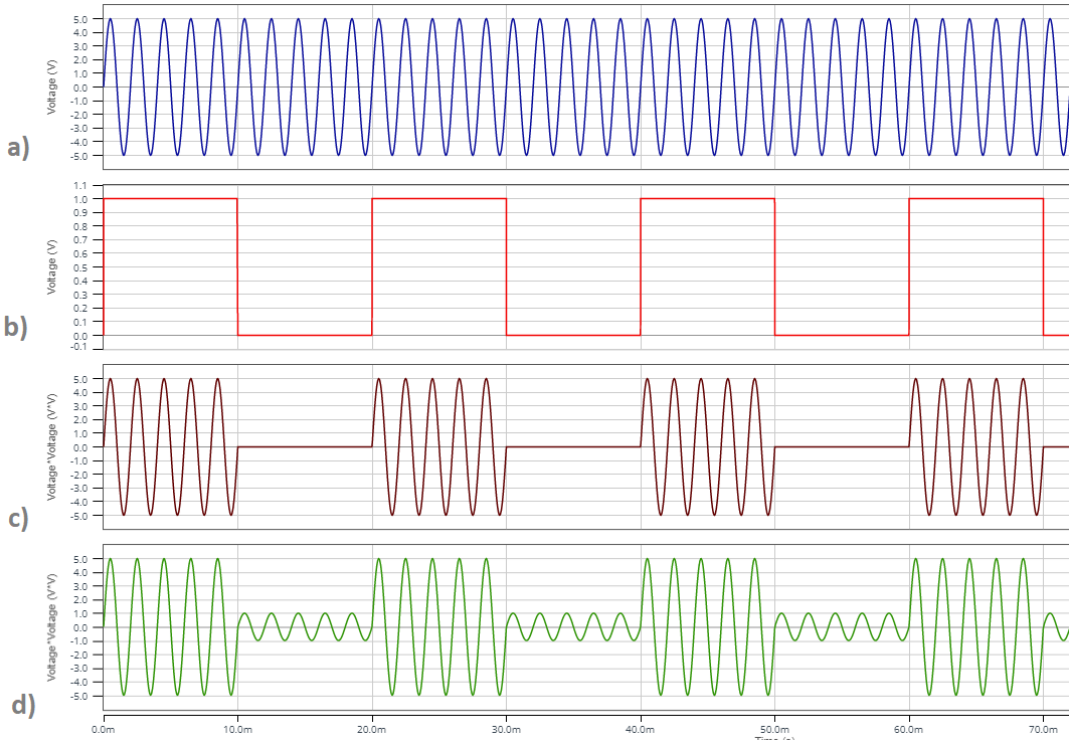


Figura 2-8: Modulação da Amplitude a) portadora, b) dados, c) OOK, d) BASK [17].

Como se pode observar na Figura 2-8, na parte superior o sinal da portadora que associado ao sinal de dados com a frequência inferior origina um sinal resultante com uma diferença nos sinais de "0" e "1" lógicos enviados. Neste caso temos duas possibilidades, *on-off Keying* (OOK), em que a amplitude do sinal enviado é "0" quando o sinal de dados é "0" lógico e *Binary Amplitude Shift Keying* (BASK), em que temos duas amplitudes, uma para "1" lógico e outra para "0" lógico.

No que à modulação FM diz respeito, mantém-se constante a amplitude do sinal da portadora, mas utiliza a variação da frequência para transmissão dos dados a enviar, como se exemplifica na Figura 2-9.

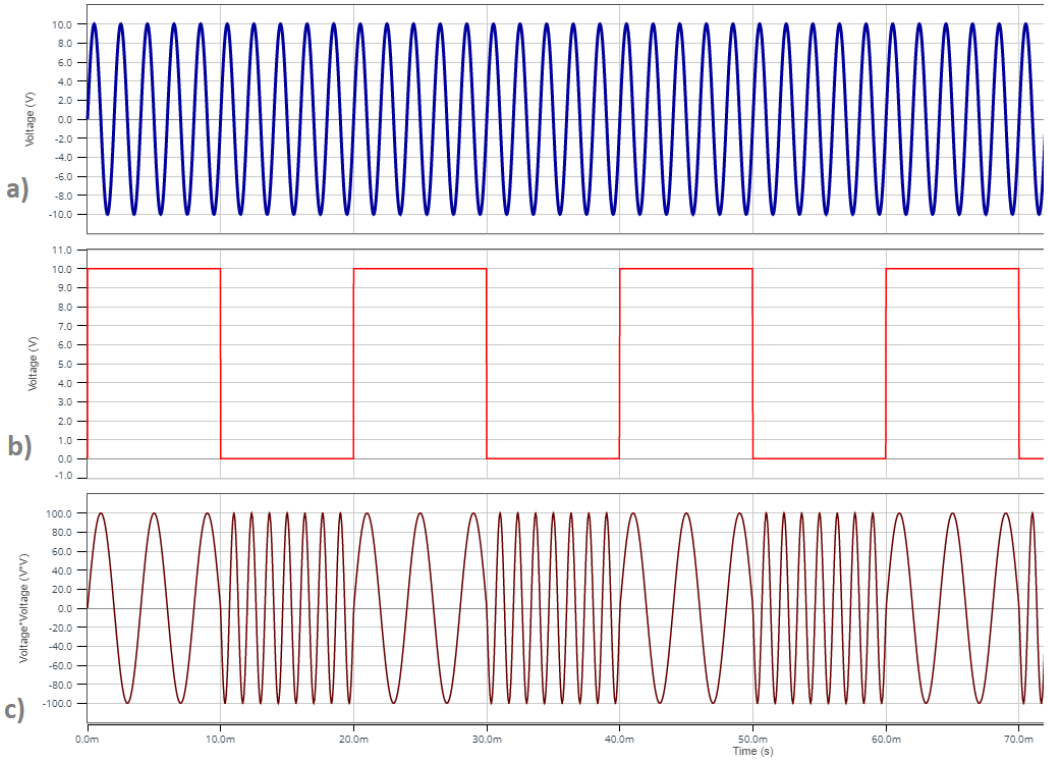


Figura 2-9: Modulação da Frequência [17].

Na parte superior encontra-se o sinal da portadora novamente à frequência de 915MHz que também associado ao sinal de dados com a frequência de 62,5kHz origina um sinal resultante com uma diferença de frequência no momento que são enviados os sinais de "0" e "1" e mantendo a frequência da portadora nos restantes momentos.

### 2.1.2. NFC

Um dos requisitos do projeto era existirem mais que uma alternativa para a identificação dos estudantes. Uma das metodologias utilizadas é o sistema comunicação de campo próximo NFC (Near-Field Communication - NFC) para o caso dos estudantes se esquecerem do cartão de

identificação (com RFID). O dispositivo identificador de NFC pode integrar objetos diversos, por exemplo o porta-chaves de veículo ou de chaves de casa.

Um sistema NFC consiste numa tecnologia de radiofrequência de curto alcance que permite a comunicação entre dispositivos muito próximos (até cerca de dez centímetros). Como o alcance da transmissão é tão curto, as transações baseadas em NFC são inerentemente mais seguras, assunto detalhado mais adiante. Os dispositivos podem comunicar entre si, podendo enviar e receber dados (um de cada vez). O NFC baseia-se em RFID já que utiliza os mesmos princípios, isto é, utiliza sinais de RF para comunicar e, tal como o próprio nome indica, comunicação de campo próximo. O NFC começou por ser padrão definido pelo NFC Forum, um consórcio global de hardware, software/aplicações, empresas de cartões de crédito, bancos, empresas de telecomunicações, entre outros [18]. Opera na frequência de 13,56 MHz e suporta diferentes taxas de transmissão de dados (106 kbps, 212 kbps e 424 kbps). Utiliza a modulação AM para comunicação entre dois dispositivos NFC que estão em proximidade. A tecnologia foi desenvolvida por fabricantes de telefones móveis que tinham como objetivo permitir troca de dados de forma simples entre dispositivos, mas atualmente as suas utilizações são muito diversas, tais como métodos de pagamento por telemóvel, aquisição e ativação de páginas de internet a partir de fontes NFC externas (p.ex. inseridas em cartazes publicitários), entre outros.

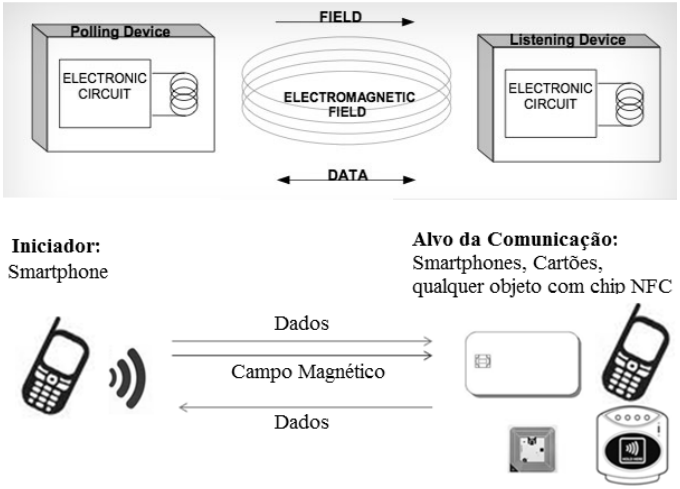


Figura 2-10: Configuração básica de sistema NFC. [19].

A comunicação por NFC é realizada entre dois dispositivos em que um assume a função de *reader* (o iniciador) e outro assume a função de *tag* (o alvo da comunicação). Desta forma, é enviado um sinal de RF do iniciador que é recebido pelo alvo.

Como observável no exemplo da Figura 2-10, o *Smartphone* que pretende comunicar por NFC com outro dispositivo, funciona como iniciador e utiliza a energia da sua bateria para enviar os

sinais RF e gerar um campo magnético em seu redor. Este campo irá criar um campo magnético induzido noutros dispositivos tais como *Smartphones*, cartões, ou outro qualquer objeto que tenho um *chip* de NFC.

**A. Modos de Comunicação**

Em NFC, o estabelecimento da comunicação pode ser em modo ativo ou modo passivo. O dispositivo ativo é aquele que gera RF e tem a sua própria fonte de alimentação. O dispositivo passivo é alimentado por outro dispositivo ativo [20][21]. Quanto ao tipo de comunicação estabelecida, este pode ser de duas formas [20][22]:

- **Comunicação bidirecional:** dispositivos capazes de ler e escrever de um para o outro. Por exemplo, podem-se conectar dois dispositivos *Android* para transferir dados entre si, tais como contatos, links ou fotos, etc.
- **Comunicação unidirecional:** a leitura e escrita para e de um chip NFC é feito por um dispositivo alimentado (telefone, leitor de cartões de crédito ou cartão de transporte de passageiros).

**B. Modos de operação**

Os dispositivos NFC podem em um conjunto de diferentes modos de operação: Modo leitor/ gravador, modo *peer-to-peer* ou modo de emulação de cartão [20]. Esses modos de operação são baseados nos padrões [19]:

- **Modo leitura / gravação:** No modo leitor/gravador, o dispositivo NFC habilitado lê *tags* NFC tal como cartões *contacless*, *smarcards* ou *tags* RFID [20][23]. Se a *tag* se encontra próxima, é detetada e podem ser lidos ou escritos nela. Um exemplo deste modo de operação são os cartazes inteligentes (*smartposter*), bastante utilizados para comunicação com *Smartphones,* que neste caso funciona como leitor. Ao aproximar o *Smartphone* do cartaz é possível receber dados ou lançar alguma aplicação nele contida, geralmente aplicação de internet para abrir uma página específica.
- **Modo Peer-to-Peer:** Dois dispositivos alimentados podem conectar-se em modo *peer-to-peer*, sendo esta uma forma específica da tecnologia NFC. Este modo permite que os dois dispositivos comuniquem entre si como se estivessem ligados em rede.
- **Modo de Emulação de Cartão:** No modo de emulação de cartão, o próprio dispositivo atua como uma *tag* NFC, colocando o dispositivo em método de comunicação passiva. No caso de um *smartphone,* este não gera o seu próprio campo de RF, em vez disso

deixa que seja o dispositivo leitor NFC a criar esse campo. Neste caso o *Smartphone* simula uma *tag* que pode ser acedida por um leitor NFC externo, tal como um terminal portátil de um ponto-de-venda *(POS – point-of-sale).*

### C. Tipos de *tag*

As *tags* NFC podem ser utilizadas praticamente em qualquer tipo de objeto. Para garantir a interoperabilidade entre diferentes fornecedores de *tags* NFC e fabricantes de dispositivos NFC, o NFC Forum definiu 5 tipos de *tags* [18] [19] [24]:

- ***Tag* do Tipo 1:** As *tags* Tipo 1 são de baixo custo e neste caso ideais para a generalidade das aplicações NFC. É baseada no padrão ISO-14443A, sendo capaz de ser lida e reescrita após saída de fábrica. A *tag* tipo 1 pode ainda ser configurada para ser apenas para modo de leitura, tem 96 bytes de memória e pode ser expansível até 2 kB**,** tendo velocidade de comunicação de 106 kbits/s e não possui nenhuma proteção contra colisões de dados.
- ***Tag* do Tipo 2:** As *tags* tipo 2 são semelhantes às *tags* tipo 1 e são derivadas da NXP / Philips MIFARE Ultralight tag [24]. São em tudo semelhantes em termos de características com as *tags* tipo 1, com a exceção de possuírem suporte anticolisão de dados.
- ***Tag* do Tipo 3:** As *tags* Tipo 3 são derivadas das *tags Sony FeliCa* [24]. Estas *tags* são mais caras do que do tipo 1 e 2. Têm base no Padrão Industrial Japonês (JIS) X 6319-4, são pré-configuradas em fábrica para ser de leitura e regraváveis, ou apenas para leitura, tem memória variável até 1 MB, suportam duas velocidades de comunicação (212 ou 424 kbits/s) e tem suporte anticolisão.
- ***Tag* do Tipo 4:** As *tags* Tipo 4 também são bastante semelhantes às *tags* de Tipo 1 e derivam das *tags* NXP *DESFire* [24]. São baseadas no padrão ISO-14443A e são pré-configuradas em fábrica para ser de leitura e regraváveis, ou apenas para leitura. Possuem memória variável até 32 kB e suportam três velocidades de comunicação diferentes (106, 212 ou 424 kbits/s) e têm suporte anticolisão.
- ***Tag* do Tipo 5:** As *tags* Tipo 5 definem como um dispositivo NFC pode interagir com uma *tag* NFC Forum Type 5, ou seja, uma *tag* ISO/IEC 15693 configurada para poder armazenar uma mensagem *NFC Data Exchange Format* (NDEF) [18]. Tal como acontece com outras especificações de operação de *tags* do NFC Forum, a especificação define como interagir, não como construir uma *tag*.

**Padrões do sistema NFC**

**1) ISO 14443**

O ISO 14443 é um padrão internacional bastante conhecido e originalmente desenvolvido para cartões do tipo *contactless*, para a frequência de operação de 13,56 MHz [24][25]. O ISO 14443 define um conjunto de protocolos que vão desde o sinal RF até ao protocolo de comando.
Existem duas versões para os sinais RF ISO 14443-2 com diferentes modulações e métodos de codificação de bits. Da mesma forma, o ISO 14443 especifica duas versões do enquadramento de pacotes e parte de protocolos de baixo nível (ISO 14443-3). Possui ainda uma parte que define uma interface de comando para transferência de informações. (ISO 14443-4).

**2) NFCIP-1**

A comunicação *peer-to-peer* entre dois dispositivos NFC é regulada pelo Interface e Protocolo de Especificações, NFCIP-1, também conhecido como ISO 18092 ou ECMA-340 [24][25][26]. O conjunto de protocolos no NFCIP-1 é baseado no ISO 14443. A principal diferença é um novo protocolo de comando, que substitui a parte superior do conjunto que compõe o protocolo geral. O NFCIP-1 inclui dois modos de comunicação que permitem que um dispositivo NFC comunique com outros dispositivos NFC de forma peer-to-peer, bem como com *tags* NFC baseadas em NFCIP-1.

**3) *FeliCa***

*FeliCa* é uma tecnologia proprietária de *tags* NFC desenvolvida pela Sony [24][27], sendo amplamente utilizada em aplicações de pagamento e transporte nos mercados asiáticos. As *tags FeliCa* também foram integradas em alguns modelos de telefones móveis com o sistema *Mobile FeliCa*. São padronizadas para a indústria japonesa e são baseadas no modo passivo do ISO 18092, com recursos de autenticação e criptografia adicionados.

**4) MIFARE**

O *MIFARE* refere-se a um tipo de *tag* NFC desenvolvida pela NXP *Semiconductors* [24]. As *tags MIFARE* são amplamente utilizadas como cartões de memória em aplicações de transporte. A principal diferença é um novo protocolo de comando, que substitui a parte superior do conjunto que compõe o protocolo geral.

### 2.1.3. Identificação por Impressão digital

O método de identificação por impressão digital já é bastante conhecido e assenta em duas grandes premissas:

- Não existem dois dedos diferentes com padrões de relevo iguais;
- Os padrões de relevo de um dedo não se alteram ao longo da vida (em condições normais).

Com estas premissas garante-se que a impressão digital é única e não variável, podendo ser uma solução para este projeto.

O funcionamento de um sensor de impressão digital tem por base (na sua forma mais simples) conseguir realizar o registo de uma impressão digital e guardá-la numa base de dados para posterior reconhecimento. Pode dividir-se em várias fases da seguinte forma [28][29]:

- Fase de Registo (*enrollment*): digitalização da imagem da impressão digital de um indivíduo e todas as suas especificidades numa memória.
- Fase de Reconhecimento: esta fase subdivide-se em dois métodos:
  - Verificação (*verification*): para os casos em que a base de dados possui apenas uma impressão digital válida. Neste tipo de identificação apenas se pretende a confirmação da identidade do utilizador do sistema, sendo o tipo de resposta binária: sim ou não. Aqui a comparação de impressões digitais é de 1:1, ou seja, uma lida e uma armazenada, este método utiliza-se em dispositivos de índole mais pessoal (p.ex. em *Smartphones*);
  - Identificação (*Identification*), para os casos em que temos mais do que uma impressão digital na base de dados e esta será selecionada de entre um conjunto. Aqui a comparação de impressões digitais é de 1:N, ou seja, uma lida de entre várias armazenada, este método utiliza-se geralmente em sistemas de controlo de acessos em empresas ou mesmo para controlo e registo de assiduidade de colaboradores;

Na Figura 2-11, são apresentados os diagramas de blocos dos procedimentos de registo, de verificação e de identificação descritos anteriormente.

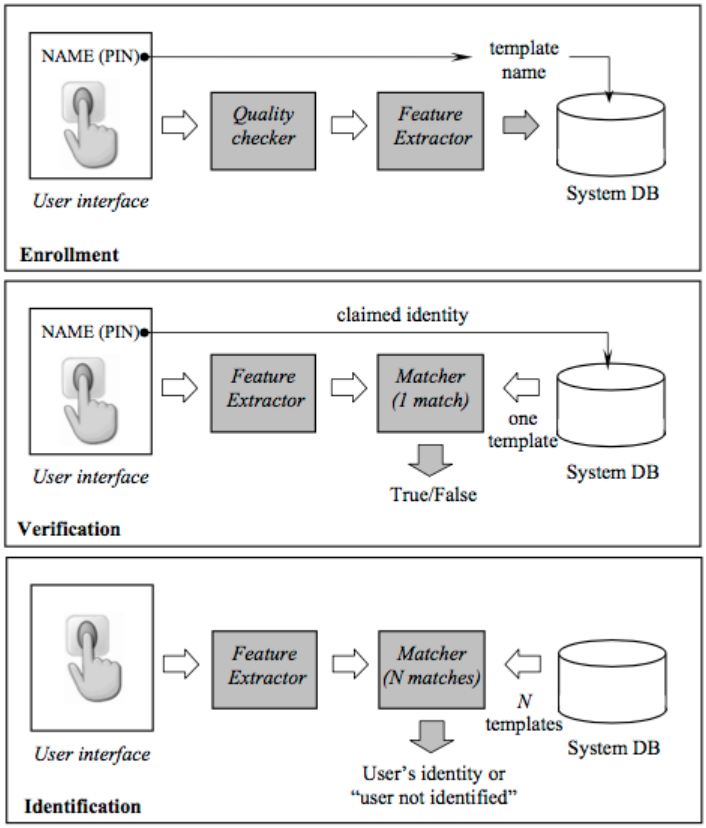


Figura 2-11: Diagramas de blocos de tarefas de registo, verificação e identificação [28].

