Instituto Politécnico de Viseu

Escola Superior de Tecnologia e Gestão de Viseu

Cipriano Luís Arede Pereira

Dispositivos de identificação

Tese de Mestrado

Sistemas e Tecnologias de Informação para as Organizações

Professor Rui Jorge dos Santos Almeida

Outubro de 2012

RESUMO

Esta tese tem por finalidade o levantamento do estado da arte no que toca a dispositivos/tecnologias de identificação de seres humanos e a elaboração de uma aplicação com o objetivo de centralizar o controlo de vários equipamentos de identificação por RFID e impressão digital guardando um registo de passagens que pode ser posteriormente consultado ou exportado para outras bases de dados para futuros tratamentos.
No estudo demos relevância às várias formas de autenticação a seguir identificadas explicando para cada uma o seu fundamento, como funciona, os principais requisitos e que equipamentos são usados:

- O código de barras
- O RFID;
- A biometria, sendo que falamos de varias tecnologias como a impressão digital, a geometria da mão, o reconhecimento facial, a retina, a íris, o reconhecimento de vasos sanguíneos, o reconhecimento de voz, a assinatura manuscrita, o Formato do ouvido e ADN.

É feita também uma pequena comparação ente tecnologias com o objetivo de tentar encontrar a melhor técnica biométrica; é ainda referida a multi-biometria, no que consiste, que tipos de multi-biometria existem, que características podem ser usadas e como são fundidas, e por fim é feito um pequeno enquadramento legal.
Na segunda parte da tese é descrita a aplicação desenvolvida. Será descrita a elaboração da aplicação com referência às tecnologias usadas e com que fundamento foram usadas, que funções foram implementadas e como foram implementadas justificando as opções tomadas. No final são mostrados alguns testes para demostrar o correto funcionamento da aplicação.

ABSTRACT

This thesis aims at lifting the state of the art when it comes to devices / technologies to identify humans and the development of an application with the aim of centralizing the control of various equipment for RFID identification and fingerprint keeping track of tickets, which can subsequently be queried or exported to other databases for future treatments.
In the study we gave importance to the various forms of authentication identified below for each explaining its foundation, how it works, the main requirements and equipment that are used:

- The barcode
- The RFID;
- Biometrics, and talked of various technologies such as fingerprint, hand geometry, facial recognition, retina, iris, blood vessels recognition, speech recognition, handwritten signature, ear and Format DNA.

There is also a small comparison of the technologies with the goal of trying to find the best biometric technique and is still referred to multi-biometrics, in the aspects of what is, what types of multi-biometrics exist, what features can be used and how they are fused, and order is made by a small legal framework.
The second part of the thesis describes the application developed. Will be described the development of the application with reference to the technologies used and on what basis were used, which functions have been implemented and also a justification of the choices made. In the final, a few tests are shown to demonstrate the correct operation of the application.

PALAVRAS CHAVE

RFID
Código de barras
Impressão digital
Íris
Retina
Reconhecimento de voz
Geometria da mão
ADN
Odor
Template
Base de dados
Leitor biométrico

KEY WORDS

RFID
Bar code
Fingerprint
Iris
Retinal
Voice Recognition
Hand geometry
DNA
Odour
Template
Database
Biometric reader

AGRADECIMENTOS

Queria dar uma nota de apreço às pessoas mais importantes da minha vida e que tanto me ajudaram e motivaram para a realização desta tese: o meu pai, Cipriano de Bastos Pereira, a minha mãe, Maria de Fatima Martis Arede e a todos os meus amigos

Por outro lado, queria agradecer ao meu orientador, Rui Jorge dos Santos Almeida pela motivação, interesse e dedicação em me ajudar na elaboração desta tese.

ÍNDICE GERAL

ÍNDICE REMISSIVO DE AUTORES

ÍNDICE DE FIGURAS

ÍNDICE DE QUADROS

ABREVIATURAS E SIGLAS

IPV	Instituto Politécnico de Viseu
ESTGV	Escola Superior de Tecnologia e Gestão de Viseu
FAR	False Acceptance Error
FRR	False Rejection Error
EER	Equal Error Rate
CER	Crossover Error Rate
ADN	Ácido desoxirribonucleico
ROC	Receiver Operating Characteristic
RFID	Radio Frequency Identification
SGBD	Sistema de Gestão de Bases de Dados
EPC	Electronic Product Code
API	Application Programming Interface
DLL	Dynamic-link library
SQL	Structured Query Language
BL	Business Layer
DAL	Data Access Layer
BD	Data Base

NOTAÇÃO

a) Maiúsculas latinas

E	Módulo de elasticidade

b) Minúsculas latinas

r	Raio

c) Maiúsculas gregas

Φ	Aresta de fronteira

d) Minúsculas gregas

ϕ	Ângulo

e) Índices inferiores gerais

C	Contacto
CM	Centro de massa
b	Unidade de alvenaria
bj	Unidade de alvenaria e junta
c	Compressão

f) Índices superiores gerais

(k)	Iteração k
t	No instante de tempo t

g) Símbolos

$\ddot{u}$	Segunda derivada de u em ordem ao tempo
$\Leftarrow$	Se

1. Introdução

1.1 Enquadramento

O ser humano é um ser que vive em sociedade, isto é, não nasceu para estar sozinho e como tal no dia-a-dia dependemos uns dos outros para qualquer situação. O problema é que não nascemos para fazer apenas as nossas funções, do mesmo modo que não nascemos para aceitar o mundo do como ele é. No fundo, cada pessoa prioriza os seus próprios interesses e algumas não hesitam em prejudicar os outros para alcançar seus próprios objetivos. Logo, o ser humano não é confiável e, assim, é cada vez mais necessário o uso de mecanismos para controlar e restringir o acesso a determinados lugares ou serviços a pessoas mal-intencionadas. A identificação e autenticação de utilizadores é um dos principais aspetos a serem considerados para garantir a segurança. Nesse contexto, os mecanismos de identificação tradicionais, baseados em login e password, já não são suficientes.
Foi assim que nasceu a necessidade cada vez maior de sistemas mais seguros e eficientes. Mas qual ou quais os equipamentos que melhor se adaptam a determinada situação que pretendemos tratar, qual a segurança que cada um me oferece, quais as vantagens e desvantagens face a outros equipamentos? São estas as questões que são necessárias responder no momento de planeamento do sistema de segurança.

1.2 Objetivos

Esta tese será dividida em duas partes: um levantamento do estado da arte no que toca a dispositivos/tecnologias de identificação de seres humanos e elaboração e documentação de uma aplicação com o objetivo de centralizar o controlo de vários equipamentos de

identificação por RFID e impressão digital guardando um registo de passagens que pode ser posteriormente consultado ou exportado para outras bases de dados para futuros tratamentos.

No estudo foram serão estudados:

- O código de barras explicando o que é, como é usado, que leitores existem e que padrões existem;
- O RFID o que é, como é usado, que tipos de tags existem, que leitores existem e quais são as suas vantagens e desvantagens;
- A biometria, em que consiste, como funciona, que requisitos têm de satisfazer, como avaliar o desempenho de sistemas biométricos, níveis de desempenho/fiabilidade (taxas FAR, FFR, EER), níveis de conforto, níveis de aceitação, segurança, ataques mais frequentes e medidas de proteção e vantagens e desvantagens do uso da biometria para identificação humana. Dentro da biometria, estudamos varias tecnologias são elas:
    - A impressão digital, o que é, como é feita a aquisição de impressões digitais, que leitores existem e que vantagens e desvantagens existem;
    - A geometria da mão, o que é, como é feita a aquisição, que equipamentos existem e que vantagens e desvantagens existem;
    - O reconhecimento facial, o que é, como é feita a aquisição, que tipos de reconhecimento facial existem, que equipamentos existem e que vantagens e desvantagens existem;
    - A retina, o que é, como é feita a aquisição e que vantagens e desvantagens existem;
    - A íris, o que é, como é feita a aquisição, que leitores existem e que vantagens e desvantagens existem;
    - O reconhecimento de vasos sanguíneos, o que é, como é feita a aquisição, que leitores existem e que vantagens e desvantagens existem;
    - O reconhecimento de voz, o que é, como é feita a aquisição e que vantagens e desvantagens existem;
    - A dinâmica da digitação, o que é, como é feita a aquisição e que vantagens e desvantagens existem;
    - A assinatura manuscrita, O que é, como é feita a aquisição e que vantagens e desvantagens existem;
    - O formato do ouvido, o que é, como é feita a aquisição e que vantagens e desvantagens existem;
    - O ADN, o que é, como é feita a aquisição e que vantagens e desvantagens existem.

É feita também uma pequena comparação entre tecnologias recorrendo a uma comparação de alguns conceitos tais como universalidade, unicidade, permanência, desempenho, aceitação, segurança e preço e um gráfico de performance, com o objetivo de tentar encontrar a melhor técnica biométrica.

É ainda referida a multi-biometria, no que consiste, que tipos de multi-biometria existem, que características podem ser usadas e como podem ser fundidas, e por fim é feito um pequeno enquadramento legal com as leis e procedimentos que são precisos tomar para implementarmos sistemas biométricos respeitando a lei Portuguesa.

Aplicação

A segunda parte da tese será elaborada e documentada uma aplicação (Figura 1-1) com o objetivo de centralizar o controlo de vários equipamentos de identificação por RFID e impressão digital existentes na qual irá constar uma base de dados com algumas tabelas: uma tabela para guardar os dados de todos os equipamentos ligados ao sistema, uma tabela para guardar os dados das pessoas que vão utilizar o sistema, uma tabela de *templates* que relaciona o id da pessoa com o id do *template*, e uma tabla de registos que guarda as passagens de cada pessoa em cada equipamento. A aplicação terá a capacidade de:

- adicionar e remover equipamentos;
- receber e enviar dados para os equipamentos;
- importar e exportar pessoas;
- exportar registos para os quatro tipos de bases de dados mais conhecidos (Sqlite, MySql, Sql Server, e Oracle);
- pesquisar registos por nome, equipamento, e data.

São ainda referidas as tecnologias usadas, e com que fundamento foram usadas, que funções foram implementadas e como foram implementadas e porque foram implementadas Por fim são mostrados alguns testes para demostrar o correto funcionamento da aplicação.

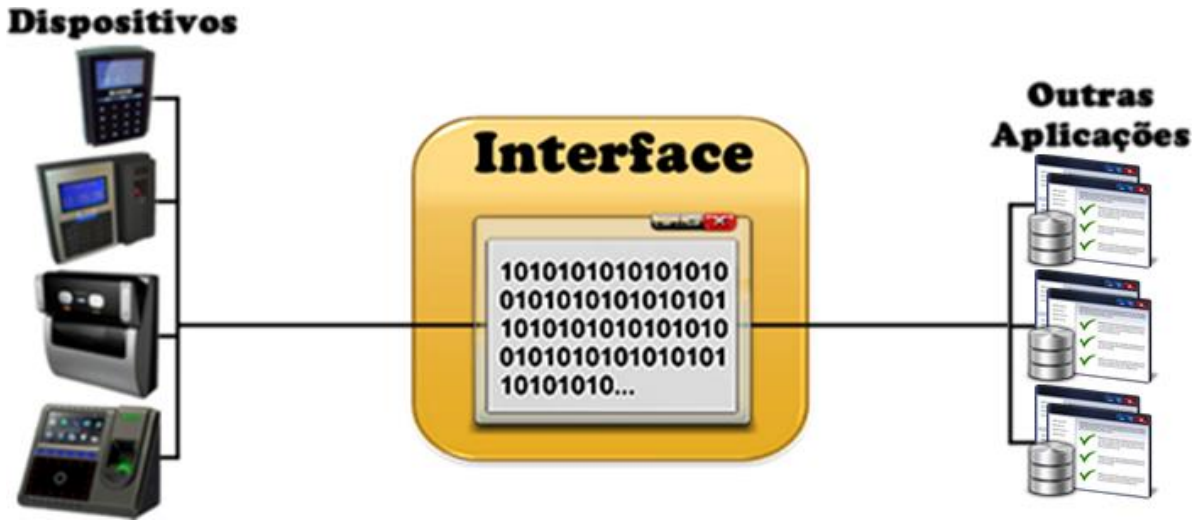


Figura 1-1: Estrutura geral da aplicação (interface a implementar).

Esta tese está organizada em cinco capítulos sendo o primeiro esta introdução.

O segundo capítulo descreve, o estado da arte das várias tecnologias, isto é, em que consistem, como funcionam, vantagens e desvantagens e a comparação entre as várias tecnologias biométricas tendo em conta vários fatores tais como:

- Universalidade;
- Unicidade;
- Permanência;
- Desempenho;
- Aceitação;
- Segurança;
- Preço.

É ainda feita uma comparação muito geral da precisão de algumas tecnologias biométricas através de um gráfico. A descrição da tecnologia multi-biométrica, o que é, para que serve e qual o seu impacto na melhoria da segurança das técnicas usadas em biometria simples, que técnicas biométricas podemos usar e de que forma podem ser fundidas, e por fim uma referência aos requisitos legais da legislação Portuguesa atual, para a implementação de equipamentos de identificação/autenticação biométrica.

O terceiro capítulo descreve como a aplicação foi desenvolvida:

- Qual foi a estrutura da aplicação e o porque da sua utilização;
- Que linguagem de programação e porque foi usada;
- Que arquitetura e o porquê da sua escolha;
- Que equipamentos e porque foi escolhido;
- Que bases de dados foram usadas e o porque da sua escolha
- Que funções foram implementadas e para que servem

O quarto capítulo descreve alguns testes e demonstração do funcionamento da aplicação.

O quinto capítulo descreve as conclusões que foram tiradas da comparação entre as várias tecnologias/equipamentos estudadas e descreve as conclusões que foram tiradas da realização da aplicação.

2. Estado da arte

Neste capítulo pretende-se apresentar uma visão geral do estado da arte no que diz respeito a algumas tecnologias de identificação biométricas e não biométricas que existem para a identificação de seres humanos. Pretende-se descrever o que são, para que servem, como funcionam, que requisitos têm de satisfazer, como avaliar o desempenho de sistemas biométricos, níveis de desempenho/fiabilidade (taxas FAR, FFR, EER), níveis de conforto, níveis de aceitação, segurança, ataques mais frequentes e medidas de proteção e algumas vantagens e desvantagens de cada uma delas. Será feita uma pequena comparação entre as várias tecnologias apresentadas e no final deste capítulo é feita uma breve referencia a muiti-biometria, no que consiste, para que serve, que características podem ser usadas e como são fundidas. Por fim surgirá uma breve referência a algumas leis que se têm de cumprir para a implementação destes sistemas.

Hoje em dia existem vários métodos de identificação e autenticação de pessoas que se dividem em 4 grandes características do ser humano (Quadro 1-1)

Quadro 2-1: Técnicas de identificação humana.

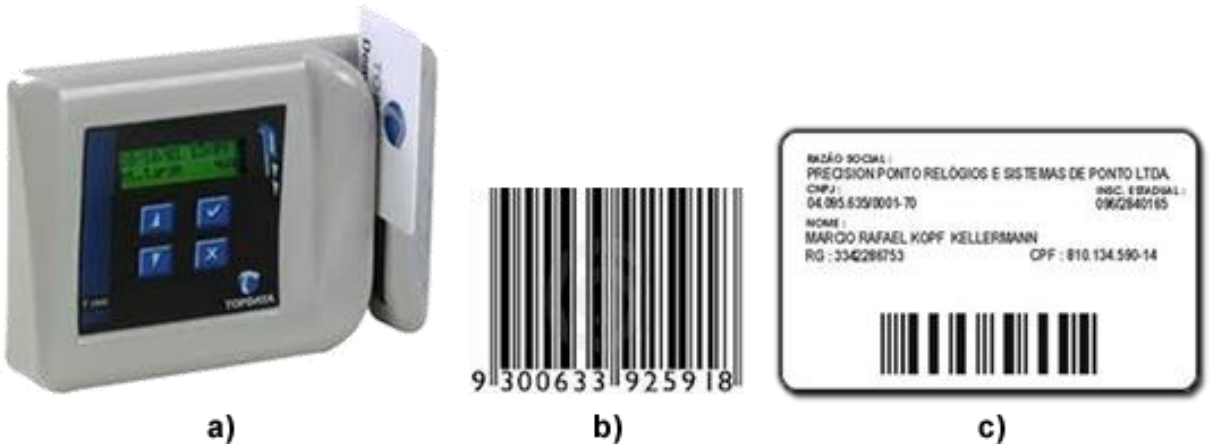
O que você…	Método/Técnica de identificação por:	O que pode acontecer
… sabe:	- Nome do utilizador - Código acesso/PIN	Pode ser esquecido Pode ser partilhado
… tem:	- Cartão - Credencias - Chaves	Pode ser perdido Pode ser partilhado Pode ser clonado
… sabe e têm:	- Cartão - Código acesso/PIN	Pode ser partilhado Pode ser roubado Pode ser perdido

… é:	- Impressão digital - Traços faciais - Vasos sanguíneos	Não pode ser perdido Não pode ser esquecido Não pode ser partilhado

Mas nem sempre foi assim, inicialmente começou-se com o tradicional login e password, isto é, "o que se sabe" mas estes podiam ser esquecidos ou partilhados por isso mais tarde apareceram os cartões, as credenciais e as chaves, isto é, "o que se tem". Mas estes também podiam ser perdidos, partilhados ou clonados por isso numa tentativa de tornar o sistema mais seguro fez-se uma junção dos dois métodos anteriores isto é "o que se sabe e o que se têm" com os cartões com PIN/Código de aceso, mas mesmo assim estes podiam ser partilhados, roubados ou perdidos. Por isso e com o rápido crescimento das necessidades de segurança e da evolução tecnológica nasceu a biometria, isto é, "o que se é" e neste grupo a apareceram os sistemas de reconhecimento de padrões biométricos, que funcionam com base nas características de diversas partes do corpo humano, por exemplo: as impressões digitais, a geometria da palma da mão ou da face, os padrões e timbre de voz, a retina ou íris, as veias do dedo ou da palma da mão, etc. O princípio fundamental destas novas técnicas é a de que cada indivíduo é único e possuí características físicas e de comportamento distintas.
Hoje em dia a biometria é usada na identificação criminal, controle de acesso, etc.

2.1 Código de barras

Código de barras é uma representação gráfica de dados que podem ser numéricos ou alfanuméricos dependendo do tipo de código de barras aplicado. As linhas paralelas e verticais escuras e os espaços entre elas têm diferentes larguras em função das várias técnicas de codificação de dados aplicada. O código mais conhecido é o que é usado nas embalagens de produtos lidos em caixas do comércio.
Um leitor ótico não é capaz de ler qualquer código de barras: ele deve estar devidamente configurado para cada tipo que lhe for apresentado, a fim de conseguir interpretar o código.



a) b) c)

Figura 2-1: a) Leitor; b) Código de barras; c) Cartão de identificação.

2.1.1Padrões

Existem vários padrões para o código de barras, no entanto o EAN/UPC é o mais usado.
O **EAN/UPC** é um padrão internacional criado para identificar produtos (a serem vendidos, movimentados e armazenados) de forma unívoca. Dentro deste padrão existe varias vertentes das quais as mais usadas são as seguintes:

- **EAN13:** é o código mais usado para identificação de produtos. É composto por 13 dígitos onde os primeiros 3 representam o país, os 4 seguintes representam o código da empresa registada na EAN, os próximos 5 representam o código do produto dentro da empresa e o 13º dígito é o dígito de validação;
- **EAN8:** é a versão reduzida do código EAN13 e serve para embalagens mais pequenas e é composto por 3 dígitos que correspondem ao país, 4 dígitos que corresponde ao código do produto e 1 dígito de validação. Estes códigos são controlados pela própria EAN e são alugados por períodos limitados de tempo uma vez que existem poucos códigos disponíveis por país.
- **UPC-A:** tem a mesma aplicação do EAN13, mas é usado para itens comercializados nos Estados Unidos e Canadá. Tem 1 dígito que representa a categoria do produto, 5 dígitos para a identificação do fabricante, 5 dígitos para a identificação do produto e 1 dígito de validação;
- **UPC-E:** é a versão UPC de 8 dígitos, obtida suprimindo 4 zeros do UPCE (entre número da empresa e número do item), 3 de 9: é um código simples de ser gerado, aceita letras e números e é livre. Costuma ser usado para codificações internas de empresas que necessitam de caracteres alfanuméricos, mas também é usado em aplicações comerciais.

2.1.2 Vantagens e desvantagens

Como vantagens do código de barras podemos destacar:

- Código exclusivo que usa um padrão internacional rígido,
- Aplicável no mundo inteiro,
- Sem repetição, o que possibilita a integração e a troca de informações entre as várias partes da cadeia produtiva,
- O código acompanha o produto.

Como desvantagens, podemos apresentar os seguintes itens:

- Burocracia. Cada empresa deve-se registar no órgão responsável (UCC nos estado unidos e canada ou no EAN par o resto do mundo), para receber um ID que a identificará exclusivamente dentro do código de barras.

2.2 RFID (*Radio Frequency Identification*)

O RFID (Radio Frequency Indentification), também chamado de etiqueta inteligente, é uma tecnologia de identificação automática que funciona através de sinais de rádio, recuperando e armazenando dados remotamente em etiquetas também chamadas de *tags*. Esta tecnologia surgiu na década 1980 mas foi só no ano de 1999, que o Instituto de tecnologia de Massachusetts (MIT) em conjunto com outros centros de investigação começaram a estudar um novo tipo de arquitetura em que as tecnologias fossem baseadas em radiofrequência para servir de referência para o desenvolvimento de novas aplicações de rastreio e localização de produtos. Com isso, eles desenvolveram o Código Eletrônico de Produtos – EPC (*Electronic Product Code*) que mais tarde foi chamado de RFID [26].

Para que um sistema RFID funcione são necessários alguns componentes (Figura 2-2):

- **Tag RFID (Transponder)** – é um dispositivo de identificação constituído por um chip e uma antena que é aplicado num "objeto" e usa um sinal de rádio frequência (RF) para comunicar;
- **Leitor RFID (transceiver)** – é um dispositivo utilizado para comunicar com a *tag*, enviando ou recebendo dados da e para a *tag* e estabelecer comunicações com o middleware;
- ***Middleware*** – é responsável pelo interface entre leitores de RFID e o sistema de gestão da empresa. É ele que incorpora o software que permite o registo das comunicações entre *tag* e leitor, solicita as informações necessárias à base de dados e fornece essas informações aos leitores para que eles possam comunicar com as *tags*, recebe e envia informações do e para o leitor mantendo o sincronismo entre todos os intervenientes no processo [26].

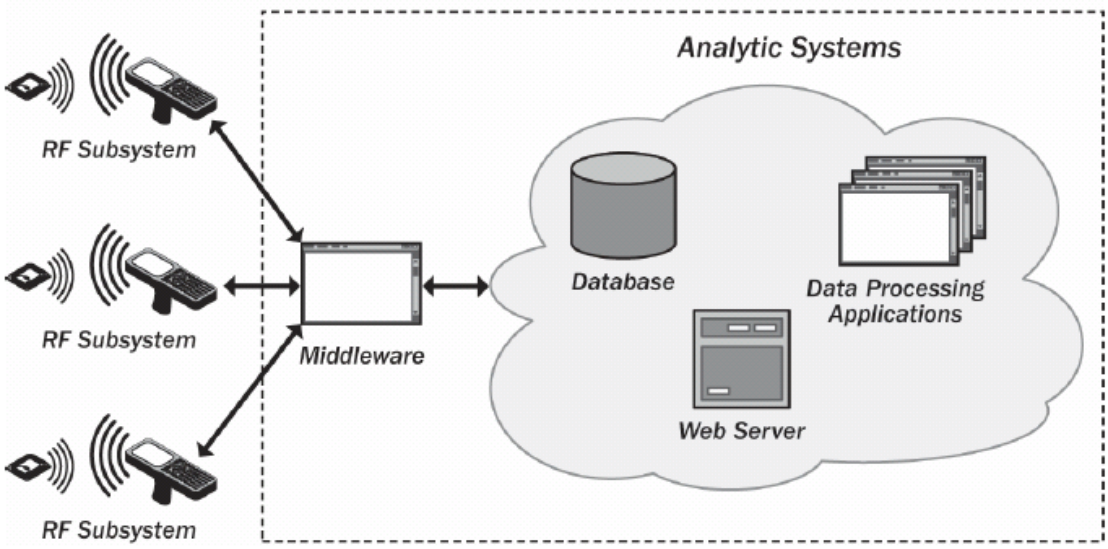


Figura 2-2: Componentes de um sistema RFID.
[Jorge Rei, 2010]

2.2.1 Leitor

Um leitor (exemplo Figura 2-3) é basicamente um aparelho que permite comunicar, interpretar e ler a informação contida nas *tags* presentes no raio de alcance da antena, através de ondas de rádio.
Alcance esse que pode ir desde 1 polegada até alguns metros dependendo do tipo de *tag* e do tipo de frequência usados.
Existem 3 tipos de leitores:

- **Fixos** – são leitores que estão montados em estruturas fixas normalmente fixados em paredes;
- **Móveis** – são leitores montados em equipamentos móveis normalmente usados no comercio de mercadorias tas como empilhadores e porta-paletes;
- **Handheld** – são leitores portais utilizados pelos operadores que fazem a leituras de *tags*.

Figura 2-3: Leitor RFID Nuxin II.
(fonte: www.innux.com)

2.2.2 *Middleware*

O *middleware* é um elemento fundamental e qualquer implementação de sistemas de RFID e deve possuir algumas características das quais destacamos as seguintes [26]:

- **Filtragem e agregação de dados** – O middleware deve recolher todos os dados vindos dos sensores e enviar, para as aplicações apenas os dados que estas precisam de acordo com as suas especificidades;
- **Distribuição de dados** – O middleware deve distribuir os dados capturados pelos leitores, sensores e outros intervenientes no processo pelas várias aplicações interessadas no formato correto e no tempo útil;
- **Leitura e gravação** – O middleware deve ter a capacidade de ler e gravar informações na memória adicional das *tags*;
- **Gestão dos leitores e impressoras/codificadoras** – O middleware deve ter a capacidade de gerir os vários equipamentos presentes no sistema independentemente do seu tipo ou fabricante;
- **Segurança –** As *tags* são uma fonte de informação pelo que essa porta de entrada deve ser devidamente protegida e a informação por elas fornecida devidamente filtrada para evitar possíveis ataques ao sistema;
- **Performance e Escalabilidade** – O middleware deve ter em conta as necessidades atuais da organização, as necessidades previsíveis a curto e médio prazo e as evoluções esperadas para a tecnologia.

2.2.3 Tags

As *tags* são pequenos elementos cujo objetivo é associar os dados lógicos a objetos físicos. Cada *tag* possui um mecanismo de memória para armazenar os dados e um mecanismo para envia-los, apesar de nem todas as *tags* possuírem chips ou baterias, todas possuem uma antena

para a transmissão de dados. No entanto existem muitas outras características que não são tão frequentes tais como a capacidade de ser desativada mediante um comando, a capacidade de ser regravada, possuir protocolos anti-colisão e encriptação entre outros…
As *tags* podem ser encontradas sob diferentes formatos das quais se destacam os *tags* passivas, as *tags* ativas, e as *tags* semi-passivas:

- **As *tags* passivas** são *tags* sem alimentação própria (Figura 2-4) para comunicarem por isso só são ativadas quando estão no raio de alcance do leitor pela(s) potência(s) emitida(s) pela(s) antena(s) do leitor, que é aproveitada pela *tag* para alimentar o circuito interno que retransmite a informação contida na *tag*. Logo para que as *tags* passivas entrem em funcionamento é necessário não só estarem ao alcance do leitor mas também que o leitor lhes dê potência suficiente para que estas tenham a capacidade de estabelecer comunicação com o leitor [26].

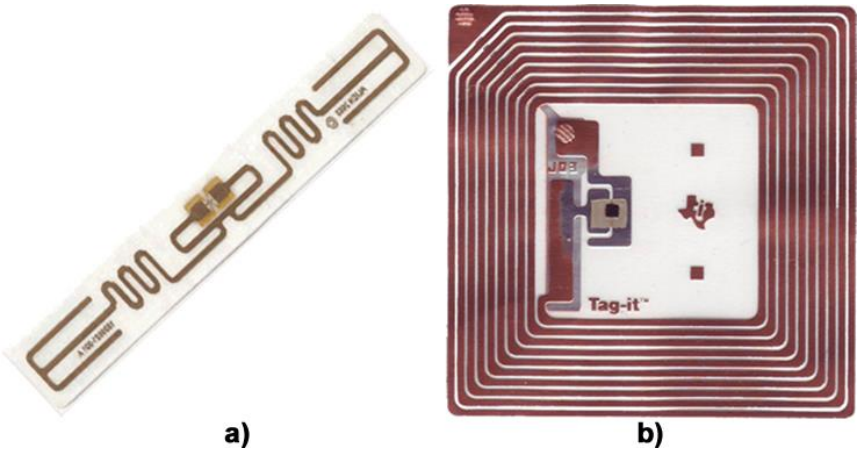


Figura 2-4: a) *Tag* UHF Passiva; b) Circuito impresso de uma *tag* passiva.

- **As *tags* ativas** são *tags* com alimentação própria e um circuito de rádio que lhes permite transmitir o próprio sinal para o leitor, ao invés de dependerem do leitor para serem alimentadas (Figura 2-5). A grande vantagem da utilização destas *tags* é principalmente o alcance que estas *tags* oferecem - atualmente na ordem das dezenas de metros, o facto de possuírem bateria permite que estejam continuamente ativas logo não precisam de muita potência para comunicar com o leitor aumentando assim ao alcance [26].

Figura 2-5: *Tag* ativa.

A figura seguinte (Figura 2-6) demostra a principal diferença entre *tags* ativas e passivas.

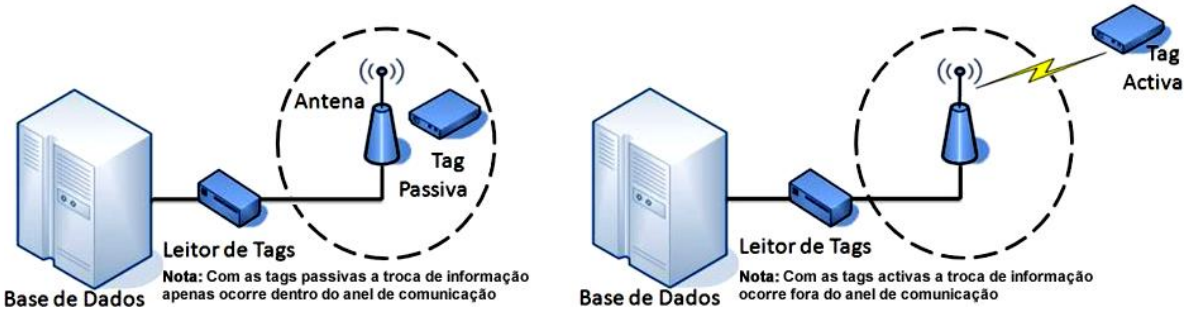


Figura 2-6: Processo da *tag* Passiva e ativa.

- **Tags semi-passivas:** são *tags* passivas com alimentação interna e podem possuir sensores. A Fonte de alimentação permite alimentar circuitos mais complexos e com maiores funcionalidades e também alimentar outros sensores. Este modo de funcionamento permite, também, aumentar o raio de ação já que toda a energia absorvida é destinada a alimentar apenas a comunicação com o leitor, sendo a parte eletrónica alimentada pela bateria. O tempo de vida da bateria é superior a 5 anos.

2.2.4 Vantagens e desvantagens de utilização de RFID

Como todas as tecnologias existem vantagens mas também existem desvantagens do uso da tecnologia RFID das quais se destacam as seguintes:

Como vantagens da Tecnologia RFID podemos destacar:

- A deteção e leitura não necessitam da proximidade ou contacto visual entre leitor e *tag* para que o reconhecimento e leitura dos dados sejam efetuados;
- O tempo de resposta é inferior a 100ms, o que torna esta tecnologia uma boa solução para capturar as informações com a *tag* em movimento.
- Capacidade de armazenamento, leitura e envio dos dados para etiquetas ativa;
- A durabilidade das etiquetas possibilita a reutilização das mesmas [26];
- Possibilita a contagens instantânea de *stock*, facilitando assim os sistemas empresariais de inventário;
- Localização dos itens ainda em processos de busca uma vez que assim que um destes itens entra no raio de alcance do leitor este revela a sua localização;
- Melhoria no reabastecimento de itens em falta e eliminação de itens com validade espirada;
- Prevenção de roubos e falsificação de mercadorias avisando os comerciantes assim que estas passam pelos leitores colocados nas portas das lojas [26];
- Facilita a contagem e coleta de dados de animais ainda no campo por não necessitarem de proximidade na leitura dos dados;

Como desvantagens, podemos apresentar os seguintes itens:

- O custo elevado da tecnologia RFID em relação aos sistemas de código de barras e o preço final dos produtos, pois a tecnologia não se limita apenas ao *microchip* anexado ao produto. Por trás da estrutura estão antenas, leitoras, ferramentas de filtragem das informações e sistemas de comunicação;
- O uso em materiais metálicos causar interferências e afetar o alcance de transmissão das antenas;
- A padronização das frequências utilizadas para que os produtos possam ser lidos por toda a indústria, de maneira uniforme;
- Etiquetas RFID sem nenhum mecanismo de segurança para proteger os seus dados podem sofrer intercetação e extravio de suas informações, Mesmo as *tags* passivas cujo alcance é reduzido podem ser intercetadas embora não seja fácil, mas quando pensamos em etiquetas ativas, o problema torna-se bem mais crítico;
- A invasão da privacidade dos consumidores por causa da monitoração das etiquetas coladas nos produtos uma vez que assim que uma *tag* passa perto de um leitor este denuncia a sua localização;
- A natureza desta tecnologia possui algumas vulnerabilidades que se não forem devidamente protegidas podem constituir uma ameaça a segurança tais como:
    - ***Eavesdropping*** – Consistem em monitorizar a comunicação entre *tag* e leitor;
    - Análise de trafego – Análise do tráfego entre o leitor e a *tag;*
    - ***Spoofing*** – Uso de uma *tag* clonada para comunicar com um leitor legítimo;
    - ***Relay attack ou man in the midle attack*** – Neste tipo de ataque o atacante cria uma ligação ente leitor e *tag* legítimos, passando a comunicação a efetuar-se por esse novo canal;
    - **Clonagem da *tag*** – Copia integral de uma *tag*;
    - ***Replay attack*** – Uso de informação capturada numa comunicação anterior entre um leitor e um *tag* legítimos;
    - **Alteração de conteúdo** – Consiste em alterar ou eliminar o conteúdo de *tags;*
    - **Destruição da *tag* –** Consiste em destruir fisicamente a *tag*;
    - ***Denial of service attack, malware´s*** **em geral** – Consiste no uso de equipamentos que bloqueiam as frequências usadas na comunicação entre *tags* e leitor;
    - ***Buffer overflow*** – Consiste em encher a memória com ataques sucessivos fazendo com que o sistema se comporte de maneira imprevisível;
    - ***Code insertion*** – Introduzir de *script* com código malicioso em locais onde não era suposto ser permitido o uso de código;
    - ***Sql injection*** - é uma técnica parecida com o *Code insertion* mas esta foca-se no código sql das bases de dados
    - Outras vulnerabilidades...

2.3 Biometria

Decompondo a palavra **biometria** obtemos as palavras gregas *bio* e *metria*. Que significam respetivamente "vida" e "medida", pode-se então definir biometria como o estudo estatístico das características físicas ou comportamentais dos seres vivos [34].
O princípio fundamental desta tecnologia é que cada individuo é único e possui características físicas e comportamentais únicas, logo estes sistemas fazem medições quantitativas das características fisiológicas e comportamentais dos indivíduos para determinar as suas identidades [28]. Teoricamente podem ser medidas quaisquer características humanas (física ou comportamental) desde que satisfaçam os seguintes requisitos:

- **Universalidade** – Isto é todas as pessoas devem possuir a característica a medir pelo sistema biométrico [30];
- **Singularidade** – É a medida da característica biométrica utilizada não deve ser igual em pessoas diferentes, ou a probabilidade disso acontecer seja muito pequena;
- **Permanência** – Isto é cada característica biométrica não deve variar com o tempo;
- **Mensurabilidade** – Isto é a característica biométrica tem de ser possível de medir de forma quantitativa, tendo em conta um modelo da característica biométrica selecionada [30].
- **Precisão e Desempenho –** Refere-se à precisão com que se realiza a identificação, tendo em conta aos recursos necessários para atingir uma medição de precisão aceitável e a fatores ambientais que afetam a precisão na identificação. Normalmente, uma maior precisão dos resultados implica em um menor desempenho do sistema;
- **Aceitabilidade** – Indica o nível de aceitação do sistema de reconhecimento biométrico por parte dos seus utilizadores [35];
- **Proteção** – Refere-se à facilidade/dificuldade de enganar o sistema com técnicas fraudulentas.

2.3.1 Funcionamento

Embora os equipamentos sejam todos diferentes e cada um recolha uma característica diferente, o modo de funcionamento geral é o mesmo para todos, isto é, para que o sistema identifique uma pessoa essa pessoa tem de fazer o registo prévio das suas características para que estas possam ser comparadas posteriormente e assim o sistema reconhecer a pessoa em causa [11]. Basicamente existem duas fases: a fase de registo e a fase de autenticação:

- **Fase de registo:** Nesta fase são capturadas as características do utilizador, das quais são extraídas as informações relevantes para a autenticação do utilizador através de funções matemáticas gerando um *template* biométrico que será gravado na base de dados juntamente com um id ou *username* [25] (Figura 2-7)

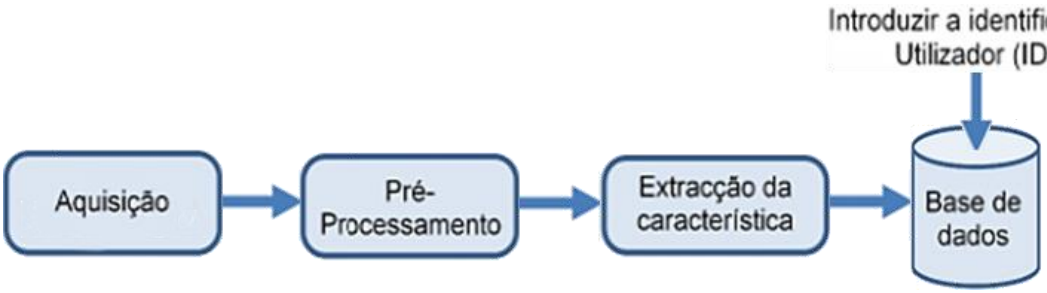


Figura 2-7: Fase de registo
[Gonçalo Lourenço, 2009].

- **Fase de autenticação:** Nesta fase existem dois modos de autenticação diferentes: a identificação e a verificação.
    - Na **identificação**, o utilizador fornece uma ou mais das suas características das quais é extraído um *template* que é comparado com todos os *templates* (1:N) guardados no sistema, cabendo ao sistema identificar ou não o utilizador (Figura 2-8). Basicamente o sistema "diz" quem é o utilizador [25].