Nos diagramas de blocos aparecem ainda os seguintes termos:

- Verificador de qualidade (*Quality Checker*): aparece no registo para garantir que a impressão digital lida reúne as condições para ser analisada, guardada e utilizada;
- Extrator de características (*Feature Extractor*): aparece tanto no registo como no reconhecimento, e consiste na conversão da imagem da impressão digital numa representação digital das características;
- Comparador (*Matcher*): realiza a comparação da imagem lida com a(s) imagem(s) na base de dados.

A recolha da imagem de impressão digital e a posterior digitalização tem em conta os conceitos de divisão por classes, de extração de minúcias (características locais na formação das estruturas das cristas papilares) e de pontos singulares.

Uma imagem de uma impressão digital pode ter entre 40 e 100 minúcias [29] e são mais do que suficiente para diferenciar um indivíduo. A Figura 2-12, apresenta vários tipos de minúcias mais comuns.

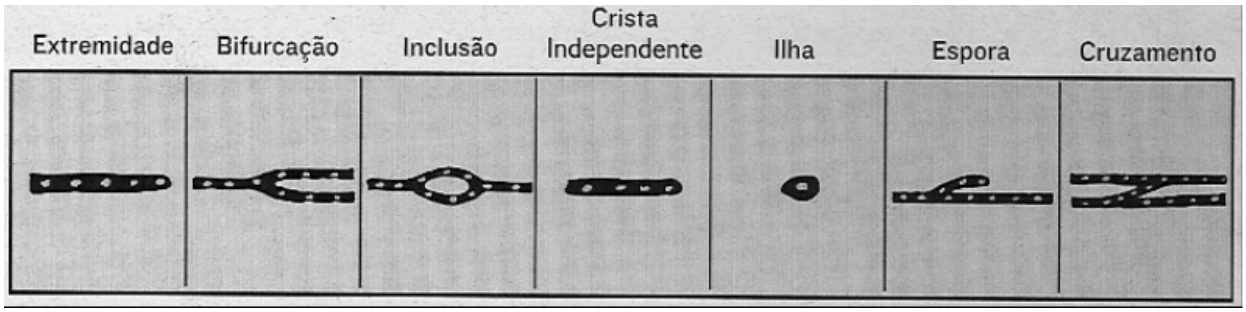


Figura 2-12: Tipos de minúcias [29].

As minúcias podem ser divididas em 5 classes [29]: arco plano (*arch*), arco angular (*tented arch*), laço à esquerda (*left loop*), laço à direita (*right loop*) e espiral (*whorl*), podendo ainda ter ainda algumas regiões singulares como laço, delta e espiral [28][29].

A Figura 2-13 apresenta um conjunto de impressões digitais pertencentes às principais classes estabelecidas.

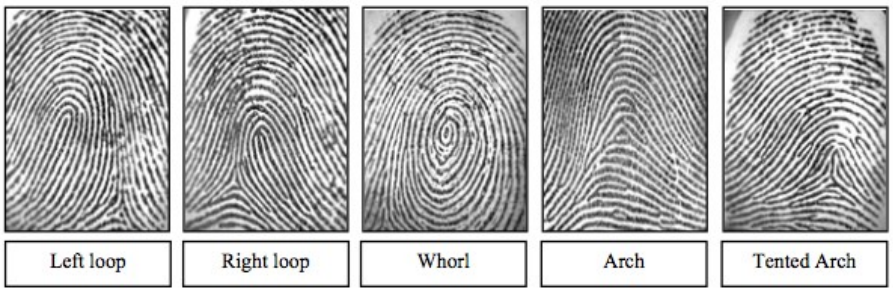


Figura 2-13: Impressão digital de cada uma das classes [28].

Observa-se que as características em cada uma das classes são visualmente bastante diferentes e que a qualquer impressão digital está inserida em uma das classes apresentadas.

Relativamente ao conceito de regiões singulares, a Figura 2-14 apresenta os cumes, vales, regiões singulares delta, laço e espiral e ainda o centro da impressão digital (*core*).

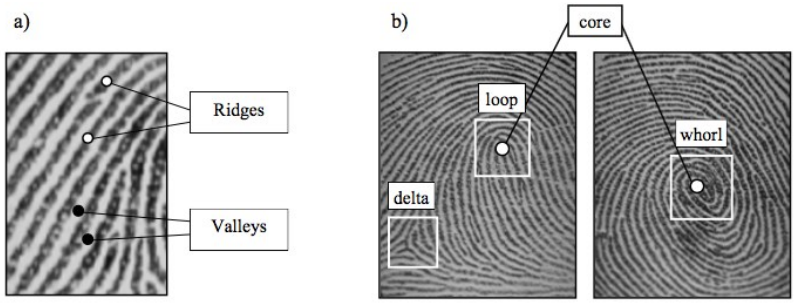


Figura 2-14: a) Cumes (*Ridges*) e Vales (*Valleys*) na epiderme do dedo; b) Regiões singulares [28].

O processo de extração de características apresentado na Figura 2-12, consiste no registo das coordenadas (x,y) e do ângulo das minúcias detetadas. A Figura 2-15, apresenta um exemplo desse processo.

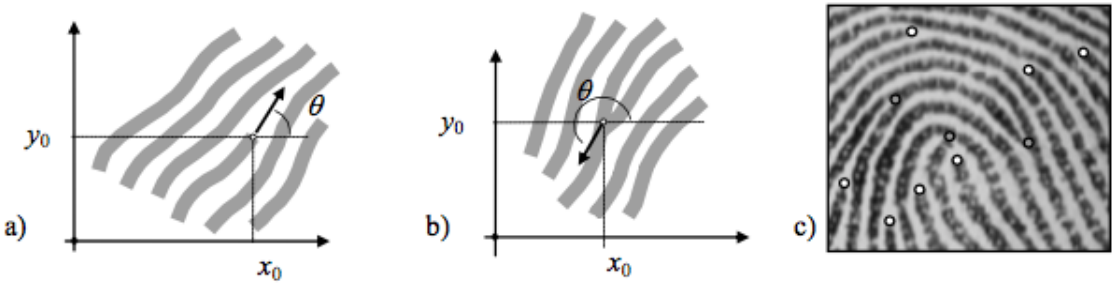


Figura 2-15: a) Extremidade; b) Bifurcação; c) Minúcias detetadas numa imagem [28].

Um dos elementos principais de um sensor de impressão digital é o elemento que realiza a captação da imagem. A grande maioria dos elementos de captação de imagens pertencem a três grupos sensoriais: ótico, estado sólido e ultrassom [28].

Os sensores óticos, são baseados na utilização de um prisma de vidro, composto por uma face superior onde se coloca o dedo, por uma face sujeita à emissão de radiação luminosa e outra face que recebe, através de uma lente e de um sensor, a luz emitida e refletida por parte do dedo, destacando os cumes e os vales que compõem a impressão digital. Os cumes refletem a luz e os vales absorvem a luz, o que permite distingui-los. Pode-se observar a esquematização da organização do sensor através da análise da Figura 2-16.

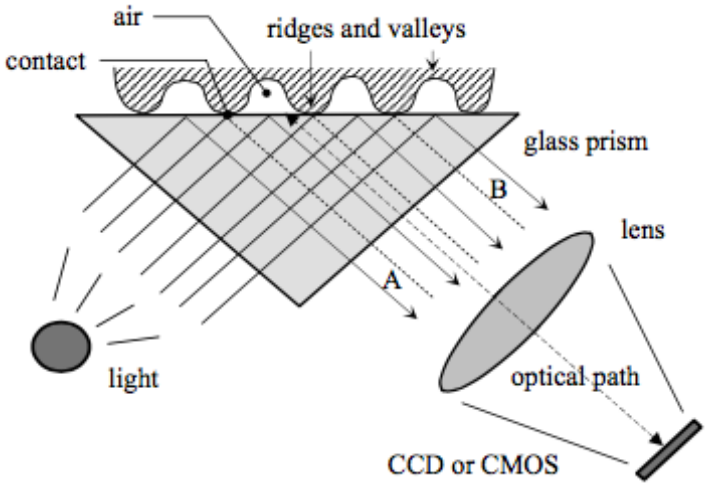


Figura 2-16: Funcionamento de um sensor de impressão digital ótico [28].

Os sensores de estado sólido (semicondutores), construídos em silício, são baseados na utilização de um arranjo de micro sensores, funcionando como pixéis e que podem aproveitar

o efeito térmico, o efeito piezoelétrico ou mesmo o efeito capacitivo. No caso do efeito capacitivo (Figura 2-17), o utilizador coloca o dedo nos micro sensores de silício e as características da sua impressão digital (cumes e vales) provocam efeitos distintos nos micro sensores, passando a funcionar como micro condensadores. A variação da distância dos cumes e dos vales produz uma variação diferenciada na capacidade dos micro condensadores.

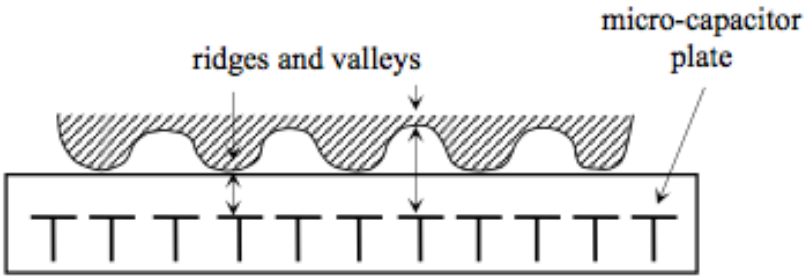


Figura 2-17: Funcionamento de um sensor de impressão digital de estado sólido.

Relativamente à captação da impressão digital por sensores de ultrassom, é utilizado o conceito da emissão da radiação sonora e na deteção do eco para medição de distâncias. Sabendo que existe diferença na distância dos cumes e dos vales ao elemento sensor, existe também um eco diferente, tal como mostra a Figura 2-18.

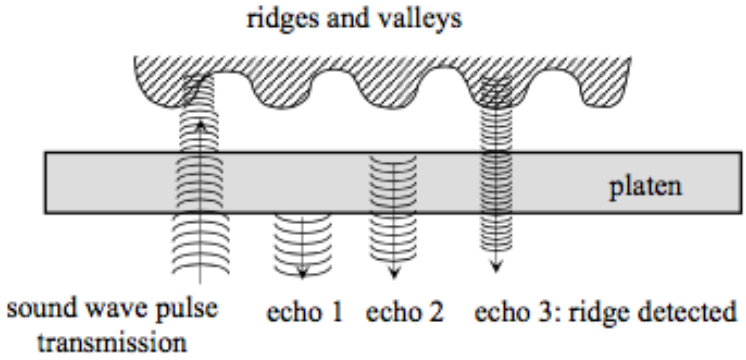


Figura 2-18: Princípio de funcionamento de um sensor de impressão digital por ultrassom.

### 2.1.4. Bluetooth

O termo *Bluetooth* é uma especificação para comunicações baseadas em sinais RF de curto alcance e utilizado, sobretudo, em dispositivos de índole pessoal. Este padrão, pertence ao grupo das redes pessoais sem fios (WPAN – *Wireless Personal Area Network*) e tem na *Bluetoot* SIG (*Bluetooth Special Interest Group*), consórcio composto por mais 36000 empresas, uma entidade que gere e desenvolve os padrões utilizados neste tipo de comunicação [30].

O padrão *Bluetooth* oferece dois tipos de métodos de comunicação, *Bluetooth Classic (Bluetooth Basic Rate / Enhanced Data Rate (BR/EDR))* e *Bluetooth Low Energy* (BLE) que operam ambas na banda de frequência ISM de 2.4GHz (2.402 – 2.480GHz). Entre as diferenças, descritas na tabela seguinte (Tabela 2-1), encontram-se o número de canais disponíveis, 79 canais para BR/EDR e 40 para BLE.

Tabela 2-2: Características principais do padrão *Bluetooth* [30][31].

| Características | *Bluetoot Classic (BR/EDR)* | *Bluotooth Low Energy (BLE)* |
|---|---|---|
| **Bandas de Frequência** | 2,4GHz ISM (2,402-2,480GHz) | 2,4GHz ISM (2,402-2,480GHz) |
| **Número de Canais** | 79 canais | 40 canais |
| **Separação entre Canais** | 1 MHz | 2 MHz |
| **Potência de Transmissão** | ≤100mW (+20dB) | ≤100mW (+20dB) |
| **Alcance** | Até 100m | Até 100m |
| **Débito Binário** | 2.1 a 24Mbps (50Mbits teóricos) | 2.1 a 24Mbps (50Mbits teóricos) |
| **Modo de Acesso** | FHSS – CDMA/TDMA | FHSS – CDMA/TDMA |
| **Modulação** | GFSK, π/ 4 DQPSK, 8DQPSK | GFSK |
| **Topologias de Comunicação** | *Point-to-Point* (com *Piconet*) | *Point-to-Point/ Broadcast/Mesh* |
| **Posicionamento do dispositivo** | - | Presença/ Proximidade/ Direção/Distância |

A Tabela 2-2 apresenta o resumo das principais características dos padrões *Bluetooth Classic* e *Bluetooth BLE.* Podemos observar que em relação a potências de transmissão, podem ir até 100mW, o que lhes confere comunicações até aproximadamente 100m, no entanto, é realizada uma divisão por classes de acordo com a potência a utilizar e respetivas aplicações [31], [32].

**A. Classes de potências**

- Classe 1 – Para aplicações industriais;
- Classe 2 – Aplicações generalista e a mais comum (*Smartphones*);
- Classe 3 – Dispositivos de baixo consumo;
- Classe 4 – Dispositivos de muito baixo consumo e curto alcance.

A

Tabela 2-3 resume as características de cada uma das classes em termos de potência transmitida e de alcance de comunicação.

Tabela 2-3: Classes de *Bluetooth* [31][32].

| Classes | *Máxima Potência Permitida* | | *Alcance* |
|---|---|---|---|
| | **mW** | **dB** | **m** |
| **Classe 1** | 100 | 20 | ~100 |
| **Classe 2** | 2,5 | 4 | ~10 |
| **Classe 3** | 1 | 0 | ~1 |
| **Classe 4** | 0,5 | -3 | ~0,5 |

### B. Modo de Acesso às ondas RF

Quanto ao modo de acesso, o padrão *Bluetooth* utiliza a tecnologia de *Frequency-Hopping Spread Spectrum* (FHSS) que consiste numa divisão dos dados a transmitir em pacotes e envia cada um dos pacotes pelo número de canais disponíveis (79 para BR/EDR e 40 para BLE). O gráfico presente na Figura 2-19 demonstra de forma simplificada o processo de FHSS.

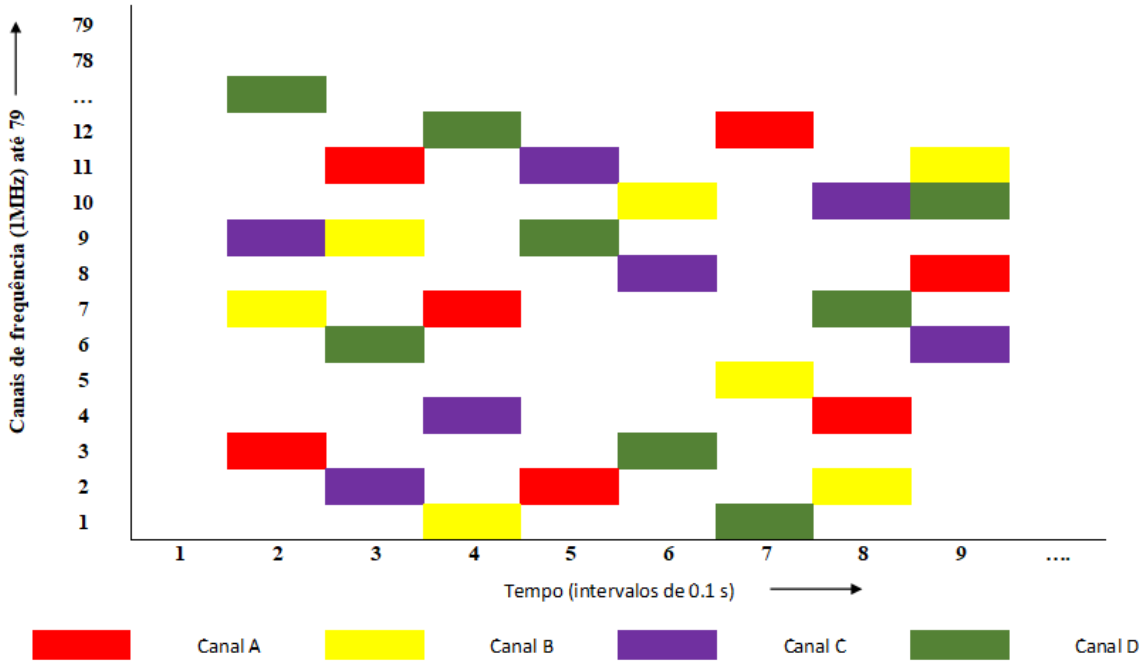


Figura 2-19: Exemplo de utilização de FHSS [31][32]

Para o caso de *Bluetooth Classic,* temos no eixo yy o número de canais disponíveis (79 canais) e no eixo xx, o tempo de duração e o tipo de pacotes enviados.

### C. Arquitetura da rede *Bluetooth*

Os sistemas com base no protocolo *Bluetooth* dividem-se em dois tipos de arquitetura:

- *Piconet*
- *Scatternet*

A arquitetura *Piconet* define-se por ter um dispositivo *Master* que comunica com dispositivos *Slave* estando limitado a um máximo de 7 dispositivos *Slave* (ver Figura 2-20). Cabe ao *Master* a função de regular a transmissão, isto é, regular os canais e os pacotes de dados a ser enviados e o próprio sincronismo de comunicação. É o *Master* que define o SCK e o ID dos *Slaves* [31][32].

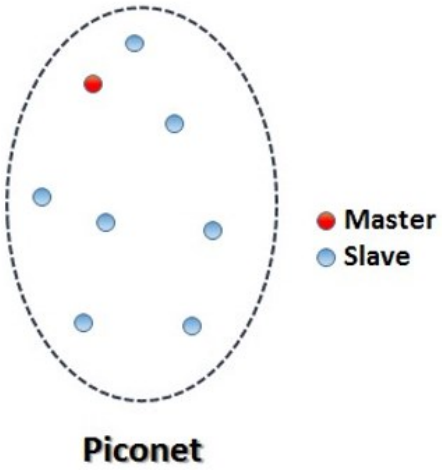


Figura 2-20: Arquitetura *Piconet* [32].

A arquitetura *Scatternet* consiste na junção de várias *Piconets*, onde o *Slave* de uma *Piconet* pode acumular a função de *Master* numa outra *Piconet* (ver Figura 2-21) permitindo a sua junção.

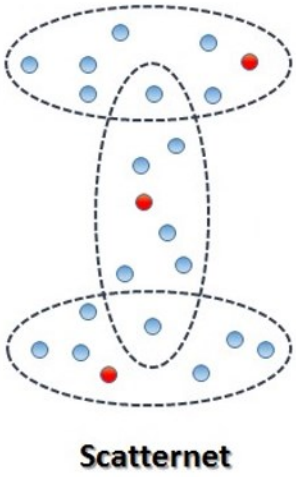


Figura 2-21: Arquitetura *Scatternet* [32].

A arquitetura *Scatternet* permite que muitos dispositivos possam estar conectados e assim partilhar uma maior área de sistema.

### *D. Bluetooth Protocol Stack*

Relativamente a protocolos, o padrão *Bluetooth* tem uma arquitetura de protocolos por camadas (ver Figura 2-22). Os protocolos estão divididos em 3 camadas principais, a camada de controlo (*Controller*), a camada de anfitrião (*Host*) e a camada de aplicações (*Application*) [31], [32][33].

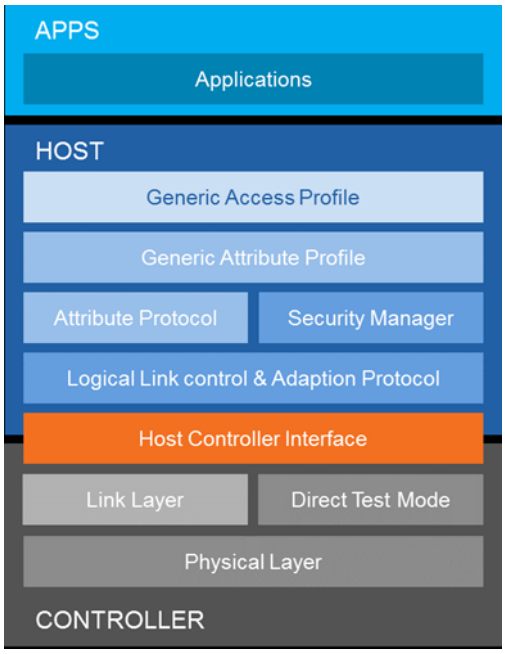


Figura 2-22: Pilha de protocolos do padrão *Bluetooth* [32].