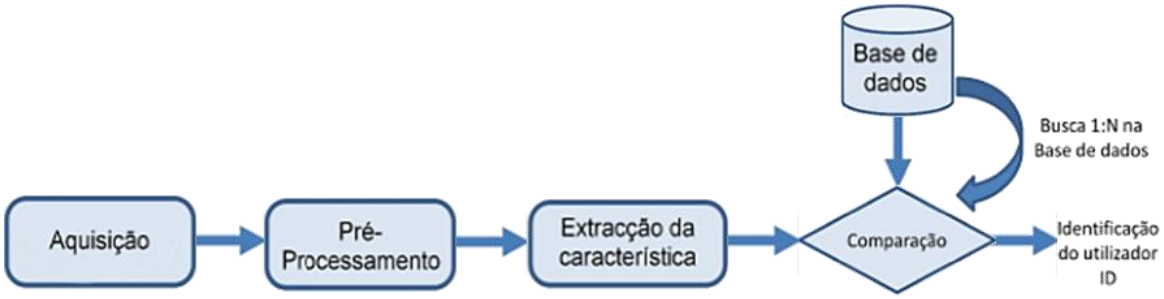


Figura 2-8: Fase de autenticação
[Gonçalo Lourenço, 2009].

    - Na **verificação** o utilizador fornece uma ou mais de suas características das quais é extraído o *template* juntamente com o seu id ou *username*, depois o sistema procura o id ou *username* e comparar a *teamplate* extraída com a *template* guardada e autenticar ou não o utilizador (Figura 2-9), basicamente o sistema verifica se o utilizador é quem alega ser [25].

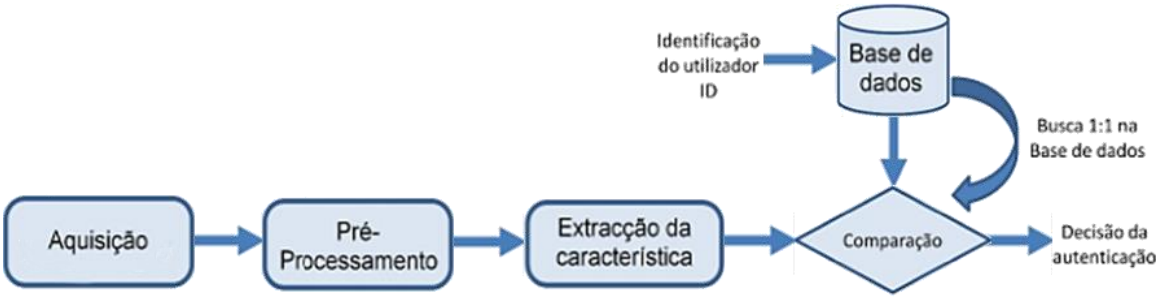


Figura 2-9: Verificação
[Gonçalo Lourenço 2009].

2.3.2 Avaliação do desempenho de um sistema biométrico

A escolha do(s) método(s) a utilizar nem sempre é fácil e pode implicar falhas de segurança ou gastos desnecessários com equipamentos inadequados. Esta escolha depende da análise de vários fatores tendo em conta vários parâmetros dos quais se destacam os seguintes:

- **Nível de desempenho/fiabilidade** – O desempenho do sistema é medido através das taxas de falsa aceitação e falsa rejeição [22];
- **Nível de conforto** – Este parâmetro é um pouco subjetivo e está ligado à facilidade com que os utilizadores usam o equipamento [22];
- **Nível de aceitação** – Este parâmetro é também um pouco subjetivo, mas de um modo geral, o sistema é tanto melhor aceite pelos utilizadores quanto menos intrusivo for.
- **Custo de implementação** – Este parâmetro é um dos mais importantes a ter em conta nos sistema e não se limita apenas a compra do equipamento temos de ter em conta toda a plataforma que está subjacente ao *hardware* ou *software* e sua manutenção.

Os sistemas biométricos não são infalíveis, isto é, podem ocorrer erros que afetem o seu desempenho, levando o sistema a tomar decisões que podem não ser as mais corretas. Estes erros, na biometria, são quantificados em dois tipos de erro: o Índice de Falsas Aceitações – FAR (*False Acceptance Rate*) e o Índice Falsas Rejeições FRR (*False Rejection Rate*). Infelizmente estas variáveis são mutuamente dependentes, logo não é possível minimizar ambas ao mesmo tempo. Assim, procura-se o ponto de equilíbrio ao qual se chama de Índice de Intersecção de Erros – EER (*Equal Error Rate*) logo quanto mais baixo for o EER mais preciso será o sistema biométrico [3].

- **FRR – Índice de Falsas Rejeições:** Consiste na percentagem de pessoas validas e registadas que o sistema rejeita ou não identifica. A falsa rejeição é por vezes designada como um erro de Tipo I não tendo muita importância na maior parte das situações, contudo, em algumas aplicações biométricas, pode ser o erro mais importante, uma vez este tipo de erro causa atrasos desnecessários no movimento de pessoais. Existem vários motivos para que este problema ocorra mas os principais são uma recolha de características insuficientes na fase de registo, má utilização dos equipamentos e fatores ambientais [19].

$$\text{FRR} = \frac{\text{Acessos autorizados Rejeitadas}}{\text{Nº Total de processos}} \qquad (2\text{-}1)$$

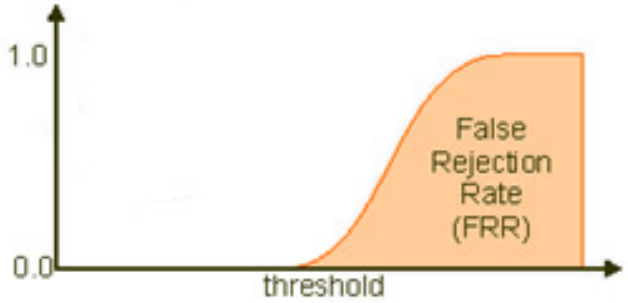


Figura 2-10: Índice de falsa rejeição (FRR)
[Bruno Lopes, 2009].

- **FAR – Índice de Falsas Aceitações:** Consiste na percentagem de pessoas não registadas ou impostores que são aceites como autenticadas e registadas por um sistema de reconhecimento biométrico (Figura 2-11). A falsa aceitação é por vezes designada como um erro de Tipo II. Normalmente é considerado o erro mais importante para sistemas biométrico de controlo de acesso [20].

$$\text{FAR} = \frac{\text{Acessos não autorizados Aceites}}{\text{Nº Total de processos}} \qquad (2\text{-}2)$$

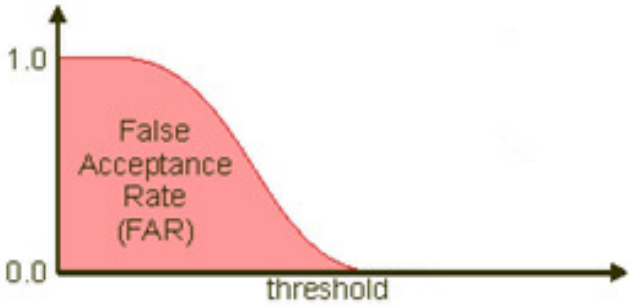


Figura 2-11: Índice de Falsos Aceitações (FAR)
[Bruno Lopes, 2009].

- **EER – Índice de Intersecção de Erros ou CER (*Crossover Error Rate*):** É o ponto, onde as taxas de FAR e FRR são iguais. No geral a sensibilidade de todos os sistemas pode ser adaptada aumentando ou diminuindo uma das taxas de FAR ou FRR isto é ao diminuir uma a outra vai aumentar ou vise versa (Figura 2-12). Então podemos afirmar que o índice de intersecção de erro (EER) fornece uma medida única, justa e imparcial de modo a podermos comparar o desempenho dos vários sistemas [20]. Logo um sistema biométrico com um EER de 2% será mais exato e fiável que um sistema com um EER de 5%.

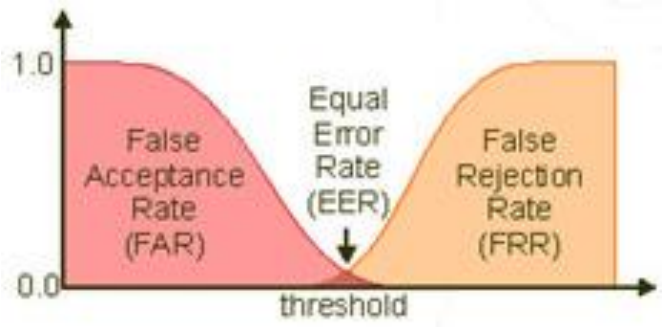


Figura 2-12: Índice de Intersecção de Erros (ERR)
[Bruno Lopes, 2009].

Dado que as taxas FAR e FRR dependem uma da outra, pode-se obter uma representação gráfica de uma taxa em função da outra onde a curva resultante é designada por *Receiver Operating Characteristic* (ROC). A curva ROC (Figura 2-13) também é uma boa representação da precisão de um sistema biométrico pelo que pode ser usada a comparação entre sistemas biométricos distintos uma vez que nem sempre temos curvas bem definidas de FAR e FRR logo é mais difícil determinar o ponto EER [20].

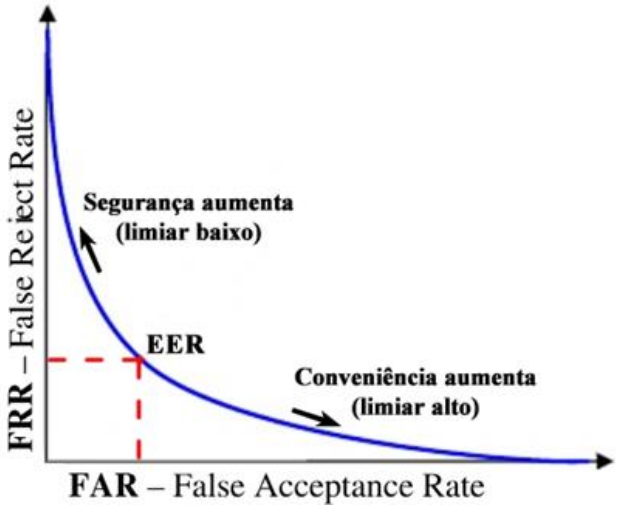


Figura 2-13: Taxa de erro FRR em função da taxa de erro FAR (ROC)
[Bruno Lopes, 2009].

2.3.3 Segurança em sistemas biométricos

Num sistema biométrico, o problema da segurança dos dados biométricos que são transmitidos entre as várias partes do sistema e também armazenados em bases de dados é garantir que, em nenhuma circunstância, estes dados possam ser indevidamente acedidos por pessoas não autorizadas causando graves problemas aos utilizadores do sistema, reduzindo a sua privacidade, e para evitar essa situação um sistema biométrico deve respeitar as seguintes propriedades:

- **Confidencialidade ou privacidade** – O sistema deve garantir que as informações só são reveladas a pessoas devidamente autorizadas [36].

- **Integridade** – O sistema deve assegurar que as informações não serão alteradas por pessoas não autorizadas;
- **Disponibilidade** – O sistema deve assegurar que as informações estarão sempre disponíveis a quem for devidamente autorizado;
- **Autenticidade** – O sistema deve assegurar que alguém é realmente quem diz ser;
- **Não-repúdio** – O sistema deve assegurar que ninguém possa negar a autoria de alguma informação que efetivamente tenha gerado.

A segurança de sistemas biométricos pode ainda ser avaliada segundo dois aspetos importantes:

- **Desempenho do sistema** – O desempenho do sistema é representado segundo as taxas de erro FAR e FRR conforme o que já foi descrito anteriormente;
- **Robustez do sistema** – A robustez de um sistema biométrico define o quanto um sistema é ou não vulnerável a possíveis ataques, que possam resultar do tipo de arquitetura usada para cada um dos módulos do sistema e sua implementação e também de como é efetuada a comunicação entre eles [44].

Na atualidade não existem sistemas 100% seguros e os sistemas biométricos não são exceção. Nos últimos anos, com os avanços da tecnologia e estudos científicos mais profundos conseguiu-se descobri mais vulnerabilidades que atualmente se tem tentado resolver [44].

As causas de um possível fracasso de um sistema podem ser organizadas em duas principais categorias:

- **Falha intrínseca** – A falha intrínseca acontece devido às limitações das tecnologias de aquisição das características, como por exemplo os sensores, de extração das características e a também das tecnologias de decisão utilizadas pelo comparador;
- **Falha devido a ataques** – A falha acontece quando impostores tentam corromper o sistema para ganhos pessoais [36].
    - **Ataque ao sistema administrativo** – A falha ocorre devido às vulnerabilidades existentes na administração do sistema biométrico; logo o administrador deve ser capaz de verificar se as informações provenientes das características biométricas são genuínas ou se foram manipuladas ou alteradas por impostores e também deve ser capaz de descobrir se algum parâmetro do sistema foi ou não alterado.
    - **Ataque a infraestruturas não seguras** – A falha ocorre devido a vulnerabilidade na infraestrutura (*hardware*, software e canais de transmissão entre as várias partes do sistema) e podem ocorrer em oito locais diferentes da arquitetura:
        - **Apresentação de uma característica falsa** – Ocorre quando uma característica falsa é apresentada no dispositivo de aquisição do sistema;
        - **Ataque de repetição** – Ocorre quando uma característica biométrica é intercetada e reintroduzida no sistema [49];

- **Substituição do módulo de extração de características** – Ocorre quando o módulo de extração de características é substituído por um programa "cavalo de troia" que produz um pré-determinado conjunto de características [49];
- **Substituição dos *templates*** – Ocorre quando os *templates* de um utilizador legítimo são substituídos por *templates* de um impostor;
- **Substituição do módulo comparador** – Ocorre quando o comparador é substituído por um programa "cavalo de troia" que altera o limiar de decisão do sistema, tornando-o menos seguro;
- **Modificação dos *templates* guardados na base de dados** – Ocorre quando os *templates* guardados na base de dados são modificados, eliminados ou introdução de novos *templates* de impostores na base de dados;
- **Interceções nos canais de comunicação entre os diferentes módulos do sistema** – Ocorre quando os dados enviados entre os diferentes módulos do sistema são intercetados e modificados;
- **Substituição da decisão do sistema sobre a autenticação** – Ocorre quando a decisão sobre a autenticação de um utilizador é alterada.

o **Ataque a características biométricas** – A falha ocorre quando um impostor consegue adquirir as características biométricas de um utilizador legítimo do sistema e as use para criar artefactos físicos.

2.3.4 Medidas para proteção dos sistemas biométricos

Face às vulnerabilidades existentes num sistema biométrico e aos possíveis ataques, foi necessário criar medidas que prevenissem esses mesmos ataques garantindo assim uma melhor segurança dos sistemas biométricos, das quais se destacam as seguintes:

- **Supervisão na aquisição das características biométricas** – supervisionar a aquisição das características reduzindo assim a possibilidade de uso de artefactos por parte de intrusos;
- **Deteção de repetição** – A aquisição da característica biométrica não é exata logo não é possível obter por exemplo duas aquisições da mesma impressão digital, exatamente iguais logo o sistema pode desprezar *templates* que sejam exatamente iguais às anteriores, inclusivamente o sistema pode solicitar a múltipla aquisição da mesma característica para verificar falsificações;
- **Resposta sumária** – O sistema responde sempre da mesma maneira quando a resposta é não o sistema responde "Não" sem explicar o porquê;
- **Desafio e resposta** – Consiste no envio de desafios ao utilizador que este deve responder corretamente para obter autorização de continuar com a autenticação.
- **Deteção de vivacidade (*liveness detection*)** – Consiste em assegurar que somente características reais, pertencentes a pessoas vivas, são aceites como válidas;

- **Multibiometria** – Consiste em usar mais do que uma característica para a autenticação
- **Modelos de proteção dos *templates*** – Estes modelos têm o objetivo de proteger os *templates* extraídos das características biométricas que são inseridos na base de dados garantido a privacidade dos utilizadores.

2.3.5 Vantagens e desvantagens da utilização da biometria

Algumas das **vantagens** de utilizar características biométricas no reconhecimento de pessoas em vez das tradicionais senhas ou cartões de identificação são as seguintes:

- As características biométricas, não podem ser esquecidas, perdidas ou simplesmente fornecidas a terceiros;
- A probabilidade de existirem duas pessoas com a mesma característica biométrica, desde que cuidadosamente escolhida, é bastante reduzida ou praticamente nula;
- As características biométricas são muito difíceis de copiar.

Mas como em todos os sistemas, não existem só vantagens também existem **desvantagens** das quais destaco as seguintes:

- Em caso de doença ou acidente algumas características biométricas podem sofrer alterações tornando a autenticação mais difícil;
- Com a idade, as características biométricas das pessoas podem alterar-se, diminuindo as taxas de sucesso na autenticação das pessoas, para evitar esta situação pode ser necessário atualizar a informação biométrica registada nas bases de dados, como acontece hoje em dia com o Bilhete de Identidade ou Passaporte;
- Caso uma característica biométrica seja roubada ou copiada não é possível substitui-la como acontece com as senhas, ou seja, não é possível substituir um olho, uma face ou outra característica física.

2.4 Impressão digital

A formação das impressões digitais das pessoas começa no sétimo mês de gestação e crescem num microambiente que é ligeiramente diferente de mão para mão e de dedo para dedo e os detalhes das impressões digitais são determinados por este microambiente, o que faz com que estes detalhes sejam únicos [54]. Nem mesmo gémeos idênticos possuem o mesmo padrão, embora partilhem cerca de 95% das características das impressões digitais [12];

A **aquisição da impressão digital** obtém-se a partir de uma imagem a preto e branco ou a cores das linhas dos dedos (Figura 2-14) que pode ser previamente estampada em papel com tinta, para posteriormente ser digitalizada por um *scanner*, mas também pode ser obtida por meio de dispositivos eletrónicos (leitores de impressão digital). No entanto o princípio básico é o mesmo que é a deteção das rugosidades dos dedos [25].

Figura 2-14: Impressão digital
[Gonçalo Lourenço, 2009].

2.4.1 Leitores

O leitor é um dispositivo eletrónico cujo objetivo é detetar os sulcos da pele. Existem vários tipos de leitores dependendo do seu sensor dos quais destaco os seguintes:

- **Sensores óticos:** são sensores baseados em fenómenos óticos, isto é, a impressão digital é lida através da reflexão da luz pela pele e é a partir da luz que é refletida de volta que a imagem é formada como se fosse uma câmara fotográfica mas a preto e branco [32];
- **Sensores de ultrassons:** são sensores baseados na reflexão de ultrassons, isto é, o sensor emite um ultrassom que será refletido pela pele (eco) e é esse eco que é usado para calcular a imagem da impressão digital [37];
- **Sensores piezoelétricos:** são sensores baseados no efeito piezoelétrico, isto é, o sensor contem dezenas de milhares de sensores que produzem um sinal elétrico quando são sujeito a uma pressão e como dependem da força exercida sobre a superfície, logo os sulcos e os vales vão exercer pressões deferentes [27];
- **Sensores Temo elétricos:** são sensores baseados no diferencial de temperatura, isto é, o sensor é composto por um material piro-elétrico que gera corrente ao detetar uma deferencial de temperatura, logo, como os sulcos estão em contacto com o sensor, o seu deferencial de temperatura será diferente do deferencial de temperatura dos vales [55];
- **Sensores condensadores:** são sensores compostos por dezenas de milhares de condensadores embutidos num chip, que em contacto com o dedo, são criadas pequenas diferenças de potencial que variam com a distância da pele aos condensadores [31].

Por serem menos compactos que os restantes, os sensores baseados em fenómenos óticos atualmente não são tão populares. Contudo são os sensores utilizados há mais tempo.

2.4.2 Vantagens e desvantagens

As principais **vantagens** da desta tecnologia são:

- O nível de precisão pode ser bastante bom dependendo do sensor usado [1];
- Existe uma longa tradição no uso da impressão digital como identificador imutável;
- Existem grandes bases de dados de impressões digitais [53];
- A impressão digital pode ser colhida facilmente e a baixo custo.

Em relação às **desvantagens**, as principais são as seguintes:

- Em algumas culturas as impressões digitais não são bem aceites por estarem ligadas a criminosos, pessoas iletradas ou por questões de higiene [1];
- A qualidade das impressões digitais varia muito dentro de uma população;
- Os sensores mais baratos podem ser comprovadamente defraudados [56].

No quadro seguinte são mostrados três exemplos dos equipamentos mais recentes.

Quadro 2-2: Leitores de impressão digital.

		
Modelo: TC200 **Fabricante:** Bio-Office	**Modelo:** 5000A **Fabricante:** Granding	**Modelo:** NuxBio III **Fabricante:** Innux

O primeiro equipamento possui sensor ótico, ecrã monocromático, teclado numérico com teclas para sinalizar entrada e saída, possibilidade de funcionamento em 3 modos (Fingerprint, ID+Password, ID + Fingerprint), capacidade para 1500 utilizadores e comunicação em TCP/IP, RS485 e USB. O segundo equipamento possui sensor ótico, ecrã LCD monocromático de 4 linhas, teclado numérico com funções campainha, entrada e saída, speaker, indicador LED, capacidade para 4000 utilizadores, comunicação em TCP/IP, RS232, RS485, e USB e possibilidade de ligação a trinco de portas automáticas. O terceiro equipamento possui sensor ótico, ecrã monocromático, leitor de tags RFID, capacidade para 4000 utilizadores, possibilidade de funcionamento em 5 modos (RFID, Fingerprint, PIN+RFID, PIN + Fingerprint, Fingerprint + RFID) e comunicação TCP/IP, RS232, RS485 e possibilidade de ligação a alarmes e trincos de portas automáticas.

2.5 Geometria da mão

Foi em 1960 que esta tecnologia apareceu pela primeira vez com o registo da primeira patente mas foi só nas décadas de 70 e 80 que esta tecnologia começou a ter mais importância. Atualmente já existem leitores modernos de mão que executam funções de controlo de acesso, registo de ponto, etc.
O objetivo desta tecnologia é a leitura das características físicas da mão de uma pessoa, baseando-se no princípio básico de que virtualmente não existem duas pessoas com mãos idênticas e que o formato da mão não sofre mudanças significativas após certa idade.
Esse é um dos métodos mais antigos que existe, no entanto não é dos mais precisos. Em contrapartida, é um dos meios de identificação mais rápidos, motivo pelo qual é comum em lugares com muito movimento.

2.5.1 Processo de aquisição

No processo de aquisição o utilizador coloca a mão numa plataforma especial que contém pinos para posicionar a mão de forma correta, depois o dispositivo leitor usa uma câmara para capturar imagens a preto e branco da silhueta da mão [21]. Em combinação com um refletor e espelhos laterais, duas imagens distintas são capturadas, uma vista de cima e outra vista de lado (Figura 2-15). O sistema converte as imagens noutras em tons de cinzento caso sejam coloridas e analisa as imagens obtendo 96 características da mão do utilizador (comprimento, largura, grossura, curvatura da mão, curvatura dos dedos, espaço entre dedos, etc…) e depois converte-as num *template* de apenas 9 bytes [48].

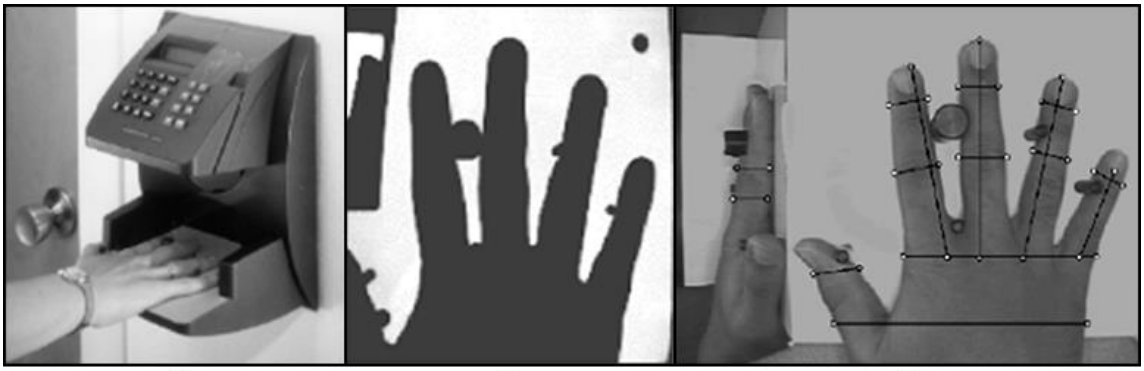


Figura 2-15: a) Leitor; b) Imagem real obtida do dispositivo; c) Medidas tipicas.
(Adaptado de [14])

2.5.2 Vantagens e desvantagens

As **principais vantagens** da tecnologia de autenticação biométrica baseada na geometria da mão são as seguintes:

- Recolha das características, fácil e não intrusiva;
- Computação bastante simples e *templates* pequenos (9 a 35 bytes), o que trona facial a construção de sistemas dedicados isolados e reduz as necessidades de armazenamento;

- Adequada para ser usada em conjunto com outras características biométricas, tais como a impressão digital [33];
- Não é relacionada com registos policiais e ou criminal como acontece com as impressões digitais.

Em relação às **desvantagens**, as principais são as seguintes:

- Como esta tecnologia requer o contacto da mão com uma superfície para que a leitura seja efetuada, existem algumas preocupações relacionadas com a higiene pública;
- Os equipamentos de aquisição têm de ter um tamanho relativamente grande devido ao facto da câmara de aquisição ter de ficar a uma certa distancia para que se obtenha o efeito ótico desejado;
- Para uma boa aquisição é necessário que o utilizador colabore colocando a mão alinhada de acordo com os pinos o que nem sempre é muito confortável;
- Não é suficientemente distinta para identificação, sendo adequada apenas para aplicações de verificação [33].

Na tabela seguinte são mostrados dois dos equipamentos mais recentes para leitura da geometria da mão.

Quadro 2-3: Leitores de geometria da mão.

	
Modelo: HandKey II Fabricante: Schlage	Modelo: Handkey gt400 Fabricante: Schlage

O primeiro equipamento possui duas camaras para geometria a 3D da mão, um pequeno ecrã, teclado físico para introdução de password ou id do utilizador, capacidade para 512 utilizadores, comunicação TCP/IP, RS-485, RS232, permite a ligação a trincos de portas automáticas e alarme. O segundo equipamento possui duas camaras para geometria a 3D da mão, ecrã, indicador LED, teclado físico numérico mais 8 botões para funções programáveis, capacidade para 512 utilizadores, comunicação TCP/IP(DHCP IP, Static IP), RS-422, RS232, USB e permite a ligação a trincos de portas automáticas e alarme.

2.6 Reconhecimento Facial

O objetivo desta tecnologia é identificar indivíduos através da análise da face. A ideia é mapear a geometria e as proporções da face, usando pontos como a distância entre os olhos, distância entre boca, nariz e olhos, distância entre os olhos e o queixo, entre outros que são examinados de modo a extrair uma combinação única para identificar o indivíduo.

2.6.1 Processo de aquisição

A aquisição de imagens da face pode ser efetuada de várias formas das quais se destacam as seguintes:

- **Imagens 2D** – Consiste na obtenção de imagens digitalizadas de fotografias (Figura 2-16), sejam elas a cores ou a preto e branco, mas também pode ser obtidas ao vivo, isto é tiradas através de câmaras digitais ou analógicas no momento da autenticação [42]. As imagens são geralmente capturadas com a cooperação do utilizador que vai ser fotografado, e em condições de iluminação controladas. Qualquer câmara serve para captar imagens 2D mas quanto melhor for a câmara melhor será o resultado [23].
- **Imagens 3D** – Consiste na obtenção de imagens a 3 dimensões (Figura 2-16) através de varias técnicas tais como uso de imagens simultâneas, onde duas câmaras 2D, cujos campos de visão são separados por um ângulo entre 8º e 15º, obtêm imagens independentes para montagem posterior [42]. Outra técnica baseia-se na projeção de um padrão de luz, cuja distorção pode ser capturada para reconstruir a aparência 3D da face, por último o varrimento a laser proporcionando um mapa tridimensional pela amostragem de cada ponto da superfície da face [24].
- **Sequências de imagens** – Consiste na obtenção de imagens para o reconhecimento facial através de vídeo. Como o vídeo tem qualidade inferior a fotografia esta técnica requer câmaras com alguma qualidade, com *zoom* e *autofócus* [25].
- **Termograma da face** – Consiste na obtenção de imagens térmicas da face através de iluminação infravermelha de baixa potência, invisível ao olho humano e ou baseados em radiação infravermelha (Figura 2-16). Estas técnicas requerem respetivamente condições de iluminação e de calor controladas para que não ocorram interferências [25].

Na Figura 2-16 encontram-se ilustrados alguns exemplos de imagens de faces humanas.

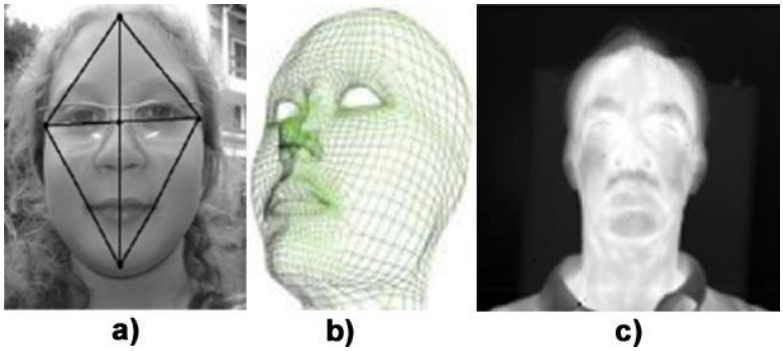


Figura 2-16: a) Imagem a 2D; b) Imagem a 3D; c) Imagem a infravermelho.
[Gonçalo Lourenço, 2009]

2.6.2 Vantagens e desvantagens

Em qualquer sistema existem vantagens e desvantagens e a tecnologia de autenticação biométrica baseada na face não foge à regra. Assim, as principais **vantagens** são as seguintes:

- Larga aceitação por parte das pessoas para este tipo de tecnologia, já que fotografias da face já são usadas rotineiramente em documentos;
- Os sistemas de reconhecimento facial são os menos intrusivos, não exigindo qualquer contacto e nem mesmo a colaboração do utilizador [38];
- Baixo custo dos equipamentos de aquisição de imagens 2D.

Em relação às **desvantagens**, as principais são as seguintes:

- Necessitam de condições de iluminação controladas [52];
- Estes sistemas podem ser facilmente enganados com a utilização de uma fotografia no ato da aquisição da face [27];
- Alguns sistemas podem ser facilmente enganado utilizando disfarces;
- É uma tecnologia biométrica suficientemente boa para aplicações de verificação de pequena escala. No entanto, é uma biometria pobre para aplicações de identificação de larga escala;
- Deferentes angulações da posição do rosto em relação a câmara prejudicam a validação do utilizador [51];
- Alterações faciais decorrentes do envelhecimento prejudicam a validação do utilizador;
- Utilização de óculos de sol, bigode, barba e expressões faciais podem dificultar o processo de reconhecimento da face.

Na tabela seguinte são mostrados três exemplos de equipamentos mais recentes.

Quadro 2-4: Leitores de reconhecimento facial.

		
Modelo: FA2 **Fabricante:** Granding	**Modelo:** FaceID F810 **Fabricante:** Kimaldi	**Modelo:** Uni 900 FaceID **Fabricante:** Uniclox

O primeiro equipamento possui duas camaras de alta definição para o reconhecimento a 3D com 18 LED's para uma correta iluminação da face do utilizador, ecrã sensível ao toque, possui 6 botões para funções programáveis, leitor de RFID, speaker para indicações de voz, capacidade para 700 faces, comunicação em TCP/IP, RS232/485, USB e wifi. O segundo equipamento possui duas camaras de alta definição para o reconhecimento a 3D, ecrã, teclado físico para introdução de password e id de utilizador, incorpora um leitor de RFID, possibilita vários modos de funcionamento (Facial, PIN + Facial, RFID + Facial, RFID), comunicação em TCP/IP, USB e RS-232 e capacidade para 500 faces. O terceiro equipamento possui duas camaras de alta definição para o reconhecimento a 3D com 14 LED's para uma correta iluminação da face do utilizador, ecrã, teclado físico para introdução de password e id de utilizador, capacidade para 500 faces, possibilita dois modos de funcionamento (Facial, PIN + Facial), comunicação em TCP/IP, USB.

2.7 Retina

A retina está situada na parte de trás do olho e é composta por células sensíveis à luz. Essas células transformam a energia luminosa das imagens em sinais nervosos que são transmitidos ao cérebro pelo nervo ótico (Figura 2-17).

Figura 2-17: Olho humano, e veias da retina
[VESPER, 2005]

Os sistemas biométricos de leitura de retina analisam a camada de vasos sanguíneos (retina) situados na parte de trás do olho, através da utilização de uma fonte de luz de baixa intensidade para oticamente reconhecer os padrões da retina [45]. Esta é uma técnica muito precisa e é praticamente impossível de ser violada devido a sua relação com os sinais vitais da pessoa que está a ser autenticada, isto é, só funciona se a pessoa estiver viva, e é considerada uma das técnicas mais seguras devido a sua unicidade extremamente alta. No entanto alguns médicos afirmam que as características únicas da retina não são extremamente estáveis e existem algumas doenças que podem alterar o formato da retina [29].

2.7.1 Processo de aquisição

A captura das características da retina requer que o utilizador se posicione em frente do aparelho de leitura (Figura 2-18) e olhe fixamente para um ponto fixo sem se mexer enquanto as imagens para a extração de características, são recolhidas.

Figura 2-18: leitor de retina.
[RETICA, 2005]

2.7.2 Vantagens e desvantagens

As principais **vantagens** da tecnologia de autenticação biométrica baseada na retina são as seguintes:

- Tecnologia extremamente segura, uma vez que o local onde a retina está localizada torna difícil a copia do seu padrão sem o consentimento da pessoa autenticada, sendo extremamente difícil produzir um equipamento que imite o padrão de reflexões e principalmente o alinhamento necessário para realizar o reconhecimento. Assim como, também não é possível remover os olhos de uma pessoa sem que a retina se degenere;
- O padrão de retina é estável ao longo da vida e como a retina faz parte de um órgão interno está num local protegido do meio ambiente logo não é afetado por ele;
- Tamanho reduzido do *template* (48 bytes) para cada olho facilita a rápida manipulação e armazenamento [45];
- Não existem casos relatados de falsa rejeição ou fraudes através deste método de reconhecimento biométrico;

- Unicidade, isto é a probabilidade de duas retinas apresentarem o mesmo padrão está na ordem de 1 em 10.000.000.

Em relação às **desvantagens**, as principais são as seguintes:

- Número significativo de pessoas que não é capaz de realizar o reconhecimento com eficiência por terem problemas visuais mais graves, ou por não saberem como usar o equipamento;
- Receio por parte das pessoas em expor os seus olhos a qualquer tipo de aparelho por medo de danificar os olhos;
- Alto custo do equipamento, devido à fraca aceitação do público e à falta de investimentos no desenvolvimento da tecnologia;
- Fraco desempenho em ambientes "*outdoor*" uma vez que a grande quantidade de luz contrai a pupila, fazendo com que menor quantidade de luz vinda do leitor chegue à retina e retorne ao leitor.
- Intrusiva, uma vez que para obter uma medição, uma pessoa deve olhar fixamente para um ponto infravermelho por cerca de 5 segundos, sem piscar posicionando-se entre 2 a 3 centímetros do leitor, tornando-se muito desconfortável para algumas pessoas.

2.8 Íris

A íris é um órgão interno que faz parte do olho e está situada atrás da córnea e do humor aquoso, entre a esclera (parte mais clara do olho) e a pupila (parte mais escura do olho) [8]. É responsável pela cor dos olhos, e ajuda a regular a quantidade de luz que entra no olho (Figura 2-19).

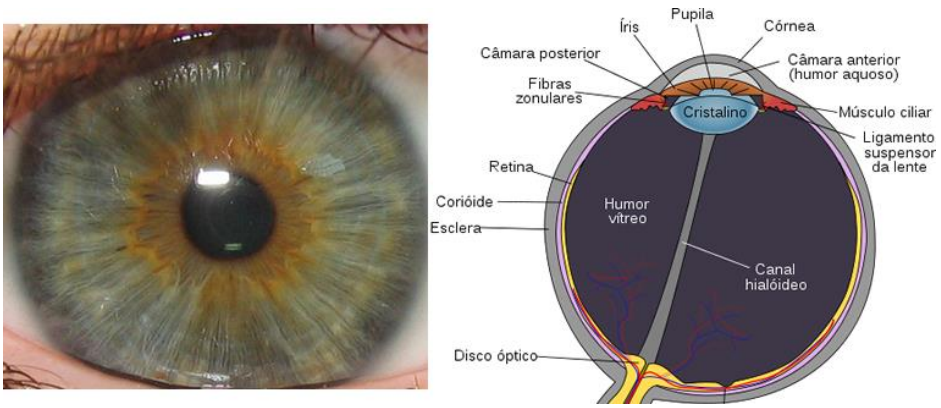


Figura 2-19: O olho humano.
(Adaptado de [16])

A formação da íris inicia-se no 3º mês de gestação e as estruturas que criam o seu padrão estão completas, na sua maioria, no 8º mês, embora a pigmentação possa continuar nos primeiros anos após o nascimento [4]. A íris é constituída por diversas características (minúcias), tais como: sardas, sulcos, listas, etc. Essas características são únicas e além disso, a íris faz parte de um órgão interno logo não está em contacto direto com o meio ambiente e

como tal a probabilidade de sofrer agressões externas é muito reduzida, logo permanece praticamente inalterada por toda a vida [6].
Com um tamanho de cerca de 11mm a íris proporciona cerca de 266 pontos únicos de identificação, e todas essas características intrínsecas da íris produzem grande autenticidade e exclusividade dentre indivíduos, logo a probabilidade de 2 indivíduos terem o mesmo padrão de íris é cerca de 1 em 10^{78} nem mesmo gémeos têm o mesmo padrão de íris [41].

2.8.1 Processo de aquisição

Para o processo de aquisição das imagens da íris a maioria dos sistemas requerem que o utilizador posicione os olhos dentro do campo visual de uma câmara de foco estrito que indica o correto posicionamento dos olhos através de um feedback visual proporcionado por um espelho [43], [50]. De seguida o equipamento recolhe as imagens através de uma câmara monocromática uma vez que a extração de características não utiliza a cor; após a recolha, o sistema identifica a íris na imagem (Figura 2-20) e envia o resultado final (*írisCode*) para o *Middleware* que compara com a base de dados e autoriza ou não o acesso do utilizador [7].

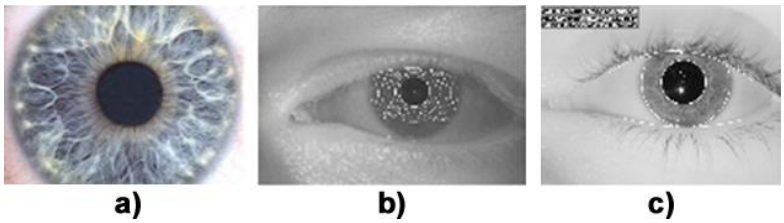


Figura 2-20: a) Íris adquirida sob condições ideais; b) Aplicação do algoritmo de extração de características; c) Íris com o seu *Íriscode* associado.
[Luciano Costa, 2008]

2.8.2 Leitor de íris

O leitor é um dispositivo eletrónico cujo objetivo é detetar as texturas da íris do olho humano. Atualmente existem várias marcas que comercializam este tipo de equipamento como por exemplo a Panasonic, LG, OKI, etc…
Mas também existem vários tipos de leitores de íris dos quais se destacam os seguintes:

- **Leitores fixos:** são dispositivos fixos (Figura 2-21) normalmente localizados numa posição em que seja fácil a sua utilização por parte dos utilizadores [9]. Normalmente estes sistemas têm um sensor de proximidade que ativa o aparelho para que a captura possa ser efetuada e só permite a passagem a pessoas autorizadas. Este tipo de equipamento é normalmente usado em escritórios, laboratórios, prisões, bancos e basicamente onde houver necessidade de assegurar e restringir o acesso a determinados espaços [10];
- **Leitores móveis:** são equipamentos compactos e manuais (Figura 2-21) e são normalmente usados como uma simples máquina fotográfica usando a íris como ponto

de focagem, podem estar ligados a um computador ou ter memória interna incluída. São normalmente usados em missões militares, na marinha

Figura 2-21: a) Leitor de íris fixo, b) Leitor de íris móvel.