A camada *Controller* é considerada uma camada de base, fornecendo os protocolos necessários responsáveis por todas as operações relacionadas com as ligações RF, pelas conexões, entre outros.

A camada *Host* possui um conjunto de protocolos responsáveis pela forma de como se acessa a dados reais, por detetar outros dispositivos BT, entre outros.

A camada *Applications* é responsável pela interface de utilizador, gestão de dados, entre outros. É nesta camada que se encontra o código desenvolvido (p.ex. microcontrolador) [32][32][33].

## 2.2. Discussão sobre Tecnologias Biométricas e Identificação por Objeto

Tal como abordado no capítulo introdutório deste relatório, os métodos de identificação por análise biométrica, estão cada vez mais desenvolvidos, diversificados e parecem permitir, na generalidade das situações, a garantia de uma maior autenticidade na identificação de pessoas. Desta forma, surge a necessidade de se abordar a problemática do tema da autenticidade na identificação de pessoas.

Se é claro que quando temos sistemas baseados em identificação por objetos tais como os já abordados neste relatório, mais precisamente no ponto 2.1, adicionam-se problemas de fraude e falsas identificações, quer seja por empréstimo ou duplicação do identificador, quer seja por roubo desse mesmo objeto identificador, estamos na presença de sistemas menos credíveis.

Se para sistemas de baixo nível de segurança isso possa ser tolerado, em sistemas de média e alta segurança urge a utilização de métodos de identificação mais fiáveis.

É desta forma que a biometria entra nos sistemas de identificação mais atuais. Sendo uma tecnologia que estuda e desenvolve sistemas para analise e deteção de dados biológicos, ou seja, as características do corpo humano tais como ADN, impressões digitais, análises de retina, de íris, de padrões de voz, padrões faciais, padrões da palma da mão, características estas comprovadamente únicas em cada indivíduo, temos a unicidade dos indivíduos garantida.

Não podemos esquecer que o princípio de funcionamento dos sistemas de identificação biométricos é similar aos sistemas que utilizam objetos, isto é, necessidade de leitura (*Scanning*), *software* que converta a informação das características biométricas para formato digital e uma base de dados para comparação. Sendo assim, também apresentam algumas limitações que se centram muito na qualidade do elemento de leitura das características biométricas e no software utilizado para a identificação. Associado a isto ainda está o fator custo, pois sistemas de leitura de melhor qualidade são, geralmente, mais dispendiosos.

Para o projeto descrito neste relatório, identificação da presença de estudantes em aulas de cursos superiores, prevê-se que a quantidade de autores de fraude seja bastante reduzida, no entanto, não podemos esquecer que se pretende um dispositivo que possibilite uma diversidade de métodos de identificação.

Desta forma, não se vê utilidade em limitar os métodos de identificação a uma das vias possíveis, biometria ou objeto.

# 3. Desenvolvimento e Implementação

No capítulo anterior foram descritos os princípios de funcionamento dos sistemas de identificação utilizados, as suas tecnologias sensoriais e modos de operação. No presente capítulo serão apresentadas as funcionalidades pretendidas para o dispositivo, os elementos e módulos mais importantes, a interligação entre as diferentes tecnologias utilizadas e o protótipo desenvolvido para acomodar todos os elementos constituintes do projeto.

## 3.1. Requisitos do Sistema

Por princípio foi decidido associar diversos métodos de identificação de pessoas, na tentativa de tornar o protótipo a desenvolver um dispositivo híbrido, quer por conceito, quer por definição. O seu utilizador poderá, desta forma, aproximar-se mais às diferentes necessidades do seu público-alvo, neste caso, os alunos que assistem às aulas que UC leciona.
Os requisitos e funcionalidades principais necessárias para o projeto destacam-se em seguida:

- Desenvolver um protótipo simples e com componentes genéricos presentes em qualquer loja de eletrónica;
- Desenvolver um protótipo de baixo custo;
- Desenvolver um protótipo capaz de ser utilizado em qualquer sala de aula;
- Desenvolver um protótipo de pequena dimensão e portável;
- Garantir a facilidade de alimentação, com e sem fios;
- Permitir a introdução de dados relativos aos alunos a identificar;
- Permitir a introdução de dados relativos às aulas a lecionar;
- Permitir a identificação com o tradicional cartão de estudante;
- Permitir a identificação com a impressão digital;
- Permitir a identificação com o sistema NFC do Smartphone;
- Permitir a identificação através do método *tag "Near Field Communication"* (NFC);
- Permitir o registo e armazenamento dos dados para posterior utilização.

## 3.2.Estrutura Funcional do Projeto

Após a análise dos requisitos e funcionalidades principais, definiu-se que o sistema deveria ter como base os seguintes blocos/módulos:

**Bloco de controlo**: composto pelo controlador, cartão microSD e relógio;

**Bloco de identificação**: composto pelos leitores das tecnologias selecionadas para identificação dos alunos, leitor de RFID, leitor de NFC e leitor de impressão digital;

**Bloco de visualização e entrada de dados:** composto por um ecrã tátil e pela placa de *Bluetooth* para comunicar com uma aplicação de *smartphone* (APP) para introdução de dados no sistema.

### 3.2.1. Diagramas de Blocos

Para uma melhor perceção dos blocos mencionados no ponto anterior pode-se observar o diagrama da Figura 3-1.

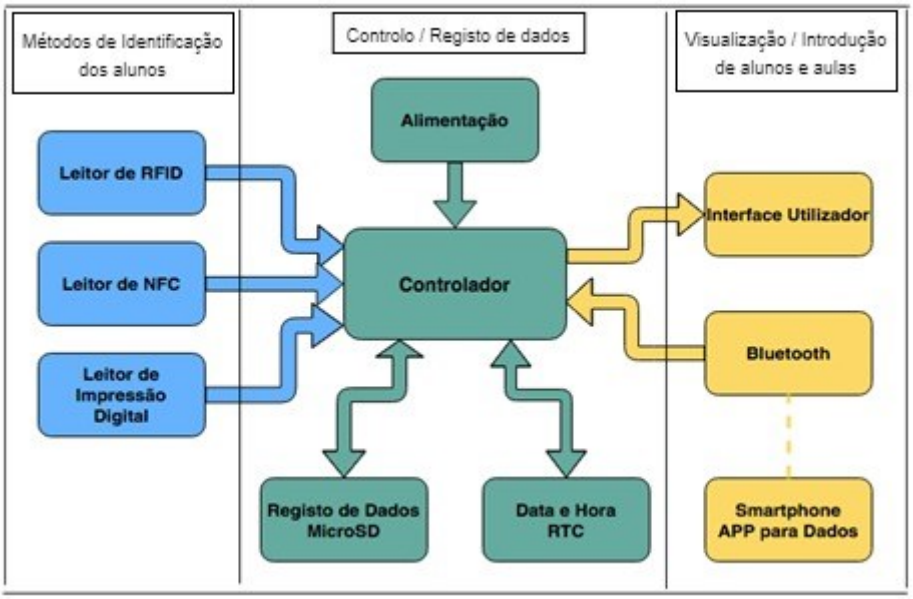


Figura 3-1: Diagrama de blocos.

### 3.2.2. Principal *hardware*

No sentido da implementação do diagrama de blocos apresentado, foi criado e desenvolvido um *shield* com o intuito de interligar as ligações ao *hardware* externo necessário, nomeadamente as ligações do ecrã gráfico, do módulo *Bluetooth*, do sensor de impressão digital, do leitor de RFID e do leitor de NFC. A Figura 3-2 apresenta a primeira versão do desenho da placa de circuito impresso desenvolvida para acomodar os conectores do *shield* e realizar de uma forma mais facilitada as ligações dos elementos de hardware externos.

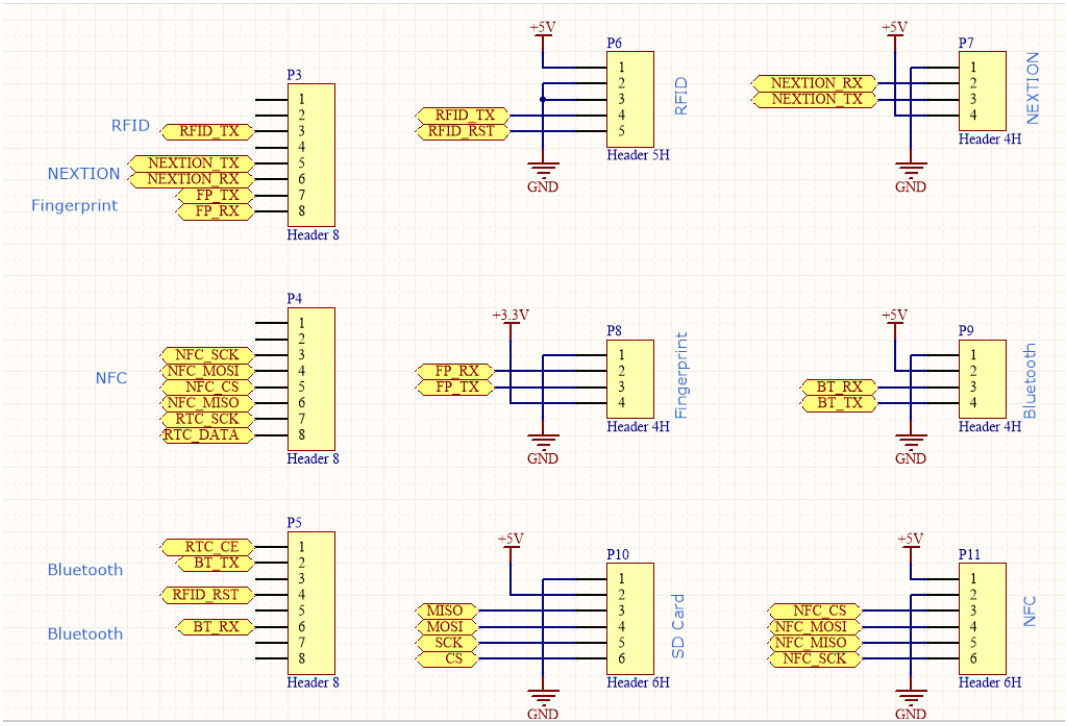


Figura 3-2: Esquema de ligações do *shield* (conectores do hardware).

Para além das conexões ao hardware externo, foi integrado no *shield*, um Relógio de Tempo Real (RTC), para permitir registar a data, hora e minutos de entrada de dados no sistema, mais precisamente, os dados associados ao registo de assiduidade dos alunos. A Figura 3-3 apresenta o esquema elétrico de ligação do Relógio de Tempo Real (RTC) inserido no *shield* e baseado do circuito integrado DS1302.

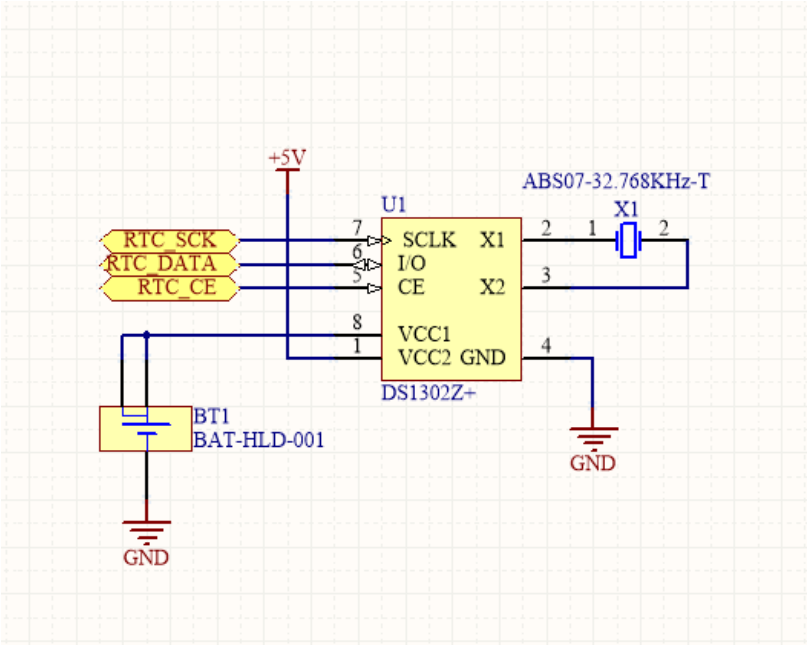


Figura 3-3: Esquema do RTC.

A Figura 3-4, apresenta o aspeto final do *shield* em 2D onde é possível observar a localização do RTC, da pilha de alimentação e das fichas de ligação do hardware externo com a respetiva identificação. São ainda identificados os pinos do controlador nas fichas P1, P2, P3, P4 e P5 para utilização dos pinos livres do controlador para possível expansão de funcionalidades.

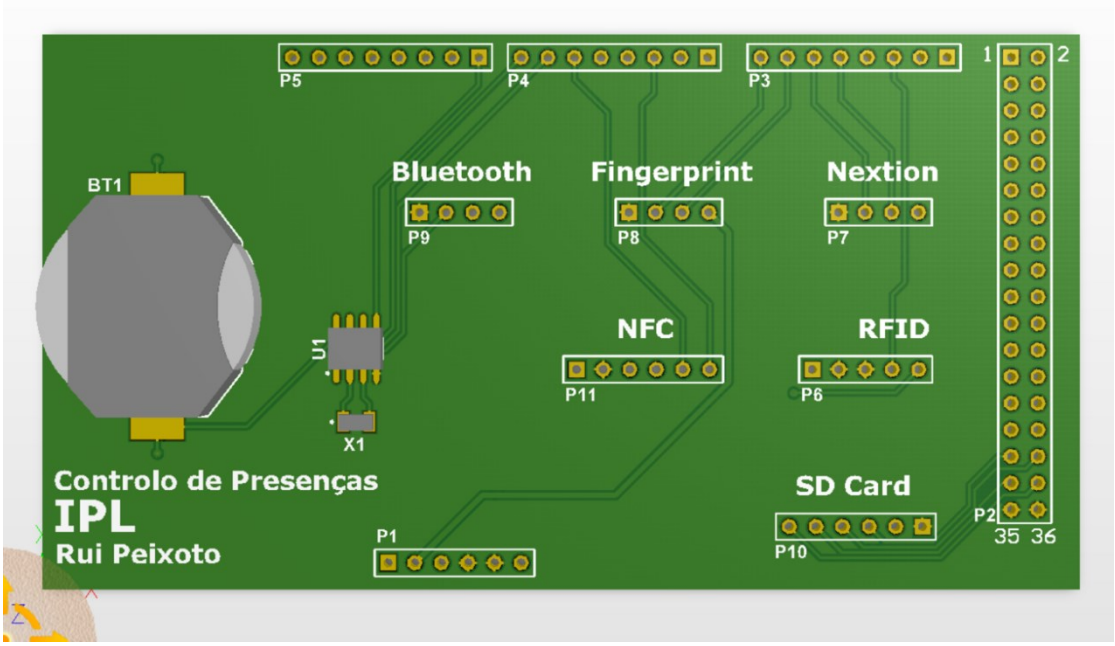


Figura 3-4: Aspeto final da primeira versão do *shield* desenvolvido.

Com o objetivo de adicionar a serigrafia com a informação da identificação dos componentes constituintes do protótipo, bem como um circuito de alimentação foi desenvolvida recentemente uma segunda versão do *shield*. O circuito de alimentação desenvolvido é apresentado na Figura 3-5,

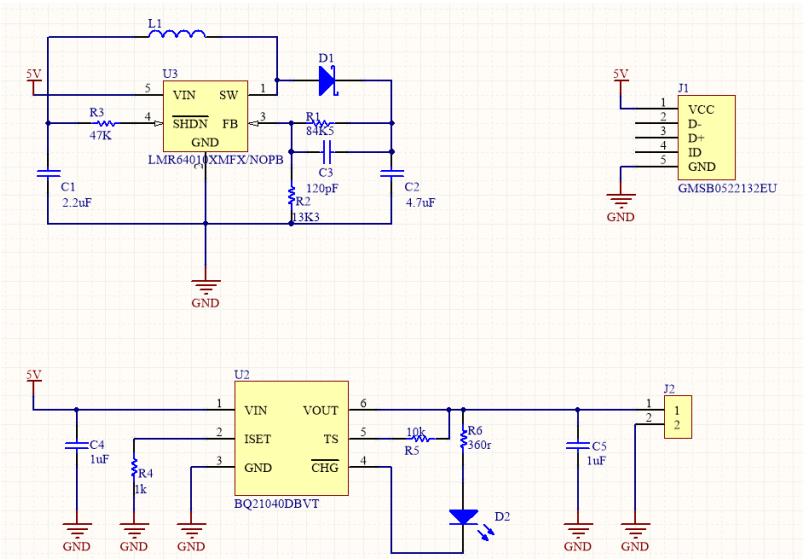


Figura 3-5: Circuito de Alimentação e carga da bateria.

O aspeto final da segunda versão do *shield* em 2D, pode ser visualizada na Figura 3-6, onde para além da visível serigrafia de identificação de fichas e pinos, se destacam no lado superior esquerdo, o adicionar das fichas de ligação para alimentação, o circuito com o regulador de tensão e o circuito de carga da bateria.

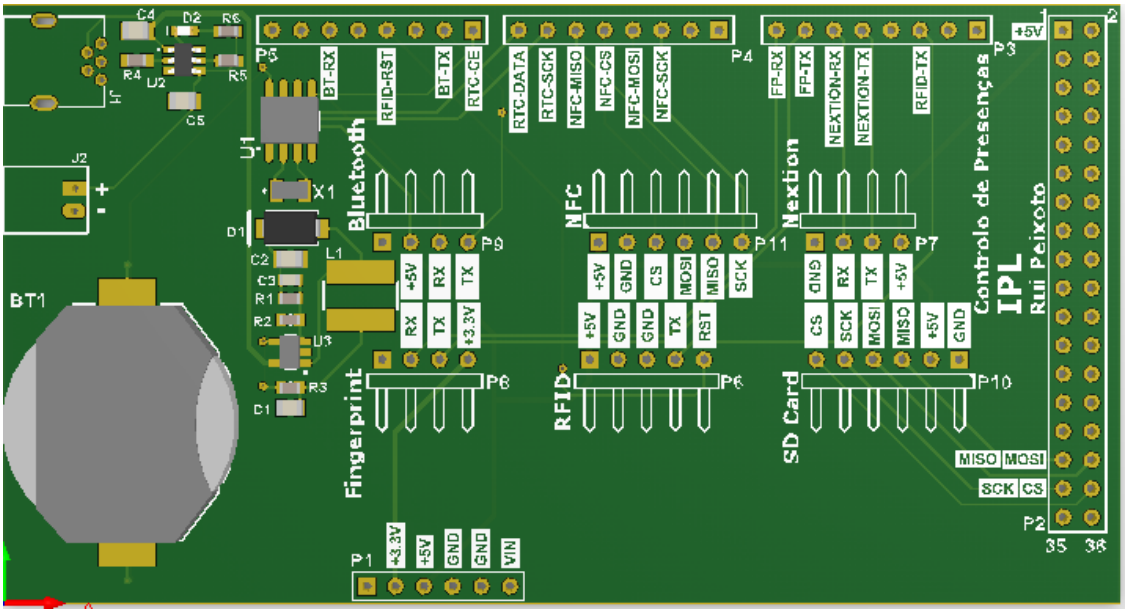


Figura 3-6: Aspeto final da segunda versão do *shield.*

Esta segunda versão aguarda, à data de conclusão do presente relatório, a chegada de componentes para respetiva soldadura, montagem e realização de testes.

## 3.3.Componentes do Projeto

Tal como indicado na introdução (ponto 1 deste relatório), o presente projeto pretende utilizar componentes eletrónicos comuns e de baixo custo, de forma que seja facilmente replicável. Existindo para cada bloco um conjunto vasto de produtos com características semelhantes, pretende-se neste ponto abordar os componentes principais utilizados neste projeto, a sua função e respetivas especificidades.

### 3.3.1. Controlador

A escolha do controlador acabou por ser influenciada na conversa inicial do trabalho, focando a facilidade de utilização, diversidade de placas, ambiente de programação intuitivo, linguagem de programação baseada em linguagem C/C++ e uma extensa comunidade de apoio, o que tornou plataforma de desenvolvimento *Arduíno* a escolha mais favorável.

O passo seguinte consistiu em selecionar a placa mais adequada, uma vez que a oferta de soluções é vasta. As placas selecionadas foram a placa *Uno*, a *Nano* e a *Mega 2560*. Como se pode observar na Figura 3-7, estas apresentam as suas diferenças principais ao nível da dimensão física. Outra das diferenças assenta no número e tipo de pinos programáveis disponíveis (*General Purpose Input Output* - GPO's).

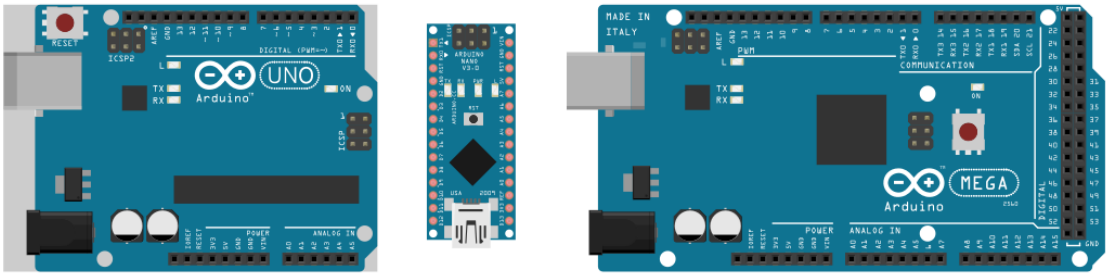


Figura 3-7: Aspeto das placas Uno, Nano e Mega respetivamente.

A Tabela 3-1 apresenta um estudo comparativo de algumas das principais caraterísticas das três placas mencionadas.

Tabela 3-1: Comparativo de placas Arduíno.

| **Placas Arduíno para comparação** | | | |
|---|---|---|---|
| **Características** | Arduíno Uno | Arduíno Nano | Arduíno Mega 2560 |
| **microcontrolador** | ATmega328P | ATmega328 | ATmega2560 |
| **Tensão de operação** | 5V | 5V | 5V |
| **Tensão de alimentação (Recomendado)** | 7-12V | 7-12V | 7-12V |
| **Entradas Digitais** | 14 (6 PWM) | 22 (6 PWM) | 54 (15 PWM) |
| **Saídas de PWM** | 6 PWM | 6 PWM | 15 PWM |
| **Entradas analógicas** | 6 | 8 | 16 |
| **Corrente DC por pino** | 20 mA | 40 mA | 20 mA |
| **Memória Flash** | 32 kB | 32 kB | 256 kB |
| **Frequência do relógio** | 16 MHz | 16 MHz | 16 MHz |
| **Comprimento (mm)** | 69,6 mm | 45 mm | 101,52 |
| **Largura (mm)** | 53,4 mm | 18 mm | 53,3 |
| **Comunicação** | UART, I2C, SPI | UART, I2C, SPI | 3xUART, SPI, I2C |

Sendo o controlador parte central do presente projeto, a sua escolha teve em conta as necessidades de ligação do *hardware* externo, focando o número de pinos necessários e os respetivos métodos de comunicação.

Uma vez que será necessário interligar o leitor de RFID, o leitor de NFC, o leitor de impressão digital, o ecrã tátil, o adaptador do cartão micro SD, o módulo *Bluetooth* e o RTC e deixar pinos disponíveis para qualquer alteração e/ou expansão, a placa *Arduíno Mega 2560* foi o recurso selecionado.

O *Arduíno Mega 2560 Rev3*, permite acesso a um maior número de pinos de entrada / saída programáveis (GPIO) - 54 pinos digitais I/O e 16 pinos de entradas analógicas e tem 256 kB de memória *flash*. A Figura 3-8 apresenta o aspeto físico da placa [34].

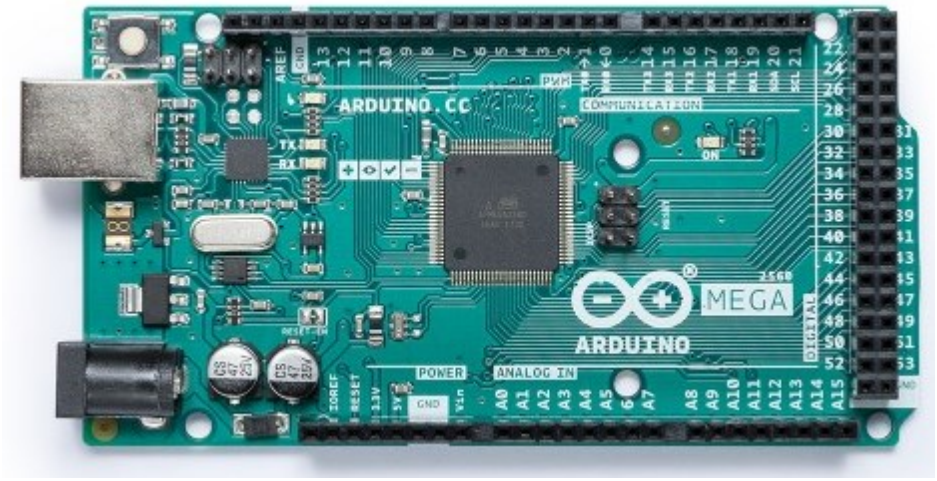


Figura 3-8: *Arduíno Mega 2560* Rev3 [34].

### 3.3.2. RFID

Tendo sido estudadas as principais características dos sistemas RFID, foi possível identificar os principais parâmetros a utilizar no desenvolvimento do projeto. Pretende-se que os utilizadores possuidores de *tag*, a aproximem do dispositivo (com o leitor de RFID), e possam ser identificados sem contacto direto com o equipamento (aplicação de curto alcance). Atualmente, os cartões de identificação individual dos estudantes do Politécnico de Leiria permitem a identificação por radiofrequência (RFID). Desta forma, aproveitando um recurso já existente e massificado no público-alvo, decidiu-se utilizar um leitor capaz de reconhecer e identificar os referidos cartões. O tipo de *tag* presente nos cartões de estudante é passiva e de baixa frequência (LF – 125 kHz), portanto de campo próximo.

A Tabela 3-2 apresenta alguns modelos de leitores de RFID disponíveis na generalidade das lojas da especialidade e as suas principais características. Dada a possibilidade de trabalhar tanto a 3.3V como a 5V e por permitir a identificação a uma maior distância (cerca de 180 mm) foi selecionado o modelo ID20 da *ID Innovations*.

Tabela 3-2: Comparativo de leitores de RFID.

| Leitores de RFID | | | |
|---|---|---|---|
| **Características** | ID Innovations - ID20 | Grove 125 kHz Reader | MIKROE-262 |
| **Frequência** | 125 kHz | 125 kHz | 125 kHz |
| **Tensão de alimentação (Recomendado)** | 2,8-5V | 4,75-5,25V | 5V |
| **Alcance de comunicação** | 180mm | 70mm | - |
| **Saídas** | TTL | TTL | - |
| **Taxa de transmissão (*baud*)** | 9600 | 9600 | 9600 |
| **Formato de saída** | ASCII/Wiegand/Magnet | Wiegand | UART |
| **Protocolo / Chip** | EM4001 | EM4100 | EM4095 |
| **Preço (Euros)*** | 49,20 | 18,08 | 26 |

* Preços à data julho de 2020.

Apesar de no mercado existirem módulos com o leitor RFID acopolado, disponibilizaando as conexões necessárias à alimentação e utilização dos pinos de comunicação do dispositivo. No entanto, uma vez que foi construído um *shield* para acomodar as todos os componentes eletrónicos do sistema, optou-se por acoplar o leitor RFID diretamente ao *shield* sem utilização de módulos externos.

O aspeto físico externo do leitor e a localização e identificação dos pinos estão disponíveis na Figura 3-9.


Figura 3-9: Esquemático do leitor de RFID da ID *Innovations* [35].

A funcionalidade de cada pino encontra-se descrito na Tabela 3-3. Os pinos utilizados para ligação do leitor são: GND (pino 1), *Reset* (pino 2), seletor de Formato de dados (pino 7), *Data* 0 (pino 9) e VCC (pino 11). Relativamente ao seletor de formato de dados, optou-se por ligar o pino 7 a GND para receber os dados em formato ASCII. Em relação à receção de dados, a saída

*Data* 0 pode ser ligado a uma entrada RX de qualquer controlador, funcionando com a interface UART.

Tabela 3-3: Identificação e função dos pinos do leitor de RFID selecionado [35].

| **Leitor de RFID ID20** | | | | |
|---|---|---|---|---|
| **Pino** | Descrição | ASCII | Magnet | Wiegan |
| **Pino 1** | *GND* (0V) | *GND* | *GND* | *GND* |
| **Pino 2** | Ativo a +5V | *Reset* | *Reset* | *Reset* |
| **Pino 3** | Ligar a antena externa e condensador | Antena | Antena | Antena |
| **Pino 4** | Ligar a antena externa | Antena | Antena | Antena |
| **Pino 5** | *Tag* presente | Sem função | *Tag* Presente | Sem função |
| **Pino 6** | Aplicação futura | Aplicação futura | Aplicação futura | Aplicação futura |
| **Pino 7** | Seletor de formato de dados | Ligar a 0V | Ligar ao pino 10 | Ligar a +5V |
| **Pino 8** | Data 1 | CMOS | *Clock* | Data Input 1 |
| **Pino 9** | Data 0 | TTL data | Data | Data Output 0 |
| **Pino 10** | Lógica a 3.1 kHz | *Buzzer* / LED | *Buzzer* / LED | *Buzzer* / LED |
| **Pino 11** | VCC (+5V) | +5V | +5V | +5V |

Na Figura 3-10 podem observar-se as principais conexões entre o leitor RFID e o microcontrolador para a utilização do método de comunicação série com o *Arduíno Mega 2560*.

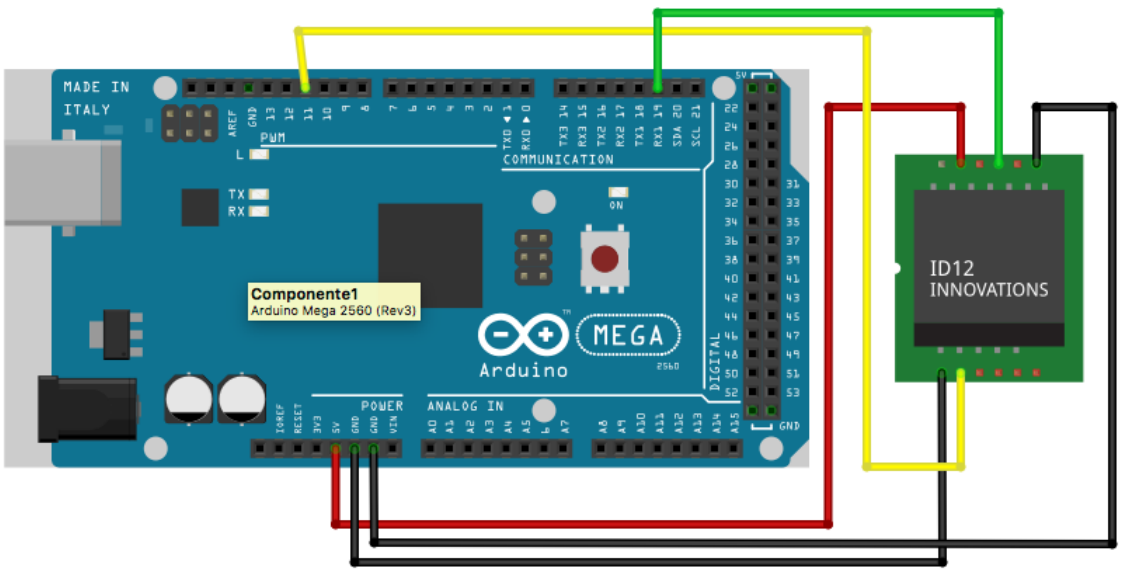


Figura 3-10: Montagem típica do leitor de RFID com o microcontrolador.

### 3.3.3. NFC

Para a tecnologia NFC foi adotado um procedimento similar ao RFID. Pretende-se que os utilizadores possuidores de *tag* NFC, se aproximem do respetivo leitor, de forma a realizarem a sua identificação.

A generalidade dos leitores de NFC das lojas de eletrónica utiliza o chip PN532 da empresa *NXP Semiconductors*, variando apenas no formado do leitor. Alguns dos leitores estão inseridos em *shields* para *Arduíno*, outros em placas independentes interligadas aos controladores através de condutores e conectores.

Na Figura 3-11, pode observar-se o aspeto físico dos leitores mais comuns.

Figura 3-11: Aspeto físico de leitores de NFC baseados no chip PN532 [36].

A Tabela 3-4 apresenta um estudo comparativo das principais características dos dois leitores NFC mais comuns, sendo possível observar a semelhança das características técnicas entre ambas, diferindo apenas no formato.

Tabela 3-4: Comparativo de leitores de NFC [36].

| Características | ITEAD PN532 | NFC Shield V1.0 Seeedstudio |
|---|---|---|
| **Frequência** | 13,56 MHz | 13,56 MHz |
| **Tensão de alimentação (Recomendado)** | 3,3-5,5V | 5V |
| **Alcance de comunicação** | 30 mm | 25 mm |
| **Chip** | PN532 | PN532 |
| **Interface comunicação** | SPI, I2C, UART | SPI, I2C, UART |
| **Padrão de comunicação** | ISO14443, Mifare, FeliCa, ISO18022 | ISO14443, Mifare, FeliCa, ISO18022 |
| **Formato da placa** | Módulo | *Shield* |
| **Preço (Euros) *** | 28,72 | 23,62 |

* Preços à data julho de 2020.

Foi selecionado o módulo da ITEAD porque, apesar de ser mais dispendioso, considerou-se mais vantajoso por ter maior adaptabilidade ao espaço reduzido dentro do protótipo. Uma vez que o NFC é para curto alcance, inferior a 30 mm, o posicionamento do leitor é uma limitação importante.

O módulo possui dois interruptores para seleção do tipo de interface de comunicação. A Figura 3-12 apresenta a identificação e posicionamento dos pinos.

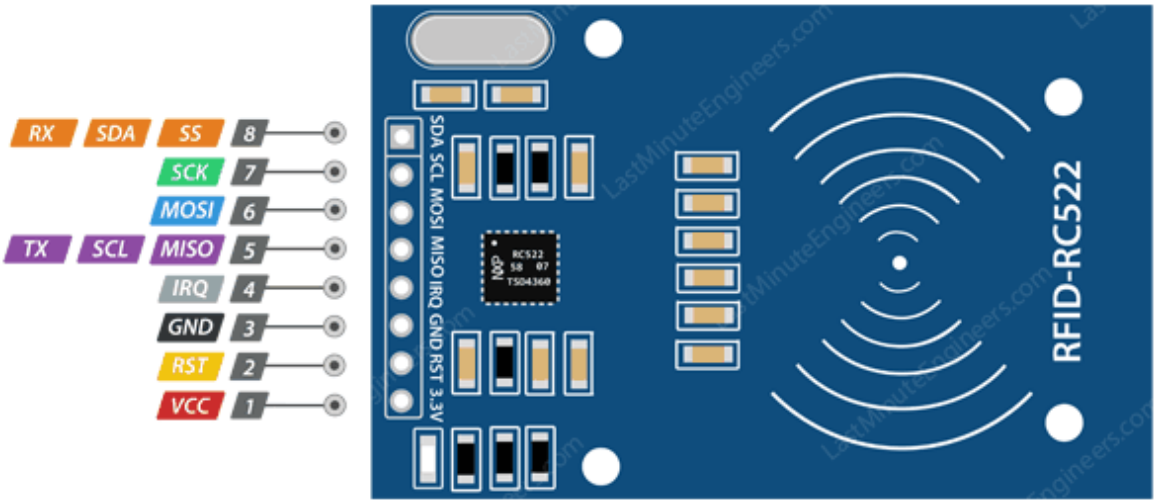


Figura 3-12: Configuração e pinos e de seleção de comunicação [37].

As *tags* de NFC podem ter o mesmo formato que as tags RFID, diferindo apenas na frequência de funcionamento (13,56 MHz).

De forma que o módulo NFC comunique com o *Arduíno* foi selecionado o método de comunicação SPI (*Serial Peripheral Interface*). Para seleção desse modo foi necessário colocar os interruptores de seleção set0 a nível baixo e set1 a nível alto. Como os conectores não são exclusivos de qualquer um dos métodos de comunicação, houve a necessidade de especificar qual o método de comunicação a utilizar. Através da análise da Figura 3-12, foi verificado que existem pinos utilizados em qualquer dos métodos de comunicação disponibilizados, são eles os pinos 5 (MISO, SC e TX) e 8 (SS, DAS e RX). O conjunto RX/TX é utilizado para comunicação série (UART), os pinos SDA/SCL para comunicação do tipo Circuito Inter-Integrado (I2C) e MOSI/SS/MISO/SCK para comunicação SPI.

A Tabela 3-5 apresenta a funcionalidade dos conectores do leitor NFC.

Tabela 3-5: Pinagem do leitor de NFC.

| Pinos PN532 | Funcionalidade |
|---|---|
| **SCK** | Clock |
| **MI** | MISO |
| **MO/SDA/TX** | MOSI / DATA / TX |
| **NSS/NCL/RX** | Slave Select / Clock / RX |
| **IRQ** | Interrupt Request |
| **RST** | Reset |
| **GND** | Ground |
| **5V** | VCC |

Como foi selecionada a comunicação por SPI, da parte do leitor de NFC utilizaram-se os pinos relógio (SCK), *Master Input Slave Output* (MISO), *Master Output Slave Input* (MOSI) e *Slave Select* (SS). Relativamente às ligações com o *Arduíno Mega*, optou-se por manipular os pinos através de software em detrimento de utilizar os nativos da placa. A razão derivou da utilização de uma biblioteca disponibilizada por um fabricante de leitores de NFC.

Na Figura 3-13 pode-se observar as principais ligações para a utilização do método de comunicação SPI com o *Arduíno Mega 2560*.

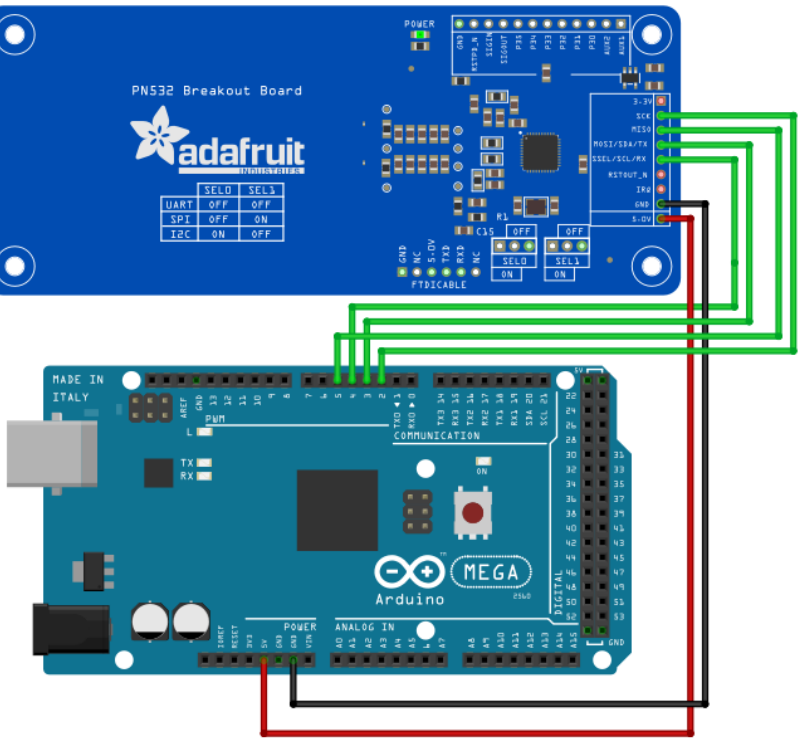


Figura 3-13: Montagem típica do leitor de NFC.

### 3.3.4. Sensor de Impressão Digital

Abordados os métodos de identificação comuns como a utilização de cartões ou outros objetos (*tags*), estes são sempre passíveis de serem esquecidos, roubados ou utilizados de forma indevida por outros utilizadores. tendo em consideração estas limitações, surge a necessidade de integrarmos um método de identificação diferente, assente em parâmetros biométricos para resolver as questões anteriores e aumentar a garantia de autenticidade na identificação.