2.8.3 Vantagens e desvantagens

As principais **vantagens** desta tecnologia são as seguintes:

- Tecnologia muito precisa com probabilidades de erro ou de aceitação muito baixas, isto é, a probabilidade de aceitar uma íris errada ou rejeitar uma íris correta são inferiores a 1%
- Unicidade: A probabilidade de uma íris ser idêntica a outra é aproximadamente 1 em 10^{78}, nem mesmo os gémeos tem o mesmo padrão de íris [45];
- Estável e segura: a íris faz parte de um órgão interno, portanto é bem protegida e é imune a doenças do olho, além disso, o padrão da íris não vária com o envelhecimento.
- Higiene: Permite que os equipamentos sejam utilizados sem que haja contacto do utilizador com o aparelho e sem exigir praticamente nada do utilizador (ele apenas deve aproximar o olho do equipamento);
- Tempo necessário para analisar e codificar da imagem de uma íris relativamente curto, cerca de 1 segundo.
- Espaço necessário para armazenamento reduzido isto é o código da íris e de máscara podem ser armazenadas em 512 bytes,

Em relação às **desvantagens**, as principais são as seguintes:

- A íris não é um alvo fácil, isto é a íris é um alvo em movimento que pode ser parcialmente oculto pelas pálpebras que piscam frequentemente, para além disso é um alvo pequeno cerca de 1cm situado atrás de uma superfície curva e refletora, é deformado pela dilatação da pupila, para ser adquirido a uma distância de cerca de 1m. Logo, exige a colaboração do utilizador para a sua colheita;
- Em locais com muito movimento o reconhecimento de íris é lento, uma vez que não é possível fazer um reconhecimento de íris adequado com alvos em movimento, logo o utilizador terá de para em frente do leitor e embora a leitura seja rápida o simples facto de ter de para já vai atrasar o fluxo de pessoas [45].

- Apesar da íris não contrair nenhuma doença diretamente, outras doenças no olho, tais como catarata, conjuntivite, tremor nos olhos ou alergias, podem prejudicar a identificação;

Na tabela seguinte são mostrados três exemplos dos equipamentos mais recentes de reconhecimento de iris.

Quadro 2-5: 3 Leitores de íris fixos.

		
Modelo: iCAM7000 **Fabricante:** Irisid	**Modelo:** iCAM4000 **Fabricante:** Irisid	**Modelo:** Id Bio Íris [5] **Fabricante:** Idonic

Os três equipamentos possuem sensor ajustável na altura para melhor conforto, o primeiro equipamento possui um monitor sensível ao toque e seis, botões físicos para funções programáveis, incorpora um leitor de RFID, um speaker, um microfone, sensores de proximidade e um pequeno espelho com indicador de alinhamento, para que seja mais fácil para o utilizador, o alinhamento da iris com sensor, sensor de 5MP, capacidade de guardar 1000000 eventos, comunicação em Ethernet(TCP/IP), RS422, RS232. O segundo equipamento possui uma camara de 5MP com 16x Zoom e dois LED's, incorpora um leitor de RFID, e um pequeno espelho com indicador de alinhamento para que seja mais fácil para o utilizador, o alinhamento da iris com sensor, comunicação em Ethernet (TCP/IP) e USB. O terceiro equipamento possui 2 pequenos espelhos com LED para indicação de alinhamento da íris, permite tempos de verificação inferiores a 1 segundo, possui um speaker para indicações por voz para auxiliar o alinhamento na íris, permite um máximo de 50 utilizadores, comunicações Ethernet(TCP/IP) em 10 Base-T/100 Base-TX.

2.9 Vasos sanguíneos (Veias)

O padrão das veias é a rede de vasos sanguíneos debaixo da pele. A ideia de usar padrões de veias como uma forma de identificação biométrica foi proposta pela primeira vez em 1992, mas só nos últimos dez anos é que tem tido maior destaque. Assim como a retina a íris a impressão digital, as veias também são características únicas nem mesmo gémeos têm o mesmo padrão de veias e nem mesmo a mesma pessoa tem o padrão de veias do lado

esquerdo igual ao do lado direito. Como as veias estão debaixo da pele, são muito difíceis de falsificar ou manipular, além disso o sensor só as reconhece se a hemoglobina estiver a fluir dentro delas e o padrão de veias modifica-se muito pouco com a idade [15].

2.9.1 Processo de aquisição

O processo de aquisição é muito semelhante tanto para a leitura do padrão de veias do dedo, da palma da mão, do punho ou do pulso [15]. Para utilizar estes sistemas o utilizador coloca o dedo, ou a palma mão, ou o punho e ou o pulso num suporte apenas para que a mão esteja estabilizada. Também existem equipamentos em que só é preciso colocar a mão suficientemente próxima para que o leitor, através de uma luz infravermelha que reage com a hemoglobina do sangue, mapeie o padrão da posição das veias (Figura 2-22). De seguida o equipamento extrai um *template* a partir desse padrão que é guardado ou comparado com a base de dados [17].

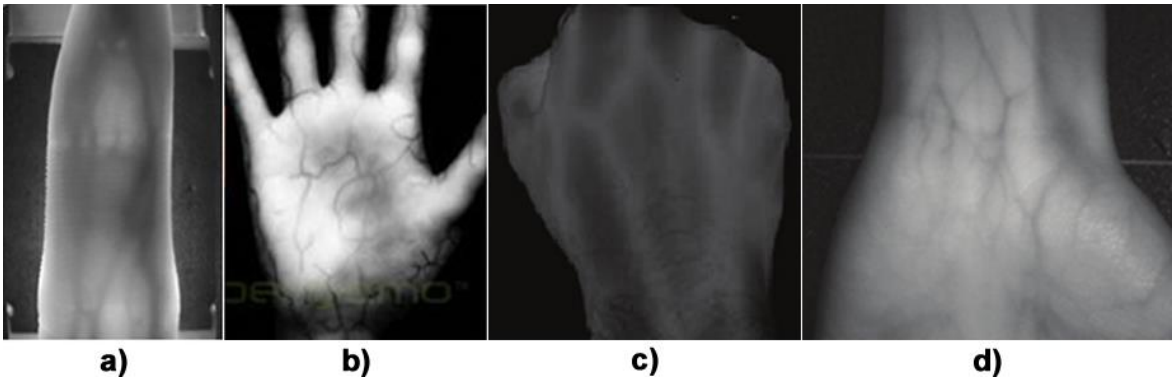


Figura 2-22: Veias: a) do dedo; b) da palma; c) do punho; d) do pulso
[Fujitsu, 2009]

2.9.2 Vantagens e desvantagens

As principais **vantagens** da tecnologia de autenticação biométrica baseada em padrões de veias são as seguintes:

- A extração do padrão pode ser feita sem contacto físico com a superfície do equipamento contribuindo para a higiene;
- As veias estão debaixo da pele, logo não estão sujeitas a alterações provocadas por sujidade ou lesões na pele, o que também dificulta a falsificação;
- O seu uso é bastante simples e prático e o tempo de análise ronda os 2 segundos;
- Singularidade – A probabilidade de haver 2 indivíduos como o mesmo padrão de veias é muito reduzida, nem mesmo gémeos têm o mesmo padrão de veias;
- Escalabilidade – O padrão de veias não sofre mudanças por longos períodos de tempo.

Em relação às **desvantagens**, as principais são as seguintes:

- Existem muitos fatores que podem afetar a qualidade da imagem capturada tais como a temperatura corporal, a temperatura ambiente, a humidade, a distribuição desigual de calor, a radiação a proximidade das veias da superfície de calibração da câmara;

- O reconhecimento de veias pode provocar receios infundados por parte dos utilizadores de que estes sistemas possam ser dolorosos por se tratar de veias;
- Custo médio: Estes sistemas são dispendiosos e requerem sensores de dimensões consideráveis.

Na tabela seguinte são mostrados três exemplos dos equipamentos mais recentes usados para leitura de vasos sanguíneos.

Quadro 2-6: Leitores de vasos sanguíneos.

		
Modelo: FingerVein **Tipo:** Dedo **Fabricante:** Kimaldi	**Modelo:** Nuxpalm **Tipo:** Mão **Fabricante:** Innux	**Modelo:** PalmSecureLT **Tipo:** Mão **Fabricante:** Fujitsu

O primeiro equipamento é um leitor de veias do dedo com teclado para introdução de *password* ou id de utilizador e com teclas dedicadas para marcar entradas ou saídas, permite a integração em rede através dos protocolos TCP/IP e UDP, permite a ligação com trincos para abrir portas automaticamente. O segundo equipamento é um leitor de palma da mão com teclado para introdução de *password* ou id de utilizador e leitor de RFID incorporado, permite a integração em rede através dos protocolos TCP/IP, permite a ligação com alarmes e trincos para abrir portas automaticamente, permite um total de 10000 utilizadores com um tempo de verificação inferior a 2 segundos, com capacidade de guardar até 100000 eventos, permite vários modos de funcionamento (cartão, palma, palma + cartão, palma + PIN, etc..). O terceiro equipamento é um leitor de palma da mão, de secretaria para acesso a computadores.

2.10 Reconhecimento de Voz

O som da voz humana é produzido pela ressonância na região vocal, em função do comprimento e formato da boca e cavidades nasais e modo como se movimentam.
O principal objetivo destes sistemas é a análise das características da voz nomeadamente o timbre de voz, cuja analise é feita comparando padrões harmónicos usando um espectrograma de som que é basicamente um gráfico que exibe a frequência do som em função do tempo

(Figura 2-23), usando cores ou tons de cinza para representar a qualidade acústica do som, pois diferentes sons criam diferentes formas no gráfico.
A tecnologia de reconhecimento de voz é extremamente fácil de ser usada e é considerada não intrusiva pelos utilizadores [18]. Apesar disso, ainda é pouco usada por não ser 100% fiável e é afetada por diversos fatores tais como o ruído ambiente, estados de emocionais (stress) e de saúde (faringite, gripes) dos utilizadores, por isso qualquer mudança na voz, por mais simples que seja, pode causar problemas no momento do reconhecimento (autenticação) [13].

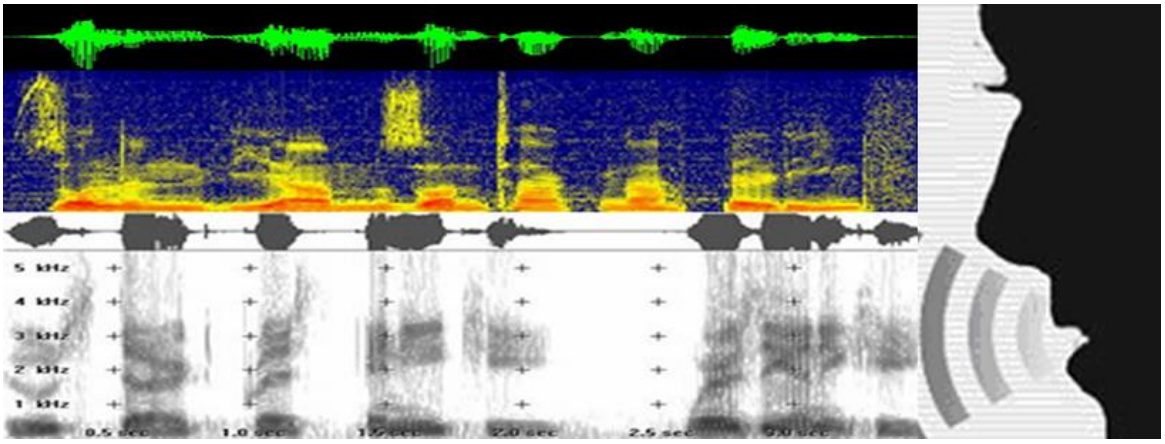


Figura 2-23: Espectrograma de timbre de voz.

2.10.1 Funcionamento

O funcionamento destes sistemas é muito simples, o utilizador apenas tem de fornecer uma amostra da sua voz através de um microfone, amostra essa que pode ser de diferentes formas das quais se destacam as seguintes:

- **Texto fixo** – Neste caso o utilizador pronuncia uma palavra ou frase pré-determinada e secreta, que é gravada durante a fase de registo;
- **Dependente do texto** – Neste caso o utilizador pronuncia uma das varias palavras ou frases pré-determinadas na fase de registo. É similar ao protocolo de texto fixo, mas com um número maior de opções;
- **Texto independente** – Neste caso o utilizador pronuncia um texto qualquer;
- **Conversacional** – Neste caso o sistema faz perguntas ao utilizador, cujas respostas são secretas.

2.10.2 Vantagens e desvantagens

As principais **vantagens** da tecnologia de autenticação biométrica baseada no reconhecimento de voz são as seguintes:

- A voz é uma característica biométrica usada intuitivamente pelas pessoas para autenticação mútua pelo que é muito fácil de ser usada;

- Os sistemas com infraestruturas telefónicas são os principais alvos destes sistemas uma vez que o utilizador usa o sistema para falar e assim o protocolo de autenticação torna-se passivo, amigável e não intrusivo [47];
- Tecnologia barata, uma vez que usa dispositivos de custos reduzidos, e além disso pode ser facilmente desenvolvida sobre sistemas telefónicos;
- Permite protocolos de autenticação de segurança incremental, isto é o sistema pode pedir mais dados de voz para que a decisão seja a correta;
- Em aplicações de texto independente e em aplicações conversacionais, os utilizadores não precisam de um processo separado de autenticação tornando assim o processo totalmente integrado.

Em relação às **desvantagens**, as principais são as seguintes:

- Estes sistemas podem ser enganados por imitações de pessoas habilidosas e ou gravações da voz de um utilizador legítimo;
- A tecnologia *"text-to-speech"* possibilita a criação de identidades inexistentes em sistemas de registo e autenticação remotos [47];
- O padrão de voz é muito frágil, pois pode ser afetado pelo estado do utilizador (saúde, emoção, pressa, sono, preguiça, etc…) e por interferências acústicas nomeadamente o ruído ambiente e as distorções caudadas pelo microfone e canal de transmissão.

Na tabela seguinte são mostrados 2 exemplos de equipamentos que acompanhados de *software* específico, podem ser usados na autenticação por reconhecimento de voz.

Quadro 2-7: Leitores equipamentos usados para a verificação da dinâmica da digitação.

	
Modelo: JBSMI06 **Fabricante:** JBSYSTEMS	**Modelo:** Todos **Fabricante:** Todos

O primeiro equipamento é um microfone de bancada que tem de ser ligado a um equipamento de processamento tal como um computador, o segundo equipamento é um telemóvel e hoje em dia existem muitos desde simples telemóveis a smartphones passando por tablet´s, que podem ser usados com sistemas de reconhecimento de voz com software adequado.

2.11 Dinâmica da Digitação

Esta tecnologia começou a ser estudada como um meio de autenticar pessoas a partir da década de 80 e tem evoluindo desde então. O objetivo desta tecnologia é medir a forma como escrevemos nos teclados independentemente do que escrevemos, isto é medir a velocidade, a pressão e o tempo do duplo clique sobre uma mesma tecla, fazendo assim um conjunto de características difíceis de serem imitadas [40].
Existem duas técnicas de verificação:

Verificação estática: A análise da dinâmica da escrita no teclado é feita num determinado tempo com um texto específico, como por exemplo ao introduzir uma palavra-passe;

Verificação contínua: A análise é mais alargada, isto é, a análise é feita a medida que se escreve e sem um tempo específico.

2.11.1 Vantagens e desvantagens

As principais **vantagens** desta tecnologia são as seguintes:

- Baixo custo uma vez que hoje em dia os teclados são extremamente baratos;
- Facilidade de utilização.

Em relação às **desvantagens**, as principais são as seguintes:

- Como esta técnica mede padrões de comportamento pode ser influenciada pelos estados de espírito do utilizador.

Na tabela seguinte são mostrados três exemplos de equipamentos que acompanhados de *software* específico, podem ser usados na autenticação por dinâmica da digitação.

Quadro 2-8: Leitores equipamentos usados para a verificação da dinâmica da digitação.

		
Modelo: KYBX-400 **Fabricante:** Stealth	**Modelo:** NZD 00003 **Fabricante:** Microsoft	**Modelo:** Teclado virtual iPad **Fabricante:** Apple

O primeiro equipamento é um teclado para locais públicos com 72 teclas e TrackBall, o segundo equipamento é um teclado normal de computador de 104 teclas com teclado numérico e o terceiro equipamento é um teclado virtual de um Tablet, mas também pode ser qualquer equipamento desde que este possua um ecrã sensível ao toque.

2.12 Assinatura Manuscrita

A assinatura manuscrita (Figura 2-24) é o método de autenticação mais usado e mais antigo que existe. Está presente em todos os documentos formais, no entanto o uso de caligrafia em sistemas biométricos pode não parecer boa ideia pois qualquer um pode aprender a imitar a caligrafia de outra pessoa em pouco tempo, até porque é relativamente fácil conseguir uma cópia da assinatura de alguém e falsifica-la [46]. Contudo, os sistemas biométricos de análise de assinatura manuscrita não se limitam apenas a analisar o que escrevemos, eles analisam o ato de escrever, registando a pressão, a aceleração, a velocidade, o ritmo, inclinação da caneta, o espaçamento entre letras, a sequência que se usa para formar as letras e a forma como se adicionam pontos e traços ao escrever ou depois de escrever cada palavra. Ao contrário da tradicional assinatura em papel, o ato de escrever é muito mais difícil de falsificar, mesmo que alguém consiga copiar a assinatura, não irá conseguir reproduzi-la da mesma forma que a pessoa legítima [27].

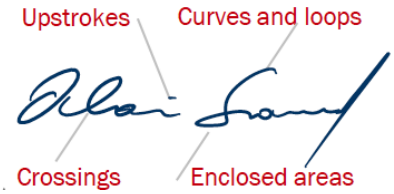


Figura 2-24: Assinatura.
[Jossy, 2012]

2.12.1 Processo de aquisição

A aquisição de uma assinatura pode ser ***offline* ou estática**, quando é introduzida por meio convencional (canetas, lápis, etc.) em documentos de papel e posteriormente digitalizada usando uma câmara ou scanner ou pode ser ***online* ou dinâmica**, quando efetuada num dispositivo eletrónico (Figura 2-25). Estes equipamentos estão preparados para capturar, com alto grau de resolução, as características dinâmicas temporais da assinatura, como a trajetória da caneta, a pressão, a aceleração, a velocidade e ritmo, a direção e elevação do traço.

Figura 2-25: Identificadores de caligrafia

2.12.2 Vantagens e desvantagens

As principais **vantagens** da tecnologia de autenticação biométrica baseada na assinatura são as seguintes:

- A assinatura dinâmica é uma combinação de informação (assinatura) e biometria (ato de escrever) e podem ser escolhidos pelo utilizador.
- Método muito bem aceite pelo utilizador;
- A assinatura dinâmica é muito difícil de ser falsificada.

Em relação às **desvantagens**, as principais são as seguintes:

- Custo elevado dos equipamentos de aquisição, uma vez que são relativamente recentes e sofisticados;
- Característica biométrica muito variável, uma vez que existem muitas pessoas com assinaturas incoerentes, logo o sistema teria de permitir lineares de decisão personalizados o que contribui negativamente para segurança.
- Esta característica biométrica possui alta variabilidade isto é existem muitas pessoas com assinaturas inconsistentes. Assim, os sistemas de verificação podem ter de permitir a configuração de limiares de decisão por utilizador.

2.13 Formato do Ouvido

O interesse do ouvido (Figura 2-26) como biometria já existe há mais de 100 anos, mas ainda se discute se o ouvido será suficientemente único para servir como método de autenticação. No entanto em 1989, nos Estados Unidos, num estudo feito pelo Xerife Alfred Iannarelli, em que testou 10.000 ouvidos, constatou-se que eram todos diferentes, no entanto em gémeos constatou-se que os ouvidos são muito semelhantes o que pôs um pouco em causa o desempenho do ouvido como medida biométrica [14].

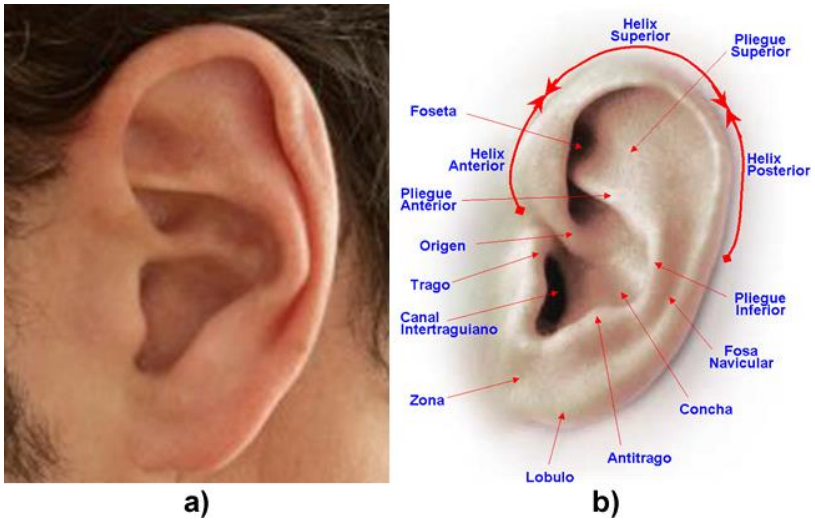


Figura 2-26: a) Foto do ouvido; b) Características do ouvido.

2.13.1 Vantagens e desvantagens

As principais **vantagens** da tecnologia de autenticação biométrica baseada no formato do ouvido são as seguintes:

- O ouvido manter-se constante ao longo do tempo;
- É extremamente simples adquirir uma amostra biométrica.

Em relação às **desvantagens**, as principais são as seguintes:

- Não existem certezas de que o ouvido seja único de pessoa para pessoa;
- Gêmeos verdadeiros costumam ter o ouvido muito semelhante.

2.14 ADN

O ácido desoxirribonucleico (ADN) ou DNA (Figura 2-27) é um composto orgânico cujas moléculas contêm as instruções genéticas que coordenam o desenvolvimento e funcionamento dos seres vivos e é constituído por quatro bases fundamentais: adenina, timina, citosina e guanina. Estas organizam-se em pares até 3 biliões de combinações e por isso é considerado como o sistema mais fiável que existe e também o mais difícil de burlar, mas também é um sistema muito caro lento e invasivo, pelo que só é usado em investigações policiais.

Figura 2-27: Sequência de ADN.

2.14.1 Processo de aquisição

O processo de aquisição e identificação é dividido em 3 fazes (preparação, sequenciação e analise):

1. Na primeira fase são retiradas amostras da pessoa (sangue, saliva, dentes, ossos, cabelos), uma vez extraídas, as amostras genéticas são separadas e purificadas;
2. Na segunda fase as amostras tratadas e purificadas são colocadas no equipamento que fará a sequenciação do ADN;
3. Na terceira fase a sequência é analisada e comparada com a sequência guardada para determinar a identidade da pessoa.

2.14.2 Vantagens e desvantagens

As principais **vantagens** da tecnologia de autenticação biométrica baseada no ADN são as seguintes:

- Preciso: a probabilidade de 2 pessoas compartilhando o mesmo perfil de ADN é menos de um em cem bilhões.

Em relação às **desvantagens**, as principais são as seguintes:

- A verificação do ADN não é feita em tempo real;
- Intrusiva: é necessário retirar uma amostra física para a analise me vez de uma representação como acontece em outras técnicas biométricas

Na tabela seguinte são mostrados dois exemplos de equipamentos de sequenciação de ADN.

Quadro 2-9: Equipamentos usados para a sequenciação do ADN.

	
Modelo: 3730 DNA Analyzer **Fabricante:** Applied Biosystems	**Modelo:** The Ion Proton **Fabricante:** Life technologies

O primeiro equipamento permite a análise de 48/96 Capillaries e permite sequenciamento entre 400 a 900 base-pairs em cerca de 2 a 48 horas dependendo da qualidade da sequenciação pretendida à saída, tem uma capacidade de 16 placas de amostras, tem uma largura de 100cm, uma profundidade de 73cm, uma altura de 89cm e um peso de 180kg aproximados. O segundo equipamento permite sequenciações de 200 base-pairs, entre 2 a 4 horas, gera um total de 10 GB de informação, tem uma largura de 54.2cm, uma profundidade de 77.5cm, uma altura de 47.4cm e um peso de 90.7kg aproximados, apesar de ser mais rápido que o primeiro equipamento, o segundo equipamento só permite uma sequenciar uma amostra de cada vez e com menor precisão que o primeiro.

2.15 Comparações dos diferentes sistemas

Mais importante que implementar um sistema biométrico é saber que sistema biométrico implementar e isso não é fácil e depende de vários fatores (universalidade, unicidade,

permanência, desempenho, aceitação e segurança) que precisam de ser tidos em conta na hora de escolher o sistema ou sistemas.
O quadro seguinte mostra uma avaliação entre algumas técnicas biométricas, no qual temos de ter em conta que uma classificação alta indica que a performance do critério avaliado é boa, e uma classificação baixa indica que a performance do critério avaliado é má. No caso do preço, uma classificação alta indica que o custo da tecnologia em causa é alto e uma classificação baixa, indica que o custo da tecnologia em causa é baixo.

Quadro 2-10: Avaliação de biométricas habitualmente usadas [Boechat 2008].

Tecnologia	Universalidade	Unicidade	Permanência	Desempenho	Aceitação	Segurança	Preço
Face	Alta	Baixa	Média	Baixa	Alta	Baixa	Médio
Impressão digital	Média	Alta	Alta	Alto	Média	Alta	Baixo
Geometria da mão	Média	Média	Média	Médio	Média	Média	Médio
Iris	Alta	Muito Alta	Alta	Alto	Baixa	Alta	Alto
Retina	Alta	Muito Alta	Alta	Alto	Baixa	Alta	Alto
Padrão vascular	Média	Média	Média	Médio	Média	Alta	Medio
Voz	Média	Baixa	Baixa	Baixo	Alta	Baixa	Muito Baixo
Dinâmica no digitar	Baixa	Baixa	Baixa	Baixo	Média	Média	Muito Baixo
Assinatura	Baixa	Baixa	Baixa	Baixo	Alta	Baixa	Baixo
Password	Baixa	Baixa	Baixa	Baixo	Alta	Média	Muito baixo
Formato da orelha	Média	Média	Alta	Médio	Alta	Média	--
Modo de andar	Média	Baixa	Baixa	Baixo	Alta	Média	--
Termograma facial	Alta	Alta	Baixa	Médio	Alta	Alta	Médio
ADN	Alta	Muito Alta	Muito Alta	Alto	Baixa	Muito Alta	Muito Alto

Outra das características que temos de ter em conta na hora de escolher um sistema de autenticação biométrica, é a precisão do sistema. A figura seguinte (Figura 2-28) representa os valores médios de FAR e FRR (tendo em conta que estes valores dependem muito do ambiente de uso dos equipamentos o que faz com que os valores sejam um pouco imprevisíveis) de algumas técnicas de autenticação biométricas mais usadas.

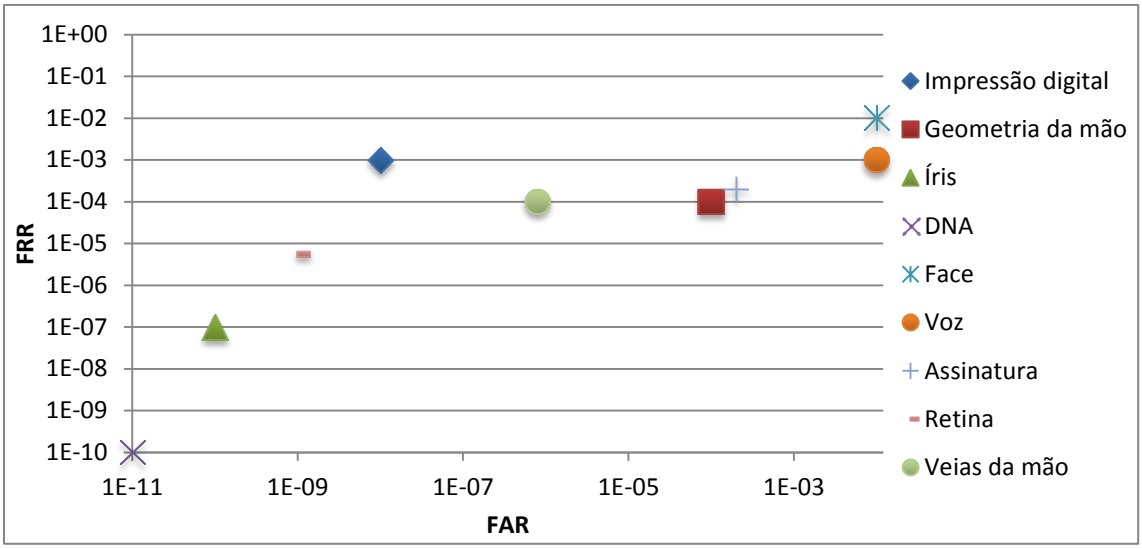


Figura 2-28: Gráfico de FAR vs FRR (valores médios)
(Adaptado de [6]).

Apesar de a tabela anterior (Quadro 2-10) ser resumida e os valores médios do gráfico anterior (Figura 2-28) serem muito gerais é possível obter um panorama geral dessas tecnologias, onde é possível verificar que não existe uma tecnologia boa para tudo. Contudo, das várias características biométricas apresentadas, o ADN, a íris, a retina, a impressão digital e o ouvido, são as mais estáveis ao longo do tempo. O ADN é a tecnologia mais precisa no entanto não produz resultados em tempo real logo a íris e a retina são as mais precisas com resultados em tempo real. Por outro lado a face, a voz e a geometria da mão são as menos precisas no entanto são mas mais aceites pelo utilizador. Logo a aplicação de uma determinada tecnologia biométrica depende fortemente dos requisitos do domínio da aplicação, isto é, nenhuma tecnologia pode superar todas as outras em todos ambientes de operação. Assim, cada uma das tecnologias é potencialmente utilizável, ou seja, não existe uma tecnologia ótima para tudo.

2.16Multi-biometria

Nos últimos anos, a autenticação biométrica tem tido melhorias consideráveis em termos de fiabilidade e precisão, mas até mesmo os melhores equipamentos ainda enfrentam inúmeros problemas, alguns deles inerentes à tecnologia em si. Nomeadamente, problemas de inscrição, devido à não-universalidade das características biométricas, suscetibilidade à falsificação biométrica ou precisão insuficiente causada pela aquisição de dados ruidoso em certos ambientes. A Multi-biometria é uma abordagem relativamente nova e nasceu para tentar para superar esses problemas e baseia-se no uso de múltiplas técnicas para autenticar pessoas, isto é, um sistema multi-biométrico pode usar vários sensores para captar a mesma característica biométrica (Multisensor) ou características diferentes (Multimodal), pode captar múltiplas características da mesma característica biométrica (Multisample / Multi-instance) e ou

múltiplos algoritmos (Multi-algoritmo) para a verificação de uma ou múltiplas características biométricas (Figura 2-29).

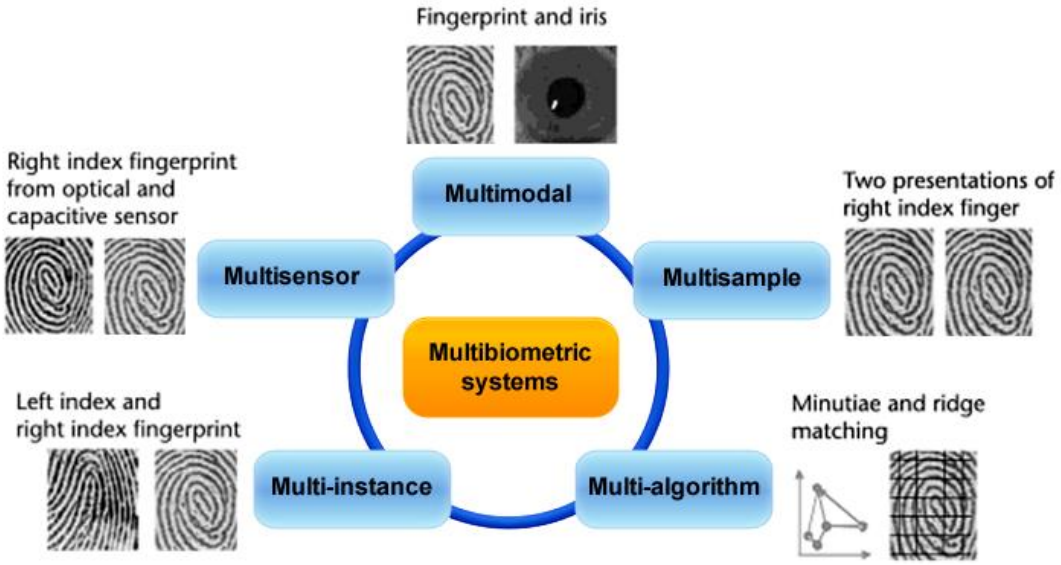


Figura 2-29: Sistema Multi-biométrico.

Existe uma variedade de fatores que devem ser considerados quando se projeta um sistema multi-biométrico, dos quais se destaca os seguintes:

- A escolha e o número de características biométricas a analisar;
- O nível de integração entre as várias características biométricas;
- A metodologia usada para integrar a informação retirada das características biométricas;
- A relação preço/desempenho.

2.16.1 Fusão das Características Biométricas

A fusão das diferentes características biométricas é a fase mais importante de um sistema multi-biométrico pois é nesta fase que o sistema junta os resultados das várias características biométricas para assim produzir uma resposta [39].
Esta fusão pode ocorrer em três níveis:

- **Fusão na etapa de extração:** Neste método (Figura 2-30), a informação extraída dos diferentes sensores é codificada num vetor e esse vetor da fusão é comparado com outro vetor armazenado na base de dados. A partir deste momento, o processo de decisão é o mesmo que num sistema biométrico simples; Este método não tem sido tão estudado quando os métodos seguintes, devido a dois problemas:
    - As características biométricas ao passarem pelo processo de fusão podem tornar-se incompatíveis ou ficarem indisponíveis se o utilizador não as possuir;
    - A geração da pontuação pode ser problemática, uma vez que já é difícil encontrar um bom classificador para um sistema biométrico simples [39].
- **Fusão na etapa de "match score":** Neste método (Figura 2-31), as características biométricas são obtidas pelos vários sensores e comparadas com os seus respetivos

templates (guardados na base de dados) individualmente, resultando numa pontuação individual para cada característica, que posteriormente são combinadas numa pontuação total, que é enviada ao módulo de decisão, combinação essa que pode ser feita das seguintes formas:

- Soma das pontuações, colocando pesos em cada característica;
- Árvore de decisão;
- Análise Linear Discriminante.

- **Fusão na etapa de decisão:** Neste método (Figura 2-32), a decisão sobra a autenticação é feita separadamente por cada sistema biométrica e no final é feita uma votação [39].

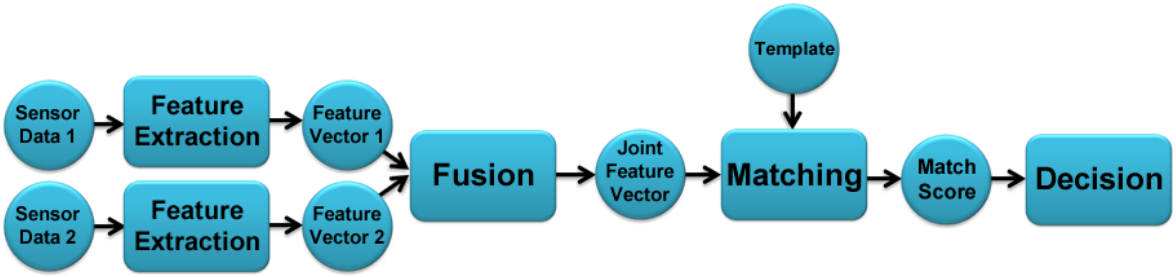


Figura 2-30: Fusão na etapa de extração.
[Bubeck, 2003]

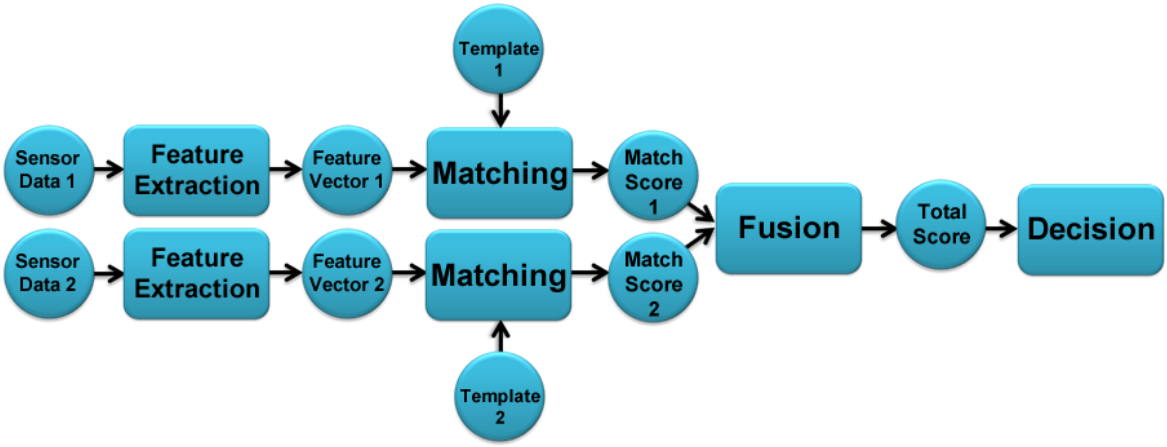


Figura 2-31: Fusão na Etapa de Matching.
[Bubeck, 2003]

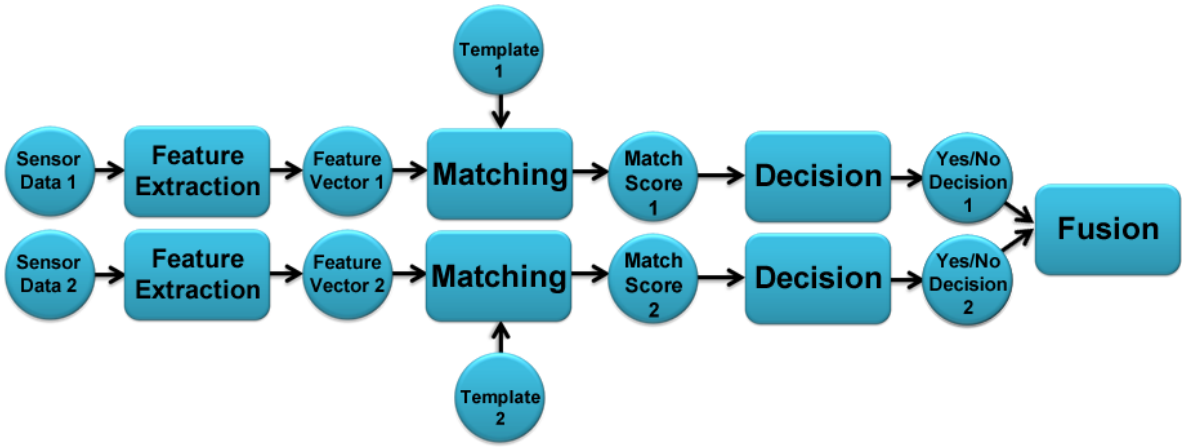


Figura 2-32: Fusão na Etapa de Decisão.
[Bubeck, 2003]

2.16.2 Resultados

Para a análise de resultados recorreu-se a um gráfico retirado do sistema proposto por Jain em 2004. Este sistema é composto por um conjunto de três características biométricas: a geometria das mãos, a face e a impressão digital.