A identificação biométrica assenta na análise de dados biológicos do corpo humano que possuem características únicas. Atualmente é comum realizar a identificação através do ADN (ácido desoxirribonucleico), da análise da retina ou íris, padrões de voz, padrões faciais, análise da impressão digital, entre outros.

Para o presente projeto, a opção recaiu sobre um sensor de impressão digital. Entre as razões para esta seleção pode-se salientar o menor custo associado ao dispositivo sensor e o seu pragmatismo/facilidade de identificação quando comparados com outros tipos de sensores biométricos.

Assim sendo, foi integrado um leitor de impressão digital que, não só, consiste numa alternativa para os utilizadores que se autenticam através das *tags* de RFID ou de NFC, como também reduz as situações de fraude associadas ao empréstimo de objetos identificadores, uma vez que a pessoa a identificar deverá utilizar a sua própria impressão digital,

Existem no mercado vários fabricantes de leitores de impressão digital com diversos preços e respetiva qualidade. Tendo em conta dois dos objetivos principais do projeto, criar um protótipo de baixo custo com materiais presentes na generalidade das lojas de eletrónica, optou-se pela utilização de leitores para desenvolvimento e baixo custo em detrimento de artigos comerciais mais complexos e dispendiosos.

Na Figura 3-14 encontram-se dois modelos bastante comuns, o DY50 (à esquerda) e o GT521F32 (à direita).

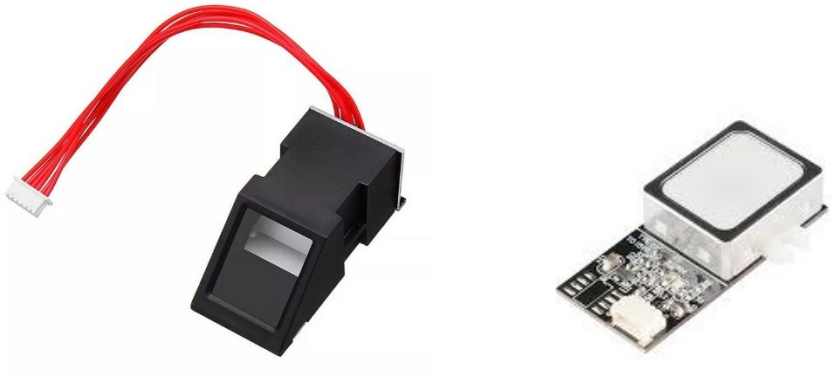

Figura 3-14: Tipos de leitores de impressão digital [38].

As características técnicas gerais, são bastante semelhantes, quer em termos de interfaces de comunicação, quer em termos de alimentação. Ambos são baseados em sensores óticos, acompanhados por um processador dedicado. A Tabela 3-6 apresenta um resumo das principais características [39].

Tabela 3-6: Características dos sensores de impressão digital.

| Características | DY50 | GT-521F32 |
|---|---|---|
| **CPU** | AS608 | ARM Cortex M3 core |
| **Sensor** | Ótico | Ótico |
| **Interface de comunicação** | UART, USB | UART, USB |
| **Armazenamento** | 200 imp. | 200 imp. |
| **Alimentação** | 3.6 – 6.0V | 3.3 – 6.0V |
| **Consumo** | 140 mA | <130 mA |
| **Taxa de Aceitação Falsa (FAR)** | <0.001% | <0.001% |
| **Taxa de Rejeição Falsa (FRR)** | <1% | <0.1% |
| **Modos Verificação/Identificação** | 1:1 – 1:N | 1:1 – 1:N |
| **Dimensões (C * L * A)** | 56 * 20 * 21.5 mm | 36.1 * 16.9 * 7.08 mm |
| **Preço (Euros) *** | 28,55 | 39,90 |

* Preços à data julho de 2020.

Após a análise da Tabela 3-6, pode observar-se que os modelos são bastante semelhantes, diferindo principalmente no processador, na taxa de rejeição falsa, nas dimensões físicas e no preço. O modelo selecionado foi o DY50 devido ao preço inferior.

A Figura 3-15 apresenta a forma de conexão do módulo ao *Arduíno* Mega. Sabendo que o módulo leitor de impressão digital utiliza a comunicação UART com a utilização de pinos RX/TX, poderiam ter sido utilizados os pinos do *Arduino Mega 2560* preparados para o efeito, ou seja, os conjuntos 0/1, 14/15, 16/17 e 18/19, no entanto, é possível observar que foram utilizados pinos digitais diferentes uma vez que estes por já se encontrarem em utilização para o restante *hardware*. Neste caso foi necessário manipular/criar, através de *software,* pinos para a comunicação UART com o sensor de impressão digital.

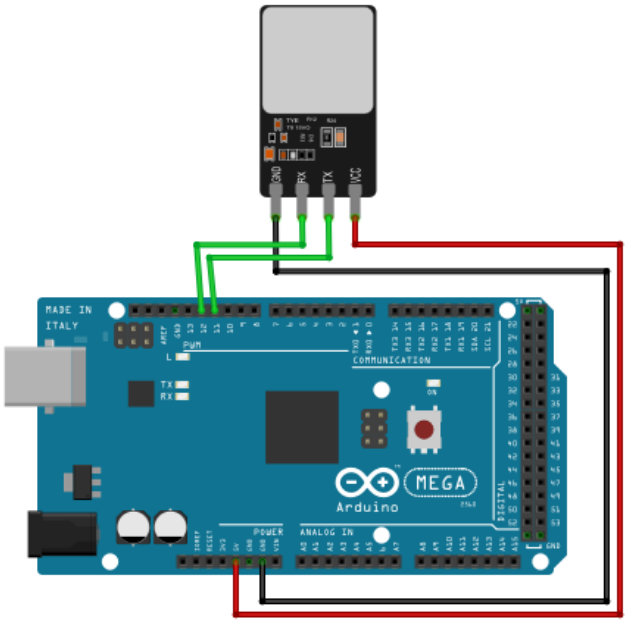


Figura 3-15: Montagem típica do leitor de impressão digital.

### 3.3.5. Integração de módulo Bluetooth

A utilização do módulo *Bluetooth*, não foi idealizada para o ato da identificação de um utilizador, isto apesar de ter o potencial para tal. Para esse efeito e considerando que, atualmente, quase todos os alunos possuem o *Smartphone* com conexão por *Bluetooth*, seria possível a construção de uma aplicação a disponibilizar aos estudantes para validação da sua presença. Após análise e ponderação sobre essa possibilidade, não foi considerada um dos requisitos principais do sistema por levantar questões de acessibilidade e segurança, que só por si poderiam necessitar de um projeto na área da informática e programação de aplicações para dispositivos móveis.

A inserção do *Bluetooth* foi, no entanto, necessário para permitir o desenvolvimento de algumas funcionalidades associadas à inserção de dados no sistema de forma mais fácil e rápida. Apesar de os dados relativos aos cursos, unidades curriculares (UC) lecionados pelo docente, alunos inscritos e a aulas que decorrem ao longo dos semestres poderem facilmente ser introduzidos através do preenchimento de um ficheiro *Excel* em qualquer computador e guardados no cartão de memória associado ao protótipo, considerando a necessidade de pontualmente/localmente se inserir uma nova aula ou um novo aluno, criou-se uma aplicação de *Smartphone*, a utilizar pelo docente e que comunica com o protótipo através de *Bluetooth*.

Para implementar a comunicação *Bluetooth* entre o smartphone e protótipo a desenvolver foram avaliados dois módulos de comunicação *Bluetooth*: HC-06 e o HM-12. O resumo das principais características são apresentados na Tabela 3-7.

Tabela 3-7: Características dos módulos Bluetooth.

| Características | HC-06 | HM-12 |
|---|---|---|
| Versão / Padrão | 2.0 / EDR | 4.0 / BLE & EDR |
| Alcance | 20 m | 60 m |
| Alimentação | 3.3VDC/5VDC | 3.3VDC/6VDC |
| Consumo | 20 mA | 10-17 mA |
| Frequência | 2,4 GHz | 2,4 GHz |
| Máx Byte RX/TX | - | 90 |
| Dimensões (C * L * A) | (39.5 * 20.5 * 1.6) mm | (27 * 13 * 0.8) mm |
| Preço (Euros) * | 6,90 | 12,90 |

* Preços à data julho de 2020

Após a análise da Tabela 3-7, pode observar-se que os modelos são bastante semelhantes, diferindo principalmente no alcance e no preço. O modelo selecionado foi o HC-06 não só devido ao preço inferior, mas também pelo facto de ter alcance inferior, o que poderá garantir uma anotação de presença mais próxima do leitor e com isso minimizar a possibilidade de troca de identidades ou a de marcação de presença fora da sala de aula.

A Figura 3-16 apresenta a forma de conexão do módulo ao *Arduíno Mega* 2560 onde pode ser observado que, à semelhança do sensor de impressão digital também foi necessário manipular/criar, através de *software,* pinos para a comunicação com o *Bluetooth*.

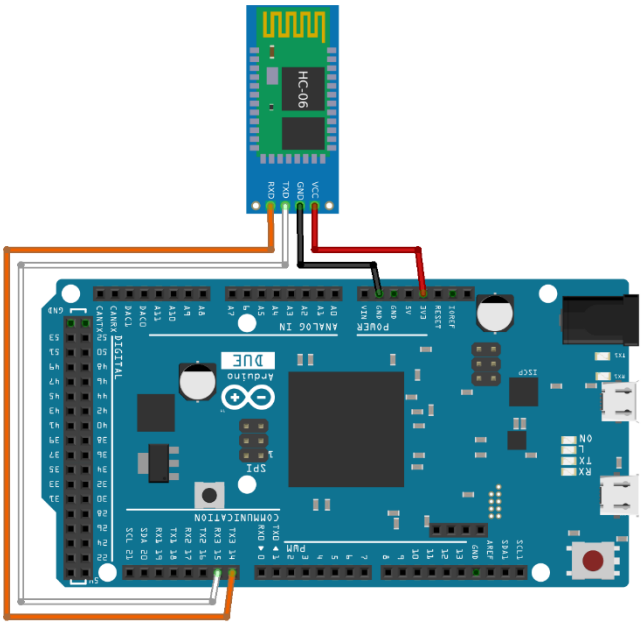


Figura 3-16: Montagem típica do módulo de *Bluetooth*.

### 3.3.6. LCD *Touchscreen* Nextion

Ao longo deste capítulo, tem sido abordado todo o *hardware* necessário à realização da introdução de dados no controlador, detalhando os módulos necessários à identificação dos alunos, leitores/sensores de RFID, NFC, impressão digital e a placa desenvolvida para permitir a ligação de todos os módulos externos.

Tendo em conta toda a circulação de dados no sistema, entendeu-se necessário permitir que o utilizador obtenha um *feedback* dessa informação e associou-se um ecrã para a sua visualização. Analisaram-se duas possibilidades distintas para permitir esta funcionalidade. A primeira, utilizando um ecrã alfanumérico de cristais líquidos (*Liquid Cristal Display* – LCD) de duas linhas de dezasseis caracteres (LCD – 16x2) apenas para visualização de dados recebidos pelo controlador. Podemos observar o ecrã e o aspeto da saída de dados na Figura 3-17. Esta seria uma solução mais interessante em termos de custo (aproximadamente 10 euros em lojas nacionais) mas mais limitada em termos de soluções, visto permitir apenas a visualização de 32 caracteres distribuídos por 2 linhas de cada vez. Para podermos controlar/selecionar a informação a mostrar, seria necessário utilizar botões ligados ao controlador *Arduíno* para interagir com o sistema, dando estímulos para seleção de opções e alteração dos dados a mostrar.

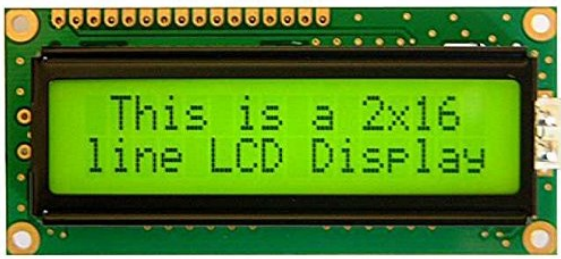


Figura 3-17: Ecrã de alfanumérico de cristais líquidos (LCD – 16x2) [40].

A segunda opção, consistiu na utilização de ecrã gráfico e tátil (*Nextion Toutchsreen* – 320x240 pixéis de resolução), que iria permitir a visualização de maior quantidade de informação, visualização de uma forma mais gráfica, adicionando cores e imagens e ainda a possibilidade de criar botões e outras soluções no próprio ecrã, dispensando assim a necessidade de adicionar botões físicos.


Figura 3-18: Ecrã tátil *Nextion* [41].

Existiam diversas soluções para ecrãs tácteis, mas decidiu-se pela opção *Nextion* (Figura 3-18) por ter um microcontrolador integrado e permitir a programação direta da interface a partir de um aplicativo desenvolvido pela marca e evitar assim o desenvolvimento de código no *Arduíno* para o efeito. A Tabela 3-8 indica algumas das principais características do ecrã [41].

Tabela 3-8: Características do ecrã táctil *Nextion*.

| Características | Nextion NX3224T024 |
|---|---|
| **Resolução** | 2.0 / EDR |
| **Painel táctil** | Resistivo |
| **Cores** | 65536 |
| **Memória flash** | 4 MB |
| **RAM** | 3584 Bytes |
| **MCU** | 48 MHz |
| **Comunicação** | UART |
| **Ecrã** | 2,4 ´´ |
| **Dimensões (C * L * A)** | (74.4 * 42.72 * 5.8) mm |
| **Preço (Euros) *** | 25,70 |

* Preços à data julho de 2020

Após análise da Tabela 3-8, verificamos que o ecrã também utiliza o método de comunicação UART. A Figura 3-19 apresenta a forma de conexão do ecrã *Nextion* ao *Arduíno Mega 2560*.

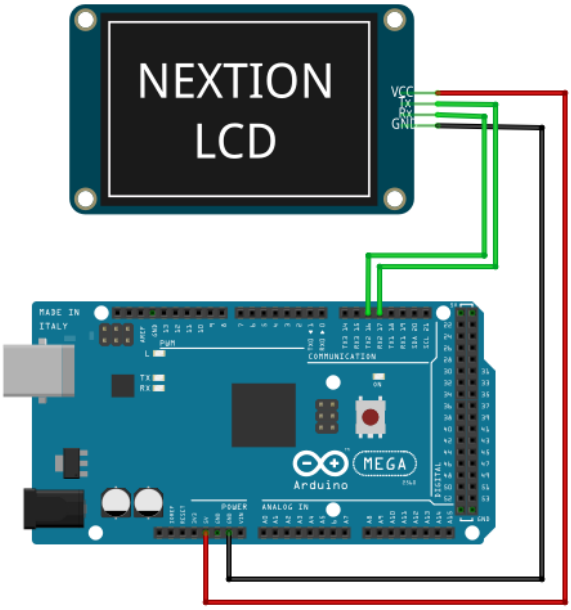


Figura 3-19: Montagem típica do ecrã *Nextion*.

Após análise da Figura 3-19, pode observar-se que foram utilizados pinos digitais referentes à porta de comunicação série 2 que utiliza os pinos 16/17 (RX2/TX2) da placa.

### 3.3.7. Outros materiais

Foram ainda utilizados outros materiais para o desenvolvimento deste projeto, nomeadamente um módulo para cartão microSD (SD- Secure Digital) e um relógio de tempo real (RTC – Real Time Clock).

Não tendo um papel fundamental à deteção ou interface do dispositivo, foram considerados auxiliares e assim não foram abordados aprofundadamente.

No entanto, o RTC foi adicionado ao *Shield* de *Arduino Mega* desenvolvido e abordado em 3.2.2.

Refere-se, ainda, que o módulo microSD, pretende armazenar os dados resultantes da presença dos alunos em aula e que pode ser retirado e realizada a sua leitura diretamente num computador. O módulo utilizado pode ser observado na Figura 3-20.

Figura 3-20 – Módulo de cartão microSD [42].

O utilizador deverá ligar previamente o cartão de memória ao computar e criar as pastas relativas a cursos, ano letivo e UC que vai ministrar no semestre para que os dados relativos a presença de estudantes possam ser organizados.

## 3.4.Compilação do Material de Projeto

A seleção e aquisição dos componentes, é parte fundamental deste projeto. Dois dos principais requisitos, como já abordado, são o baixo custo e a facilidade de aquisição nas lojas da especialidade.

A análise de custos teve em conta dois pontos de vista:

- Aquisição do material em lojas de eletrónica nacionais, permitindo a aquisição e uma entrega quase imediata (1 ou 2 dias), pondo em causa a possibilidade de obtenção do melhor preço.
- Aquisição do material em lojas globais associadas ao mercado global, em que o preço é significativamente inferior, sendo que a entrega, na maioria das vezes, é superior a 60 dias.

A Tabela 3-9 apresenta um estudo comparativo dos custos associados à aquisição dos materiais no mercado nacional e no mercado global (preços à data de julho de 2020).

Tabela 3-9: Análise de custos de aquisição.

| Material | Preço Lojas PT (Euros) | Preço Fornecedor Estrangeiro (Euros) |
|---|---|---|
| **Arduíno Mega 2560 (compatível)** | 21,53 | 5,15 |
| **Módulo RFID – ID20 / Outro** | 49,20 | 0,94 |
| **Módulo NFC – PN532** | 28,72 | 3,23 |
| **Sensor de Imp. Digital – DY50** | 28,55 | 4,89 |
| **Módulo *Bluetooth* – HC-06** | 6,90 | 1,64 |
| **LCD – Nextion** | 25,70 | 11,43 |
| **Módulo Cartão MicroSD** | 4,49 | 1,65 |
| **Módulo RTC - DS1302** | 4,24 | 0,79 |
| **Alimentação – Bateria 2000 mA** | 17,10 | 8,68 |
| ***Shield* (5 unidades)** | 1,69 | 1,69 |
| **Preço Total (Euros)** | 188.12 | 34,09 |

* Preços à data julho de 2020

Após a análise dos custos, pode ser verificado que para tornar o preço do dispositivo competitivo, teríamos de optar pela aquisição ao mercado global. A redução do custo é aproximadamente 5x inferior.

Sendo este um protótipo de prova de conceito, não foi tido em conta a integração de módulos no *shield*, ou mesmo pensado o desenvolvimento total da placa contendo o microcontrolador e a totalidade dos componentes, o que iria baixar ainda mais o preço.

# 4. Software

No capítulo anterior foram abordados os módulos de *hardware* necessários ao desenvolvimento do projeto e características importantes como a funcionalidade geral, o custo associado e facilidade de aquisição, tendo sido apresentadas e justificadas as respetivas escolhas do material a utilizar. Foi ainda apresentado o desenvolvimento do *shield*, as formas de comunicação entre os diversos dispositivos e as respetivas ligações elétricas e foi ainda adicionado o estudo do sistema de alimentação para o protótipo final.

No presente capítulo serão abordados os recursos de *software* utilizados, o seu desenvolvimento, dando ênfase às características/princípios chave, considerados fundamentais para o funcionamento do protótipo.

## 4.1. Aplicação para *Smartphone*

Como abordado na subsecção 3.3.5 do presente documento, foi necessário integrar no projeto a comunicação por *Bluetooth* para realizar a conexão entre o sistema e um *Smartphone.* Esta necessidade surgiu para permitir a introdução de dados de forma mais fácil e rápida, evitando o desenvolvimento de um teclado *qwerty* no écran tátil (que envolveria a necessidade de criar um botão por cada caracter, um para cada número e sem esquecer os caracteres especiais).

O objetivo será permitir ao utilizador do sistema (p.ex: o docente) introduzir novos dados, como novas aulas para registo de assiduidade ou introdução de dados de novos alunos, associando-os às turmas existentes, através da aplicação no seu *Smartphone*. O utilizador poderá ainda confirmar os dados introduzidos no ecrã de interface (*Nextion*).

Para a criação da aplicação *mobile* foi utilizada a plataforma *MIT APPInventor,* que é uma ferramenta online baseada numa programação por blocos, desenvolvida pelo *Massachusets Institute of Technology* (MIT) [43].

A plataforma utiliza dois conceitos fundamentais:

- desenvolvimento da interface: parte gráfica e visível para o utilizador da aplicação
- desenvolvimento do programa associado à interface: blocos de programação que permitem executar as funcionalidades desejadas.

A Figura 4-1 apresenta a janela de construção da interface: os recursos presentes na palete do lado esquerdo podem ser posicionados no ecrã do *smartphone*, representado no centro da página.

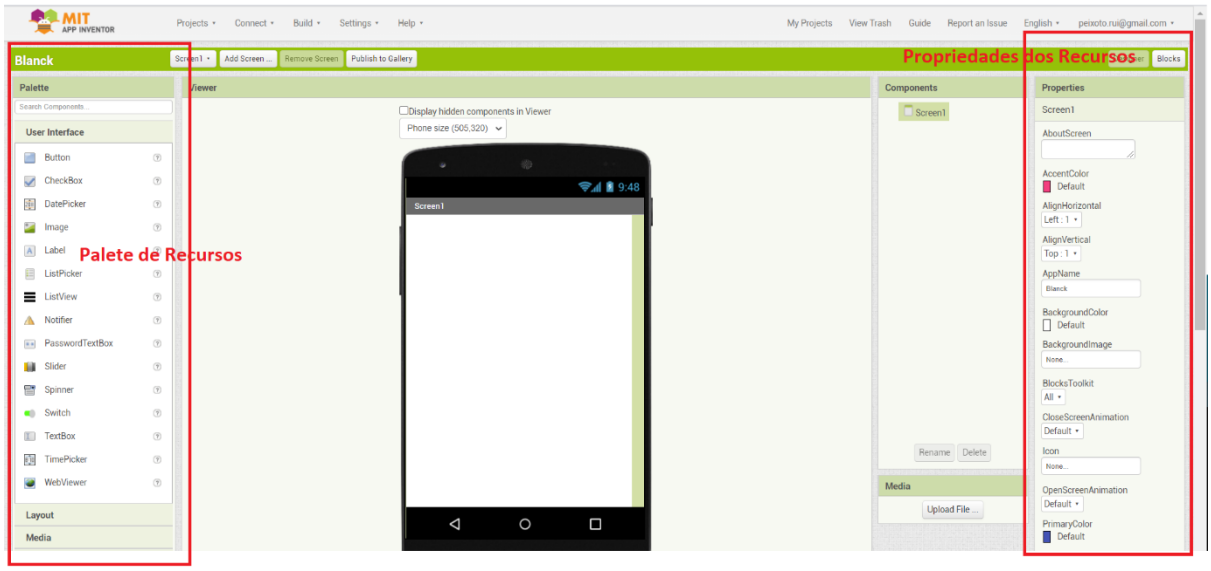


Figura 4-1: Ambiente de criação da interface [43].

Do lado direito, no quadro de propriedades do recurso selecionado para utilização, é possível definir os atributos a associar ao recurso escolhido ou ao próprio ecrã principal.

A Figura 4-2, apresenta a janela de blocos de programação: à esquerda fica a lista de tipos de blocos de programação, em que cada um tem associado um conjunto de autorizações e características a adicionar. Na figura estão visíveis alguns blocos do tipo controlo, compostos, entre outros, por estruturas de seleção do tipo "se", "se/então", estruturas de repetição, entre outras.

Os blocos são posicionados no ecrã também através do sistema de clique e arrasto, tal como na janela de desenho da interface. Do lado direito da janela, podemos observar os botões de seleção do modo de programação, ou seja, a mudança do ambiente da interface para o ambiente de programação de funcionalidades por blocos.


Figura 4-2: Ambiente de seleção de blocos [43].

De forma a esquematizar o funcionamento da aplicação, foi elaborado um fluxograma para definir os procedimentos e forma de atuação do utilizador. Dada a dimensão do fluxograma, e por forma a ficar legível e interpretável, optou-se por, em alguns casos, criar blocos macro para o funcionamento da introdução de alunos e para a introdução de turmas / aulas.

A Figura 4-3 apresenta o fluxograma principal da aplicação, sendo na Figura 4-4 apresentados os blocos de introdução de alunos e na Figura 4-5 apresentados os blocos de introdução de turmas / aulas.

Para iniciar o processo de comunicação entre o smartphone e o protótipo é necessário realizar o emparelhamento entre os dispositivos. Ao abrir a aplicação, e já na janela inicial, o utilizador deverá clicar no botão de conexão do *Bluetooth* e selecionar o endereço do dispositivo que estará disponível no formato de lista. Após a conexão ter sido realizada, a aplicação solicita o código Pin do dispositivo, que por omissão e até à primeira utilização terá o código 0000, guardado em memória (*EEPROM*). O controlador (*Arduíno Mega 2560*) responde com o envio do Pin guardado. Após a resposta, se o código for o inicial (0000), irá abrir a janela para definição de novo código de utilizador, solicitando a introdução de um novo código e atualizá-lo na memória do controlador.

Caso o dispositivo já tenha sido utilizado e tenha código Pin definido, abre a janela do menu de funcionalidades, que se apresenta na Figura 4-6.

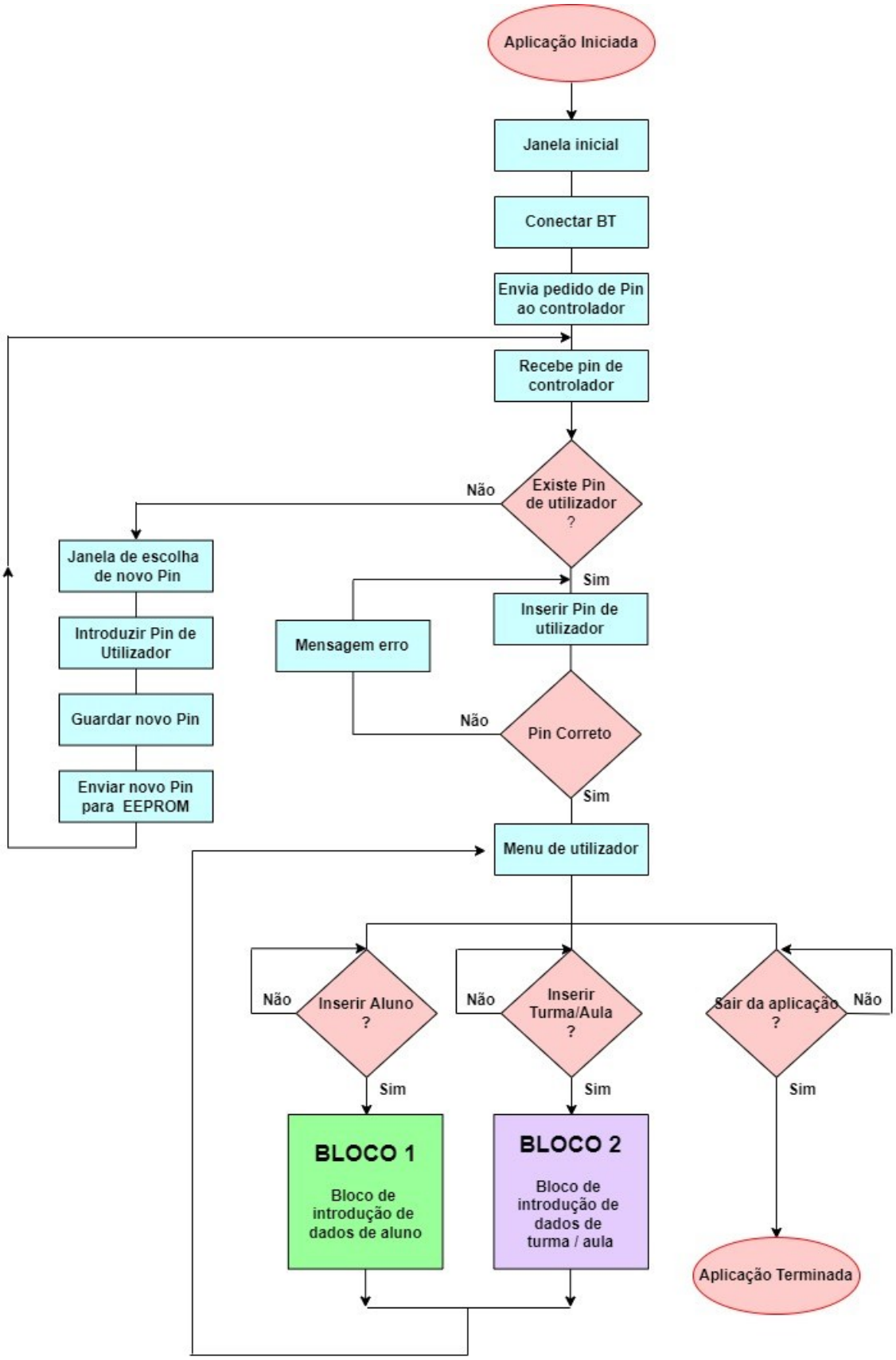


Figura 4-3: Fluxograma principal da aplicação para *smartphone.*

Na janela "*Menu de utilizador"*, apresentam-se de três opções:

- *"Inserir Aluno":* introduzir novos alunos ao sistema de registo de assiduidade.
- *"Inserir Turma / aula":* introduzir uma nova aula de uma turma;
- "*Sair*": fechar e sair da aplicação.

Como referido anteriormente, foram colocados blocos no fluxograma principal (ver Figura 4-3) responsáveis pelas funcionalidades de introdução de dados.

No bloco 1 (Figura 4-4) caso seja selecionada a opção "*inserir aluno*", surgirá a uma nova janela para introdução dos dados do aluno, permitindo no final três opções: "*limpar os dados*" inseridos, *"enviar dados*" inseridos ou "*voltar*" ao menu anterior. Caso seja selecionada a opção *"limpar dados*", permanece-se na mesma janela, caso sejam selecionadas as opções de "*enviar dados*" ou de "*voltar*", regressar-se-á ao menu de utilizador.

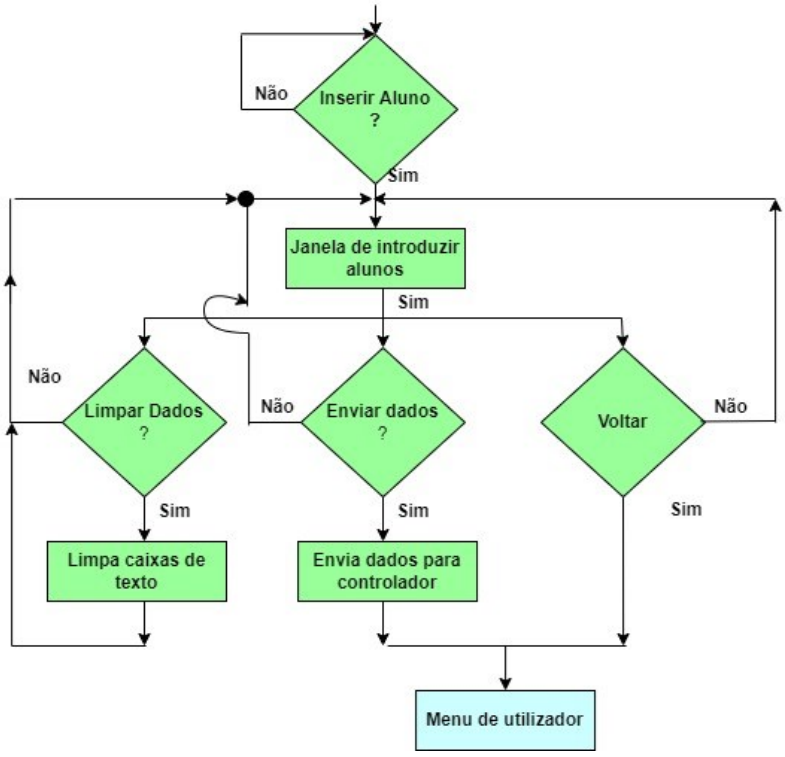


Figura 4-4: Fluxograma do bloco 1 (introdução de dados de alunos).

No caso do bloco 2 (Figura 4-5) caso seja selecionada a opção "*inserir turma / aula*", surgirá uma nova janela para introdução dos dados de uma nova aula. Após preenchimento surgem as mesmas três opções: "*limpar os dados*" inseridos, *"enviar dados*" inseridos ou "*voltar*" ao menu anterior, com o processo de funcionamento idêntico ao descrito anteriormente.

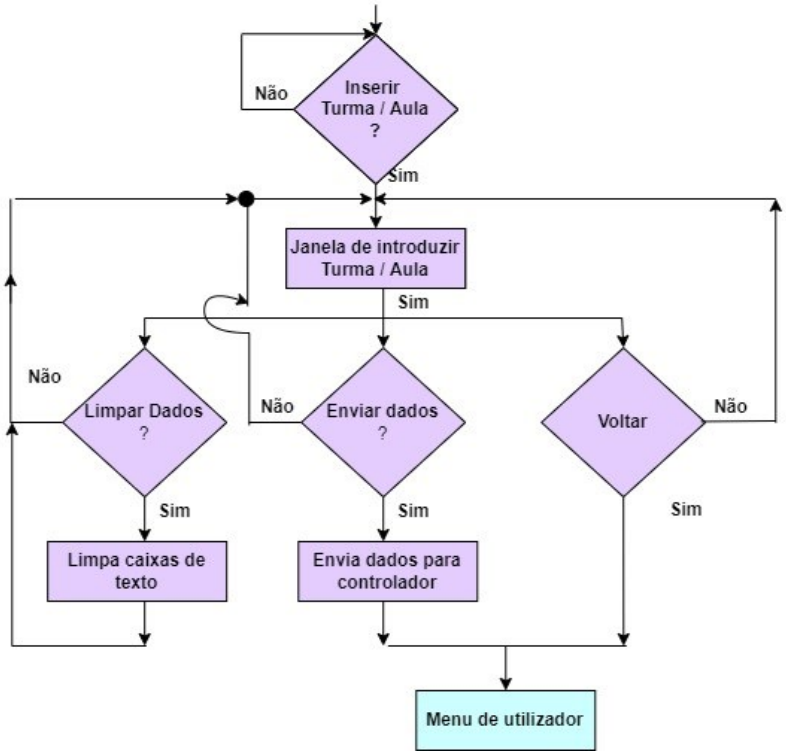


Figura 4-5: Fluxograma do bloco 2 (introdução de dados de turma / aula).

Relativamente ao aspeto do menu principal da interface da aplicação, este pode ser observado na Figura 4-6.


Figura 4-6: Janela principal da aplicação para *Smartphone.*

Se a opção for a de "Conectar BT", temos acesso à lista de dispositivos emparelhados por *Bluetooth* com o *smartphone* onde devemos selecionar o endereço do módulo do dispositivo de controlo de acessos que foi previamente emparelhado. Os blocos responsáveis pela conexão BT e pela saída da aplicação encontram-se na Figura 4-7, onde se verifica que é criada uma lista com os endereços disponíveis, através do bloco "*ListPicker.BeforePicking*" e que a aplicação irá conectar ao endereço selecionado através do conjunto "*ListPicker.AfterPicking", "Set ListPicher.Selection", "BluetoothCliente. Connect"*.

Relativamente ao botão de fecho da aplicação, para além do bloco de fecho da aplicação, "*Close Application*", está adicionado um bloco de desconexão do módulo *Bluetooth*, "*BluetoothClient.Disconnect*", para garantir que após a utilização com sucesso esta ligação possa ser quebrada.

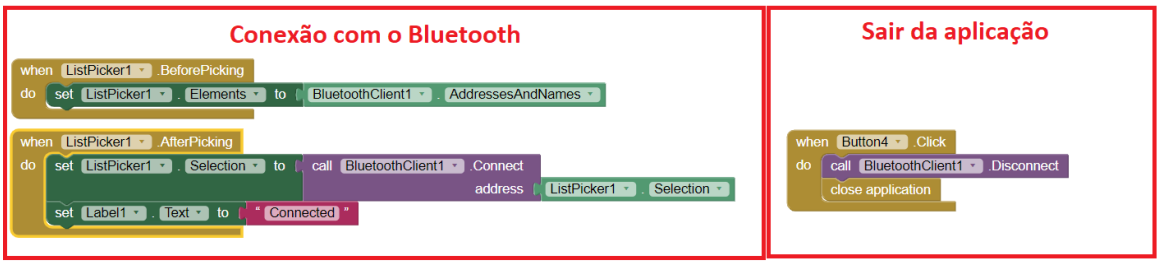


Figura 4-7: Blocos para conexão BT e sair da aplicação [43].

Se a opção for "Inserir Aluno", o ecrã mostrará o ambiente da Figura 4-8, onde se observam as opções disponíveis para preencher, "Número de Aluno", "Nome", "Curso" e os botões de "Limpar Dados", "Enviar Dados" e "Voltar para o menu anterior.

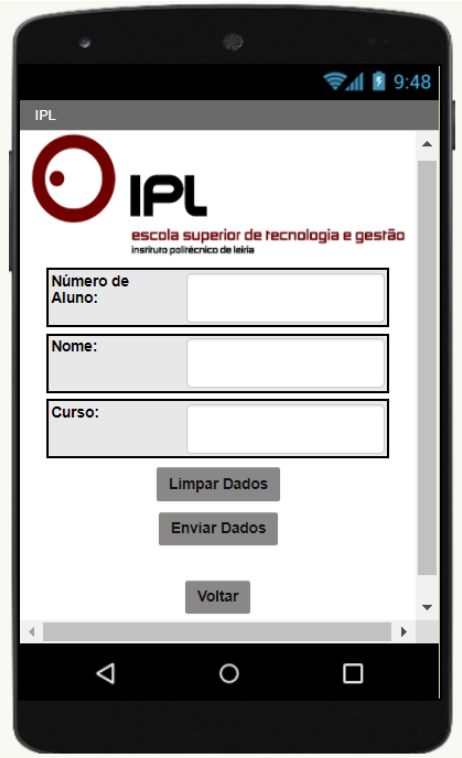


Figura 4-8: Janela de Inserir alunos.

Nesta janela, clicando em cima das respetivas caixas, podem ser preenchidos os campos informativos do aluno. Caso existam enganos, os dados podem ser apagados clicando no botão "Limpar Dados". Se a opção for a do envio da informação, deverá ser pressionado o botão "Enviar Dados" que realizará o envio da informação para o controlador em formato de *string* separada por vírgulas (CSV – *"comma-separated values"*).

A Figura 4-9 apresenta os blocos responsáveis pelas funcionalidades de eliminar dados e enviar dados.

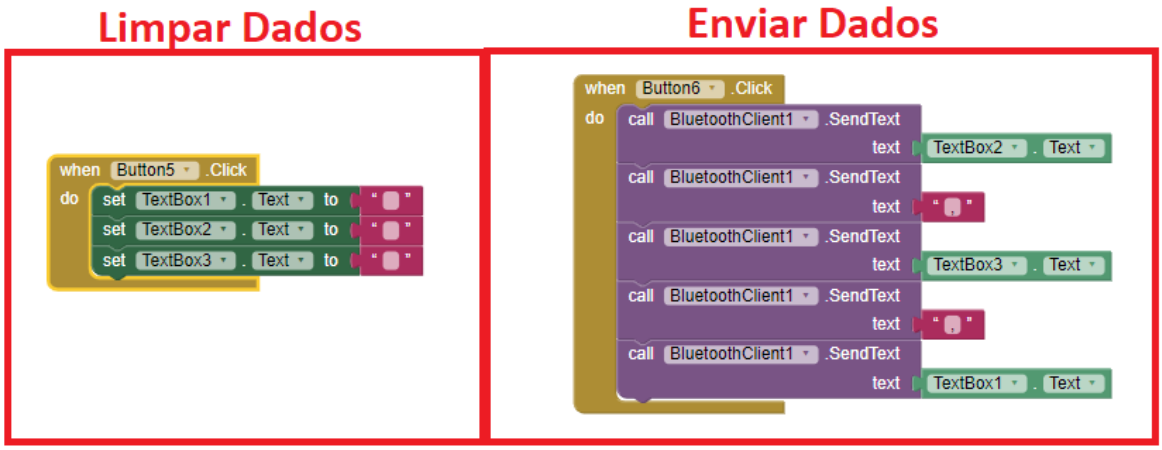


Figura 4-9: Blocos de funções de eliminar dados e enviar de dados [43].

Se a opção for "Inserir Turma/Aula", o ecrã mostrará o ambiente da Figura 4-10, onde podemos observar as opções disponíveis para preencher, "Curso", "UC", Turma e "Aula nº".