Para a demostração do sistema proposto por Jain foram recolhidas cinco amostras de cada característica biométrica a cada um dos 100 indivíduos que fizeram parte da experiencia. A demostração deu origem ao gráfico seguinte (Figura 2-33), cujos dados foram obtidos empiricamente, usando os seguintes pesos: 0,6 para impressão digital; 0,2 para geometria das mãos e 0,2 para geometria da face [43].

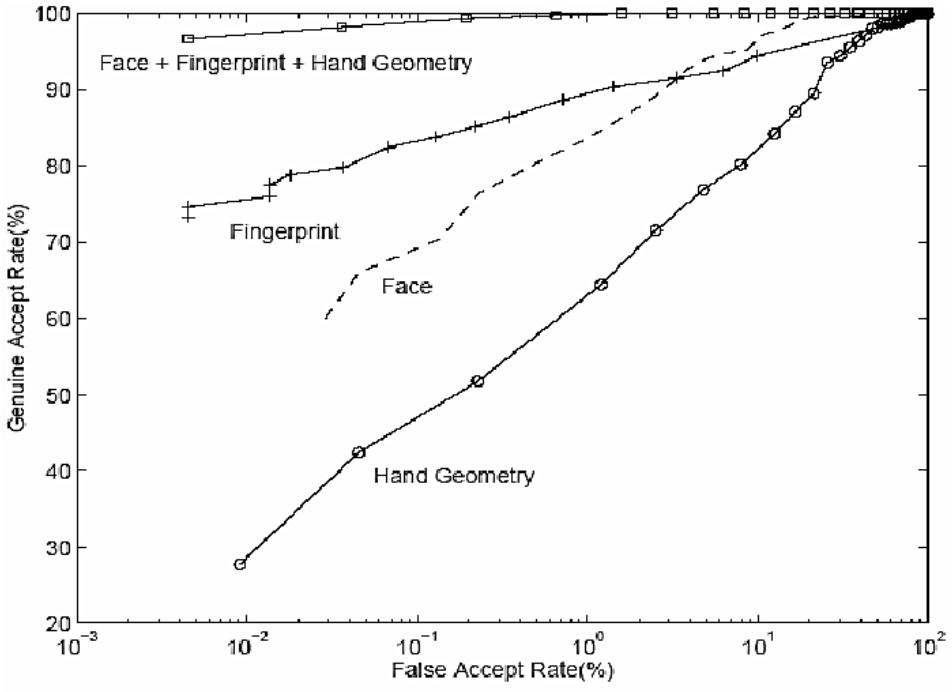


Figura 2-33: Gráfico da curva ROC.
[Jain, 2004]

Pela análise do gráfico (Figura 2-33) podemos afirmar que com multi-biometria é possível aumentar a precisão de um sistema de autenticação e quanto mais técnicas forem usadas mais preciso será o sistema na sua globalidade em contra partida quanto mais técnicas usarmos mais demorado e mais desconfortável será o processo de autenticação bem como será necessário mais espaço de armazenamento nas bases de dados das características biométricas.

2.17Enquadramento Regulamentar e Lei

A Lei de Proteção de Dados Pessoais é uma organização com poderes para verificar o cabal cumprimento da lei referente ao armazenamento de dados pessoais. Essa organização, a Comissão Nacional de Proteção de Dados (CNPD), funciona junto da Assembleia da República e detém um vasto leque de competências, desde a emissão de pareceres até à deliberação sobre a aplicação de coimas, podendo a sua atividade verificadora ser acionada mediante denúncias ou queixas de particulares.
Segundo a lei Portuguesa a implementação de sistemas biométricos requer a aprovação da comissão de proteção de dados, porque uma característica biométrica é considerada como dado pessoal e deve respeitar todas as condições estabelecidas na Lei 67/98, nomeadamente:

- O tratamento deve ser feito com respeito pela reserva da vida privada (artigo 2.º) e para finalidades determinadas, explícitas e legítimas (art. 5.º n.º 1 al. b);
- Os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade e proporcionados aos objetivos que se pretendem atingir (art. 5.º n.º 1 al. c);
- O responsável só pode proceder ao tratamento se, de acordo com a natureza dos dados (artigo 6.º e 7.º), estiverem preenchidas as «condições de legitimidade»;
- O responsável deve fazer a notificação destes tratamentos à CNPD (art. 27.º n.º 1).
- O responsável deve assegurar o direito de informação em relação à existência de tratamento, dados pessoais tratados, finalidades e entidades a quem os dados podem ser transmitidos (cf. artigo 10.º);
- O responsável não pode utilizar os dados biométricos para finalidade diversa da determinante da recolha (artigo 5.º n.º 1 alínea b) da Lei 67/98);
- Aos titulares dos dados deve ser assegurado o direito de acesso, retificação ou oposição, nos termos dos artigos 11.º e 12.º alínea a).

Para saber mais a cerca da legislação em vigor e do que se tem de fazer poderá ser consultado o ANEXO 1

3. Parte pratica: Interface

Neste capítulo pretende-se apresentar como a aplicação foi construída identificando a sua estrutura, que tecnologias foram usadas (linguagem de programação escolhida, equipamento escolhido e bases de dados escolhidas), e porque foram usadas. Também se descreve como a arquitetura foi pensada (arquitetura de 3 camadas), como foi implementada e porque foi usada, que funções foram implementadas, como foram implementadas e porquê foram implementadas e finalmente será mostrado e explicado algum código de algumas funções que consideramos mais importantes.

3.1 Introdução

Com a existência de vários equipamentos de autenticação, de várias marcas e de vários tipos e, como cada fabricante faz o seu próprio controlador, o processo de integração de vários equipamentos de várias marcas ou de vários tipos é uma tarefa um pouco difícil.
Da necessidade de unificar e simplificar a integração destes equipamentos com outras aplicações presentes no sistema, nasceu a ideia de criar uma aplicação que centralizasse e controlasse todos os dados recebidos dos vários equipamentos, e que fosse possível importar e exportar dados de várias bases de dados.

3.2 Tecnologias e Ferramentas Utilizadas

No desenvolvimento desta aplicação foram utilizadas diversas tecnologias, sem as quais seria impossível chegar aos resultados obtidos.

3.2.1 Terminal OutLock 3 Bio Online

O **OutLock 3 Bio Online** (Figura 3-1) é um terminal biométrico da Acronym, para ligação em rede. Este terminal permite a leitura de etiquetas RFID e impressões digitais.

Figura 3-1: Terminal OutLock 3 Bio Online
(Fonte [2]).

A capacidade de leitura de tags RFID e impressões digitais num só e o facto de só me ter sido facultado este equipamento, foram fatores determinantes na escolha desde equipamento, para o teste das funcionalidades de autenticação.

O este equipamento retorna dois tipos de dados importantes:

- **O código das *tags* RFID:** neste caso sempre que passamos uma *tag* RFID o equipamento envia duas variáveis para a aplicação: uma variável do tipo *string*, contendo o IP do equipamento que efetuou a leitura e um variável do tipo texto com o código da *tag* lida
- **O *template* biométrico** (impressão digital encriptada**):** neste caso, quando registamos uma nova impressão digital, o equipamento envia duas variáveis: uma do tipo *string* indicando o IP do equipamento que fez a leitura e uma variável do tipo *byte array* com novo *template* recolhido (impressão digital encriptada). Quando enviamos um *template* gravado numa das bases de dados também temos de indicar para onde enviar através de uma variável do tipo *string* contendo o ip do equipamento de destino e uma variável do tipo *byte array* contendo o *template* biométrico a gravar no equipamento, mas como nenhuma base de dados suporta campos do tipo *byte array* a *template* na recolha é convertida para *string* e só depois é que é gravada, no envio o processo é o inverso.

Nota: Para ligar o equipamento ao computador temos primeiro definir um ip para cada equipamento usado e ainda definir para que ip é que cada um dos equipamentos vai "responder" e para isso foi usado o programa "SetAddr.exe" que não era muito compatível

com os sistemas mais recentes por falta de uma dll presente em sistemas operativos mais antigos. Depois do equipamento ter o endereço definido já pode ser ligado diretamente a um computador ou ligado numa rede, ligando um cabo de rede do equipamento a um *switch* (mais a frente na fase de testes será mostrado com recurso a figuras o processo de configuração deste equipamento) desde que o computador, a quem o dispositivo responde, esteja ma mesma rede.

3.2.2 WampServer Version 2.2

O WampServer version 2.2 é um servidor apache muito usado para testar páginas de internet nomeadamente páginas em php com recurso a uma base de dados em MySQL.
Na figura seguinte (Figura 3-2) é possível ver a versão da base de dados MySQL.

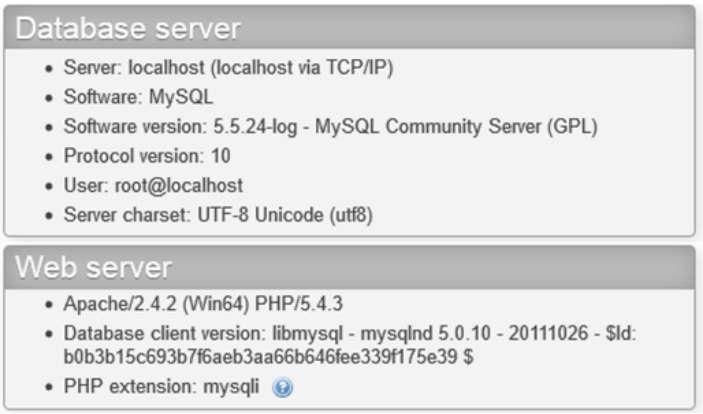


Figura 3-2: versão do servidor de base de dados MySQL.

No trabalho foi usada a versão do MySQL 5.5.24, apenas como teste, para testar o comportamento da aplicação e aceder a dados presentes numa base de dados deste tipo.
A escolha deste servidor deve-se ao facto de ser gratuito e muito fácil e rápido de configurar.

3.2.3 Sqlite

O SQLite é uma biblioteca em linguagem C que implementa uma base de dados SQL embutida. Os programas que usam a biblioteca SQLite podem ter acesso à base de dados SQL sem executar um processo SGBD (Sistema de gestão de base de dados: este sistema gere as operações de entrada e saída de dados de uma base se dados) separado.
Na figura seguinte (Figura 3-3) é possível ver a versão da base de dados.

(Name)	System.Data.SQLite
Aliases	global
Copy Local	True
Culture	
Description	ADO.NET Data Provider for SQLite
Embed Interop Types	False
File Type	Assembly
Identity	System.Data.SQLite
Path	C:\CCharpLibs\System.Data.SQLite.dll
Resolved	True
Runtime Version	v4.0.30319
Specific Version	False
Strong Name	True
Version	1.0.79.0

Figura 3-3: Versão da base de dados

No trabalho foi usada a versão do SQLite 1.0.79.0, para guardar todos os dados referentes a aplicação (lista de equipamentos, lista de conexões e log) e como base de dados externa apenas como teste, tendo como objetivo verificar o comportamento da aplicação em aceder a dados contidos numa base de dados deste tipo.

3.2.4 Microsoft SQL Server 2008

O Microsoft SQL Server 2008 é um SGBD (sistema de gestão de bases de dados) criado pela Microsoft.
Na figura seguinte (Figura 3-4) é possível ver a versão da base de dados e suas componentes.

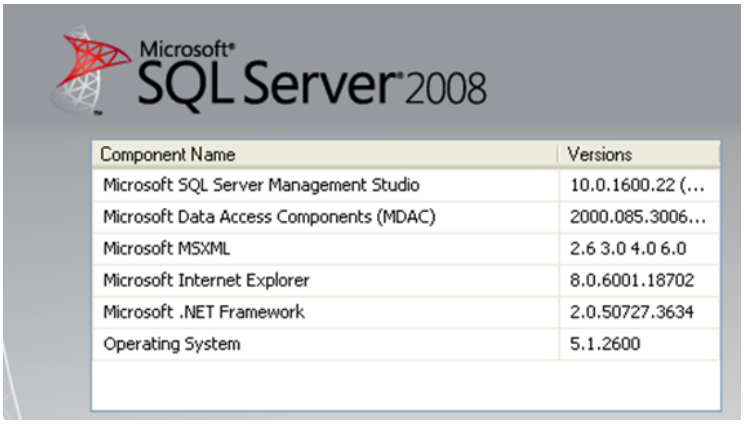


Figura 3-4: Versão da base de dados e componentes.

No trabalho foi usada a versão do Microsoft SQL Server 2008 Express Edition, apenas para verificar o comportamento da aplicação quando se acede a dados presentes numa base de dados deste tipo.

A escolha desta versão do servidor de base de dados da Microsoft deve-se ao facto de ser uma versão gratuita e muito "leve" que serviu perfeitamente para testar a ligação do programa a este tipo de base de dados

3.2.5 Oracle Database 11gR2

O Oracle Database 11gR2 é um SGBD (sistema de gestão de bases de dados) criado pela Oracle Corporation.
Com o comando **select * from v$version** é possível ver versão e as componentes existentes (Figura 3-5).

	BANNER
1	Oracle Database 11g Express Edition Release 11.2.0.2.0 - Production
2	PL/SQL Release 11.2.0.2.0 - Production
3	CORE11.2.0.2.0Production
4	TNS for 32-bit Windows: Version 11.2.0.2.0 - Production
5	NLSRTL Version 11.2.0.2.0 - Production

Figura 3-5: Versão do servidor de base de dados Oracle

No trabalho foi usada a versão do Oracle SQL Express Edition, apenas para testar comportamento da aplicação no acesso a dados presentes numa base de dados deste tipo.
A escolha desta versão do servidor de base de dados da Oracle deve-se ao facto ser uma versão gratuita e de não ser preciso uma versão muito elaborada uma vez que este SGBD só foi usado para efetuar testes.

3.2.6 Oracle VM VirtualBox

O Oracle VM VirtualBox é um software de virtualização desenvolvido pela empresa Innotek depois comprado pela Sun Microsystems que posteriormente foi comprada pela Oracle, cujo objetivo é criar ambientes para instalação de sistemas distintos. Ele permite a instalação e utilização de um sistema operativo dentro de outro, assim como seus respetivos softwares, como dois ou mais computadores independentes, mas compartilhando fisicamente o mesmo hardware (Figura 3-6).

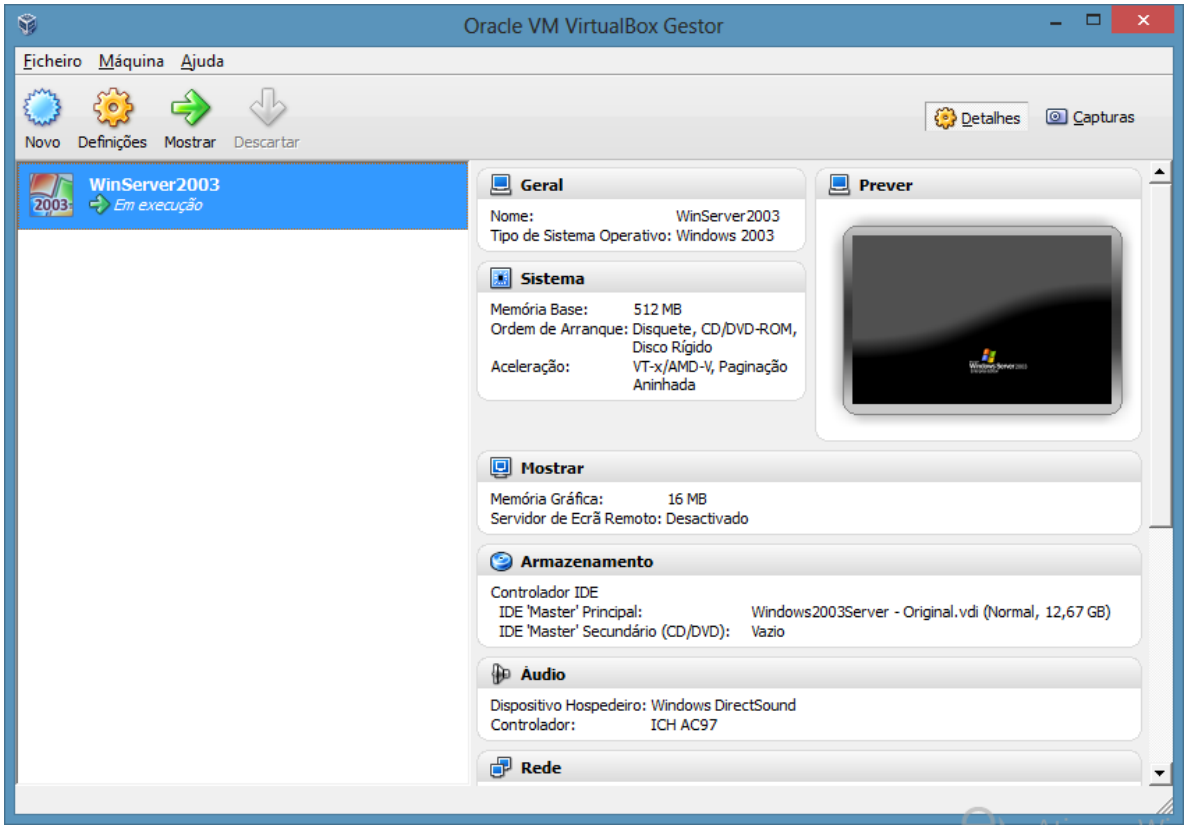


Figura 3-6: Oracle VM VirtualBox

No trabalho foi usado com uma instalação do sistema operativo Windows Server 2003 contendo os servidores de base de dados SQL Server e Oracle com os quais se efetuaram os testes.
A escolha deste software deve-se a facilidade de uso e a vasta experiencia com este software.

3.2.7 Microsoft Visual Studio 2010, C# 4.0

O Microsoft Visual Studio é um pacote de programas da Microsoft para o desenvolvimento de software, deste pacote estão linguagens de aplicação como o Visual Basic (VB), C, C++, C# (C Sharp) e J# (J Sharp). Mas também contem uma linguagem de desenvolvimento na área web, usando a plataforma do ASP.NET (Figura 3-7).

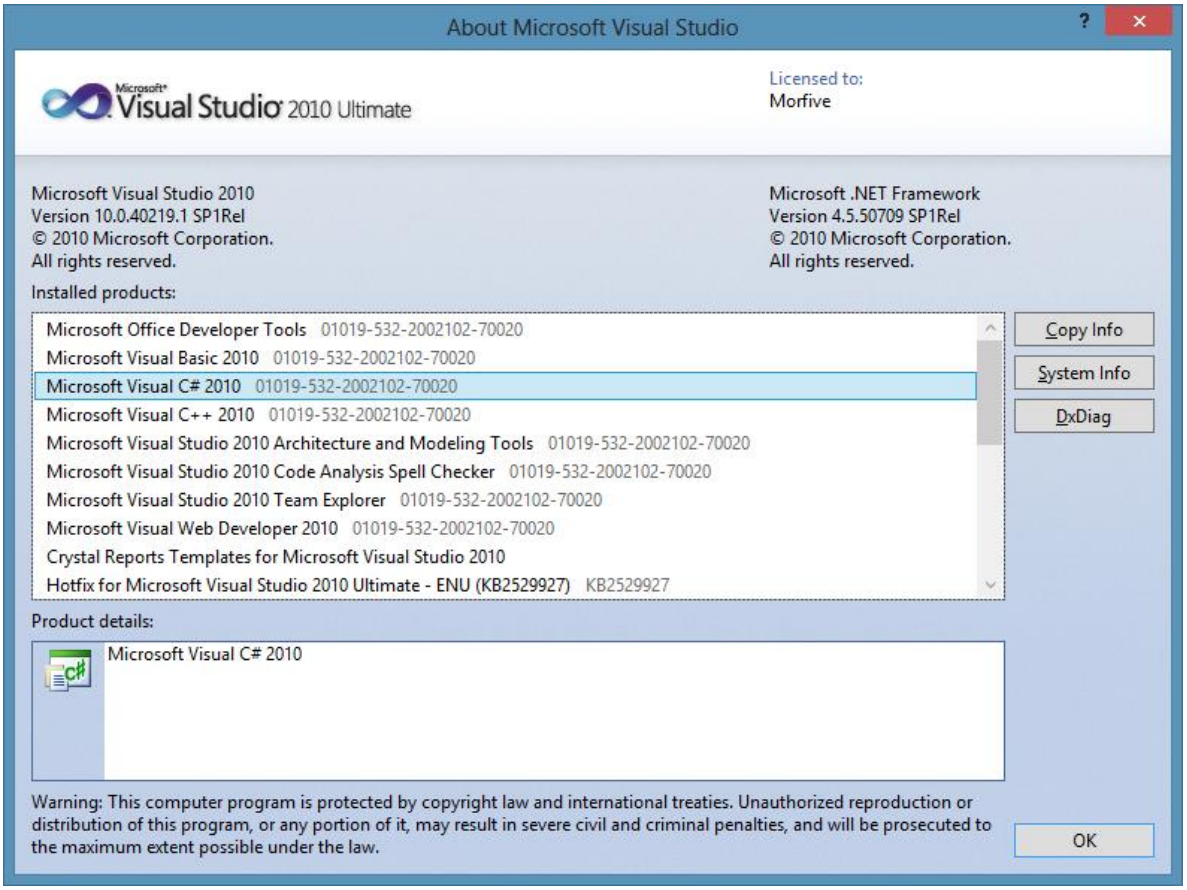


Figura 3-7: Microsoft Visual Studio 2010

Para o desenvolvimento da aplicação utilizou-se o Microsoft Visual Studio 2010 com a linguagem Visual C#.

A escolha desta linguagem deve-se ao facto de que é uma linguagem de programação orientada a objetos, o que torna mais fácil o aproveitamento de código e a implementação da arquitetura de software em três camadas, facilidade em implementar todas as funções desejadas bem como a facilidade de interligação com a AtiveX do equipamento e por fim devido a larga experiencia com a linguagem.

3.3 Estrutura da aplicação

A ideia principal é a separação da aplicação em módulos para simplificar a introdução de novos módulos. Assim a aplicação foi dividida em vários módulos:

- O módulo *layout*, onde estão presentes todas as funções necessárias para receber e mostrar dados ao utilizador,
- Os módulos SQLServer, SQLite, MySQL e Oracle que contêm todas as funções necessárias para a comunicação entre a aplicação e as respetivas bases de dados
- O módulo equipamento, que contem todas as funções necessárias para a comunicação com os equipamentos do fabricante Acronym (Figura 3-8).

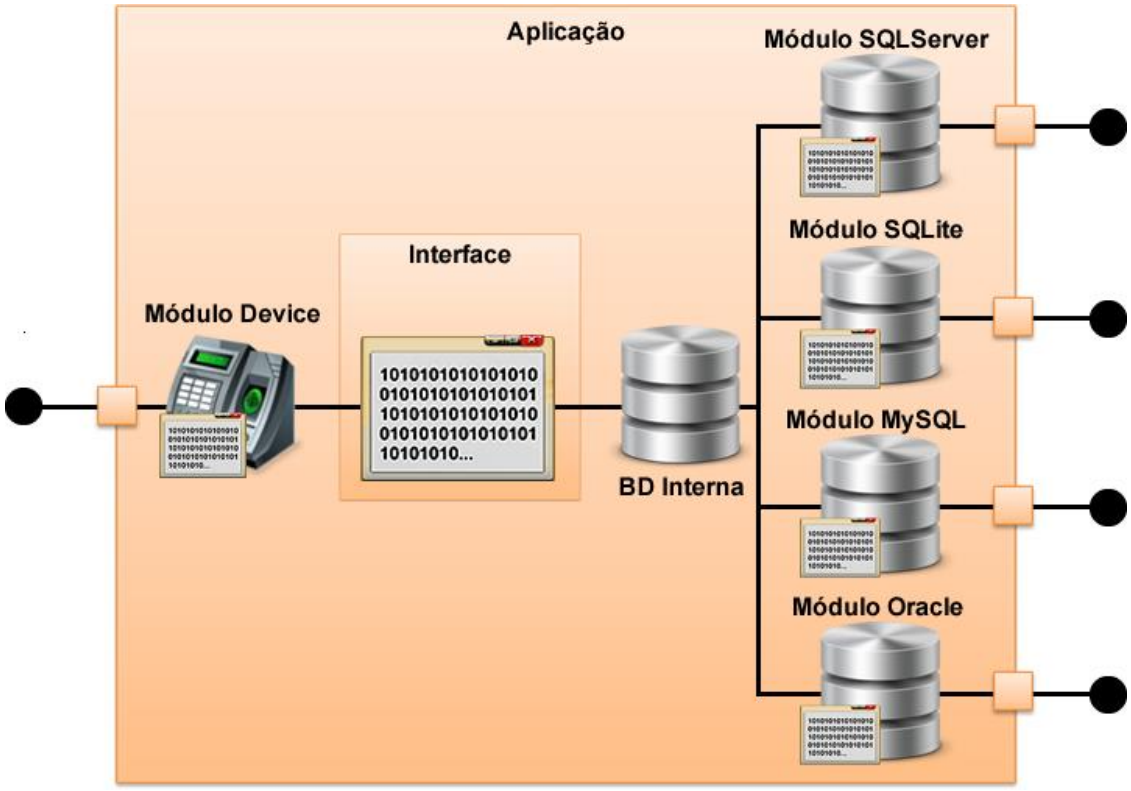


Figura 3-8: Estrutura da aplicação.

3.3.1 Base de dados interna

Para guardar todos os dados referentes à aplicação recorreu-se a uma base de dados em SQlite por ser fácil de usar e por não necessitar de servidor para funcionar. Na Figura 3-9 é possível ver o diagrama de entidade-relacionamento usado.

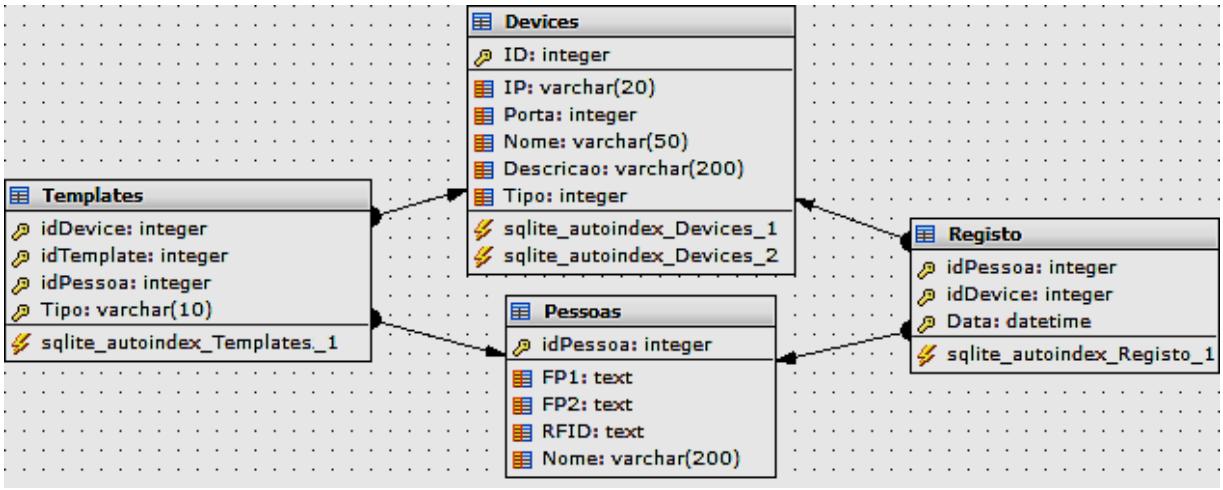


Figura 3-9: Diagrama de entidade-relacionamento da base de dados interna.

A tabela "*Templates*" guarda a lista de correspondências entre os *templates* biométricos guardados (impressões digitais) e cada equipamento. Uma vez que o equipamento identifica cada *template* com um número limitado pela quantidade de *templates* que pode guardar, que

no caso do equipamento utilizado para fazer os testes era 60000 *templates*, o id de cada *template* no equipamento é de 1 a 60000; no entanto, se tivermos utilizadores com ID´s superiores a associação não seria possível, mas, como nem todos os utilizadores tem acesso a todos os equipamentos, esta tabela guarda uma referência entre id do *template* e id do utilizador por equipamento.
Na tabela "Devices" são guardados todos os dados referentes aos equipamentos de autenticação ligados ao sistema.
Na tabela "Pessoas" são guardados os dados das pessoas que estão autorizadas a usar os equipamentos de identificação. Finalmente a tabela "Registo" guarda as passagens (entradas e saídas) de cada utilizador em cada equipamento que ao mesmo tempo representam os locais onde cada utilizador se identificou.

3.4 Arquitetura em 3 camadas

Esta arquitetura envolve a separação de diversas funcionalidades lógicas recorrendo à separação por camadas, com o objetivo de separar a lógica de apresentação, a lógica de negócio e a ligação com a base de dados na lógica de acesso a dados.
A separação em três camadas torna o sistema mais flexível de modo a que cada uma das camadas pode ser alterada separadamente. Qualquer alteração numa determinada camada não influencia as restantes desde que o mecanismo de comunicação entre elas permaneça inalterado.

3.4.1 Interface Layer

A Camada de apresentação é responsável pelas interações com o utilizador onde lhe são apresentados dados. Permite também a introdução de dados/ ações por parte deste.

3.4.2 Business Layer

Esta é a camada com a lógica de negócio. Esta camada implementa as regras do negócio, referentes aos comportamentos a assumir e validações a efetuar. Basicamente é a camada intermedia que liga a camada "*interface layer*" com a camada "*data access layer*", onde ficam as funções e regras de cada funcionalidade, isto é, se quisermos gravar uma pessoa a ordem é dada pela camada "*interface layer*" que será enviada à camada *business layer* para ser validada e reenviada para a base de dados correspondente que estará na camada "data *access layer*". Esta camada é responsável por manter os equipamentos em funcionamento e de reenviar os dados devidamente tratados provenientes do módulo do equipamento, da camada *data access Layer* para os módulos de base de dados da camada *data access Layer*.

3.4.3 Data Access Layer

Esta camada é primeiramente responsável pelos acessos aos dados. É sua responsabilidade garantir a perfeita comunicação com a base de dados através de consultas SQL e executando-as através de uma API. Neste projeto foram usados 4 tipos de bases de dados o Sqlite, o MySql, o SqlServer e o Oracle.

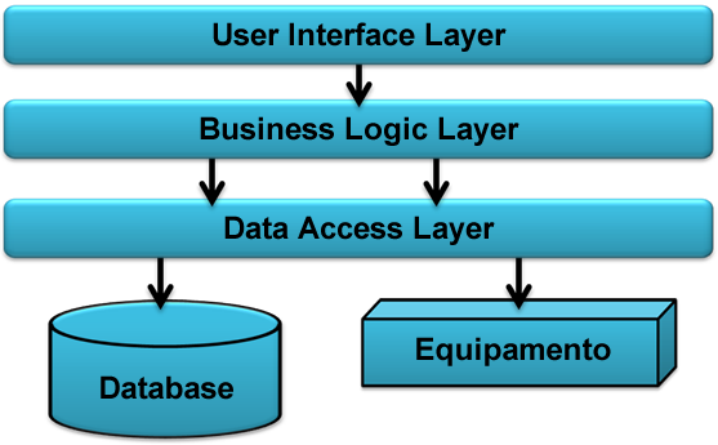


Figura 3-10: Arquitetura – 3 camadas.

Na arquitetura de 3 camadas (Figura 3-10) é de destacar que não existe comunicação direta entre a camada de apresentação e a camada de acesso a dados. Toda a informação passa pela camada que contém a lógica de negócio (funcionalidade/finalidade). Após implementação desta arquitetura, os benefícios tornam-se evidentes uma vez que o código torna-se partilhado e não duplicado. Muitos dos componentes da camada de apresentação podem aceder a mais que um componente e/ou partilhar o mesmo componente na camada de lógica de negócio. Por sua vez, todos os componentes da camada de lógica de negócio partilham o mesmo componente da camada de acesso a dados. Com a implementação desta arquitetura, o código torna-se mais gerido, permitindo a extensibilidade do mesmo. Muitos dos componentes da camada de apresentação podem aceder a mais que um componente e/ou partilhar o mesmo componente na camada de lógica de negócio. Por sua vez, todos os componentes da camada de lógica de negócio partilham o mesmo componente da camada de acesso a dados.
A grande vantagem de um sistema de 3 camadas é a possibilidade de alterar qualquer uma das camadas, sem a necessidade de alterar as restantes camadas, por exemplo: A alteração de um DBMS (*Data Base Management System:* conjunto de programas responsáveis pela gestão de uma base de dados) para outro, apenas necessita de alteração no componente existente na camada de acesso a dados; A alteração na Interface da aplicação, por exemplo de desktop para Web, apenas necessita de alteração nos componentes da camada de apresentação.

3.5 Implementação das 3 camadas

3.5.1 *Data Acess Layer*

Na camada de dados (Figura 3-11) efetua-se a conexão com os vários equipamentos e com as diferentes bases de dados.
Criaram-se as seguintes classes: “MySqlOUT”, “OracleOUT”, “SQLliteIN”, “SQLliteOUT”, “SqlServerOUT” e o controlo “ucEvo3Terminal”.

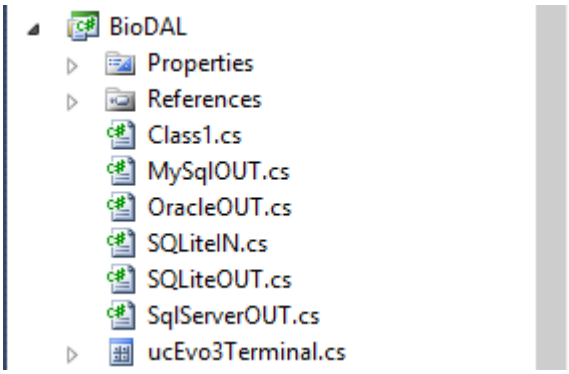


Figura 3-11: *Data Acess Layer*.

Na tabela seguinte apresentam-se as classes e os métodos que cada uma tem implementado.

Quadro 3-1: Métodos das classes bases de dados

	SQLlite IN	SQLlite OUT	MySql OUT	Oracle OUT	SqlServer OUT
Estado	X	X	X	X	X
opcLeitura	X	X	X	X	X
opcEscrita	X	X	X	X	X
ListaPessoas	X	X	X	X	X
GravarPessoa		X	X	X	X
DellPessoa	X	X	X	X	X
ListaRegistos	X	X	X	X	X
gravarRegisto	X	X	X	X	X
DellRegisto	X				
ListaTabelas		X	X	X	X
ListaCampos		X	X	X	X
listaDevices	X				
newDevice	X				
updateDevice	X				
DellDevice	X				
getDeviceID	X				
newUpTemplate	X				
DellTemplate	X				
DellTemplateByDevice	X				
DellTemplateByPessoa	X				
listTemplateByDevice	X				
getTemplateByPessoa	X				
newRegisto	X				

A seguir é explicado para que servem cada um dos métodos:

- O método "**Estado**": verifica o estado de uma base de dados externa, isto é, este método tenta abrir a base de dados (Figura 3-12) e se não ocorrer nenhum erro é porque a base de dados está "*online*"; se ocorrer algum erro é porque a base de dados está "*offline*";

```
sqlite_conn.Open(); // abre uma base de dados em Sqlite
Oracle_conn.Open(); // abre uma base de dados em Oracle
sqlServer_conn.Open(); // abre uma base de dados em Sql Server
mysql_conn.Open(); // abre uma base de dados em MySql
```

Figura 3-12: Instruções usadas para abrir as diversas bases de dados

- O método "**opcLeitura**" é responsável pelas operações de leitura das diversas bases de dados e podemos dizer que é muito semelhante de base de dados para base de dados. Assim sendo, a figura seguinte mostra as instruções mais importantes do código usado neste método para a base de dados interna (Figura 3-13).

```
sqlite_conn.Open(); //Abre a base de dados
DataTable DT = new DataTable(); //cria a tabela
//Cria o DataAdapter com "txtQuery" que contem as instruções SQL
SQLiteDataAdapter SQLiteDA = new SQLiteDataAdapter(txtQuery, sqlite_conn);
SQLiteDA.Fill(DT);  // coloca em DT os dados da pesquisa
sms = "";
return DT;
```

Figura 3-13: Excerto do código do método "opcLeitura" da base de dados interna.

- O método "**opcEscrita**" é responsável pelas operações de escrita das diversas bases de dados e podemos dizer que este método é muito semelhante de base de dados para base de dados por isso a figura seguinte mostra as instruções mais importantes do código usado neste método para a base de dados interna (Figura 3-14).

```
sqlite_conn.Open(); //Abre a base de dados
//Cria o comando com "txtQuery" que contem as instruções SQL
SQLiteCommand command = new SQLiteCommand(txtQuery, sqlite_conn);
command.ExecuteNonQuery(); //executa o comando e escreve na BD
command.Dispose(); //destroi o comando
sms = ""; //Menssagen a retornar
return true; // retorno "true" se não ocorreu nenhum erro
```

Figura 3-14: Excerto do código do método "opcEscrita" da base de dados interna.