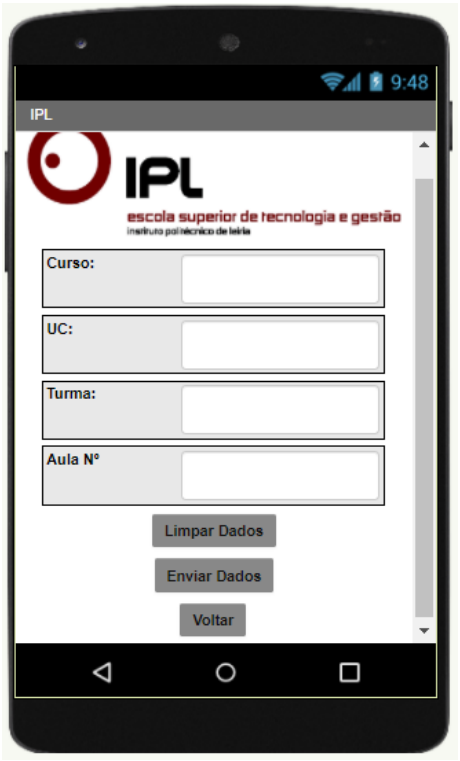


Figura 4-10: Janela de inserir turma/aula.

Deve ser referido também que, quer seja na janela de inserção de aluno, quer seja na janela de inserção de turma/aula, as caixas têm exemplos do formato que deve ser introduzido em cada um dos campos.

## 4.2. Construção da interface do dispositivo

De forma a permitir a visualização e gestão da informação gerada pelo sistema, tal como abordado na subsecção 3.3.6 deste documento, foi necessário integrar no protótipo uma interface.

A escolha da solução, um ecrã táctil (*Nextion*) com microcontrolador dedicado e uma plataforma de desenvolvimento dedicada, *Nextion Editor* [44], permitiu a construção de todo o ambiente gráfico.

A Figura 4-11 apresenta a janela de construção da interface do dispositivo, onde se observa a caixa de recursos *Toolbox* do lado esquerdo, que através do método de clique e arraste, podem ser posicionados na janela que representa o ecrã. As páginas criadas para o projeto (*Pages*)

ficarão do lado direito, de forma sequencial, representado no lado direito da página. Por baixo, teremos a caixa de atributos dos componentes utilizados em cada página, onde se destacam o identificador do componente (*ID*) e o seu nome. Estes atributos serão utilizados pelo controlador para conseguir identificar quais foram pressionados, no caso dos botões, ou onde colocar informação gerada ou enviada pelo *smartphone*, no caso das caixas de texto. Já a caixa de eventos será necessária para adicionar informação que também será necessária à comunicação com o controlador, nomeadamente o número da página atual.

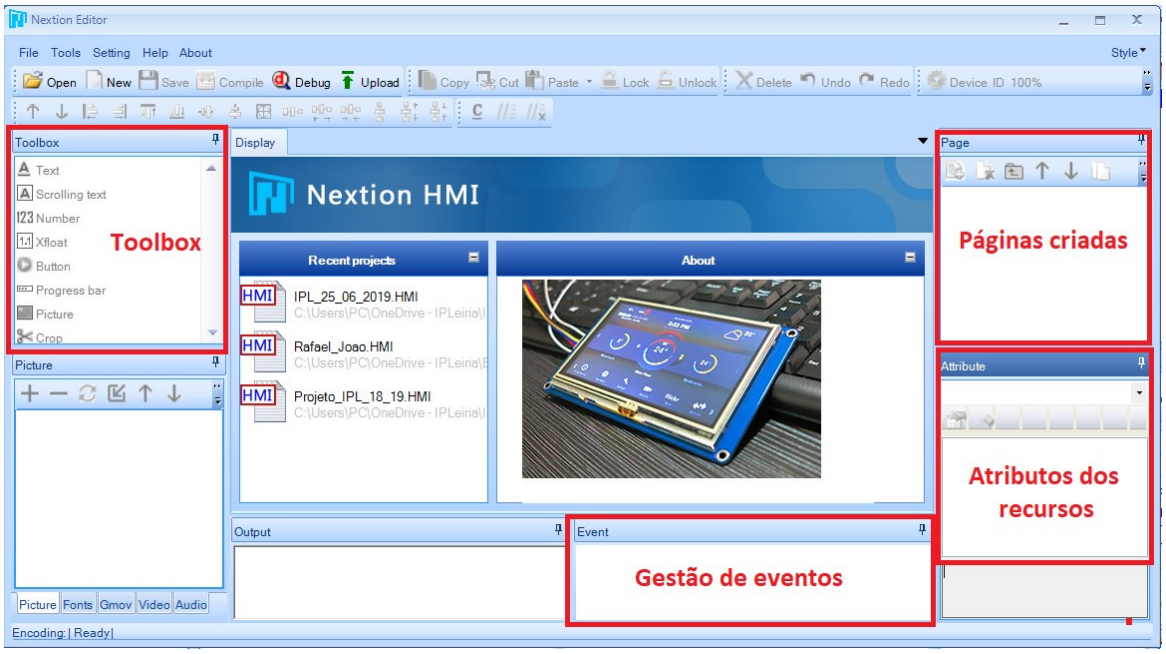


Figura 4-11: Ambiente de programação do *Nextion Editor*.

Relativamente ao funcionamento do programa construído para a interface, foi também elaborado um fluxograma definindo os procedimentos e forma de atuação do utilizador. Dada a dimensão do fluxograma, e por forma a ficar legível e interpretável pelo leitor, optou-se por, em alguns casos, criar blocos macro para o funcionamento da gestão de alunos e para a gestão de aulas.

A Figura 4-12, apresenta o fluxograma principal da aplicação e as Figura 4-13 e Figura 4-14, apresentam os blocos de gestão de alunos e gestão de aulas respetivamente.

Ao ligarmos a alimentação do dispositivo, visualizamos a janela inicial e o utilizador deverá selecionar a opção pretendida.

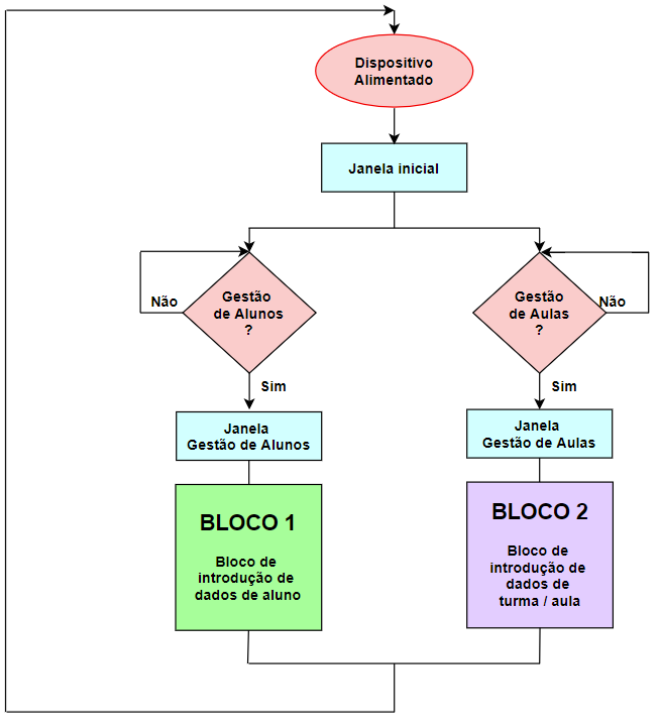


Figura 4-12: Fluxograma da interface do sistema.

Na janela inicial são apresentadas duas opções:

- *"Gestão de Alunos"*: introduzir novos alunos ao sistema de registo de assiduidade ou apagar alunos já inseridos;
- *"Gestão de aulas"*: introduzir uma nova aula de uma turma ou apagar uma aula já inserida.

Como referido anteriormente, foram colocados blocos no fluxograma principal (Figura 4-12) responsáveis pelas funcionalidades de gestão de dados do sistema.

No caso do bloco 1 (fluxograma da Figura 4-13), caso seja selecionada a opção "*gestão de alunos*", surgirá uma nova janela para selecionar a inserção ou remoção de um estudante. Escolhendo a opção *"Inserir Aluno"*, será necessário selecionar o ciclo de estudos e o curso, e introduzir os dados referentes ao estudante: número de estudante, nome, curso. Deve, ainda, ser realizada a leitura do código RFID do cartão de estudante, *tag* NFC e a impressão digital premindo os respetivos botões no ecrã. Após serem inseridos os dados, deve ser pressionado o botão "*Guardar*".

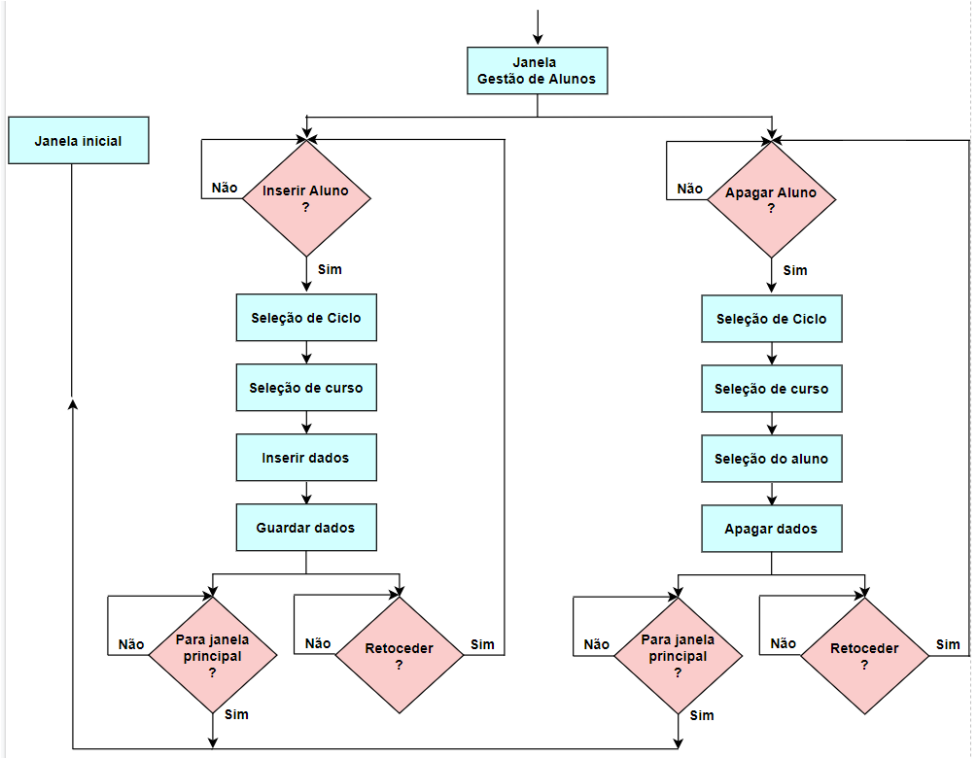


Figura 4-13: Fluxograma do bloco gestão de alunos.

No caso de selecionar a opção *"Apagar Aluno",* o procedimento será muito semelhante ao anterior, teremos de selecionar o ciclo de estudos, selecionar o curso, selecionar o aluno e premir o botão para apagar.

No caso do bloco 2, no fluxograma da Figura 4-14, caso seja selecionada a opção "*gestão de aulas*", levará a uma nova janela que terá um procedimento geral com os passos descritos anteriormente para a gestão de alunos, mas neste caso, associado à opção de gestão de turma.

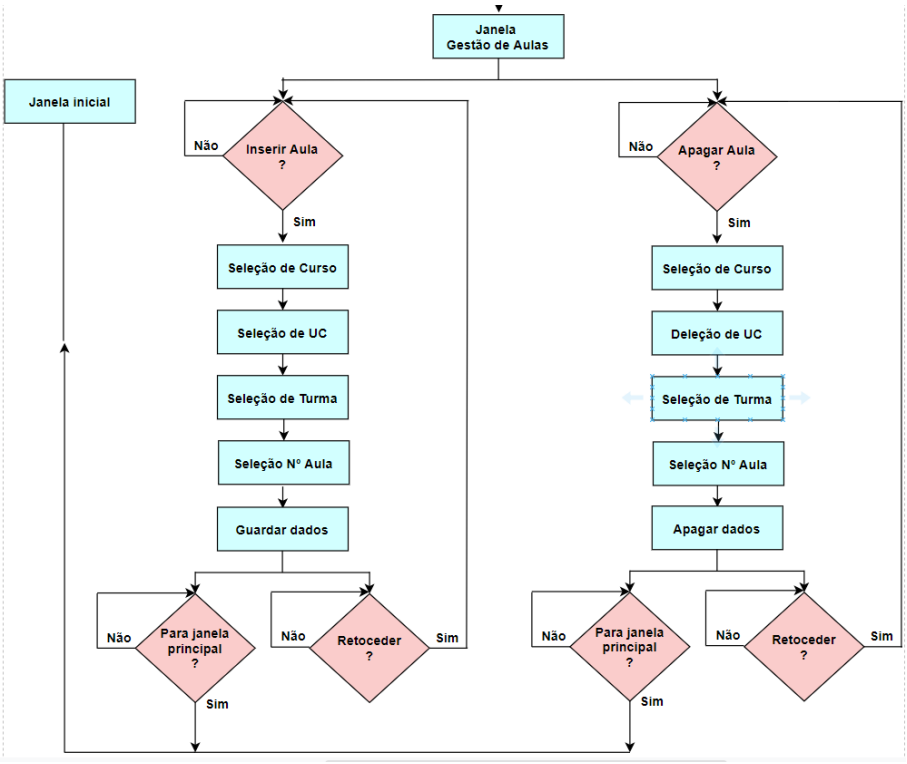


Figura 4-14: Fluxograma do bloco gestão de aulas.

A Figura 4-15 apresenta a janela principal da interface do ecrã, onde constam os botões de seleção de gestão de alunos e gestão de aulas. No lado superior direito verificamos a existência de várias páginas que apresentam as diversas funcionalidades abordadas no fluxograma.

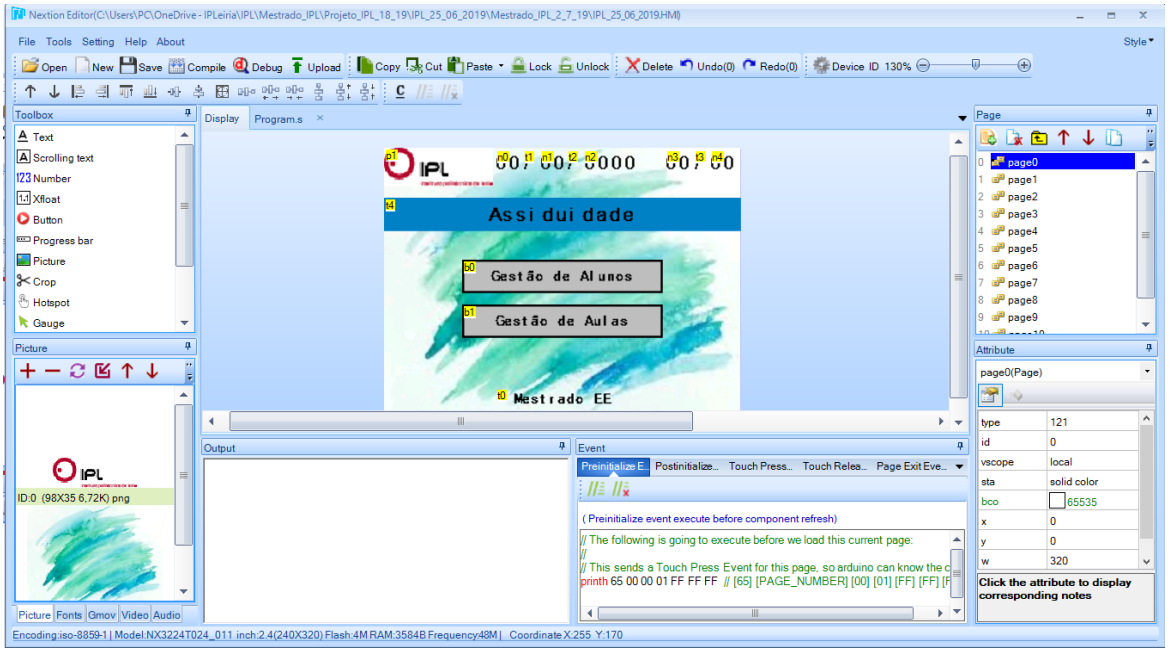


Figura 4-15: Janela principal da interface do sistema.

Podemos observar o aspeto de algumas dessas páginas de seleção de opções na Figura 4-16. Estas figuras representam o formato das janelas de navegação entre menus.

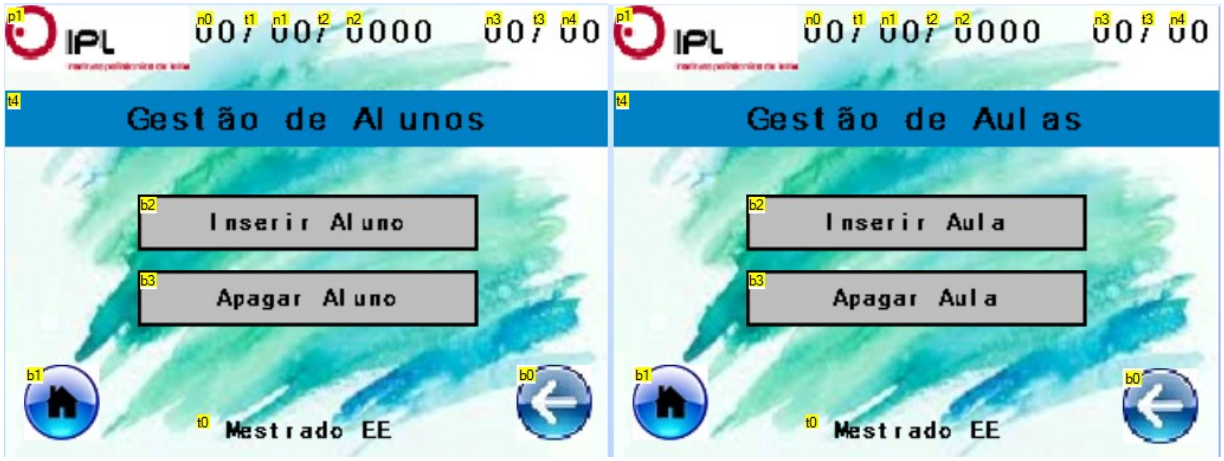


Figura 4-16: Janelas de seleção de funcionalidades.

Em cima, para além do logótipo do IPLeiria, foram colocados os dados relativos a data e hora e no centro os botões de seleção de opções.

Se a seleção for "*Inserir Aluno*", a janela apresentará as diversas opções de dados a inserir (ver Figura 4-17)

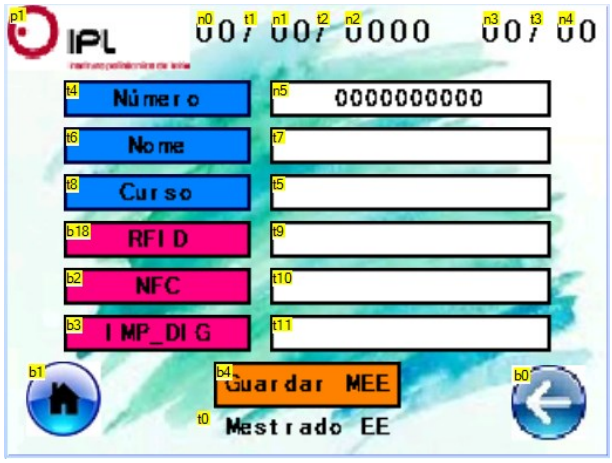


Figura 4-17: Janelas de introdução de dados.

Podemos verificar que existem 2 conjuntos de dados diferentes, a azul os dados de recebidos da aplicação de *Smartphone* relativos a "Número", "Nome" e "Curso", e a rosa os dados de identificação de presença em aula, *tag* "RFID", *tag* "NFC" ou "Impressão digital".

No caso das opções azuis, as caixas de texto em frente a cada parâmetro receberão os dados preenchidos e enviados pelo *Smartphone*.

No caso das opções rosa, foram utilizados botões para selecionar qual o parâmetro de introdução de dados pretendido pelo utilizador.

# 5. Testes de funcionamento

Finalizada a abordagem a aspetos construtivos e especificidades do *hardware* e *software* utilizados neste protótipo, explica-se agora o seu modo de funcionamento. O docente utilizador deve, antecipadamente, criar todas as pastas relativas aos cursos, regime, UC, e tipo de aula no computador e depois inserir o cartão no dispositivo criado. Este processo deve ser realizado uma vez no início de cada semestre. A Figura 5-1, apresenta o formato da nomenclatura e as pastas e subpastas criadas.

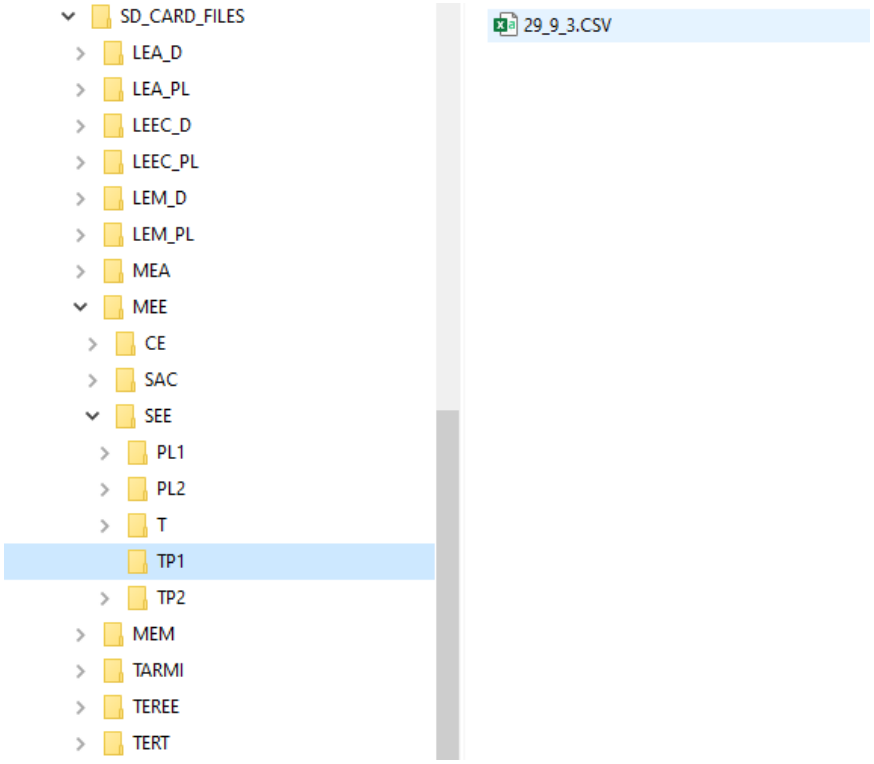


Figura 5-1: Pastas criadas no cartão de memória.

Observando a Figura 5-1 verificamos que no interior da pasta MEE (Mestrado eme Engenharia Eletrotécnica) se encontram as UC's lecionadas pelo docente. No caso da imagem, está selecionada a UC de SEE (Sistemas Elétricos de Energia). No interior da UC está o tipo regime da aula e verificamos que a seleção foi TP1 (Teórico-Prática turno 1). No interior de TP1 encontra-se um ficheiro criado para registar as presenças em aula com o nome relacionado com a data em que esta ocorreu e com o número da aula. A escolha deste formato de pastas deveu-se ao facto de os nomes a dar aos ficheiros de registos de alunos ter o limite de 8 caracteres, o que limita bastante a necessidade de indicar todos os dados (Curso, UC, regime, data da aula).

Após ter criado as pastas e inserido o cartão no dispositivo, poe dar início à criação de aulas registo de alunos.

Relativamente ao registo de dados de alunos para posterior identificação, optou-se por criar ficheiros com os alunos escalados por curso (Figura 5-2).

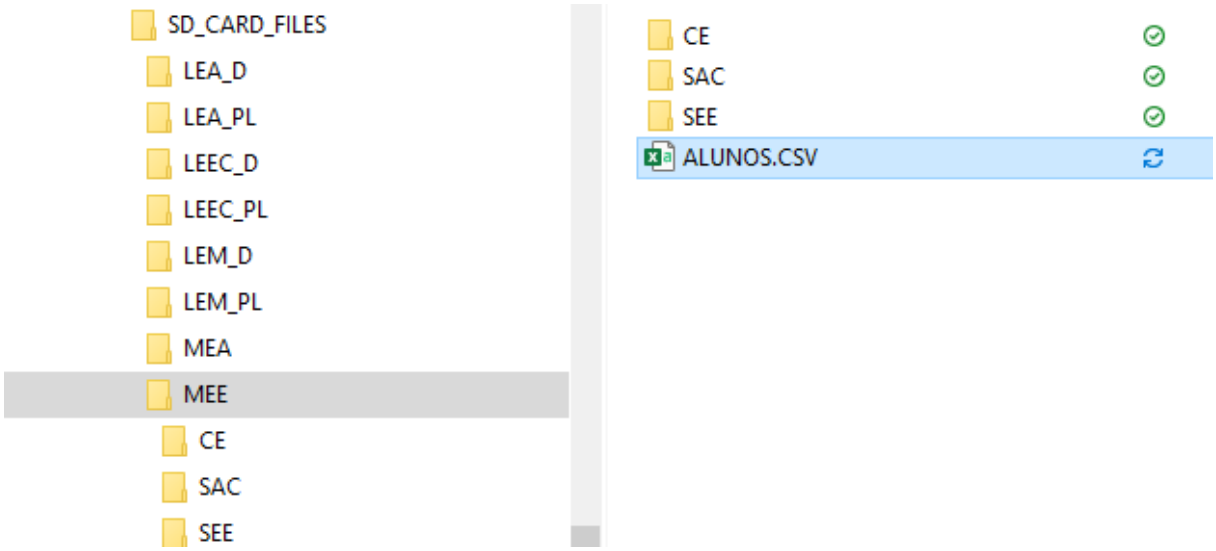


Figura 5-2: Ficheiro para registo de alunos de MEE.

Desta forma ao introduzir-se os dados de um aluno, caso seja o primeiro a ser introduzido, será criado um ficheiro com o nome "ALUNOS" no interior da pasta de cada curso. Caso já exista o ficheiro, o novo aluno será inserido no ficheiro existente.

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Numero | Nome | Curso | RFID | NFC | ImpDig | Data | Hora | |
| 2 | 2111070 | Rui Peixoto | MEE | 6F003515[ | 0 | 0 | 06/04/2020 | 18:50 | |
| 3 | 2111070 | Rui Peixoto | MEE | 6F003515[ | 0 | 0 | 06/04/2020 | 18:50 | |
| 4 | 2111070 | Rui Peixoto | MEE | 6F003515[ | 0 | 0 | 06/04/2020 | 18:50 | |
| 5 | 2111081 | Manuela Moura | MEE | | 4193218219641120 | 1 | 06/04/2020 | 18:54 | |
| 6 | 2180091 | Marco Fernandes | MEE | 6F003515[ | 8872197019641120 | 2 | 06/04/2020 | 18:56 | |

Figura 5-3: Ficheiro alunos.

Na Figura 5-3, podemos verificar alguns alunos introduzidos e os dados que cada um forneceu. Os espaços sem informação são propositados, uma vez que os alunos podem não ter interesse em registar determinada informação, no entanto, será realizado o registo mesmo assim.

A introdução de curso, nome e número de estudante, são inseridos através da APP de *Smartphone* e enviados para o dispositivo através de *Bluetooth*. Em seguida, podem ser introduzidos os dados relativos ao cartão de estudante (RFID), *tag* de NFC (Identificador alternativo) e impressão digital (Figura 5-4).


Figura 5-4: Interface do dispositivo e APP de *Smartphone* na introdução de alunos.

Caso pretenda, o docente pode guardar os dados presentes no ecrã do dispositivo, premindo o botão de "Guardar". Os dados serão guardados no ficheiro alunos no interior da pasta MEE. Relativamente à introdução de aulas, o processo é análogo ao anterior, sendo que também os dados inseridos na APP servirão para indicar o local onde criar a aula, com a data e número de aula respetivos.


Figura 5-5: Interface do dispositivo e APP de *Smartphone* na introdução de aulas.

Observando a Figura 5-5, verificamos os dados inseridos na APP e enviados para o dispositivo.

# 6. Conclusões

Na fase inicial deste trabalho, foram identificados os principais objetivos e motivações (1.2) das quais se retiraram os requisitos funcionais para o protótipo (3.1). Finalizada a fase de desenvolvimento, teste e análise de resultados deste projeto, foi possível validar alguns dos deles.

Do conjunto de requisitos destacaram-se os seguintes como fundamentais:

1. Desenvolver um protótipo simples e com componentes genéricos presentes em qualquer loja de eletrónica;
2. Desenvolver um protótipo de pequena dimensão e portável;
3. Permitir o registo e armazenamento dos dados para posterior utilização.
4. Permitir a identificação com o tradicional cartão de estudante;

Foi demonstrado e desenvolvido um protótipo com recurso a componentes comuns presentes em qualquer loja de eletrónica e de utilização recorrente nos projetos da área. Quanto à simplicidade, e sendo um dispositivo agregador de diversas formas de identificação, podemos afirmar que quanto maior a quantidade e diversidade de métodos de identificação utilizados, maior o grau de complexidade do protótipo.
Relativamente à dimensão, o protótipo tem 145x75x50mm para comprimento, largura e altura. Considerando a quantidade de hardware e a necessidade da sua colocação no interior de uma caixa, a apreciação da sua dimensão pode variar consoante os parâmetros desejados pelo utilizador.
Foi inserido um módulo de cartão microSD para registo de todos os dados necessários à gestão do sistema o que confere a possibilidade de registo de todos os dados gerados ao longo das aulas.
Foi demonstrada a utilização de leitor de RFID para utilização do cartão de estudante já em vigor na IPLeiria. Foi identificada a frequência utilizado para os cartões em uso e selecionado um leitor compatível para o dispositivo.

Foram ainda abordados os seguintes requisitos:

5. Desenvolver um protótipo de baixo custo;
6. Desenvolver um protótipo capaz de ser utilizado em qualquer sala de aula;
7. Permitir a introdução de dados relativos aos alunos a identificar;
8. Permitir a introdução de dados relativos às aulas a lecionar;
9. Permitir a identificação com a impressão digital;
10. Permitir a identificação com o sistema NFC do Smartphone;
11. Permitir a identificação através do método *tag "Near Field Communication"* (NFC);

Foi realizada uma análise de custos que permite verificar uma diferença significativa entre os custos para fornecimento do material por via nacional comparativamente com via internacional.
Foi demonstrado que o protótipo é portável, assim sendo pode ser utilizado em qualquer sala de aula.
Foi demonstrado que permite a introdução de dados de alunos através da utilização da aplicação de *Smartphone.*
Foi demonstrado que permite a introdução de aulas a lecionar também através da utilização da aplicação de *Smartphone.*
Foi inserida e demonstrada a utilização de sensor biométrico, neste caso, leitor de impressão digital para alternativa de identificação de alunos.
Foi equacionada a utilização do recurso NFC inserido nos *Smartphones* atuais, mas essa funcionalidade foi abandonada devido ao facto de o ID do Smartphone ser dinâmico, ou seja, a cada vez que é solicitada a identificação gera um novo ID. Esta situação não permite registar em base de dados o ID único do aluno.
Foi inserido uma alternativa para *tags* ta tecnologia NFC para colmatar a ausência do Smartphone e poder associar a qualquer objeto de índole pessoal (p.ex. porta-chaves).

Em termos globais, considera-se que a diversidade de tecnologias de identificação permite maior flexibilidade na sua utilização, o que fornece maior garantia que qualquer aluno presente possa fazer a sua identificação através do dispositivo.
A escolha do controlador *Arduino Mega* 2560 pode ser limitador se se pretender desenvolver funcionalidades baseadas em comunicação através da internet. Com outro controlador com ligação à internet e ultrapassadas as questões de privacidade e de proteção de dados, poderiam ser integradas funcionalidades adicionais e uma possível integração nas plataformas de gestão já utilizadas no IPLeiria.

**Desenvolvimento futuro**

Relativamente a desenvolvimento futuro, sugere-se possam ser selecionados e utilizados componentes mais avançados, robustos e de menor dimensão, nomeadamente, seleção de leitor/leitores de RFID mais avançados, de maior alcance e de leitura e identificação de várias *tags* em simultâneo para que sejam detetados os alunos sem a necessidade de aproximar o cartão do leitor, bastando entrarem na sala. Seleção de leitor de impressão digital com menores taxas de aceitação e rejeição falsas, ou mesmo a seleção de outros métodos de análise biométrica, tal como, reconhecimento facial, reconhecimento da retina ou reconhecimento do padrão de voz.
Pode, ainda, ser estudada a integração de todo o hardware numa só placa, reduzindo acentuadamente dimensões globais, problemas com cablagem e, sobretudo, redução de custos o que possibilitaria uma produção em série.

# Referências Bibliográficas


[1] D. Pedro, D. de Bragança, and J. Xavier Mousinho da Silveira, "Implantação do sistema administrativo - Decreto nº 23 de 6 de Maio de 1832."

[2] "IRN.Justica.Gov.pt." https://irn.justica.gov.pt/Sobre-o-IRN/A-nossa-historia (accessed Jun. 20, 2020).

[3] "Marcos Históricos." https://irn.justica.gov.pt/Portals/33/Marcos%20Hist%201_7_2019.pdf?ver=2019-07-01-121527-147 (accessed Jun. 20, 2020).

[4] "Ficheiro:Bilhete de Identidade de Manuel de Arriaga (2JAN1914).png – Wikipédia, a enciclopédia livre." https://pt.wikipedia.org/wiki/Ficheiro:Bilhete_de_Identidade_de_Manuel_de_Arriaga_(2JAN1914).png (accessed Jun. 20, 2020).

[5] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Apr. 2012, pp. 1282–1285. doi: 10.1109/CECNet.2012.6201508.

[6] L. Kumari, K. Narsaiah, M. K. Grewal, and R. K. Anurag, "Application of RFID in agri-food sector," *Trends in Food Science & Technology*, vol. 43, no. 2, pp. 144–161, Jun. 2015, doi: 10.1016/j.tifs.2015.02.005.

[7] C. E. Realini and B. Marcos, "Active and intelligent packaging systems for a modern society," *Meat Science*, vol. 98, no. 3, pp. 404–419, Nov. 2014, doi: 10.1016/j.meatsci.2014.06.031.

[8] Y. Xiao, S. Yu, K. Wu, Q. Ni, C. Janecek, and J. Nordstad, "Radio frequency identification: technologies, applications, and research issues," *Wireless Communications and Mobile Computing*, vol. 7, no. 4, pp. 457–472, May 2007, doi: 10.1002/wcm.365.

[9] D. K. Klair, K. W. Chin, and R. Raad, "A survey and tutorial of RFID anti-collision protocols," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 3, pp. 400–421, 2010, doi: 10.1109/SURV.2010.031810.00037.

[10] V. Chawla and D. Ha, "An overview of passive RFID," *IEEE Communications Magazine*, vol. 45, no. 9, pp. 11–17, Sep. 2007, doi: 10.1109/MCOM.2007.4342873.

[11] Klaus Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, Second Edition. Chichester, West Sussex, 2003.

[12] R. Want, "An Introduction to RFID Technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, Jan. 2006, doi: 10.1109/MPRV.2006.2.

[13] "Actag." http://www.actag.com/tags.php (accessed Jun. 20, 2020).

[14] H. B. Oecd -Paris, "EPCglobal-RFID standards & regulations," 2005.

[15] "EPCglobal | GS1." https://www.gs1.org/epcglobal (accessed Jul. 03, 2020).

[16] "RFID Tags - EPC-RFIDEPC-RFID." https://www.epc-rfid.info/rfid_tags (accessed Jul. 03, 2020).

[17] R. Moscatiello, "Basic Concepts in RFID Technology." Accessed: Jul. 06, 2020. [Online]. Available: https://1library.net/document/q0p1rn9z-basic-concepts-in-rfid-technology.html?utm_source=seo_keyword_list

[18] "NFC Forum." https://nfc-forum.org/our-work/specification-releases/specifications/nfc-forumtechnical-specifications/ (accessed Jul. 03, 2020).

[19] "Near Field Communication (NFC) Technology and Measurements White Paper", Accessed: Jul. 06, 2020. [Online]. Available: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma182/1MA182_5E_NFC_WHITE_PAPER.pdf

[20] N. S. S. Shobha, K. S. P. Aruna, M. D. P. Bhagyashree, and K. S. J. Sarita, "NFC and NFC payments: A review," in *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, 2016, pp. 1–7. doi: 10.1109/ICTBIG.2016.7892683.

[21] E. Haselsteiner, "Security in Near Field Communication ( NFC ) Strengths and Weaknesses," 2006.

[22] "Everything you need to know about NFC and mobile payments." https://www.cnet.com/tech/mobile/how-nfc-works-and-mobile-payments/ (accessed Jul. 20, 2020).

[23] J.-H. Cho, J. Kim, J.-W. Kim, K. Lee, K.-D. Ahn, and S. Kim, "An NFC transceiver with RF-powered RFID transponder mode," in *2007 IEEE Asian Solid-State Circuits Conference*, Nov. 2007, pp. 172–175. doi: 10.1109/ASSCC.2007.4425758.

[24] R. Kumar Mahur, "A Seminar Report On NFC." Accessed: Jul. 20, 2020. [Online]. Available: https://pt.slideshare.net/RahulKumar540/seminar-on-nfc

[25] "About the Technology - NFC Forum." https://nfc-forum.org/what-is-nfc/about-the-technology/ (accessed Dec. 29, 2021).

[26] "ECMA-340 - Ecma International." https://www.ecma-international.org/publications-and-standards/standards/ecma-340/ (accessed Dec. 29, 2021).

[27] "Sony Corporation - FeliCa - Overview of FeliCa - The FeliCa System." https://www.sony.net/Products/felica/about/scheme.html (accessed Dec. 29, 2021).

[28] D. Maltoni, "A Tutorial on Fingerprint Recognition," in *LNCS*, vol. 3161, Springer-Verlag, 2005, pp. 43–68. doi: 10.1007/11493648_3.

[29] E. De, E. De, S. Carlos, and R. S. Casado, "UNIVERSIDADE DE SÃO PAULO EXTRAÇÃO DE MINÚCIAS EM IMAGENS DE IMPRESSÕES DIGITAIS." Accessed: Jul. 25, 2020. [Online]. Available: https://www.teses.usp.br/teses/disponiveis/18/18152/tde-15102008-135808/publico/Ricardo.pdf

[30] "About Us | Bluetooth® Technology Website." https://www.bluetooth.com/about-us/ (accessed Aug. 08, 2021).

[31] C. Beard and W. Stallings, "Wireless Communication Networks and Systems 1 st edition CHAPTER 12 BLUETOOTH AND IEEE 802.15 Bluetooth and IEEE 802.15 12-1," 2016.

[32] "Apontamentos TeSP: ERT, UC: Redes de Acesso DEP. ENGENHARIA ELETROTÉCNICA."

[33] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance Evaluation of Bluetooth Low Energy: A Systematic Review," *Sensors*, vol. 17, no. 12, p. 2898, Dec. 2017, doi: 10.3390/s17122898.

[34] "Arduino Mega 2560 Rev3 — Arduino Official Store." https://store.arduino.cc/products/arduino-mega-2560-rev3 (accessed Dec. 29, 2021).

[35] "ID Innovations ID SERIES DATASHEET Classic RFID module products." Accessed: Jun. 20, 2020. [Online]. Available: http://id-innovations.com/httpdocs/EM%20moudule%20SERIES%20V27%20(2008-4-05).pdf

[36] "PN532 - PTRobotics." https://www.ptrobotics.com/module/iqitsearch/searchiqit?s=PN532 (accessed Jul. 20, 2020).

[37] "In-Depth: What is RFID? How It Works? Interface RC522 with Arduino." https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/ (accessed Jul. 20, 2020).

[38] "Fpm10a módulo de leitor de impressão digital, leitor óptico de sensor para fechadura da porta módulo de scanner de impressão digital para interface de comunicação serial

arduino|Sensores de pressão| - AliExpress.” https://pt.aliexpress.com/item/32982364002.html?spm=a2g0s.9042311.0.0.2742b90a5Xbxbv (accessed Jul. 20, 2020).

[39] “Biométricos.” https://www.botnroll.com/pt/101-biometricos (accessed Jul. 20, 2020).

[40] “Arduino Lab 02 – Sensor de luminosidade e display de LCD 16×2 – EasyTrom Labs.” https://easytromlabs.com/arduino/arduino-lab-02-sensor-de-luminosidade-e-display-de-lcd-16x2/ (accessed Jul. 20, 2020).

[41] “Home - Nextion.” https://nextion.tech/ (accessed Jul. 20, 2020).

[42] “MicroSD Card Adapter w/ Level Shifters | Conversores.” https://www.ptrobotics.com/conversores/6540-microsd-card-adapter-w-level-shifters.html (accessed Aug. 10, 2020).

[43] “MIT App Inventor | Explore MIT App Inventor.” https://appinventor.mit.edu/ (accessed Jul. 20, 2020).

[44] “DOWNLOAD - Nextion.” https://nextion.tech/nextion-editor/ (accessed Oct. 15, 2019).