- Os métodos "**ListaPessoas**" (Figura 3-15), "**listaDevices**", "**ListaRegisto**" (Figura 3-16) e "**listTemplateByDevice**" são semelhantes visando listar os equipamentos, as pessoas, os registos e os *templates*, respetivamente, no caso dos registos a lista depende da pesquisa nomeadamente dos parâmetros ("IDPessoa", "IDDevice", "Data" e "Hora");

```
string txtQuery = "SELECT * FROM Pessoas";
tabela = opcLeitura(ref sms, txtQuery);
```

Figura 3-15: Excerto do código do método "ListaPessoas "

```
string txtQuery = "SELECT * FROM vRegistos";
if (_IDDevice != ""){ //Se o parâmetro "_IDDevice" estiver preenchido adiciona-o a Query
    txtQuery += " WHERE (idDevice like '%" + _IDDevice + "%' OR nomeDevice like '%" + _IDDevice + "%')";
    nItens++; //Adiciona mais 1 ao numero de parâmetros
}
if (_IDPessoa != ""){ //Se o parâmetro "_IDPessoa" estiver preenchido adiciona-o a Query
    if (nItens == 0) { //Se o número de parâmetros for 0
        txtQuery += " WHERE (idPessoa like '%" + _IDPessoa + "%' OR nomePessoa like '%" + _IDPessoa + "%')";
        nItens++; //Adiciona mais 1 ao numero de parâmetros
    }else { //Se o número de parâmetros for diferente de 0
        txtQuery += " AND (idPessoa like '%" + _IDPessoa + "%' OR nomePessoa like '%" + _IDPessoa + "%')";
    }
}
```

Figura 3-16: Excerto do código do método "ListaRegisto"

- Os métodos "**GravarPessoa**" (Figura 3-17) e "**gravarRegisto**" são semelhantes pretendendo é adicionar ou alterar os dados das pessoas ou registos, à base de dados interna;

```
string find = "SELECT * FROM Pessoas WHERE idPessoa ='" + _IDPessoa + "'";
if (opcLeitura(ref sms, find).Rows.Count == 0) // Verifica se a pessoa existe
{ // Se a pessoa não existir adiciona a pessoa há base de dados
    string txtQuery = "INSERT INTO Pessoas (idPessoa, Nome, FP1, FP2, RFID) VALUES (" +
            _IDPessoa + ", '" + _NomePessoa + "', '" + _FP1 + "', '" + _FP2 + "', '" + _Rfid + "');";
    return opcEscrita(ref sms, txtQuery);
}else{ //Se a pessoa existir atualiza os dados da pessoa na base de dados
    string txtQuery = "UPDATE Pessoas SET Nome = '" + _NomePessoa + "', FP1 = '" + _FP1 + "', FP2 = '" +
            _FP2 + "', RFID = '" + _Rfid + "' WHERE idPessoa = " + _IDPessoa + ";";
    return opcEscrita(ref sms, txtQuery); //Chama o método para escrever na base de dados
}
```

Figura 3-17: Excerto do código do método "GravarPessoa"

- Os métodos "**newDevice**" (Figura 3-18) e "**newRegisto**" (Figura 3-19) são semelhantes e o principal objetivo é adicionar equipamentos ou registos, respetivamente à base de dados interna;

```
string txtQuery = "INSERT INTO Devices (Nome, IP, Porta, Descricao) VALUES " +
        "('" + _Nome + "', '" + _IP + "', " + _Porta + ", '" + _Descricao + "');";
```

Figura 3-18: Excerto do método "newDevice" - Query novo equipamento.

```
DateTime MyDate = DateTime.Now; //Cria a variável "MyData" com a data e hora atual
//Cria a variável "_Data" com a data e hora da variável "MyData" pré formatada
String _Data = MyDate.ToString("yyyy-MM-dd HH:mm:ss");
```

Figura 3-19: Excerto do método "newRegisto" - Adicionar a data e hora atual.

- O método "**newUpTemplate**" insere ou atualiza um *template* na base de dados interna, isto é o método recebe os dados referentes ao *template* e verifica se já se a pessoa já tem algum *template* gravado, caso não tenha a é gerado um numero aleatório entre 1 e 60000 que servirá como id do *template* e então grava na base de dados caso os dados já existam, caso tenha o id do *template* anterior é aproveitado para identificar o novo *template* também (Figura 3-30);

```
do{ //Executa enquanto o id gerado exista na BD
    Random _r = new Random(); // Cria uma variável randómica
    _IDTemplate = _r.Next(1, MaxTemplate + 1); // Gera um número aleatório entre 1 e o número máximo
    find3 = "SELECT * FROM Templates2 WHERE idTemplate = " + _IDTemplate + "";
} while (opcLeitura(ref sms, find3).Rows.Count != 0); // Procura na BD para ver se o novo ID existe
string txtQuery = "INSERT INTO Templates2 (idDevice, idTemplate, idPessoa, Tipo) VALUES (" + _IDDevice +
        ", " + _IDTemplate + ", " + _IDPessoa + ", '" + _Tipo + "');";
IDTemplate = _IDTemplate; // Atribui o novo id a variável de saida
return opcEscrita(ref sms, txtQuery); // Chama o método para gravar na BD
```

Figura 3-20: Excerto do código do método ” newUpTemplate” - Criar novo id *template*

- O método “**updateDevice**” (Figura 3-21) atualiza os dados de um equipamento na base de dados interna;

```
string txtQuery = "UPDATE Devices SET Nome = '" + _Nome + "', IP = '" + _IP +
    "', Porta = " + _Porta + ", Descricao = '" + _Descricao + "' WHERE ID = " + _ID + ";";
```

Figura 3-21: Excerto do código do método “updateDevice”

- Os métodos “**DellPessoa**” (Figura 3-22), “**DellDevice**”, “**DellRegisto**”, “**DellTemplate**”, “**DellTemplateByDevice**” e “**DellTemplateByPessoa**” são semelhantes, sendo que o principal objetivo é remover uma pessoa, um equipamento, um registo ou um *template* respetivamente, no caso dos dois últimos métodos também são removidos dados neste caso *templates* mas em vez de um de cada vez removo todos os *templates* de um certo equipamento ou pessoa respetivamente, da base de dados.

```
txtQuery = "DELETE FROM Pessoas WHERE idPessoa = " + _IDPessoa + "";
```

Figura 3-22: Excerto do código do método ” DellPessoa”

- O método “**ListaTabelas**” lista as tabelas existentes da base de dados correspondente (Figura 3-23);

```
//Sqlite
string txtQuery = "SELECT name FROM sqlite_master WHERE "+
        "type = 'table' AND name NOT LIKE 'sqlite_%'";
//Oracle
string txtQuery = "select table_name from user_tables";
//SQL Server
string txtQuery = "SELECT name FROM sys.Tables";
//MySql
string txtQuery = "SHOW TABLES FROM " + BDNome + "";
```

Figura 3-23: Instruções para listar tabelas para cada BD

- O método “**ListaCampos**” lista os campos da tabela e base de dados correspondentes (Figura 3-24);

```
//Sqlite
string txtQuery = "pragma table_info(" + _tabela + ")";
//Oracle
string txtQuery = "SELECT column_name FROM cols WHERE "+
    "table_name = '" + _tabela + "'";
//SQL Server
string txtQuery = "SELECT name FROM sys.columns WHERE "+
    " OBJECT_NAME(object_id) = '" + _tabela + "'";
//MySql
string txtQuery = "SHOW COLUMNS FROM " + _tabela + "";
```

Figura 3-24:Instruções para listar campos de uma dada tabela para cada BD

- Os métodos "**getDeviceID**" e "**getTemplateByPessoa**" são semelhantes, mas o principal objetivo destes métodos é o mesmo, devolver um id, o id do equipamento com um determinado ip ou o id da *template* com um determinado id da pessoa;

A seguinte são apresentam-se os métodos que foram implementados para o equipamento OutLock 3 Bio Online:

- O evento "**evo3_BoardOpen**" é um evento responsável por receber o ip dos equipamentos cuja conexão foi estabelecida (Figura 3-25). Assim que a conexão com o equipamento é estabelecida, este método recebe o ip e verifica de o ip pertence à lista de equipamentos ligados e caso não pertença adiciona-o e envia o ip e o número de *templates* gravadas no equipamento para a camada BL através do evento "evDeviceON".

```
private void evo3_BoardOpen(object sender, AxIOBCTRLLib._DIOBCtrlEvents_BoardOpenEvent e){
    lock (LockBoardOpen){ //Impede que o processo seja acedido novamente enquanto não terminar
        string IP = e.szIPAddress.ToString();
        bool Existe = false;
        foreach (string MyDeviceIP in Evo3DeviceLigado){
            if (MyDeviceIP == IP){ // verifica se o ip já está na lista
                Existe = true;
                break;
            }
        }
        if (!Existe){ // se o equipamento não estiver ocupado faz
            Evo3OnOffBio(IP, false); //Ativar Sensor Biometrico
            Evo3DeviceLigado.Add(IP); // Adiciona o IP do equipamento há lista de equipamentos ligados
            evo3.ClearScreen(IP); //Limpa o ecra
            evo3.RefreshScreen(IP); // atualiza device
            Evo3WriteText(6, 4, IP, "A ligar..."); //envia texto
            Evo3Setup(IP); //Setup, Ativar RFID
            Evo3OnOffLuz(IP, true); // liga a luz de fundo
            evo3.RefreshScreen(IP); // refresca o ecra com o novo texto
            int ntemplates = evo3.GetNumberTemplates(IP);
            evDeviceON("Evo3", IP, ntemplates);
            Evo3beep(IP); // Aviso sonoro
        }
    }
}
```

Figura 3-25: Código do evento " evo3_BoardOpen "

- O evento "**evo3_BoardClosed**" é um evento responsável por receber o ip dos equipamentos qua acabaram de ser desligados do sistema, Assim que a conexão com o equipamento é perdida, este método recebe o seu ip e altera o estado na lista de equipamentos;
- O evento "**evo3_Reader**" é um evento responsável por receber o ip e o código das *tags* RFID, isto é sempre é lida um *tag* RFID pelo leitor este método recebe o ip do equipamento e verifica de o ip esta na lista de equipamentos ocupados e caso não esteja adiciona a lista de ocupados e verifica se o ip pertence a algum equipamento em modo de recolha, caso esteja envia o ip e o RFID para a camada BL, através do evento "evDeviceRFID", para que o RFID seja adicionado a lista de novos RFID's caso contrario envia ip e RFID para a camada BL, através do evento "evDeviceRFID" para ver se existe algum utilizador com o RFID lido (Figura 3-26);

```
bool RFIDOcupado = true;
foreach (string myDevicesIP in Evo3RFIDOcupado){
    if (myDevicesIP == IP){ // verifica se o ip já está na lista
        RFIDOcupado = false;
        break;
    }
}
if (RFIDOcupado){ // se o equipamento não estiver ocupado faz
    Evo3RFIDOcupado.Add(IP); // Adiciona o IP do equipamento há lista de equipamentos ocupados
    Evo3beep(IP); // Aviso sonoro
    Evo3OnOffLuz(IP, true); // liga a luz de fundo
    if (IPnewRFID == IP){ //Verifica se o IP pertence a um equipamento em modo de recolha
        evDeviceRFID("Evo3", IP, RFID); //envia IP e RFID para a camada BL
        Evo3RFIDOcupado.Remove(IP); //Remove o IP do equipamento há lista de equipamentos ocupados
    }else{
        evo3.ClearScreen(IP); //Limpa o ecra
        evo3.RefreshScreen(IP); // atualiza device
        Evo3WriteText(5, 2, IP, "A processar..."); //envia texto
        evDeviceRFID("Evo3", IP, RFID); //envia IP e RFID para a camada BL
        Task.Factory.StartNew(() => {
            Thread.Sleep(2500); //Aguarda 2500ms
            Evo3RFIDOcupado.Remove(IP); //Remove o IP do equipamento há lista de equipamentos ocupados
        });
```

Figura 3-26: Excerto do código do evento " evo3_Reader "

- O evento "**evo3_Bio**" é um evento responsável por receber o ip e id *template*, isto é sempre que é lida uma impressão digital pelo leitor, este método (Figura 3-27) recebe o ip do equipamento que é comprado com a lista de equipamentos para saber se o equipamento está ou não ocupado e no caso de não estar ocupado, verifica se o id da *template*, é valido, se for valido, envia o id da *template* para a camada BL, através do evento "evDeviceBio";

```
bool BioOcupado = true;
foreach (string myDevices in Evo3BioOcupado){
    if (myDevices == IP){ // verifica se o ip já está na lista
        BioOcupado = false;
        break;
    }
}
if (BioOcupado){ // se o equipamento não estiver ocupado faz
    lock (LockBio){ //Bloqueia o processo enquanto não terminar
        Evo3BioOcupado.Add(IP); // Adiciona o IP do equipamento há lista de equipamentos ocupados
        Evo3beep(IP); // Aviso sonoro
        Evo3OnOffLuz(IP, true); // liga a luz de fundo
        evo3.ClearScreen(IP); //Limpa o ecra
        evo3.RefreshScreen(IP); // atualiza device
        if (IDtemplate == 0){ //Se o template não for conhecido
            Evo3WriteText(4, 4, IP, "Acesso negado!");
            evDeviceBio("Evo3", IP, 0);
            Thread.Sleep(2000); //Aguarda 2000ms
            EstadoSMS(IP);
            Evo3BioOcupado.Remove(IP); //Remove o IP do equipamento há lista de equipamentos ocupados
        }else{
            Evo3WriteText(5, 2, IP, "A processar..."); //envia texto
            evDeviceBio("Evo3", IP, IDtemplate);
            Task.Factory.StartNew(() => { MessageBox.Show("ucEVO3Terminal_Registando..."); });
            Thread.Sleep(4000); //Aguarda 4000ms
            Evo3BioOcupado.Remove(IP); //Remove o IP do equipamento há lista de equipamentos ocupados
```

Figura 3-27: Excerto do código do evento "evo3_Bio"

- O evento "**evo3_BioNew**" é um evento responsável por receber as novas impressões digitais, isto é sempre que um equipamento é colocado em modo de recolha de impressões digitais as impressões digitais lidas são recebidas por este método que por sua vez os envia as *templates* recolhidas, para a camada BL, através do evento "evDeviceBioNew".

A função seguinte é a mais importante deste evento e é responsável por converter o *template* de *byte array* para *string* e indicar se o *template* é valido ou não (Figura 3-28)

```
int nIDTemplate = 1;
System.Byte[] dBytes = new System.Byte[384]; //byte[384] variavel para guardar template
dBytes = (System.Byte[])evo3.GetNewTemplate2(IP, ref nIDTemplate); //recolhe template do device
string hex = BitConverter.ToString(dBytes); //Converte byte para string em hexadecimal
string templateTemp = hex.Replace("-", ""); //Converte byte para string em hexadecimal
Evo3OnOffBio(IP, false); //Desativa Sensor Biometrico
if (nIDTemplate != 0){ // Se a template for valida
    Evo3WriteText(6, 2, IP, "Gravado..."); //envia texto para o equipamento
    Evo3WriteText(1, 5, IP, "Pode Retirar o dedo!"); //envia texto para o equipamento
    evDeviceBioNew("Evo3", IP, templateTemp); //Envia dados para a camada BL
}else{ //se a template não for valida
    Evo3WriteText(1, 1, IP, "ERRO de aquisicao"); //envia texto para o equipamento
    evDeviceBioNew("Evo3", IP, ""); //Envia dados para a camada BL
}
```

Figura 3-28: Função que verifica e converte o *template* de *byte array* para *string*

- O método "**Evo3getEstado**" é responsável por verificar o estado dos equipamentos;
- O método "**Evo3LigarDevice**" é responsável por ligar cada equipamento;
- O método "**Evo3DesligarDevice**" é responsável por desligar cada equipamento;
- O método "**Evo3VerNTemplates**" é responsável por ver quantos *templates* estão gravados no equipamento;

- O método "**Evo3DellAllTemplates**" é responsável por remover todos os *templates* de um equipamento;
- O método "**Evo3newTemplate**" ativa o modo de recolha de impressões digitais através da instrução seguinte (Figura 3-29);

```
return evo3.Enroll(IP, 60000); //Ativa o mode re recolha de impressões digitais
```

Figura 3-29: instrução para ativar o modo de recolha de impressões digitais

- O método "**sendTemplate**" é o método responsável por enviar a lista de *templates* para os equipamentos, este método recebe o ip do equipamento, o id do *template* e a *templare* no formato de *string*, depois verifica se o *template* é valida, se for valida, converte-a de *string* para *byte array*, que é o formato do equipamento, depois de convertida, a *template* é enviada para o equipamento (Figura 3-30).

```
public bool sendTemplate(string _IP, int _IDTemplate, string _TemplateSend){
    lock (LockSendTemplate){ //Impede que o processo seja acedido novamente enquanto não terminar
        bool Operacao = true;
        if (_TemplateSend != ""){ //Verifica se o template é valido
            //Converte o template de string para byte array
            System.Byte[] byteTemplate = new System.Byte[384];
            for (int x = 0; x < 384; ++x) { byteTemplate[x] = Convert.ToByte(_TemplateSend.Substring(x * 2, 2), 16); }
            //envia o template convertido para o equipamento
            if (Evo3SendTemplate(_IP, _IDTemplate, byteTemplate, "FLA") != 0){ Operacao = false; }
            Evo3OnOffBio(_IP, true); //Ativar Sensor Biometrico
        }
        return Operacao;
    }
}
```

Figura 3-30: Código do método" sendTemplate"

- O método "**NewRFID**" ativa o modo de recolha de RFID;
- O método "**StopNewRFID**" desativa o modo de recolha de RFID;
- O método "**Resposta**" envia um texto para o equipamento, proveniente da camada BL
- Os eventos "**evDeviceON**" (Figura 3-31), "**evDeviceOFF**", "**evDeviceRFID**", "**evDeviceBio**" e "**evDeviceBioNew**" são semelhantes, mas o principal objetivo destes eventos é o mesmo, enviar dados para a camada BL sempre quem um evento ocorra;

```
//Cria um um Delegate
public delegate void EventoDeviceON(string Fabricante, string ip, int nTemplates);
public event EventoDeviceON evDeviceON;   //Cria um evento
```

Figura 3-31: Declaração do evento " evDeviceON "

3.5.2 *Business Layer*

Nesta camada define-se a utilidade e finalidade dos dados (Figura 3-32).

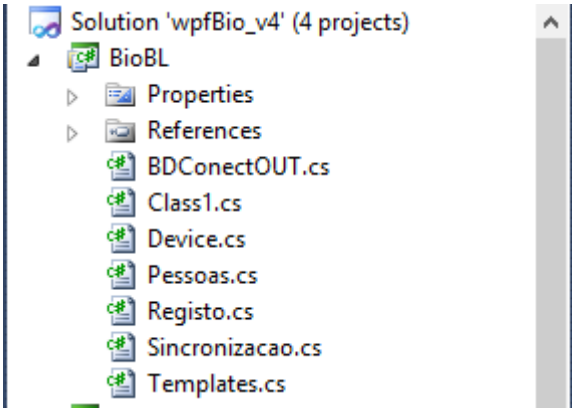


Figura 3-32: *Business Layer*.

Criaram-se as seguintes classes: "Device", "Pessoas", "Registro", "Templates", "BDConectOUT" e "Sincronizacao":

- A classe "Device" é responsável pelas funcionalidade de controlo dos equipamentos e pelas funcionalidades referentes à tabela equipamentos na base de dados interna;
- A classe "Pessoas" é responsável pelas funcionalidades referentes as pessoas da tabela da base de dados interna mas também externa;
- A classe "Registo" é responsável pelas funcionalidades referentes aos registos da tabela da base de dados interna mas também externa;
- A classe "BDConectOUT" é um objeto que que serve para guardar os dados da conexão com as bases de dados externas;
- A classe Sincronização é responsável por verificar se os registos estão repetidos e criar uma lista de registos que será gravada nas bases de dados interna e ou nas bases de dados externas.

Estas classes são responsáveis por interligar o *layout* e a parte técnica da comunicação com os vários tipos de bases de dados e equipamentos.

Na tabela seguinte apresentam-se as classes e os métodos que cada uma tem implementado.

Quadro 3-2: Métodos das classes bases de dados

	Device	Pessoas	Registro	Templates
StartStatus	X			
ReloadStatusDevice	X			
NewRFID	X			
StopRFID	X			
EnviarTemplate	X			
newTemplate	X			
DellAllTemplates	X			
VerNtemplates	X			
EnviarALLTemplates	X			
Evo3Terminal_evDeviceBioNew	X			
Evo3Terminal_evDeviceBio	X			
Evo3Terminal_evDeviceRFID	X			
Evo3Terminal_evDeviceOFF	X			

Evo3Terminal_evDeviceON	X			
listarDevices	X			
DellDevice	X			
EditDevice	X			
addDevice	X			
GravarPessoa		X		
ExisteRFID		X		
GravarTemplate		X		
DellPessoa		X		
listarPessoas		X		
listarTabelasOUT		X		
listarCamposOUT		X		
listarPessoasOUT		X		
sincronizarPessoas		X		
GravarPessoaOUT		X		
newRegisto			X	
DellRegisto			X	
listarRegisto			X	
listarRegistoOUT			X	
ExportarRegisto			X	
GravarRegistoOUT			X	
DellTemplate				X
DellAllTemplateByPessoa				X
listarTemplatesByDevice				X

A seguir é explicado para que serve cada método:

- O método "**StartStatus**" é responsável por manter os equipamentos ligados e tenter ligar os equipamentos desligados.
- O método "**ReloadStatusDevice**" auxilia o método anterior e altera o estado nos equipamentos na lista isto é sempre que um equipamento é ligado ou desligado este método coloca "*Online*" ou "*Offline*" no *layout* do equipamento respetivo;
- O método "**newRFID**" envia um pedido à camada DAL para que o equipamento seja colocado em modo de recolha de RFID's;
- O método "**stopRFID**" envia um pedido à camada DAL para que o equipamento seja retirado do modo de recolha de RFID's;
- Os métodos "**EnviarTemplate**" (Figura 3-33) e "**EnviarALLTemplates**" são semelhantes, mas o principal objetivo destes métodos é enviar *templates* para o equipamento a única diferença é que o segundo envia todas as *templates* e o primeiro envia um de cada vez.

```
foreach (Device myDevice in lstDevice){ // Percorre a lista de equipamentos
    if (myDevice.Id == IDDevice){ //Verifica se o equipamento é o procurado
        if (myDevice.Estado == "Online"){ // Verifica se o equipamento esta ONLINE
            pessoa.listarPessoas(ref sms); //Chama o metodo listar pessoas
            foreach (Pessoas myPessoa in pessoa.ListPessoasIN){ // Percorre a lista de Pessoas
                if (myPessoa.Id == PessoaID){ //Verifica se a pessoa é a procurada
                    string TemplateSend = "";
                    switch(Tipo){ // verifica qual é o tipo da template
                        case "FP1": TemplateSend = myPessoa.FP1; break;
                        case "FP2": TemplateSend = myPessoa.FP2; break;
                    }
                    if (TemplateSend != ""){ // Caso a template seja vasia
                        System.Byte[] byteTemplate = new System.Byte[384]; // Cria um array de bytes
                        bool templateValida = true;
                        for (int x = 0; x < 384; ++x){ //converte a template de string para byte array
                            try{ //converte a template de string para byte array
                                byteTemplate[x] = Convert.ToByte(TemplateSend.Substring(x * 2, 2), 16);
                            }catch (Exception){ templateValida = false; break; } // Erro
                        }
                        if (templateValida){ // se a template for valida
                            //Grava a template na tabela de templates(associações)
                            if (template.addEditTemplate(ref sms, ref IDTemplate, IDDevice, PessoaID, Tipo, 60000)){
                                //Envia a template para a BD
                                return Evo3Terminal.sendTemplate(myDevice.Ip, IDTemplate, TemplateSend);
                            }
```

Figura 3-33: Excerto do código do método" EnviarTemplate"

- O método "**newTemplate**" envia um pedido à camada DAL para que o equipamento entre em modo de recolha e aguarda pela recolha de *template*.
- O método "**VerNtemplates**" envia um pedido à camada DAL para que seja consultado o número de *templates* gravadas num dado equipamento.
- O método "**Evo3Terminal_evDeviceBioNew**" recebe os novos *templates* do evento "evDeviceBioNew" da camada DAL, isto é sempre que uma pessoa regista uma nova *template* (impressão digital), esse *template* é recebido na camada DAL que por sua vez o envia para este método na camada BL, que verifica se os *templates* são validados, caso sejam grava o novo *template* na lista de *templates* e mostra uma pequena mensagem no log técnico indicando se a operação foi bem-sucedida ou não (Figura 3-34).

```
foreach (Device myDevice in lstDevice){ //percorre a lista de equipamentos
    if (myDevice.Ip == ip){ //verifica se o equipamento é o procurado
        if (Template != ""){ // se o template for valido
            template.Conteudo = Template; // Adiciona o template a lista
            Evo3NewBio = false;
            templateOK = true;
            ...
            break;
        }else{ // se o template for Invalido
            Evo3NewBio = false;
            templateOK = false;
            ...
            break;
        }
```

Figura 3-34: Excerto do código do método "Evo3Terminal_evDeviceBioNew"

- O método "**Evo3Terminal_evDeviceBio**" recebe os *templates* do evento "evDeviceBio" da camada DAL, isto é sempre que uma pessoa faz a leitura da impressão digital, essa leitura é recebida na camada DAL que por sua vez envia o id

da *template* e o ip do equipamento para este método na camada BL, ou seja este método recebe o ip do equipamento e verifica se está na lista, caso esteja verifica se o *template* pertence a alguém, caso pertença envia um pedido à camada DAL para que seja gravado um novo registo de passagem dessa pessoa, e envia um pedido para a camada DAL para que seja enviada uma mensagem para o equipamento autorizando o aceso, caso contrário envia um pedido à camada DAL para que seja enviada a mensagem de acesso negado (Figura 3-35).

```
foreach (Device myDevice in lstDevice){ //percorre a lista de equipamentos
    if (myDevice.Ip == ip){ //Verifica se o equipamento é o procurado
        string msg = "";
        string sms = "";
        bool UserValido = false;
        //listar todos os templates do equipamento "Id"
        template.listarTemplatesByDevice(ref sms, myDevice.Id);
        if (IDtemplate != 0){
            //percorre a lista de templates
            foreach (Templates myTemplate in template.ListTemplates){
                if (myTemplate.Id == IDtemplate){ //Verifica se o template é o procurado
                    registo.PessoaID = myTemplate.IdPessoa; //copia o id da pessoa para o registo
                    registo.DeviceID = myDevice.Id; //copia o id do equipamento para o registo
                    registo.newRegisto(ref sms); //Grava o registo na BD
                    UserValido = true;
                    Evo3Terminal.Resposta(myDevice.Ip, 7, 4, "Bem vindo"); //Envia uma resposta..
                    ...
                    break;
                }
            }
            if (!UserValido){ //se o utilisador não for valido
                Evo3Terminal.Resposta(myDevice.Ip, 4, 4, "Acesso negado!"); //Envia uma resposta..
                ...
            }
        }else{ //se o template não for valido
        ...
```

Figura 3-35: Excerto do código do método “Evo3Terminal_evDeviceBio”

- O método “**Evo3Terminal_evDeviceRFID**” recebe os códigos RFID do evento “evDeviceRFID” da camada DAL, isto é sempre que uma pessoa passa o cartão no leitor, o código RFID é recebido na camada DAL que por sua vez envia o código RFID e o ip do equipamento para este método na camada BL, ou seja este método recebe o ip do equipamento verifica se está na lista, caso esteja verifica se o código RFID pertence a alguém, caso pertença envia um pedido para a camada DAL para que seja gravado um novo registo de passagem dessa pessoa, e envia um pedido à camada DAL para que seja enviada uma mensagem para o equipamento autorizando o aceso, caso contrário envia um pedido à camada DAL para que seja enviada a mensagem de acesso negado (Figura 3-36).

```
foreach (Device myDevice in lstDevice){ //percorre a lista de equipamentos
    if (myDevice.Ip == ip){ //Verifica se o equipamento é o procurado
        string msg = "";
        string sms = "";
        bool UserValido = false;
        if (IPNovaRFID == ip){ //Se o equipamento está em mode de recolha
            evDeviceNewRFID(ip, rfid); // Envia dados para a camada BL
            ...
        }else{ //Se o equipamento não está no modo de recolha
            pessoa.listarPessoas(ref sms); //Lista as pessoas
            //Percorre a lista de Pessoas
            foreach (Pessoas myPessoa in pessoa.ListPessoasIN){
                if (myPessoa.RFID == rfid){ //Verifica se o RFID é o procurado
                    registo.PessoaID = myPessoa.Id; //copia o id da pessoa para o registo
                    registo.DeviceID = myDevice.Id; //copia o id do equipamento para o registo
                    registo.newRegisto(ref sms); // Grava o registo na BD
                    UserValido = true;
                    break;
                }
            }
            if (UserValido){ //Se o utilizador for valido
                Evo3Terminal.Resposta(myDevice.Ip, 7, 4, "Bem vindo");
                ...
            }else{ //Se o utilizador for invalido
                Evo3Terminal.Resposta(myDevice.Ip, 4, 4, "Acesso negado!");
                ...
            }
```

Figura 3-36: Excerto do código do método "Evo3Terminal_evDeviceRFID"

- O método "**Evo3Terminal_evDeviceOFF**" recebe os ip dos equipamentos recebidos pelo evento "evDeviceOFF" da camada DAL, alterar o estado desses equipamentos para "*Offline*";
- O método "**Evo3Terminal_evDeviceON**" recebe os IP's dos equipamentos e o número de *templates* dos equipamentos recebidos pelo evento "evDeviceON" da camada DAL, e depois envia esses IP's e o número de *templates* que esse equipamento tem guardado para este método na camada BL, ou seja este método verifica se o equipamento já está *online*, caso não esteja altera o estado para "*Online*" e verifica se o número de *templates* guardado no equipamento corresponde ao número de *templates* guardado na base de dado, caso não correspondam é chamado o método "EnviarALLTemplates" para que sejam enviadas todos os *templates* pertencentes a esse equipamento;
- Os métodos "**listarPessoas**" (Figura 3-37), "**listarDevices**", "**listarRegisto**", "**listarPessoasOUT**", "**listarRegistoOUT**" e "**listarTemplatesByDevice**" são semelhantes, sendo que o principal objetivo é listar as pessoas da base de dados interna, os equipamentos, os registos da base de dados interna, as pessoas da base de dados externa, os registos da base de dados externa e os *templates* respetivamente. Estes métodos enviam um pedido à camada DAL para que este consulte as tabelas respetivas e adiciona esses dados às listas respetivas.

```
DataTable tabela = new DataTable();  //cria a tabela
BioDAL.SQLiteIN BDPessoa = new BioDAL.SQLiteIN(); // Chamada da camada BL
BDPessoa.listaPessoas(ref tabela, sms); //Pesquisa as pessoas na base de dados da camada DAL
lstPessoasIN.Clear(); //limpar a lista de pessoas
foreach (DataRow rDevice in tabela.Rows){ // percorre a tabela
    Pessoas pessoaItem = new Pessoas(); //Cria um item da pessoa
    pessoaItem.PessoaId = Convert.ToInt32(rDevice["idPessoa"]); //Copia para o item o id da pessoa
    pessoaItem.PessoaNome = rDevice["Nome"].ToString(); //Copia para o item o nome da pessoa
    pessoaItem.PessoaFP1 = rDevice["FP1"].ToString(); //Copia para o item o template do dedo 1
    pessoaItem.PessoaFP2 = rDevice["FP2"].ToString(); //Copia para o item o template de dedo 2
    pessoaItem.PessoaRFID = rDevice["RFID"].ToString(); //Copia para o item o rfid
    lstPessoasIN.Add(pessoaItem); //adiciona o item a lista
}
```

Figura 3-37: Excerto do código do método "listarPessoas"

- Os métodos "**listarTabelasOUT**" e "**listarCamposOUT**" são semelhantes no seu funcionamento, a única diferença é que o primeiro lista os nomes das tabelas de uma base de dados externa o segundo lista o nome dos campos de uma dada tabela de uma base de dados externa;
- Os métodos "**DellPessoa**", "**DellDevice**", "**DellRegisto**", "**DellTemplate**" e "**DellAllTemplateByPessoa**" são semelhantes e o principal objetivo destes métodos é o mesmo, remover uma pessoa, um equipamento, um registo ou um *template*, respetivamente, mas o ultimo método, ao contrário dos outros, que só removem um item de cada vez, remove todos os *templates* de uma pessoa;
- O método "**EditDevice**" envia um pedido que será processado pela camada DAL para que os dados antigos, de um equipamento, sejam substituídos por novos dados e finalmente envia novo pedido a essa mesma camada DAL para que o equipamento seja reiniciado;
- O método "**addDevice**" faz um pedido à camada DAL para que o novo equipamento seja adicionado na base de dados interna e por fim envia um pedido a camada DAL para que o novo equipamento seja ligado;
- Os métodos "**GravarPessoa**" (Figura 3-38), "**GravarTemplate**", "**GravarPessoaOUT**" e "**GravarRegistoOUT**" são semelhantes e o principal objetivo destes métodos é adicionar ou alterar pessoas internas, *templates*, pessoas externas ou registos externos. Estes métodos enviam um pedido à camada DAL para que a pessoa, *template* ou registo, sejam adicionados ou alterados na base de dados interna e/ou externa;

```
public bool GravarPessoa(ref string sms)
{
    BioDAL.SQLiteIN BDPessoa = new BioDAL.SQLiteIN();
    return BDPessoa.GravarPessoa(ref sms, PessoaId.ToString(),
                PessoaNome, PessoaFP1, PessoaFP2, PessoaRFID);
}
```

Figura 3-38: Código do método "GravarPessoa"

- O método "**ExisteRFID**" verifica se o código RFID pertence ou não a alguém;

- O método "**sincronizarPessoas**" recebe os dados da conexão e a operação a executar e depois, se a opção for importar, percorre a lista de pessoas a sincronizar e chama o método "GravarPessoa" que por sua vez envia um pedido para a camada DAL por cada pessoa a gravar na base de dados interna. Se a opção for exportar, percorre a lista de pessoas a sincronizar e chama o método "GravarPessoaOUT" que por sua vez envia novo pedido à camada DAL por cada pessoa a gravar na base de dados externa. Finalmente se a opção for sincronizar, percorre a lista de pessoas a sincronizar e chama os métodos "GravarPessoa" e "GravarPessoaOUT" por cada pessoa a gravar na base de dados interna e na base de dados externa, respetivamente (Figura 3-39);

```
switch(operacao){
    case"IMPORTAR": //// IMPORTAÇÃO ////////////////////////////////////////////
        foreach (Pessoas mySinc in ListPessoasIN){ // Percorres a lista de pessoas a importar
            if (!BDPessoa.GravarPessoa(ref sms, mySinc.Id.ToString(), mySinc.Nome, mySinc.FP1,
                                       mySinc.FP2, mySinc.RFID)){ return false; } // Chama o metodo...
        }   //.."GravarPessoa"  da camada DAL para gravar as pessoas na base de dados externa
        return true;
    case"EXPORTAR": //// EXPORTAÇÃO ////////////////////////////////////////////
        foreach (Pessoas mySinc in lstPessoasOUT){ // Percorres a lista de pessoas a exportar
            if (!GravarPessoaOUT(ref sms, bdConect, mySinc.Id, mySinc.Nome, mySinc.RFID,
                mySinc.FP1, mySinc.FP2)) { return false; } // Chama o metodo...
        }                       //.."GravarPessoaOUT" para gravar as pessoas na base de dados
        return true;
    case"SINCRONIZACAO": //// SICRONIZAÇÃO ////////////////////////////////////////
        foreach (Pessoas mySinc in lstPessoasIN){ // Percorres a lista de pessoas a sincronizar
            if (BDPessoa.GravarPessoa(ref sms, mySinc.Id.ToString(), mySinc.Nome, mySinc.FP1,
                                      mySinc.FP2, mySinc.RFID)){ // se não ocoreram erros ao gavar..
                                      //..pessoas na base de dados interna
                if (!GravarPessoaOUT(ref sms, bdConect, mySinc.Id, mySinc.Nome, mySinc.RFID,
                    mySinc.FP1, mySinc.FP2)) { return false; } // Chama o metodo...
                    //.."GravarPessoaOUT" para gravar as pessoas na base de dados
            }else { return false; } // se ocoreram erros
        }
    return true;
```

Figura 3-39: Excerto do código do método "sincronizarPessoas"

- O método "**newRegisto**" recebe os dados do registo e envia um pedido à camada DAL para que o novo registo seja adicionado à base de dados interna;
- O método "**ExportarRegisto**" recebe os dados da conexão e percorre a lista de registos a exportar e chama o método "GravarRegistoOUT" por cada registo para gravar os dados do registo na base de dados externa correspondente (Figura 3-40);

```
public bool ExportarRegisto(ref string sms, BDConectOUT bdConect)
{
    BioDAL.SQLiteIN BDRegisto = new BioDAL.SQLiteIN();
    foreach (Registo mySinc in lstRegistoOUT){
       if (!GravarRegistoOUT(ref sms, bdConect, mySinc.Data, mySinc.PessoaID, mySinc.DeviceID)){ return false; }
    }
    return true;
}
```

Figura 3-40: Código do método "ExportarRegisto"

- O método "addEditTemplate"
- A classe "**Sincronizacao**" recebe duas listas de pessoas: a lista interna e a lista externa e retorna a lista sincronizada e a lista de conflitos, isto é, este método percorre a primeira lista (Figura 3-41) e compara as pessoas com a segunda lista. Se a pessoa não

existir é adicionada à segunda lista (Figura 3-43); caso a pessoa exista é verificado campo a campo e se o campo em causa não existir é adicionado a pessoa da segunda lista, caso o campo exista é adicionado à lista de conflitos (Figura 3-42).

```
public Sincronizacao(List<Pessoas> Lista1, List<Pessoas> ListaDestino, ref List<Pessoas> lstConflitos){
    //Lista 1 é sincronizada com a ListaDestino isto é os elementos da Lista1 vão ser comparados com os da..
    //..Lista Destino e se esistirem cria a lista de conflitos se não existirem são acresentados..
    lstConflitos = new List<Pessoas>();
    lstConflitos.Clear();
    bool existe = false;
    foreach (Pessoas myLista1 in Lista1){ existe = false; //percorre a lista1
        if (myLista1.tChecked > 0){ //Verifica que elementos estão selecionados na lista 1
            foreach (Pessoas myListaDestino in ListaDestino){ //percorre a listaDestino
                if (myLista1.Id == myListaDestino.Id){ //EXISTE - Verifica se o elemento da lista 1 existe na lista 2
```

Figura 3-41: Excerto do código do método "Sincronização – Compara a 1ª lista com a 2ª lista"

```
if ((myLista1.tChecked == 1)||(myLista1.tChecked == 3)||(myLista1.tChecked == 5)||(myLista1.tChecked == 7))
{ //Verifica se o campo a comparar é o RFID
    if ((myListaDestino.RFID != null) && (myListaDestino.RFID != "")){ //Verifica de o campo RFID..
        Pessoas pessoaItem = new Pessoas();                            //..existe na lista de destino
        pessoaItem.Id = myLista1.Id;
        pessoaItem.Nome = myLista1.Nome;
        pessoaItem.RFID = myLista1.RFID;
        pessoaItem.FP1 = "";
        pessoaItem.FP2 = "";
        lstConflitos.Add(pessoaItem); //Adiciona o campo a lista de conflitos
    }else{ myListaDestino.RFID = myLista1.RFID; } //Se o campo RFID da Lista 2 estiver vasio é alterado..
}                                                 //..com o valor da lista 1
```

Figura 3-42: Excerto do código do método "Sincronização – Se o campo RFID existe"

```
if (!existe){ //NÃO EXISTE - Se o elemento da lista 1 não existir é adicionado a lista 2
    Pessoas pessoaItem = new Pessoas();
    pessoaItem.Id = myLista1.Id;
    pessoaItem.Nome = myLista1.Nome;
    if ((myLista1.tChecked == 1)||(myLista1.tChecked == 3)||(myLista1.tChecked == 5)||(myLista1.tChecked == 7)){
        pessoaItem.RFID = myLista1.RFID; }
    if ((myLista1.tChecked == 2)||(myLista1.tChecked == 3)||(myLista1.tChecked == 6)||(myLista1.tChecked == 7)){
        pessoaItem.FP1 = myLista1.FP1; }
    if ((myLista1.tChecked == 4)||(myLista1.tChecked == 5)||(myLista1.tChecked == 6)||(myLista1.tChecked == 7)){
        pessoaItem.FP2 = myLista1.FP2; }
    ListaDestino.Add(pessoaItem);
}
```

Figura 3-43: Excerto do código do método "Sincronização – Não existe pessoa"

3.5.3 *Interface Layer*

Nesta camada define-se o *layout* da aplicação (Figura 3-44). Todos os formulários, menus e botões são definidos nesta camada e qualquer alteração é independente das outras camadas.

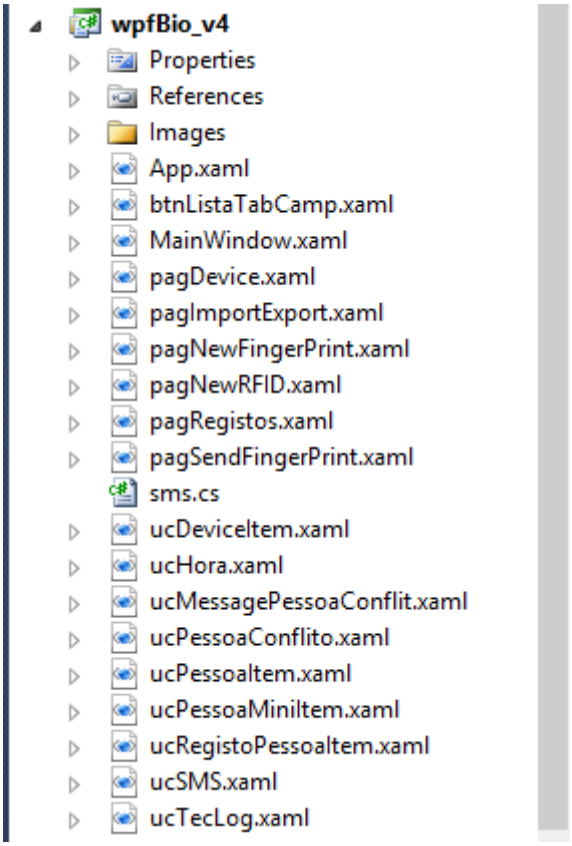


Figura 3-44: Interface layer

Dado que os elementos desta camada são formulários amenas indicaremos para que serve cada um dos elementos.

- O formulário "**MainWindow**" é o formulário principal isto é, é onde é possível ver a lista de equipamentos e onde serão mostrados todos os outros formulários e mensagens;
- O formulário "**pagDevice**" é o formulário de introdução e consulta dos dados do equipamento
- O formulário "**pagImportExport**" é o formulário onde são importados, exportados ou sincronizados os dados das pessoas mas também onde é possível remover pessoas da base de dados interna;
- O formulário "**pagNewFingerPrint**" é o formulário onde é possível adicionar novas impressões digitais;
- O formulário "**pagNewRFID**" é o formulário onde é possível associar códigos RFID a pessoas pré registadas no sistema
- O formulário "**pagRegistos**" é o formulário onde é possível exportar e consultar o registo de passagens por pessoa, equipamento, e ou data e hora;
- O formulário "**pagSendFingerPrint**" é o formulário onde é possível enviar *templates* (impressões digitais) pré registadas no sistema para os equipamentos;
- O controlo "**btnListaTabCamp**" é responsável por mostra a lista de tabelas e a lista de campos;

- O controlo "**ucDeviceItem**" é responsável por mostrar os dados do equipamento na lista de equipamentos do formulário "MainWindow";
- O controlo "**ucHora**" é responsável por fornecer uma forma mais simpres e controlada de introduzir uma hora nas pesquisas do formulário "pagRegistos"
- O controlo "**ucMessagePessoaConflit**" é responsável por mostrar a lista de conflitos numa importação, exportação ou sincronização de pessoas ou registos e onde é possível escolher dos elementos em conflito quais serão mantidos ou alterados;
- O controlo "**ucPessoaConflito**" é responsável por mostrar os dados da pessoa e o item que esta em conflito na lista de conflitos no controlo "ucMessagePessoaConflit"
- O controlo "**ucPessoaItem**" é responsável por mostrar os dados da pessoa na lista de pessoas dos formulários "pagNewFingerPrint", "pagNewRFID", "pagSendFingerPrint"
- O controlo "**ucPessoaMiniItem**" é responsável por mostrar os dados da pessoa na lista interna e externa de pessoas de pessoas do formulário "pagImportExport"
- O controlo "**ucRegistoPessoaItem**" é responsável por mostrar os dados do registo na lista de registos do formulário "pagRegistos"
- O controlo "**ucSMS**" é responsável por mostrar todas as mensagens informativas e de confirmação, por exemplo, sempre que ocorre algum erro este controlo é mostrado com a mensagem do erro;
- O controlo "**ucTecLog**" é responsável por receber e mostrar um pequeno log que serve para vermos se a aplicação esta a funcionar corretamente.
-

4. Testes e demonstração da aplicação

Neste capítulo apresenta-se como funciona a aplicação assim como são referidos alguns testes com o objetivo de demostrar o correto funcionamento da aplicação. Serão exibidas e demonstradas as operações de ligação do equipamento, introdução de novos equipamentos, importação/exportação/sincronização de pessoas, atribuição de *tags* RFID, novas impressões digitais, enviar *templates* para o equipamento, marcação de alguns registos tanto RFID como impressões digitais e finalmente pesquisa e exportação de registos.

4.1.1 Configuração do equipamento

Primeiro que tudo é necessário configurar o equipamento que pretendemos ligar ao sistema, para isso devemos ligar o equipamento a um computador e executar a aplicação (Figura 4-1). (**Nota:** a dll "DComunic.dll" tem se estar dentro da mesma pasta que o programa "SetAddr.exe" no caso de houver alguma dll em falta basta executar o seguinte comando na linha de comando **"regsvr32 caminho\nome.dll"** o caminho é o endereço da pasta onde a dll que queremos adicionar está e o nome é o nome da dll.)
No programa, temos de indicar o ip de *broadcast* da rede, o IP do terminal escolhido por nós, o IP do computador para o qual o equipamento envia as respostas (computados que irá executar a nossa aplicação) e, finalmente, a porta que será usada para comunicar com o equipamento. É também possível ativar ou desativar algumas funções do equipamento, nomeadamente o leitor de RFID e o tipo de *tags* usadas.

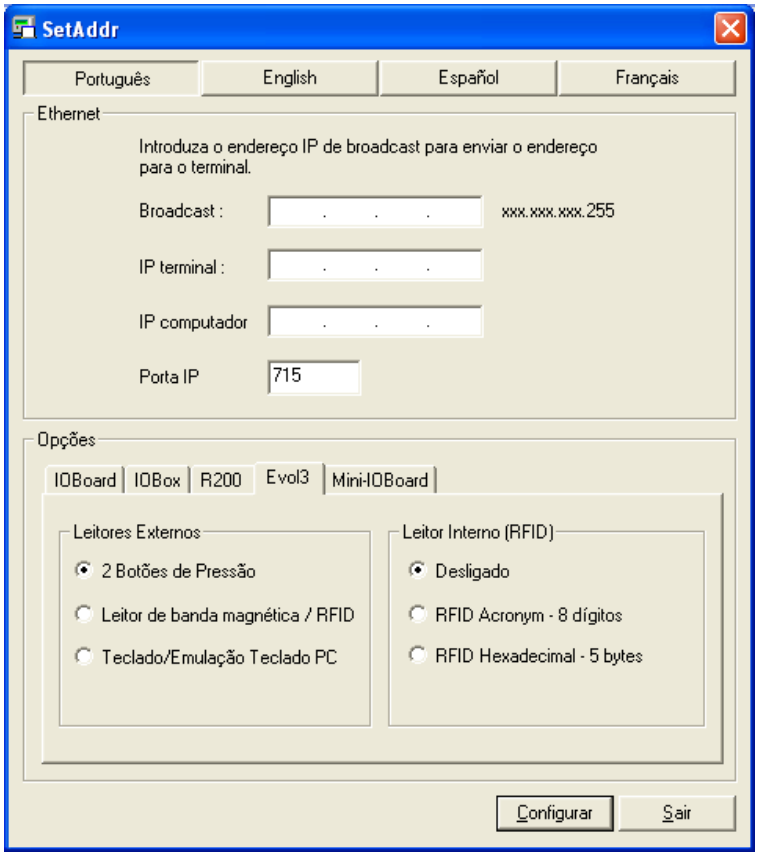


Figura 4-1: Programa de configuração do equipamento.

Após a configuração o equipamento pode ser ligado a diretamente ao computador que irá executar a nossa aplicação ou ligado a um switch na mesma rede que o computador que irá executar a nossa aplicação.

4.1.2 Adicionar um novo equipamento

Para adicionar um novo equipamento o administrador ou a pessoa responsável tem de executar a aplicação num computador que esteja na mesma rede do equipamento que queremos ligar e deve deixá-la a executar, uma vez que é esta aplicação que controla tudo e mantem o sistema a funcionar; logo para que o sistema funcione, esta aplicação tem de estar em funcionamento contínuo.
Após executar a aplicação ira aparecer o seguinte *layout.* (Figura 4-2).

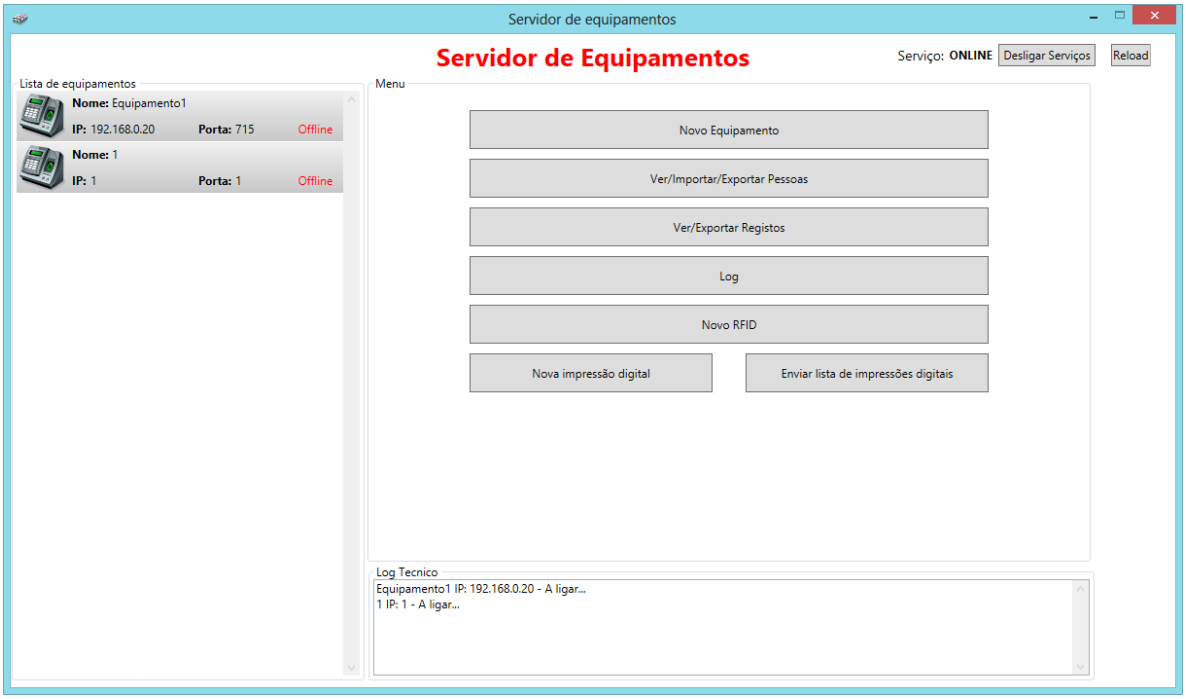


Figura 4-2: Menu principal.

Depois escolhemos a opção "Novo equipamento" que mostrará o seguinte *layout* (Figura 4-3).

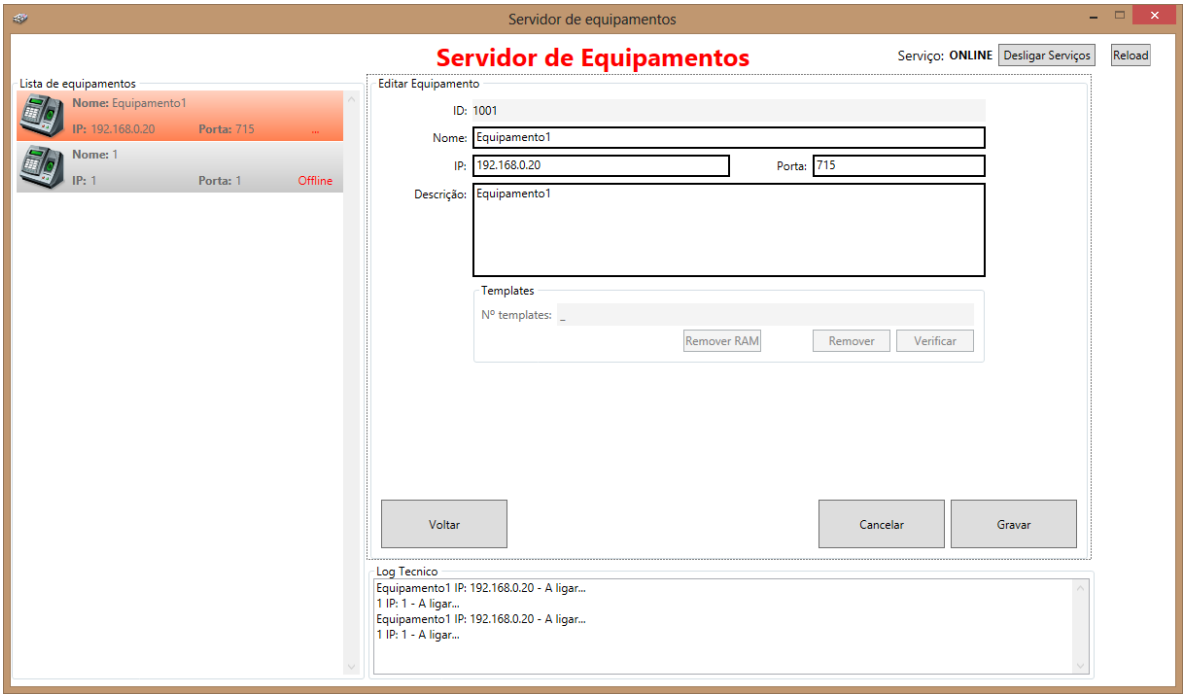


Figura 4-3: Novo equipamento.

Preenchidos, todos os dados necessários, clicamos no botão "Gravar" que devolverá a seguinte mensagem (Figura 4-4).

Figura 4-4: Mensagem de confirmação

A figura seguinte (Figura 4-5) confirma que o processo funcionou a 100% e que o novo equipamento foi adicionado à base de dados interna. O **antes** é o estado da tabela antes de adicionarmos o novo equipamento e o **depois** é o estado da tabela depois de clicarmos no botão "Gravar" (Figura 4-3) e de nos ser mostrada a mensagem de confirmação (Figura 4-4).

Figura 4-5: Gravar equipamento na base de dados interna.

Passados alguns segundos depois da mensagem de confirmação (Figura 4-4) ser mostrada, esta desaparece automaticamente possibilitando a edição das configurações do equipamento que acabamos de adicionar. É também possível ver que esse equipamento foi adicionado à lista de equipamentos (ponto 1 da Figura 4-6), que ficará no estado "A ligar…" (ponto 2 da Figura 4-6), ao mesmo tempo que a aplicação inicia a comunicação com o equipamento (ponto 3 da Figura 4-6) e até que a mesma seja estabelecida.

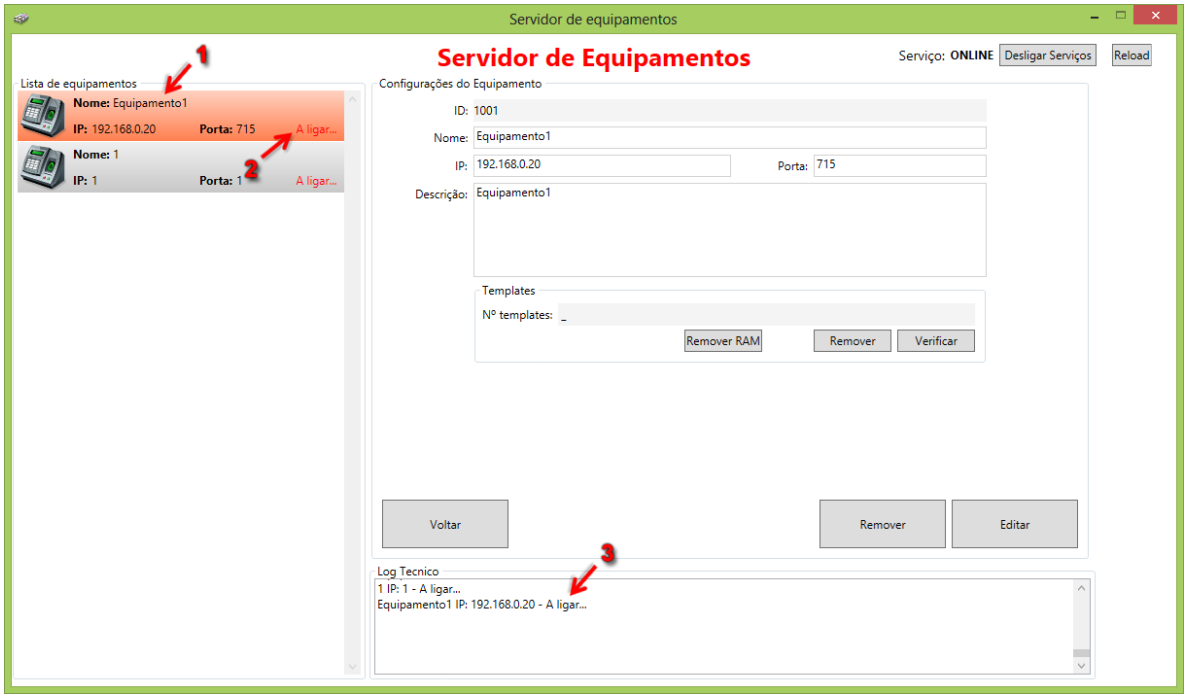


Figura 4-6: Ver equipamento depois de gravado.

4.1.3 Importar, exportar ou sincronizar pessoas

Para ver, importar, exportar ou sincronizar pessoas é necessário que a base de dados externa esteja ligada na mesma rede que o programa e que esteja *online*. Para estas operações vamos ao menu principal (Figura 4-2) e escolhemos a opção "Ver/Importar/Exportar Pessoas" que deverá apresentar o seguinte *layout* (Figura 4-7):

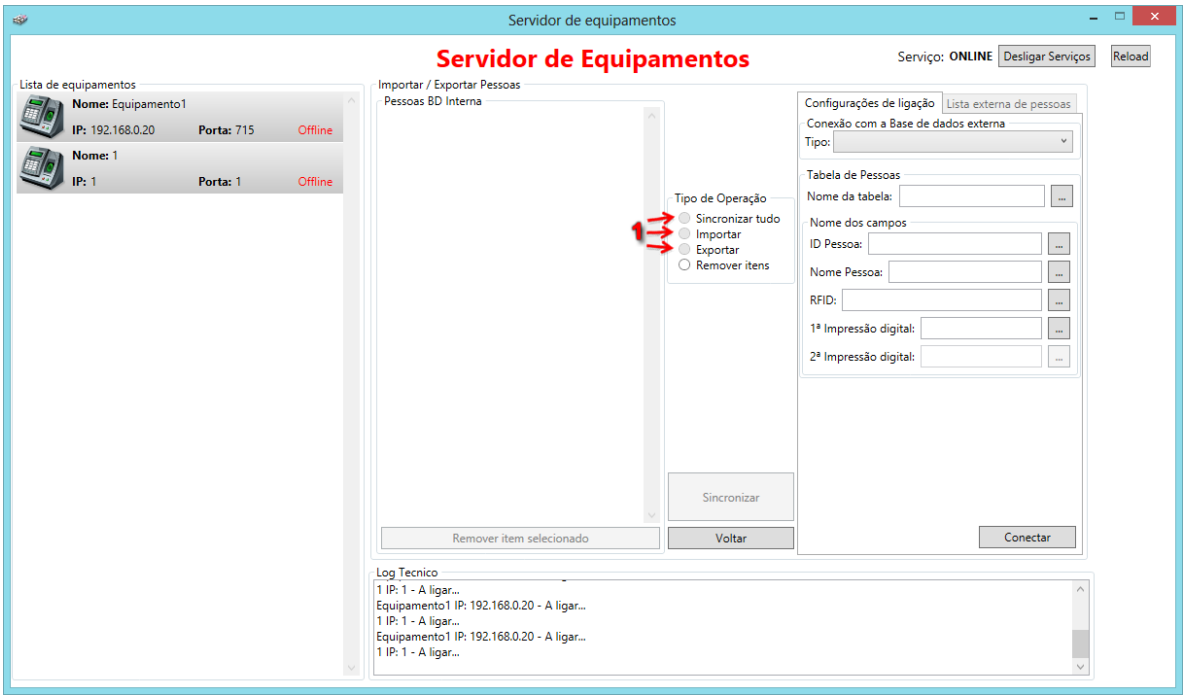


Figura 4-7: Ver/Importar/Exportar/Sincronizar pessoas.

Para importar, exportar ou sincronizar, temos de configurar a ligação a uma base de dados externa que contenha os dados que precisamos.
Para adicionarmos uma base de dados to tipo "SQLite", clicamos no tipo e escolhemos a opção correspondente (pontos 1 e 2 da Figura 4-8), depois indicamos o caminho e *password* da base de dados (ponto 3 da Figura 4-8).

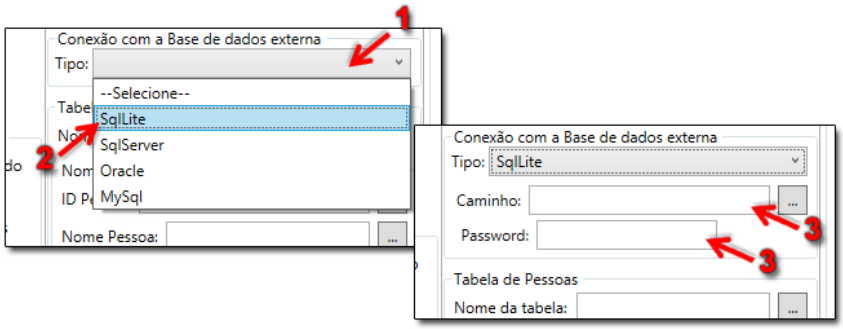


Figura 4-8: Base de dados do tipo SQLite.

Para adicionarmos uma base de dados to tipo "SQLServer", clicamos no tipo e escolhemos a opção correspondente (pontos 1 e 2 da Figura 4-9), depois indicamos o ip, a porta, o *login e password* de acesso e o nome da base de dados (ponto 3 da Figura 4-9).

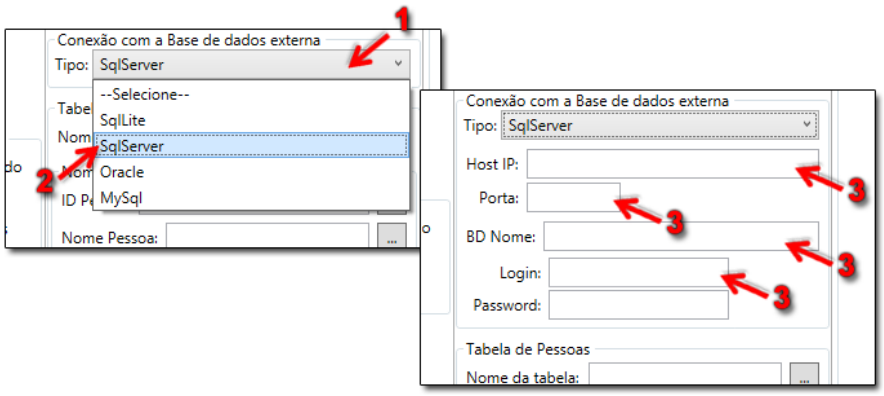


Figura 4-9: Base de dados do tipo SQLServer.

Para adicionarmos uma base de dados to tipo "MySql", a operação é em tudo semelhante à anterior (pontos 1, 2 e 3 da Figura 4-10).

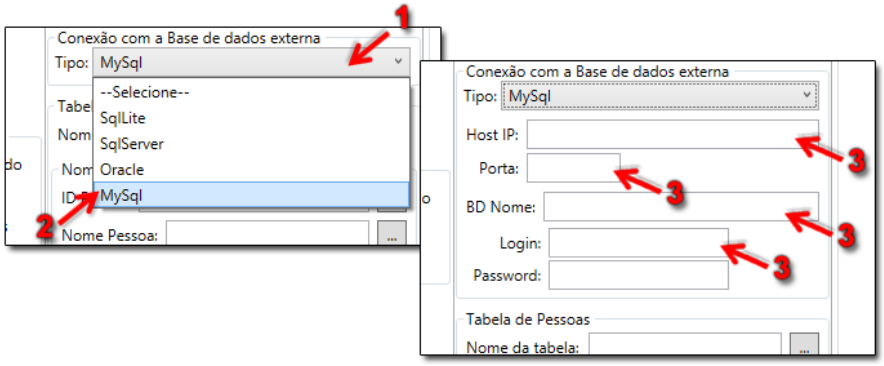


Figura 4-10: Base de dados do tipo MySql

Para adicionarmos uma base de dados to tipo "Oracle", clicamos no tipo e escolhemos a opção correspondente (pontos 1 e 2 da Figura 4-11), depois indicamos o IP, a Porta, o SID, o *loguin e password* de acesso (ponto 3 da Figura 4-11).

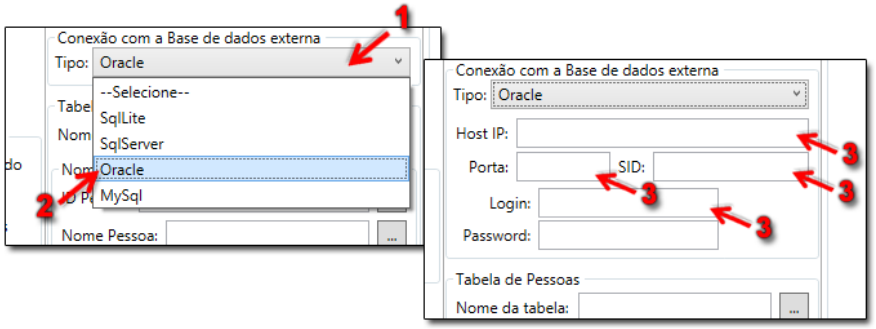


Figura 4-11: Base de dados do tipo Oracle.

Depois preenchermos os dados da ligação, indicamos os nomes dos campos clicando nos botões ao lado de cada campo (ponto 1 da Figura 4-12)

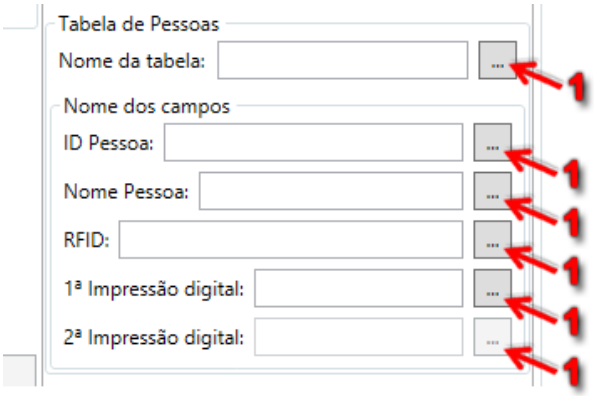


Figura 4-12: Definir os nomes dos campos

Para cada campo aparece uma lista de tabelas ou campos respetivamente (se tivermos preenchido corretamente os campos anteriores e a base de dados estiver *online)* da qual escolhemos um nome para o campo correspondente (ponto 2 da Figura 4-13).

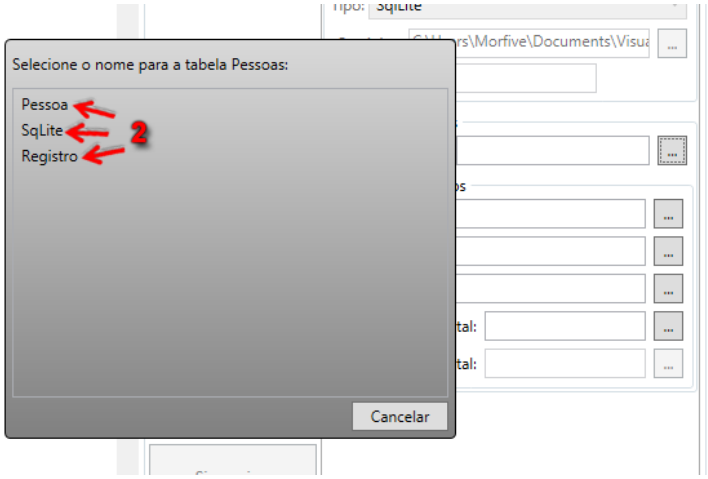


Figura 4-13: Lista de tabelas ou campos.

Ao clicar no nome ele é colocado na caixa correspondente (Figura 4-14) e a lista desaparecerá.

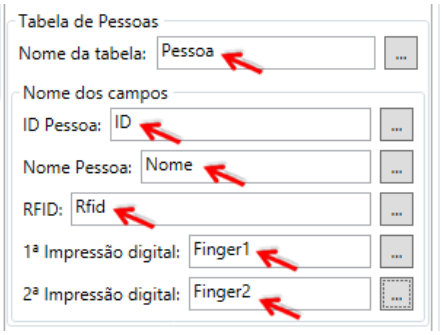


Figura 4-14: Campos da tabela pessoas.

Finalmente é só clicar no botão "Conectar" que se a operação for bem-sucedida aparecerá a lista de pessoas, isto se a base de dados externa tiver pessoas (Figura 4-15)

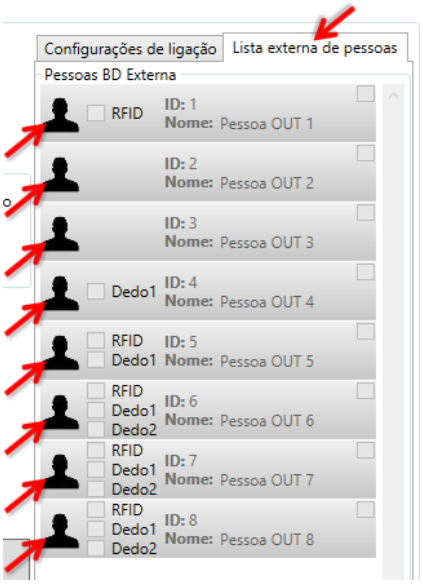


Figura 4-15: Lista de pessoa da base de dados externa.

Após termos a lista de pessoas da base de dados externa podemos importar, exportar ou sincronizar (Figura 4-16).

Figura 4-16: a) Sincronizar pessoas; b) Importar pessoas; c) Exportar pessoas

Se a importação for bem-sucedida é mostrada a mensagem de confirmação seguinte (Figura 4-17).

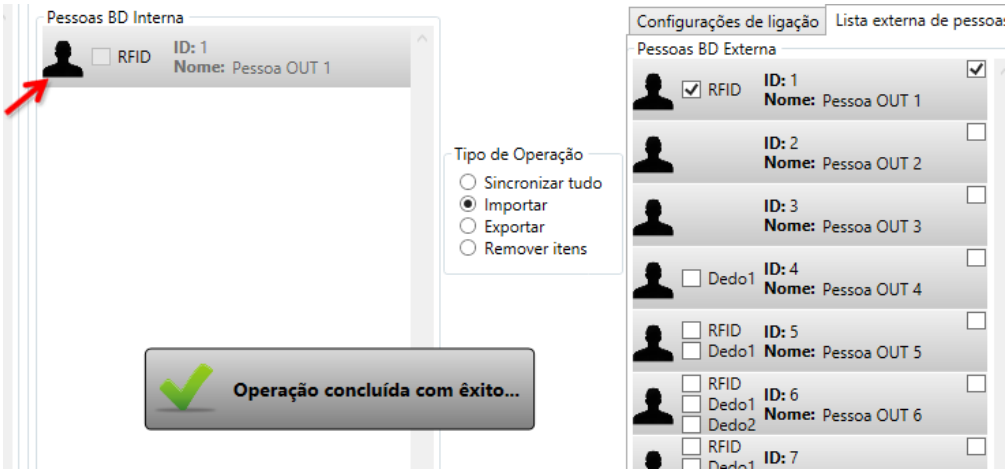


Figura 4-17: Importação da pessoa selecionada bem-sucedida

Se a exportação for bem-sucedida aparecerá a seguinte mensagem de confirmação (Figura 4-18).

Figura 4-18: Exportação da pessoa selecionada bem-sucedida

Se a sincronização for concluída com sucesso será mostrada a seguinte mensagem de confirmação (Figura 4-19).

Figura 4-19: Sincronização bem-sucedida

No caso de haver pessoas com *templates* iguais será mostrada a lista seguinte, para que sejam escolhidos os *templates* a manter (Figura 4-20).

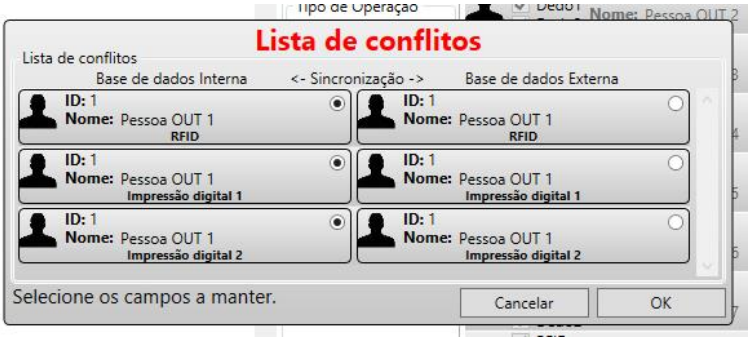


Figura 4-20: Lista de conflitos.

Para a importação, a figura seguinte (Figura 4-21) confirma que o processo funcionou a 100%, que a importação da pessoa selecionada da base de dados externa foi bem-sucedida e que a mesma foi adicionada à base de dados interna. O **antes** é o estado da tabela da base de dados interna antes da importação e o **depois** é o estado da tabela depois de clicarmos no botão "Sincronizar" (Figura 4-7) e de nos ser mostrada a mensagem de confirmação (Figura 4-17).

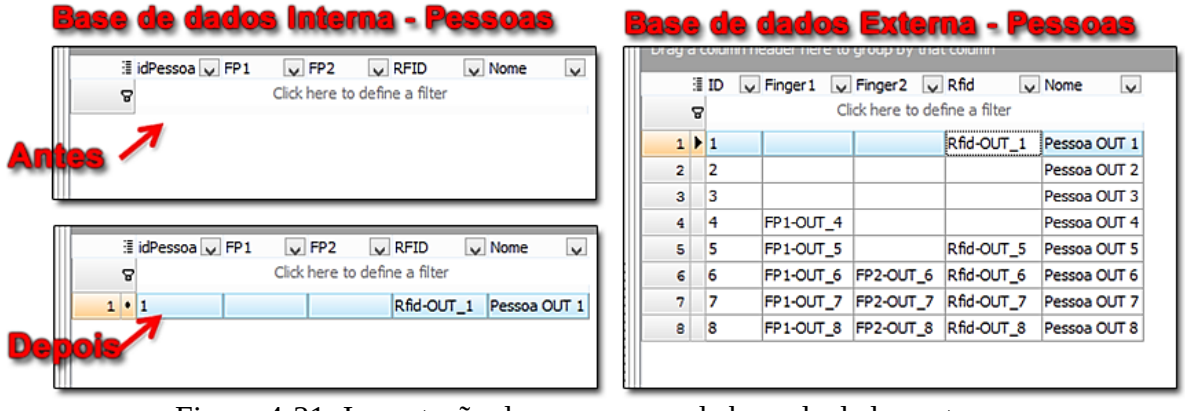


Figura 4-21: Importação de uma pessoa da base de dados externa.

Para a exportação, a figura seguinte (Figura 4-22) confirma que o processo funcionou a 100%, que a exportação da pessoa selecionada foi bem-sucedida e que os *templates* da pessoa da base de dados interna foram adicionados à pessoa da base de dados externa. O **antes** é o estado da tabela da base de dados externa antes da exportação e o **depois** é o estado da tabela depois de clicarmos no botão "Sincronizar" (Figura 4-7) e de nos ser mostrada a mensagem de confirmação (Figura 4-18).

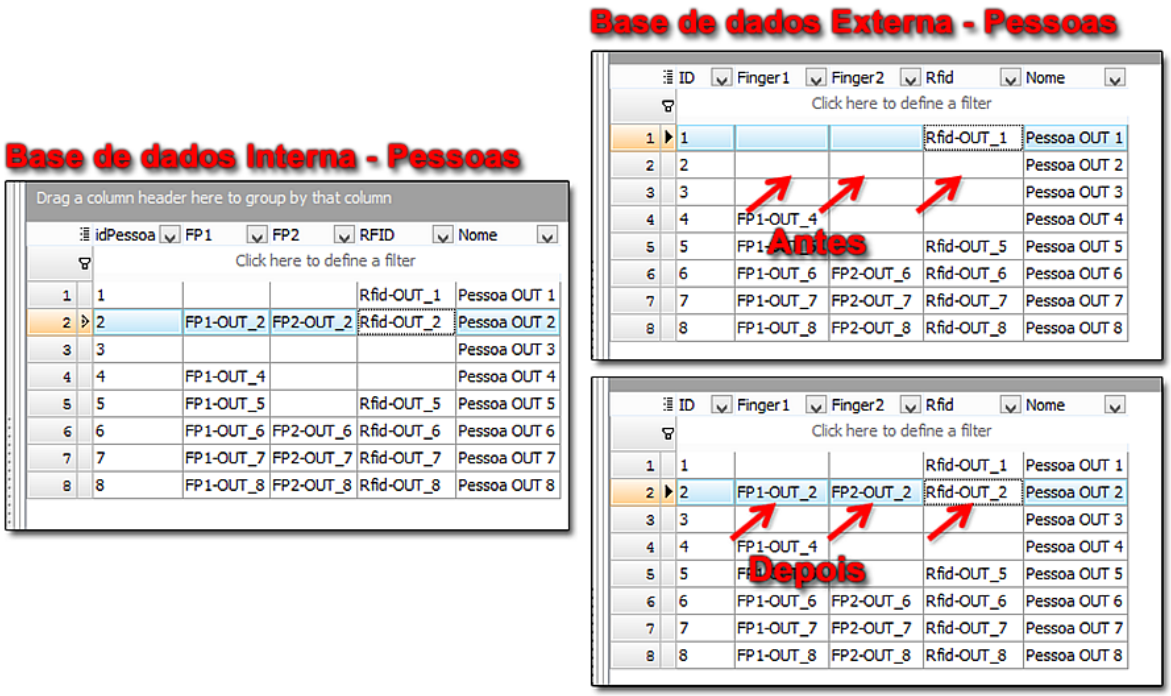


Figura 4-22: Exportação dos dados da pessoa da base de dados interna

Para a sincronização, a figura seguinte (Figura 4-23) confirma que o processo funcionou a 100%, que a sincronização das pessoas foi bem-sucedida e que as pessoas da base de dados externa foram adicionadas à base de dados interna e os *templates* na base de dados interna foram adicionados ou atualizados na base de dados externa. O **antes** é o estado das tabelas das base de dados interna e externa antes da sincronização e o **depois** é o estado das tabelas depois de clicarmos no botão "Sincronizar" (Figura 4-7) e de nos ser mostrada a mensagem de confirmação (Figura 4-19).

Figura 4-23: Sincronização da tabela pessoa.

4.1.4 Atribuir uma *tag* RFID a uma pessoa

Para atribuir uma *tag* RFID é necessário ir ao menu principal (Figura 4-2) e escolher a opção "Novo RFID" que irá mostrar o seguinte *layout* (Figura 4-24)

Figura 4-24: Atribuir RFID.

Depois escolhemos um equipamento e, se estiver *online*, aparecerá o seguinte *layout* (Figura 4-25) com a lista de pessoas registadas na base de dados interna. Depois temos de clicar no

botão “Iniciar Captura” para que o equipamento selecionado entre em modo de aquisição (Figura 4-26).

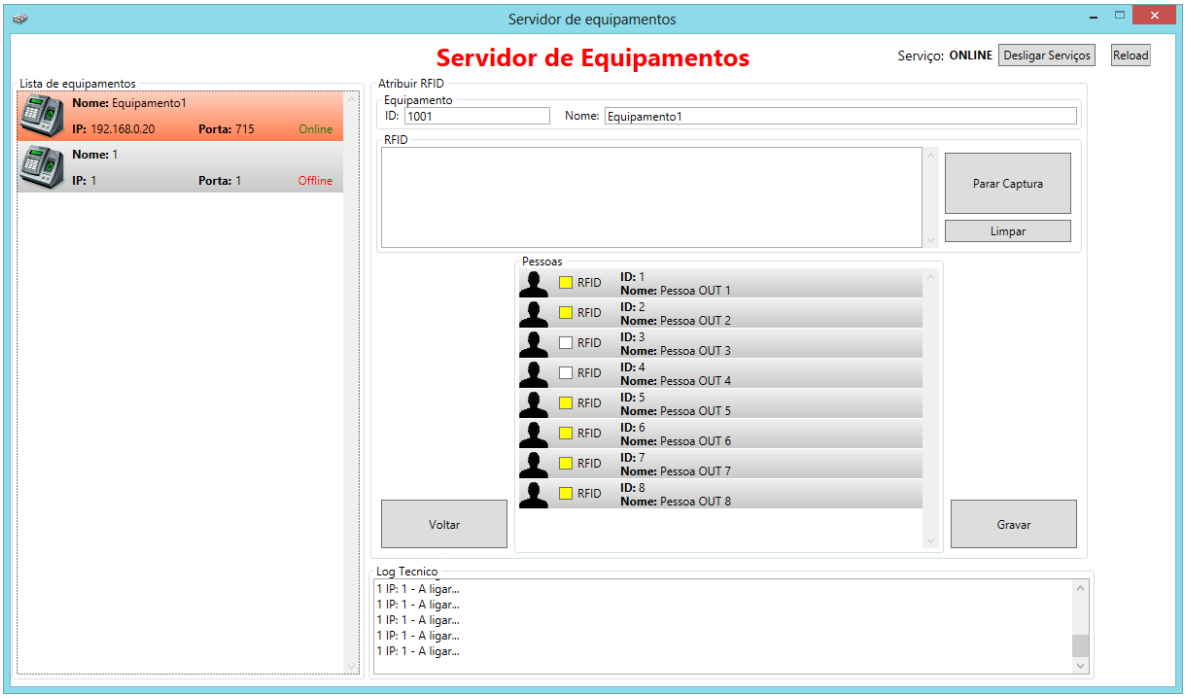


Figura 4-25: Atribuir RFID (Equipamento selecionado).

Figura 4-26:Equipamento do modo de captura de *tags* RFID.

Assim que uma *tag* é passada no leitor, o código dessa *tag* é adicionado a lista (ponto 1 da Figura 4-27), assim que o código da *tag* que queremos atribuir estiver na lista temos de clicar no botão “Parar Captura”, para libertar o leitor. Depois selecionamos o código RFID que queremos atribuir e selecionamos a pessoa a que vamos atribuir o código (pontos 1 e 2 da Figura 4-27) por fim clicamos em “Gravar”.

Figura 4-27: Selecionar RFID e pessoa.

Se a operação for bem-sucedida aparecerá a mensagem seguinte (Figura 4-28).

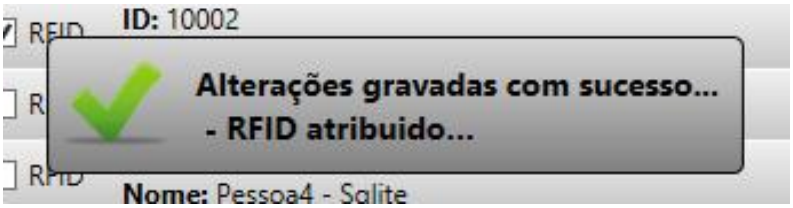


Figura 4-28: Mensagem de confirmação.

A figura seguinte (Figura 4-29) confirma que o processo funcionou a 100% e que o código RFID foi atribuído a pessoa, da base de dados interna. O **antes** é o estado da tabela antes de atribuirmos o código RFID à pessoa e o **depois** é o estado da tabela depois de clicarmos no botão "Gravar" (Figura 4-27) e de nos ser mostrada a mensagem de confirmação (Figura 4-28).

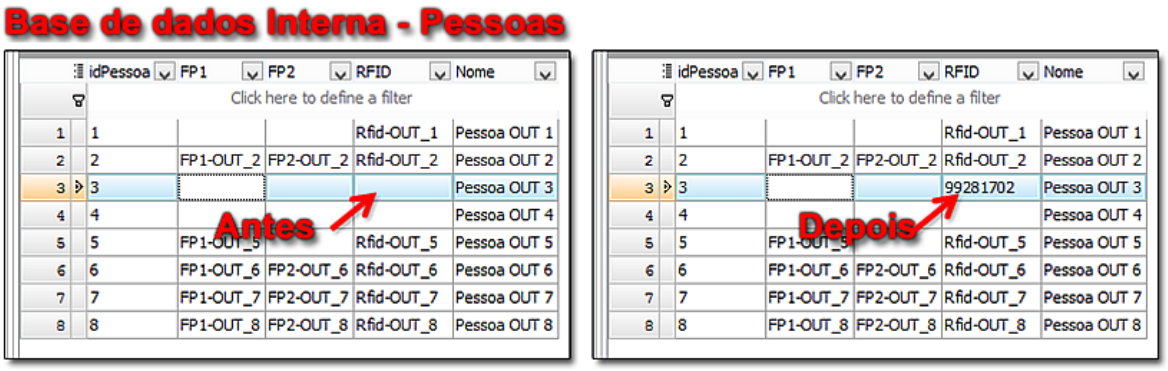


Figura 4-29: Atribuir RFID a pessoa selecionada na base dados interna.

4.1.5 Registar nova impressão digital

Para registar uma nova impressão digital é necessário ir ao menu principal (Figura 4-2) e escolher a opção "Nova impressão digital" que mostrará o seguinte *layout* (Figura 4-30).

Figura 4-30: Nova impressão digital.

Depois escolhemos um equipamento, se o equipamento estiver *online* aparecerá o seguinte *layout* (Figura 4-31).

Figura 4-31: Nova impressão digital (Equipamento selecionado)

Depois de escolhermos o dedo da pessoa (Ponto 1 da Figura 4-31) que queremos gravar e clicamos em "Recolher e Gravar". O programa ativa o modo de recolha do equipamento escolhido (Figura 4-33) e aguarda que o *template* biométrico seja recolhido. Enquanto espera o programa mostra a mensagem seguinte (Figura 4-32).

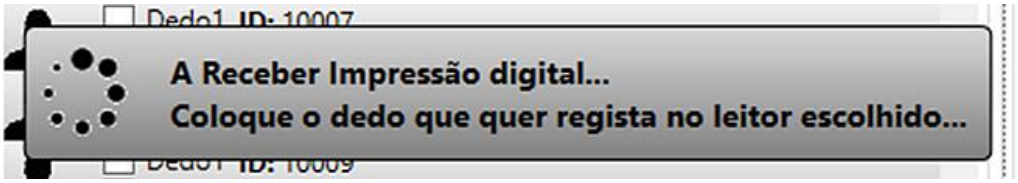


Figura 4-32: Mensagem de espera enquanto captura a nova impressão digital.

Figura 4-33: Equipamento, registo de nova impressão digital.

Após a captura bem-sucedida da impressão digital, o programa grava o *template* biometrico gerado (a partir da impressão digital recolhida) e mostra a menssagen seguinte (Figura 4-34).

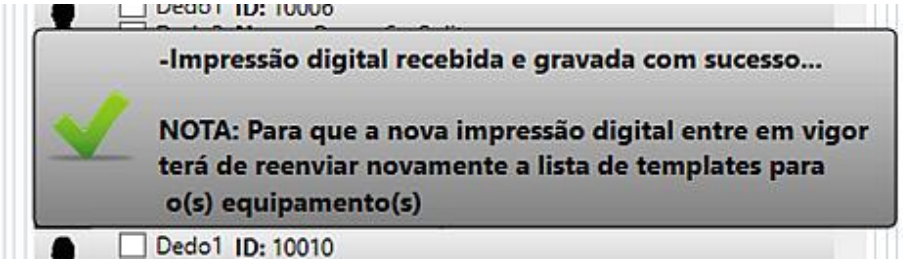
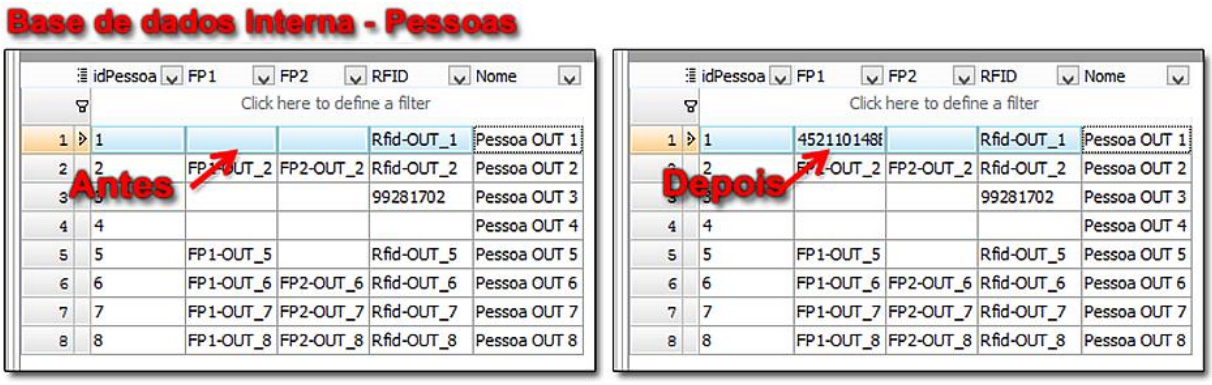


Figura 4-34: Mensagem de confirmação *template* recolhido e gravado.

A figura seguinte (Figura 4-35) confirma que o processo funcionou a 100% e que o *template* biométrico (da impressão digital recolhida) foi recolhido e atribuído ao dedo da pessoa na base de dados interna. O **antes** é o estado da tabela antes de adicionarmos o novo *template* (impressão digital) para o dedo 1 e o **depois** é o estado da tabela depois de clicarmos no botão "Recolher e Gravar" (Figura 4-31) e após da recolha bem-sucedida da *template* e de nos ser mostrada a mensagem (Figura 4-34) de confirmação.

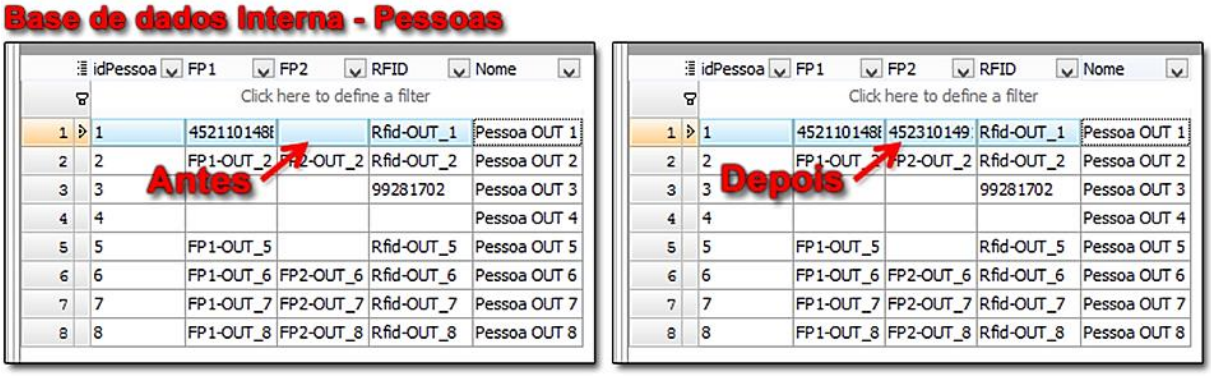


	idPessoa	FP1	FP2	RFID	Nome
	Click here to define a filter				
1	1			Rfid-OUT_1	Pessoa OUT 1
2	2	FP1-OUT_2	FP2-OUT_2	Rfid-OUT_2	Pessoa OUT 2
3	3			99281702	Pessoa OUT 3
4	4				Pessoa OUT 4
5	5	FP1-OUT_5		Rfid-OUT_5	Pessoa OUT 5
6	6	FP1-OUT_6	FP2-OUT_6	Rfid-OUT_6	Pessoa OUT 6
7	7	FP1-OUT_7	FP2-OUT_7	Rfid-OUT_7	Pessoa OUT 7
8	8	FP1-OUT_8	FP2-OUT_8	Rfid-OUT_8	Pessoa OUT 8

	idPessoa	FP1	FP2	RFID	Nome
	Click here to define a filter				
1	1	4521101488		Rfid-OUT_1	Pessoa OUT 1
2	2	FP1-OUT_2	FP2-OUT_2	Rfid-OUT_2	Pessoa OUT 2
3	3			99281702	Pessoa OUT 3
4	4				Pessoa OUT 4
5	5	FP1-OUT_5		Rfid-OUT_5	Pessoa OUT 5
6	6	FP1-OUT_6	FP2-OUT_6	Rfid-OUT_6	Pessoa OUT 6
7	7	FP1-OUT_7	FP2-OUT_7	Rfid-OUT_7	Pessoa OUT 7
8	8	FP1-OUT_8	FP2-OUT_8	Rfid-OUT_8	Pessoa OUT 8

Figura 4-35: Gravar a nova impressão digital no utilizador (dedo 1) na base de dados interna.

A figura seguinte (Figura 4-36) confirma que o processo também funcionou a 100% para o dedo 2.



	idPessoa	FP1	FP2	RFID	Nome
	Click here to define a filter				
1	1	4521101488		Rfid-OUT_1	Pessoa OUT 1
2	2	FP1-OUT_2	FP2-OUT_2	Rfid-OUT_2	Pessoa OUT 2
3	3			99281702	Pessoa OUT 3
4	4				Pessoa OUT 4
5	5	FP1-OUT_5		Rfid-OUT_5	Pessoa OUT 5
6	6	FP1-OUT_6	FP2-OUT_6	Rfid-OUT_6	Pessoa OUT 6
7	7	FP1-OUT_7	FP2-OUT_7	Rfid-OUT_7	Pessoa OUT 7
8	8	FP1-OUT_8	FP2-OUT_8	Rfid-OUT_8	Pessoa OUT 8

	idPessoa	FP1	FP2	RFID	Nome
	Click here to define a filter				
1	1	4521101488	4523101499	Rfid-OUT_1	Pessoa OUT 1
2	2	FP1-OUT_2	FP2-OUT_2	Rfid-OUT_2	Pessoa OUT 2
3	3			99281702	Pessoa OUT 3
4	4				Pessoa OUT 4
5	5	FP1-OUT_5		Rfid-OUT_5	Pessoa OUT 5
6	6	FP1-OUT_6	FP2-OUT_6	Rfid-OUT_6	Pessoa OUT 6
7	7	FP1-OUT_7	FP2-OUT_7	Rfid-OUT_7	Pessoa OUT 7
8	8	FP1-OUT_8	FP2-OUT_8	Rfid-OUT_8	Pessoa OUT 8

Figura 4-36: Gravar a nova impressão digital no utilizador (dedo 2) na base de dados interna.

4.1.6 Enviar lista de *templates* (impressões digitais) para o equipamento

Para enviar uma lista de *templates* para o equipamento é necessário ir ao menu principal (Figura 4-2) e escolher a opção "Enviar lista de impressões digitais" que devera mostrar o seguinte *layout* (Figura 4-37)

Figura 4-37: Enviar lista de impressões digitais.

Depois de escolher um equipamento, se o mesmo estiver *online*, aparecerá o seguinte *layout* (Figura 4-38).

Figura 4-38: Enviar lista de impressões digitais (equipamento selecionado)

Depois escolhemos os utilizadores que tiverem *templates* gravadas da base de dados que irão ter acesso ao equipamento selecionado (ponto 1 da Figura 4-39).

Figura 4-39: lista de impressões digitais selecionada.

De seguida clicamos em "Atualizar e enviar" que mostrará a seguinte mensagem (Figura 4-40) enquanto a aplicação grava a correspondência entre id *template* e id pessoa na tabela *templates* da base de dados interna e envia a lista de *templates* para o equipamento selecionado.

Figura 4-40: Mensagem a enviar.

Se o processo for bem-sucedido, isto é, se a correspondência entre id *template* e id pessoa for gravada com sucesso e a lista de *templates* tiver sido enviada com sucesso será mostrada a mensagem seguinte (Figura 4-41).

Figura 4-41: Mensagem de confirmação lista de *templates* enviada.

A Figura 4-42 confirma que o processo funcionou a 100% e que a correspondência entre o id *template* e o id pessoa de cada *template* da lista foram adicionados à tabela *template* na base de dados interna. O **antes** é o estado da tabela antes da correspondência entre o id *template* e o id pessoa e o **depois** é o estado da tabela depois de clicarmos no botão "Atualizar e enviar" (Figura 4-39) e de nos ser mostrada a mensagem de confirmação (Figura 4-41).

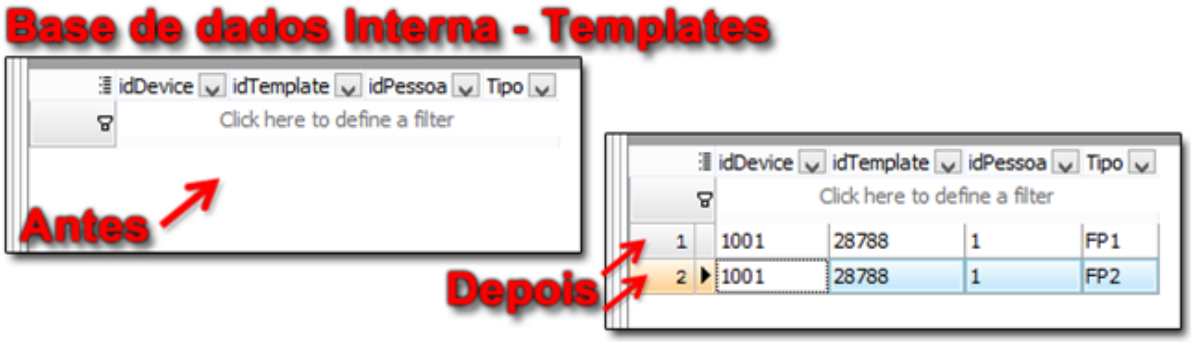


Figura 4-42: Gravar correspondência entre o id *template* e o id pessoa

4.1.7 Marcação de ponto por impressão digital

Para efetuar uma marcação por impressão digital o utilizador coloca o dedo no leitor (Figura 4-43) e o leitor verifica se a *template* gerada já existe na memória interna do equipamento. Se existir o equipamento envia o id do *template* para a aplicação que procura o id da pessoa correspondente na tabela *templates* e depois adiciona um novo registo de passagem na tabela de registo na base de dados interna. Caso contrário é mostrado uma mensagem ao utilizador indicando "Acesso negado" (Figura 4-44)

Figura 4-43: Marcação por impressão digital de um utilizador valido.

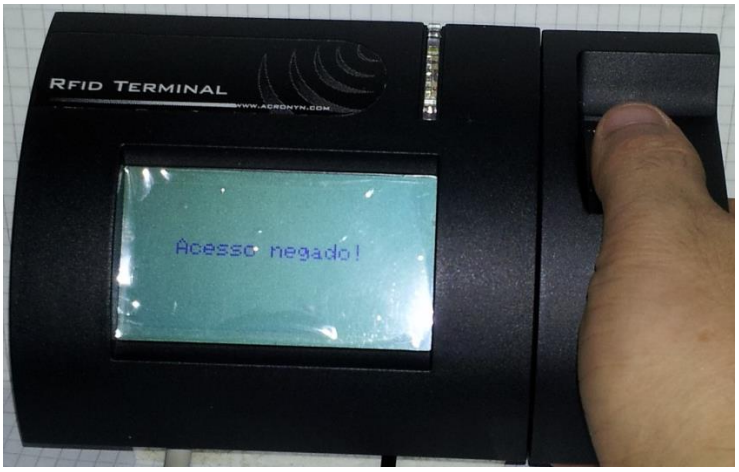


Figura 4-44: Marcação por impressão digital de um utilizador inválido.

A figura seguinte (Figura 4-45) confirma que o processo funcionou a 100% e o registo de passagem do utilizador, foi adicionado à tabela registo, na base de dados interna. O **antes** é o estado da tabela antes da marcação por impressão digital do utilizador e o **depois** é o estado da tabela depois dessa validação (Figura 4-43).

Figura 4-45: Registo de passagem por impressão digital, do utilizador na BD interna

4.1.8 Marcação de ponto por RFID

Para efetuar uma marcação por RFID o utilizador passa a *tag* RFID no leitor (Figura 4-46) e este envia o código da *tag* para a aplicação que verifica se o código RFID pertence a alguém. Se encontrar uma correspondência válida na tabela pessoas, adiciona um novo registo de passagem na tabela registo na base de dados interna. Caso contrário é mostrado uma mensagem ao utilizador indicando "Acesso negado" (Figura 4-47).

Figura 4-46: Marcação por RFID *tag* conhecida.

Figura 4-47: Marcação por RFID *tag* desconhecida.

A figura seguinte (Figura 4-48) confirma que o processo funcionou a 100% e o registo de passagem do utilizador, foi adicionado à tabela registo, na base de dados interna. O **antes** é o estado da tabela antes da marcação por RFID do utilizador e o **depois** é o estado da tabela depois dessa validação (Figura 4-46).

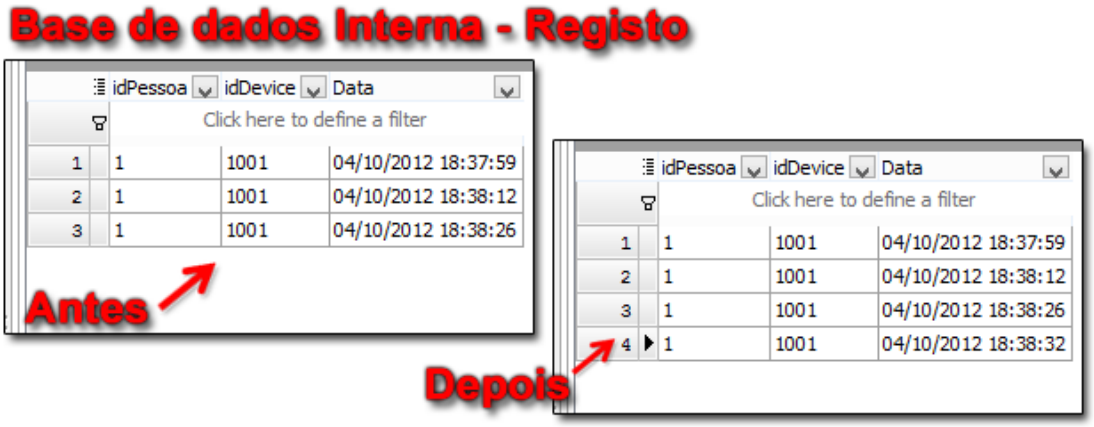


Figura 4-48: Registo de passagem por RFID, do utilizador na BD interna

4.1.9 Exportar Registos

Para exportar registos da base de dados interna para uma base de dados externa vamos ao menu principal (Figura 4-2) e escolhemos a opção "Ver/Exportar Registos" que deverá apresentar a seguinte *layout* (Figura 4-49)

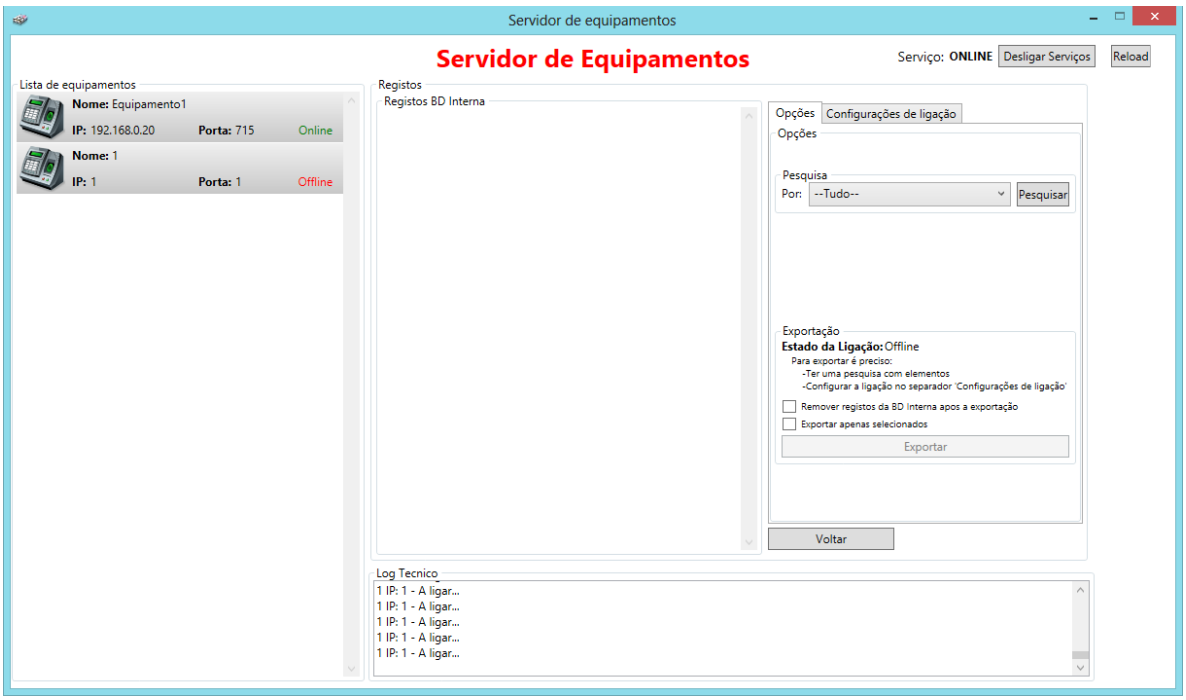


Figura 4-49: Ver/Exportar Registos

Primeiro que tudo temos de configurar a ligação com a base de dados externa. Para isso devemos clicar no separador "Configurações de ligação" (Figura 4-50), onde o procedimento será idêntico ao já descrito anteriormente no subcapítulo 4.1.3 referente às figuras: Figura 4-8, Figura 4-9, Figura 4-10 e Figura 4-11.

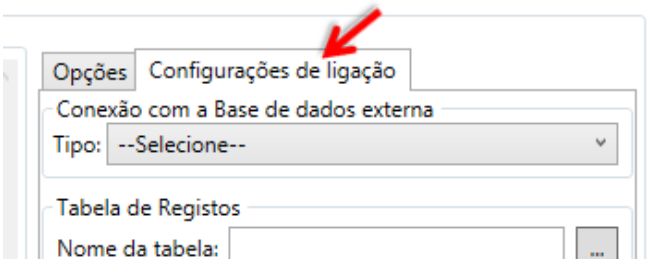


Figura 4-50: Separador "configurações de ligação"

Depois escolhemos os nomes dos campos clicando nos botões ao lada de cada campo (ponto 1 da Figura 4-51)

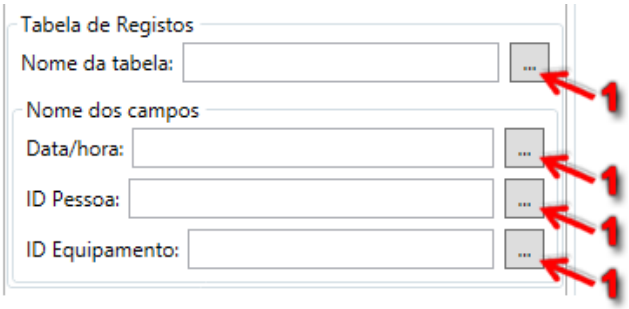


Figura 4-51: Definir os nomes dos campos

Para cada campo aparece uma lista de tabelas ou campos (se tivermos preenchido corretamente os campos anteriores e a base de dados estiver *online)* da qual escolhemos um nome (ponto 2 da Figura 4-52).

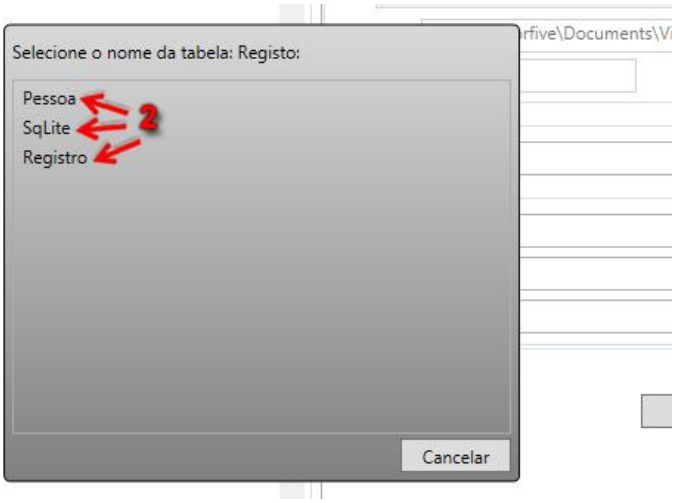


Figura 4-52: Lista de tabelas ou campos.

Ao clicar no nome ele é colocado na caixa correspondente (Figura 4-53) e a lista desaparecerá.

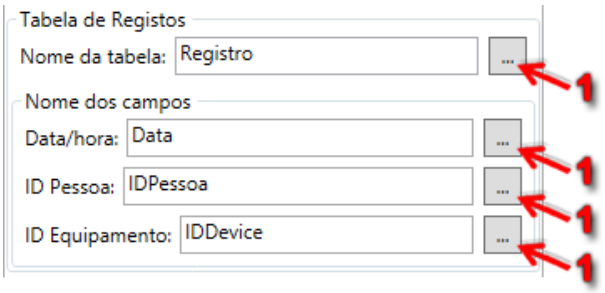


Figura 4-53: Campos da tabela registos

Finalmente é só clicar no botão "Conectar" que se a operação for bem-sucedida aparecerá no separador "Opções", o estado da ligação como "*Online*" (Figura 4-54).

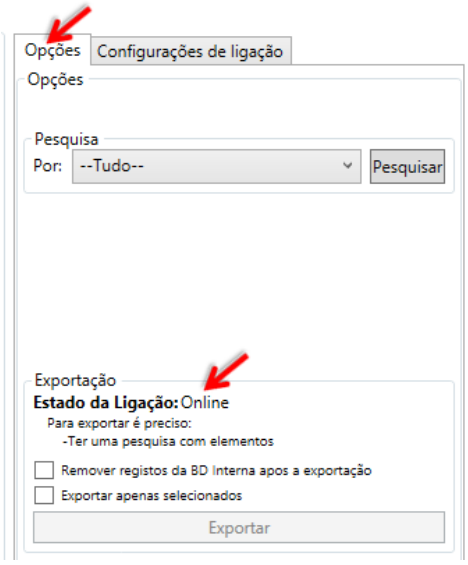


Figura 4-54: Base de dados ligada.

Agora temos de pesquisar os registos que queremos exportar, pesquisa essa que pode ser feita mediante a introdução de alguns parâmetros, nomeadamente o ID ou nome da pessoa, o ID ou nome do equipamento e um intervalo de datas.

Para mostrar todos os registos, selecionamos "tudo" na caixa de pesquisa (pontos 1 e 2 da Figura 4-55) depois clicamos em pesquisar (ponto 3 da Figura 4-55).

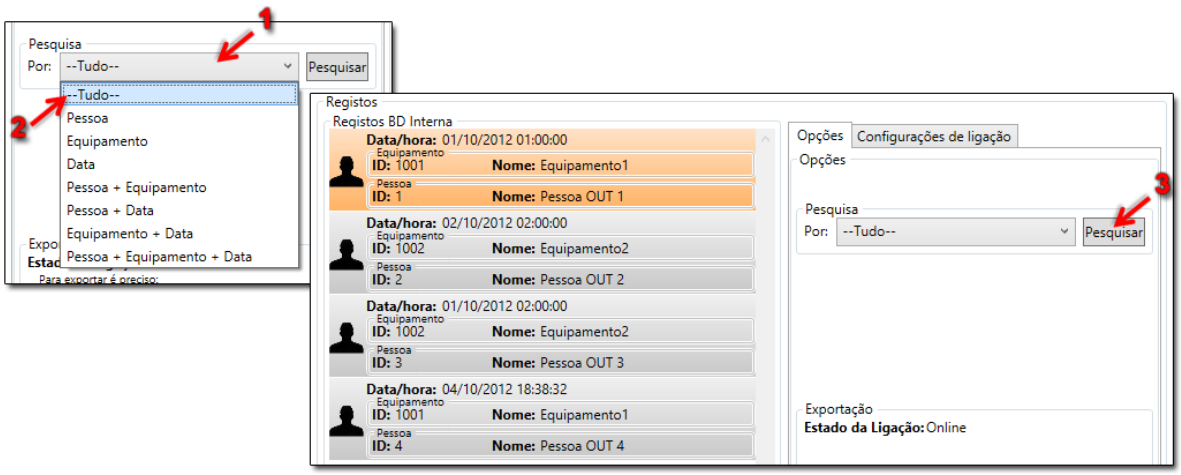


Figura 4-55: Pesquisa por todos os registos

Para pesquisarmos os registos de uma pessoa temos de selecionar "Pessoa" na caixa de pesquisa (ponto 1 e 2 da Figura 4-56) depois indicamos o id ou nome da pessoa e clicamos em pesquisar (ponto 3 e 4 da Figura 4-56)

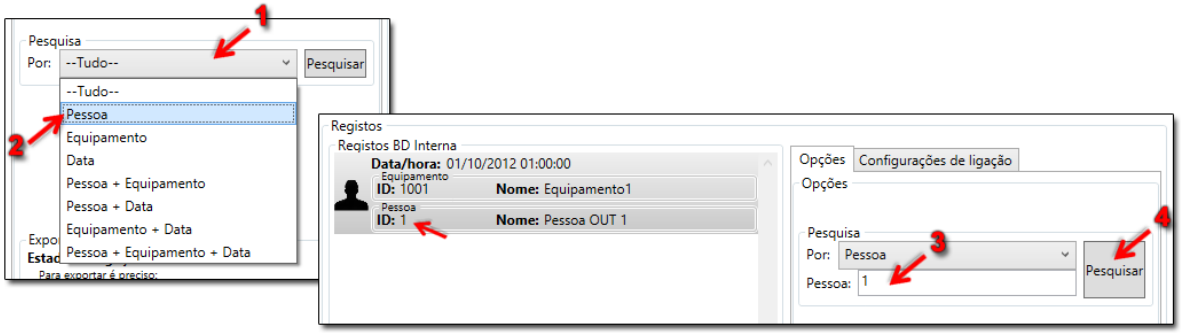


Figura 4-56: Pesquisa de registos por pessoa.

Para pesquisarmos os registos de um equipamento temos de selecionar "Equipamento" na caixa de pesquisa (ponto 1 e 2 da Figura 4-57) depois indicamos o id ou nome do equipamento e clicamos em pesquisar (ponto 3 e 4 da Figura 4-57)

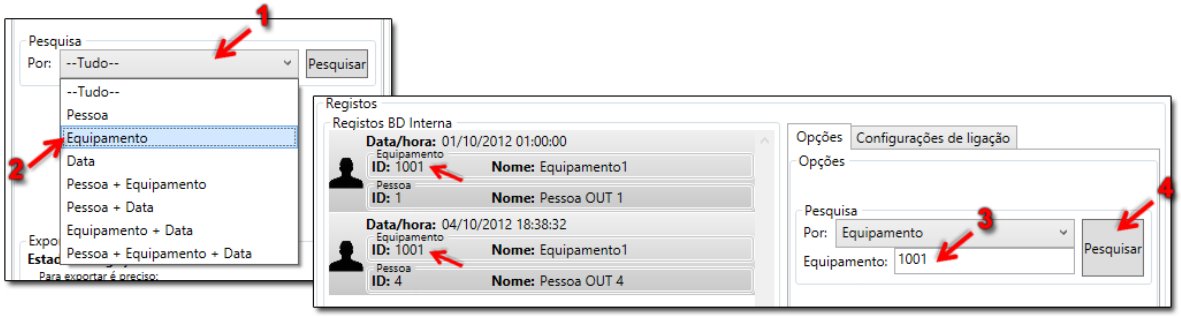


Figura 4-57: Pesquisa de registos por equipamento

Para pesquisarmos os registos num dado intervalo de datas temos de selecionar "Data" na caixa de pesquisa (ponto 1 e 2 da Figura 4-58) depois indicamos a data e hora inicial e a data e hora final do intervalo e clicamos em pesquisar (ponto 3, 4 e 5 da Figura 4-58)

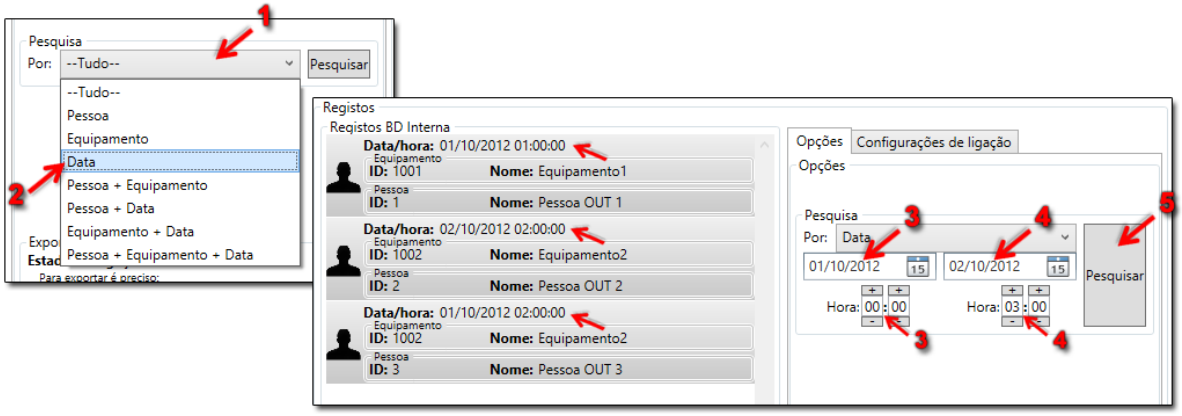


Figura 4-58: Pesquisa de registos por data e hora

Apos termos a pesquisa efetuada e a base de dados externa ligada (ponto 1 da Figura 4-59) podemos ainda optar por exportar apenas registos selecionados ou todos os registos referentes a pesquisa efetuada (ponto 3 da Figura 4-59), podemos ainda remover da base de dados

interna os registos exportados para isso basta selecionar “Remover registos da BD interna apos a exportação” (ponto 2 da Figura 4-59).

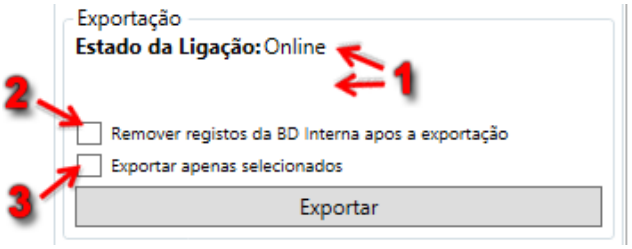


Figura 4-59: Estado e opções da exportação

Para exportar apenas registos selecionados, clicamos em “Exportar apenas selecionados” (ponto 1 da Figura 4-60) e depois selecionamos os registos a exportar (ponto 2 da Figura 4-60).

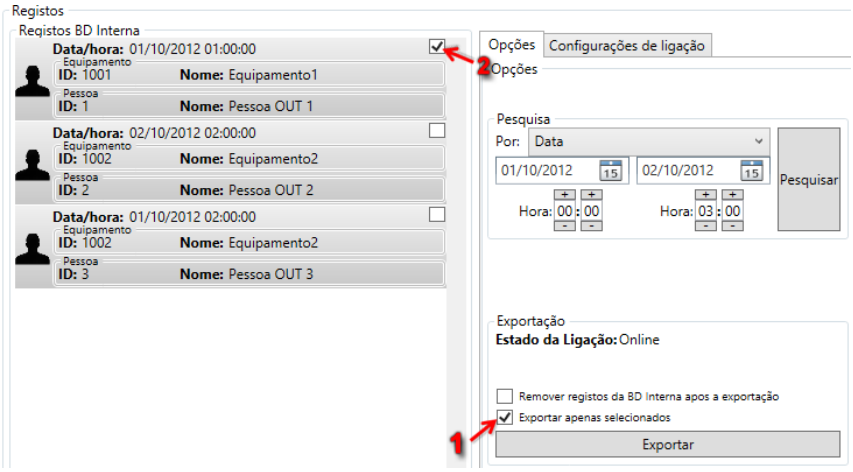


Figura 4-60: Exportar apenas registos selecionados.

Finalmente clicamos no botão “Exportar”, que se a operação for bem-sucedida, será mostrada a mensagem seguinte (Figura 4-61)

Figura 4-61: Mensagem de confirmação

A figura seguinte (Figura 4-62) confirma que o processo funcionou a 100% e que o registo selecionado (neste caso a pessoa 1) foi exportado da base de dados interna. Para a base de dados externa O **antes** é o estado da tabela antes da exportação e o **depois** é o estado da tabela depois do registo ser exportado e nos ser mostrada a mensagem de confirmação (Figura 4-61).

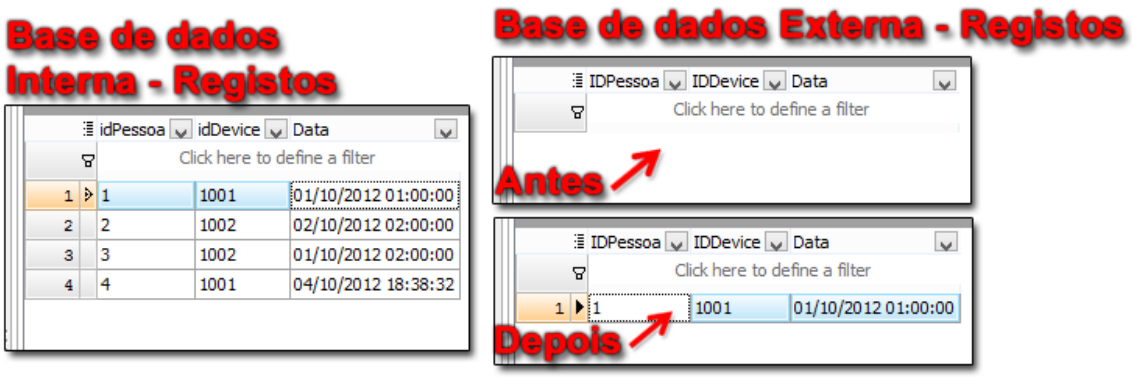


Figura 4-62: Exportar Registos.

4.1.10 Remover Equipamento

Para remover um equipamento primeiro temos de o selecionar clicando em cima dele (Figura 4-63);

Figura 4-63: Equipamento selecionado.

Depois clicamos no botão “Remover” que nos mostra a mensagem seguinte (Figura 4-64)

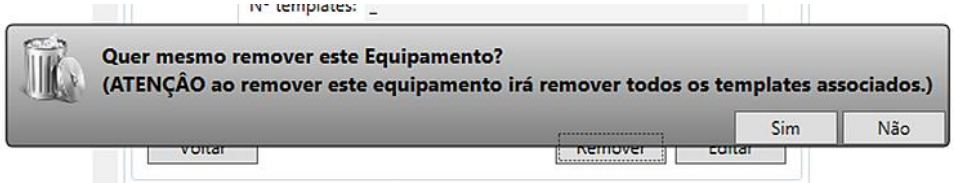


Figura 4-64: Mensagem remover equipamento

Posteriormente clicamos no botão “*sim*” e se a operação tiver sucesso vai aparecer a seguinte mensagem (Figura 4-65).

Figura 4-65: Mensagem equipamento removido.

A figura seguinte (Figura 4-66) confirma que o processo funcionou a 100% e que o equipamento foi removido da base de dados interna. O **antes** é o estado da tabela antes do equipamento ser removido e o **depois** é o estado da tabela depois do equipamento ser removido e nos ser mostrada a mensagem de confirmação (Figura 4-65).

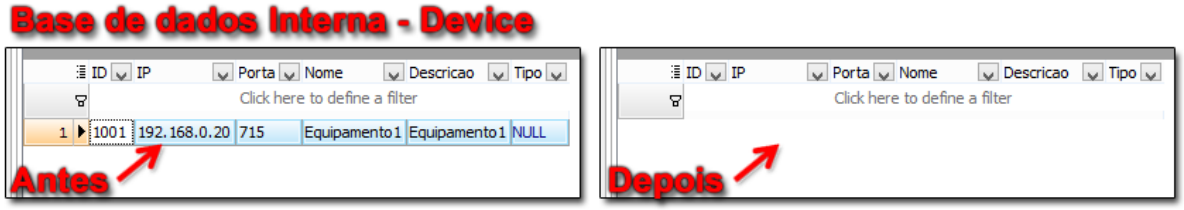


Figura 4-66: Remover equipamento da base de dados interna.

4.1.11 Remover Pessoa

Para remover uma pessoa da base de dados interna vamos ao menu principal (Figura 4-2) e escolhemos a opção "Ver/Importar/Exportar Pessoas" que deverá apresentar a seguinte *layout* (Figura 4-67)

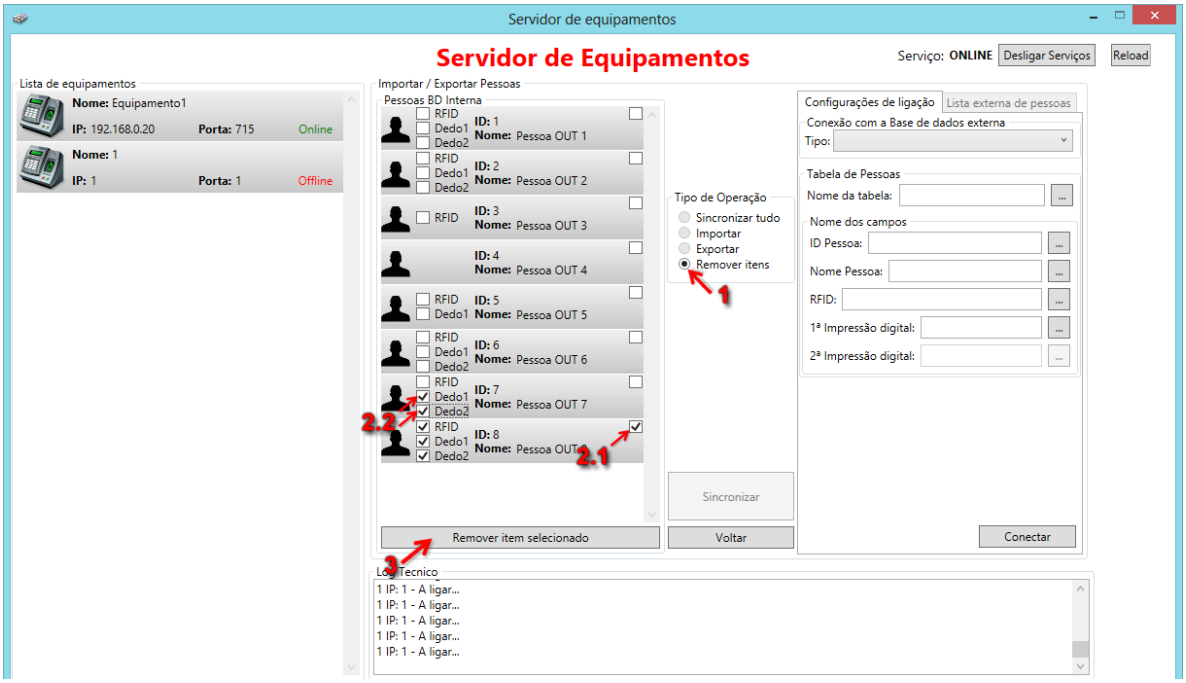


Figura 4-67: Ver/Importar/Exportar/Sincronizar pessoas.

Depois escolhemos a opção "Remover itens" (ponto 1 da Figura 4-67), depois selecionamos as pessoas (ponto 2.1 da Figura 4-67) ou *templates* (ponto 2.2 da Figura 4-67) a remover e por

fim clicamos no botão ”Remover itens selecionados” (ponto 3 da Figura 4-67) que deverá mostra a mensagem seguinte (Figura 4-68)

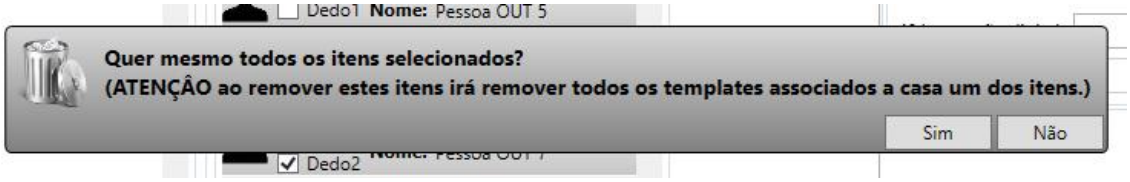


Figura 4-68: Mensagem remover Base de dados

Depois clicamos no botão *sim* e vai aparecer a seguinte mensagem (Figura 4-69) em caso de sucesso da operação.

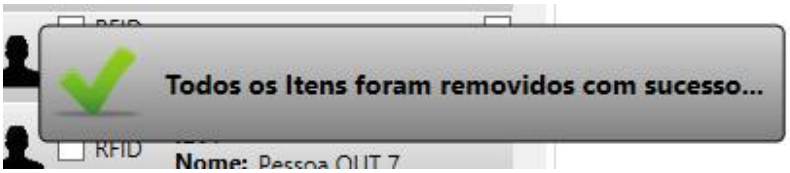


Figura 4-69: Mensagem base de dados removida.

A figura seguinte (Figura 4-70) confirma que o processo funcionou a 100% e que a pessoa selecionada e os *templates* selecionados foram removidos da base de dados interna. O **antes** é o estado da tabela, antes dos itens serem removidos e o **depois** é o estado da tabela depois dos itens serem removidos e nos ser mostrada a mensagem de confirmação (Figura 4-69)

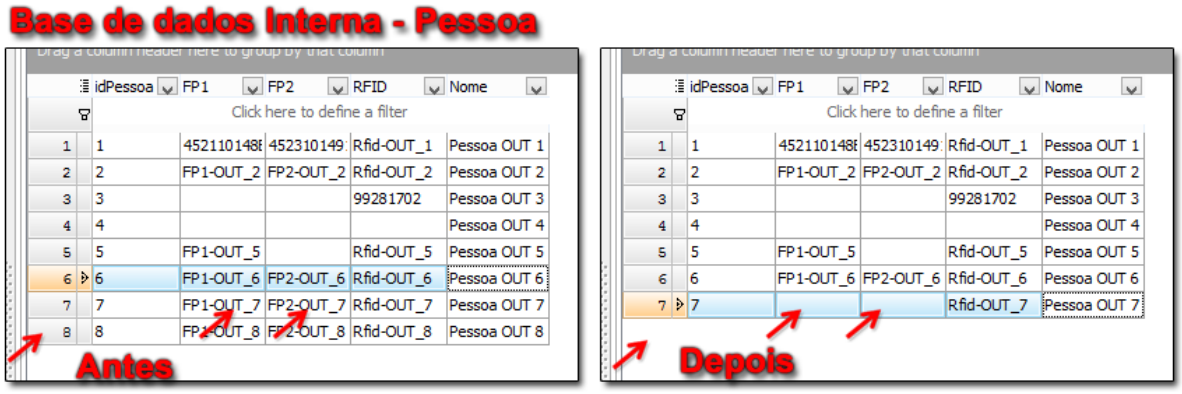


Figura 4-70: Remover conexão da base de dados interna.

5. Conclusão

Neste capítulo pretende-se apresentar as conclusões obtidas ao logo desta tese, indicar alguns problemas que surgiram na implementação, apresentar algumas sugestões para implementações futuras e fazer uma analise critica das funcionalidades e viabilidade destes sistemas/tecnologias.

Depois de estudarmos as várias tecnologias podemos concluir que os sistemas de autenticação biométrica atuais já estão com um nível de precisão muito bom mas, mesmo com todos os avanços tecnológicos destes equipamentos, ainda continuam com alguns problemas por resolver pelo que podemos concluir que não existem sistemas de autenticação perfeitos para todas as situações. Assim, todos são potencialmente úteis, uns mais outros menos, tudo dependendo do cenário de operação e da segurança pretendida. Por exemplo, se pretendemos fazer autenticação de operários numa fábrica onde existem máquinas ruidosas em funcionamento nunca poderíamos usar o reconhecimento de voz, uma vez que esta tecnologia é altamente afetada pelo ruido, mas podíamos implementar um sistema de reconhecimento impressões digitais, ou qualquer outro que não seja afetado pelo ruido. Por outro lado, se pensarmos que a zona é altamente restrita e tem de haver um nível de segurança no acesso muito alto então nessa situação não basta um sistema simples: temos de implementar um sistema mais seguro como a iris e/ou a retina. Se a segurança não é o mais importante mas sim a capacidade de validar muitas pessoas então teremos de optar por um sistema mais rápido e menos preciso e neste caso a geometria da mão poderia ser uma ótima escolha.
Relativamente ao uso da multi-biomeria concluímos que melhora significativamente a precisão de sistemas que usam apenas uma biometria, uma vez que o uso de varias biometrias em conjunto atenua os erros e limitações que podem ocorrer quando usamos essas mesmas biometrias separadamente. Quantas mais biometrias estiverem envolvidas no processo, maior precisão terá o sistema, mas em contrapartida o sistema também será mais lento e mais desconfortável para o utilizador, logo o numero de biometrias e que biometrias serão fundidas

num sistema deste tipo tem de ser bem pensado tendo em conta o nível de precisão o conforto para os utilizadores e, mais importante, a viabilidade, isto é, não convém aplicar um sistema muiti-biometrico com biometrias lentas ou com muitas biometrias, num local onde é necessário autenticar muitas pessoas num curto espaço de tempo.

Relativamente à elaboração da aplicação, podemos concluir que o uso da linguagem de programação C# revelou-se uma escolha acertada uma vez que é uma linguagem de fácil compreensão e foi relativamente fácil fazer a integração com o equipamento de autenticação biométrica e RFID utilizado na parte pratica.
A aplicação desenvolvida foi capaz de:

- Ligar-se ao equipamento;
- Adicionar e remover equipamentos;
- Permitir a consulta da lista de pessoas;
- Permitir a importação, exportação e sincronização de pessoas entre quatro tipos de bases de dados externas mais conhecidas (MySql, Sqlite, Oracle, Sql Server) e a base de dados interna;
- Remover pessoas e/ou *templates* na base de dados interna, quando estas, já não são necessárias;
- Recolher informação lida pelo equipamento, nomeadamente impressões digitais e etiquetas RFID;
- Registar novas impressões digitais e atribuir etiquetas RFID a utilizadores;
- Atribuir *templates* biométricos a cada equipamento;
- Registar o ponto de cada pessoa registada em cada equipamento na base de dados interna;
- Permitir o acesso de pessoas autorizadas e negar o acesso a pessoas não autorizadas;
- Consultar a lista de registos internos
- Exportar a lista de registos, mediante uma consulta prévia, para os quatro tipos de bases de dados externas mais conhecidas (MySql, Sqlite, Oracle, Sql Server);
- Aplicação desenvolvida num ambiente modular que permite a adição de novas funcionalidades mais facilmente.

Existiram alguns problemas, nomeadamente ao tentar ligar o equipamento que foi fornecido ao computador por não trazer manual de instruções. Desta forma tivemos de fazer várias tentativas com vários sistemas operativos, porque a aplicação “SetAddr.exe” não tinha a dll “DComunic.dll” que já não é usada nos sistemas mais recentes. Por fim conseguimos ligar o equipamento utilizando o sistema operativo Windows XP do qual copiamos a dll “DComunic.dll” para a pasta da aplicação, fazendo com que esta já funcione nos sistemas operativos mais recentes.
Isto significa que na utilização de equipamentos de identificação mais antigos, temos de ter em conta a evolução dos sistemas operativos uma vez que estes equipamentos podem usar

programas com algumas dll's que já não são usadas ou não são compatíveis com os sistemas mais recentes, fazendo com que estas aplicações não funcionem.
Ainda relativamente ao equipamento notamos que se forçarmos o dispositivo nomeadamente na leitura das impressões digitais o equipamento "encrava" e reinicia, logo podemos concluir que este tipo de equipamentos pode-se tornar instável se tiver que ler muitas impressões digitais num espaço de tempo muito pequeno de tempo.
Tivemos também algumas dificuldades na configuração de algumas bases de dados para efetuar os testes, nomeadamente o Oracle e o Sql Server, devido a alguns problemas com as configurações, uma vez que houve alguns conflitos de portas usadas que depois de detetados foram facilmente resolvidos.

Como sugestões para trabalhos futuros podemos sugerir a implementação de mais equipamentos de outras marcas e de biometrias diferentes, implementação de tipos de bases de dados menos conhecidos tais como: IBM Informix, PostgreSQL, Firebird, HSQLDB, IBM DB2, mSQL, TinySQL, JADE, ZODB, etc. e também a importação/exportação para ficheiro nomeadamente ficheiros XML.

Finalmente a elaboração deste trabalho contribuiu para conhecer melhor algumas técnicas de autenticação biométrica assim como seus pontos fortes e fracos aos quais temos de ter em conta quando escolhemos um sistema biométrico, assim como contribuiu para aumentar o conhecimento ao nível da programação e integração destes equipamentos.

Em resumo, embora tivesse um universo de teste muito limitado, posso concluir que estas tecnologias são viáveis para o reconhecimento e autenticação de pessoas (numa escala não muito elevada de utilizadores) de forma simples para os utilizadores e para as entidades que pretendem fazer esse controlo.

REFERÊNCIAS

[1]. Afsar, F. et al (2004) – Fingerprint Identification and Verification System using Minutiae Matching. Proceedings of National Conference on Emerging Technologies. Islamabad;

[2]. Página: ACronym em português – Soluções para Controlo de Acessos: http://www.controlo-acessos.com;

[3]. Liu, S.e.S., (2001) – "A Practical Guide to Biometric Security Technology," IEEE Computer Society);

[4]. Wildes, R. (2005) – Iris Recognition. In Wayman, J. et al. Biometric Systems – Technology, Design and Performance Evaluation. Springer;

[5]. Pagina: Idonic people & electronic – Biometria e sistemas biométricos: http://www.idonic.com/index.php?id=333;

[6]. DAUGMAN, J., (January 2004) – "How Iris Recognition Works" , University of Cambridge;

[7]. DAUGMAN, J., (November 2006) – "Probing the Uniqueness and Randomness of IrisCodes" , Proceeding of IEEE;

[8]. DAUGMAN, J. (December 2001) – "The importance of being random: statistical principles of Iris Recognition", University of Cambridge;

[9]. WILLIAMS, G. O, (August 2006) – "Iris Recognition Technology" , Iridian Technologies, 2001;

[10]. NSTC Subcommittee on Biometrics,"Iris Recognition";

[11]. Davies, S. (1994) Touching Big Brother – How biometric technology will fuse flesh and machine, Information Technology & People, Vol 7, No. 4;

[12]. Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L. e Jain, A. K. (2002) – FVC2002: Second Fingerprint Verification Competition, Proceedings of the International Conference on Pattern Recognition – ICPR2002;

[13]. CHOU, Wu; JUANG, B.H. (2002) – Pattern Recognition in speech and Language Processing. CRC Press, Inc;

[14]. Alexandre Fernandes de Moraes, (2006) – Método para avaliação da tecnologia biométrica na segurança de aeroportos, São Paulo;

[15]. Zhang, Y.B.; Li, Q.; You, J.; Bhattacharya, (2007) P.Palm vein extraction and matching for personal authentication. In Proceedings of the 9th International Conference on Advances in Visual Information Systems, Shanghai, China;

[16]. Wikipédia. Olho humano. http://pt.wikipedia.org/wiki/Olho_humano;

[17]. Huang, B.N.; Dai, Y.G.; Li, R.F. (2010) Finger-vein au thentication based on wide line detector and pattern normalization. In Proceedings of the 20th International Conference on Pattern Recognition, Istanbul, Turkey;

[18]. Samuel K. Lee, (2005) – Proof of concept: iraqi enrollment via voice authentication project, California;

[19]. Alexandre Nunes de Oliveira, (2009) – Proposta de utilização da biometria aplicada na segurança das transações bancárias, Hamburgo;

[20]. Bruno Miguel D´Avó Vieira Lopes, (2009) – Modelos Computacionais para Sistemas Automáticos de Identificação de Impressões Digitais;

[21]. Hélder José da Silva Matos, (2011) – Reconhecimento Biométrico Baseado na Geometria da Mão, Porto;

[22]. Fábio André Ferreira Marques, (2008) – Viabilidade de Implementação de um Sistema Biométrico de Autenticação, Aveiro;

[23]. Bruno Elias Penteado, (2009) – Autenticação biométrica de usuários em sistemas de e-learning baseada em reconhecimento de faces a partir de vídeo;

[24]. Sídnei Augusto Drovetto Junior, (2007) – Reconhecimento facial 3d utilizando o simulated annealing com as medidas surface interpenetration measure e m-estimator sample consensus, Curitiba;

[25]. Gonçalo Filipe da Fonseca Lourenço, (2009) – Reforço da Segurança das Biométricas utilizando Codificação de Fonte Distribuída, Lisboa;

[26]. Jorge Rei, (2010) – RFID Versus Código de Barras da Produção à Grande Distribuição, Porto;

[27]. Jossy P. George, (2012) – Development of efficient biometric recognition algorithms based on fingerprint and face, Bangalore;

[28]. Privacy International, Statewatch e European Digital Rigts (Março, 2004) – An Open Letter to the ICAO .A second report on 'Towards an International Infrastructure for Surveillance of Movement';

[29]. RIBEIRO, Sérgio Santiago (2008) – Tecnologias de controle de acesso e sua aplicação no sistema de segurança aeroportuário. Brasília: Monografia. Universidade de Brasília;

[30]. Curado, Manuel (Nov 2006) – "Pessoas transparentes, Base de dados e Biometria" - Conferência no Colóquio de Bioética da Universidade do Minho;

[31]. Faria, Diego Resende (Dezembro 2005) – "Reconhecimento de impressões digitais com baixo custo computacional";

[32]. Filipe Magalhaes, Helder Oliveira e Aurelio Campilho. (2009) –A new method for the detection of singular points in fngerprint images. Proceedings of the IEEE Workshop on Applications of Computer Vision, páginas 157–162;

[33]. Tsapatsoulis e C.S. Pattichis. (2009) – Palm geometry biometrics: A score-based fusion approach. Proce - edings of AIAI, 425:158–167;

[34]. Jain, A.K., Ross A., and Prabhakar, S., (January 2004) – "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and System for Video Technology, vol. 14, no. 1, pp. 4-20;

[35]. PINHEIRO, José Mauricio. (2008) – Biometria nos Sistemas Computacionais – Você é a Senha.Rio de Janeiro: Ciência Moderna;

[36]. VIGLIAZZI, Douglas, (2006) – Biometria: Medidas de Segurança. Florianópolis: Visual Books;

[37]. Putte, T. e Keuning, J. (2000) – Biometrical fingerprint recognition: don´t get your fingers burned, Proceedings of IFIP TC8/WG8.8 Forth Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers 289-303;

[38]. O'TOOLE, A. J.; ROARK, D. A.; ABDI, H. (2002) – Recognizing Moving Faces: A Psychological And Neural Synthesis. Trends in Cognitive Science, 6:261-266;

[39]. Bubeck, (2003) – Uwe M. "Multibiometric Authentication - An Overview of Recent Developments", San Diego State University, USA;

[40]. Boechat, G. (Fevereiro 2008) – Dissertação de Mestrado - Proposta de um modelo de arquitectura biométrica para identificação pessoal com estudo da dnâmica da digitação, Universidade Federal de Pernambuco. Recife, Brasil;

[41]. Bowyer, K. W., e Flynn, P. J. (2008) – Image understanding for iris biometrics: A survey, in Computer Vision and Image Understanding, vol. 110, edição 2, pp 281–307;

[42]. Chang, K., Bowyer, K., e Flynn, P. (2003) – Multimodal 2D and 3D biometrics for face recognition. IEEE International Workshop on Analysis and Modeling of Faces and Gestures, pages 187–194;

[43]. COSTA, Luciano (2007) – Um Modelo de Autenticação Biométrica para WEB Banking. Florianópolis: Dissertação de Mestrado, Universidade Federal de Santa Catarina;

[44]. Jain, A. K., Nandakumar, K., e Nagar., A. (Janeiro de 2008) – Biometric Template Security. EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics.

[45]. Júnior, C. A. (2005) – Biometria com Enfoque em Reconhecimento de Iris, Trabalho final do curso. Universidade Estadual de Londrina;

[46]. Kazienko, J. F. (2003) – Dissertação de mestrado: Assinatura digital de documentos eletrônicos através da impressão digital. Programa de Pós-Graduaçãoem Ciência da Computação. Universidade Federal de Santa Catarina;

[47]. Przybocki, M., e Martin, A. (2004) – NIST speaker recognition evaluation chronicles. Technical report, Speech Group, Information Access Division, Information Technology Laboratory National Institute of Standards and Technology USA. Publicado na Conferência The Odissey;

[48]. Sanchez-Reillo, R., Sanchez-Avila, C., e Gonzalez Marcos, A.(2000) – Biometric identification through hand geometry measurements.IEEE Transactions on PatternAnalysis and Machine Intelligence, 22(10):1168–1171;

[49]. [Uludag 2004] Uludag, U., Pankanti, S., Prabhakar, S., e Jain., A. K.(2004) – "Biometric cryptosystems: issues and challenges, Proceedings of the IEEE", vol. 92, no. 6, pp. 948–960.

[50]. [Wildes 1997] Wildes, R.(1997) – "Iris recognition: an emerging biometric technology, in Proceedings of the IEEE", vol. 85, no. 9.

[51]. [Zhao 2003] Zhao, W., Chellappa, R., Phillips, P. J., e Rosenfeld, A. (2003) – "Face recognition: A literature survey. ACM Computing Surveys", 35(4):399–458.

[52]. [Turk 1991] Turk, M., e Pentland, A.(1991) – "Face recognition using eigenfaces.In IEEE Computer Society Conference on Computer Vision and PatternRecognition", pages 586–591. Maui, HI, EUA.

[53]. Chunfeng Hu, Jianping Yin, En Zhu, Hui Chen and Yong Li, (2008) – "Fingerprint Alignment using Special Ridges," International Conference on Pattern Recognition, pp. 1-4;

[54]. Dadgostar, M Tabrizi, P R Fatemizadeh and E Soltanian-Zadeh, (2009) – "Feature Extraction Using Gabor-Filter and Recursive Fisher Linear Discriminant with Application in Fingerprint Identification," Seventh International Conference on Advances in Pattern Recognition, pp. 217 – 220;

[55]. Jain, A K, Yi Chen and Demirkus, (2007) – "Pores and Ridges: HighResolution Fingerprint Matching Using Level 3 Features," IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 15-17;

[56]. Manvjeet Kaur, Mukhwinder Singh, AkshayGiridhar and Parvinder S. Sandhu, (2008) – "Fingerprint Verification System using Minutiae Extraction Technique," Proceedings of World Academy of Science, Engineering and Technology, vol. 36, pp. 497-502.

APÊNDICE 1

ANEXO 1

PRINCÍPIOS SOBRE A UTILIZAÇÃO DE DADOS BIOMÉTRICOS NO ÂMBITO DO CONTROLO DE ACESSOS E DE ASSIDUIDADE

Considerando que:

1. O recurso a sistemas biométricos tem vindo, recentemente, a apresentar-se como um meio tecnológico que visa substituir ou reforçar a segurança dos meios tradicionais de controlo de entradas e saídas, sendo ainda de extrema utilidade quando se pretende – por razões de segurança ou de segredo – restringir, nomeadamente, o acesso a locais cuja entrada é privilégio de alguns.
2. Os sistemas biométricos têm outras vantagens em relação aos sistemas tradicionais, na medida em que a informação necessária para permitir o acesso não é «perdível» ou suscetível de apropriação ilícita. Por outro lado, a pessoa não necessita de recordar números, códigos ou qualquer outra chave de identificação.
3. Na introdução de novos sistemas não pode deixar de ser feita uma comparação, nas várias perspetivas relevantes (em particular em termos de proteção de dados) entre os sistemas que existem e aqueles que se pretendem instalar.
4. Para alguns autores a biometria assenta na mensuração e na enumeração, utilizando as estatísticas e o cálculo de probabilidades com o objetivo de dar aos fenómenos biológicos uma «expressão quantitativa plausível», o que permite afirmar que se a biometria traz um pouco de precisão, ela fá-lo em detrimento da certeza.
5. Os critérios a utilizar para a escolha de um sistema biométrico têm em conta, nomeadamente, o conforto na utilização, a precisão, a relação qualidade/preço e o grau de segurança.
6. As características biométricas não deixam de representar uma parte da individualidade das pessoas, estando ligadas intrinsecamente à própria pessoa.
7. A introdução do sistema no âmbito da relação de trabalho deverá procurar obter a adesão dos trabalhadores e não ser imposto, na medida em que a sua eficácia depende, também, em grande medida, de fatores psicológicos que são determinantes para a aprendizagem na utilização do sistema e na cooperação dos utilizadores, quer no momento da captura quer na fase de comparação.

8. A vulgarização dos sistemas de videovigilância e o uso descontrolado desta nova forma de tratamento demonstra, em algumas situações, que é fundamental que se tomem medidas realistas para evitar que se instale no posto de trabalho, sem justificação visível, um «clima securitário» e de suspeição generalizado, quer em relação a clientes quer a trabalhadores.
9. Importa ter uma posição prudente e equilibrada que incentive os fabricantes de sistemas biométricos a adotar soluções técnicas que, protegendo a privacidade, minimizem os riscos de utilizações indevidas.
10. Os equipamentos biométricos registam, normalmente, uma representação digital (template) e não uma amostra biométrica passível de ser reproduzida, ou seja, o template armazenado não tem utilidade nenhuma noutros sistemas e não pode ser usado para reproduzir os dados biométricos originais. Isto é, na generalidade dos casos, os sistemas biométricos não utilizam a tecnologia de digitalização da imagem obtida, mas fazem a «codificação» dos dados recolhidos.
11. O sistema biométrico que, através do processo de algoritmização, gerou o template que representa numericamente a característica biométrica captada, não permite fazer a reversão e, por conseguinte, descodificar e reproduzir, de forma digitalizada, a imagem da característica biométrica (v.g. representação digitalizada da impressão digital, da íris, da geometria da mão ou da geometria facial).
12. O responsável do tratamento não dispõe, por isso, de uma base de dados de características biométricas, mas de uma lista estruturada e numeralizada dessas características.
13. Será diferente para a invasão da privacidade o armazenamento através da digitalização e referenciação das características biométricas ou a constituição de uma base de dados dos *templates* dessas características.
14. A centralização das características biométricas em bases de dados apresenta perigos acrescidos para a privacidade, razão pela qual não é admissível, por princípio, o seu relacionamento com outro tipo de tecnologias (v.g. videovigilância).
15. Esse relacionamento não prejudica a possibilidade de utilização de «sistemas multimodais», caracterizados pelo recurso a mais de uma característica biométrica para conferir uma maior eficácia e rigor às operações de reconhecimento ou autenticação.
16. As empresas que comercializam sistemas biométricos garantem, muitas vezes, que está totalmente assegurada a privacidade uma vez que esses sistemas não permitem a «reversão» ou comparação dos *templates*, tanto mais que as chaves dos respetivos *templates* estão na posse do fabricante e são inacessíveis às entidades que fornecem ou adquiram os equipamentos.
17. O template, que representa a característica biométrica do indivíduo, pode ser gravado ou memorizado no sistema central, em terminais ou num suporte que o seu titular traz consigo (v.g. um cartão, um equipamento ou um código de barras).

18. Esta última tecnologia pode ser vantajosa, em termos de preservação da privacidade, para obviar à constituição de bases de dados centrais com armazenamento de características biométricas e permite uma maior rapidez na identificação do utilizador, em particular quando o sistema gere muitos utilizadores ou precisa de fazer a verificação remota. Porém, não será de esquecer que tem o inconveniente de exigir que o utilizador não se esqueça de transportar o cartão ou código de barras consigo, obrigando, ainda, à produção de novo cartão em caso de extravio ou má conservação.
19. A qualidade e aceitação de um sistema biométrico dependem, fundamentalmente, da avaliação do seu grau de desempenho.
20. O grau de desempenho depende, em certa medida, da sua capacidade de resposta em termos de velocidade de identificação e, especialmente, da taxa de precisão ou de erro que apresenta.
21. Um sistema biométrico que não seja fiável cumpre de forma deficiente as finalidades que se propõe atingir, correndo o risco de tratar – especialmente em «sistemas de identificação» – informação desatualizada.
22. A existência de uma grande probabilidade de «falsos utilizadores» poderem ser aceites permite que – no contexto de uma empresa ou serviço público onde o sistema visa controlar o horário de trabalho – as apontadas deficiências no desempenho potenciem a troca de identificação de alguns trabalhadores (eventualmente com características semelhantes) e a consequente anotação de atrasos, faltas ou presenças de forma indevida.
23. A aquisição de sistemas biométricos passa pela adoção de soluções alternativas para suprir as suas insuficiências, especialmente as que resultam das taxas de falsas rejeições, aceitações ou impossibilidade temporária de o trabalhador apresentar o seu dado biométrico para autenticação ou reconhecimento.
24. Estes sistemas não são infalíveis e não vêm resolver todos os problemas de autenticação ou identificação, razão pela qual será de esperar que existam limitações e «imponderáveis» em matéria de qualidade de desempenho.
25. Certos sistemas biométricos apresentam alguns riscos por não estarem convenientemente testados e por utilizarem técnicas recentes, cuja eficácia ainda não se mostra comprovada.
26. O titular tem o direito de saber se a sua característica biométrica se encontra armazenada e obter a respetiva comprovação, nomeadamente através do desencadeamento da operação de reconhecimento ou de autenticação.
27. A finalidade do tratamento assenta na necessidade de agilizar o cumprimento de um objetivo que a lei reconhece integrar-se no âmbito dos poderes de controlo da entidade responsável pelo tratamento: a fixação do horário de trabalho, o controlo da assiduidade e o registo do tempo de trabalho. Deste registo depende, ainda, a contabilização e o controlo do trabalho suplementar.

28. A operação de recolha das características biométricas com a finalidade de controlo do horário de trabalho não envolve, em si mesmo, uma violação da integridade física do trabalhador, do seu direito à privacidade ou da sua intimidade.
29. A peculiaridade deste novo método de controlo da assiduidade resulta da necessidade de o trabalhador ter de aceitar que elementos da sua identidade física, morfológica ou comportamental sejam captados e armazenados numa base de dados (ou noutro suporte) e apresentados perante um «sistema de reconhecimento» no início e termo do período de trabalho diário.
30. Independentemente da autorização da CNPD, o titular dos dados pode, em abstrato, por força do artigo 12.º al. a) da Lei 67/98, opor-se ao tratamento sempre que haja «razões ponderosas e legítimas relacionadas com a sua situação particular» e que se apresentem com relevância para fazer prevalecer o seu direito sobre os interesses do responsável pelo tratamento.
31. Quando a CNPD considerar que o dado biométrico se apresenta como o meio adequado para assegurar uma «finalidade legítima» – o controlo do horário de trabalho – e autorizar o tratamento com essa finalidade não cabe à CNPD pronunciar-se sobre os procedimentos e o dever de cooperação em tudo o que seja necessário à captação das características biométricas.
32. O dever de cooperação só se pode concretizar, no entanto, quando a entidade responsável pelo tratamento assegurar, junto do trabalhador, um efetivo dever de informação prévio em relação às finalidades determinantes da recolha, destinatários e condições de utilização daqueles dados, em cumprimento do disposto no artigo 10.º n.º 1 da Lei 67/98, bem como o esclarecimento de dúvidas e receios que esta nova tecnologia possa suscitar.
33. Os dados em si mesmos (impressão digital, geometria facial, íris ou retina) não se enquadram no conceito de «vida privada», nem as finalidades prosseguidas permitem um enquadramento dessas categorias de dados na previsão do artigo 7.º n.º 1 da Lei 67/98.
34. As «condições de legitimidade» do tratamento só poderão ser enquadradas numa das previsões do artigo 6.º da Lei 67/98.
35. Será de afastar o consentimento como «condição de legitimidade», em face da posição em que o trabalhador se encontra.
36. Será de afastar, igualmente, a aplicação da alínea b) do artigo 6.º na medida em que, perante a omissão do Código do Trabalho e da legislação aplicável à Função Pública em relação à possibilidade de controlo por meio de sistemas biométricos, não é possível concluir – perante disposições legais tão genéricas sobre "registo de horas de trabalho prestadas pelo trabalhador" – que se tenha pretendido fundamentar nessas disposições qualquer forma de controlo deste tipo.
37. Se não for estabelecido contratualmente o tratamento de dados biométricos por razões inerentes e determinadas pela especial natureza do contrato (v.g. entrada em

locais de «alta segurança»), a mera celebração do contrato não determina, só por si, uma legitimação para o tratamento destes dados.

38. O simples facto de ter sido celebrado um contrato não implica, só por si, que o trabalhador esteja obrigado a fornecer «informações adicionais» relativas às suas características biométricas, tanto mais que esses elementos de identificação, contrariamente ao que acontece com o nome, não são imprescindíveis à perfeição da declaração negocial.
39. A legitimidade para o tratamento de dados com a finalidade de controlo do horário de trabalho (assiduidade) só poderá ter como fonte a previsão do artigo 6.º al. e) da Lei 67/98, uma vez que o tratamento é feito na «prossecução de interesses legítimos do responsável».
40. O artigo 6.º alínea e) da Lei 67/98 obriga a CNPD, em cada caso concreto, a apurar se «não prevalecem os interesses ou os direitos liberdades e garantias dos titulares dos dados» sobre o interesse legítimo invocado pelo responsável pelo tratamento.
41. Este procedimento é o que melhor se ajusta à aplicação do princípio da proporcionalidade e, por isso, o tratamento deve deixar de ser feito quando se revele injustificado, por ser desajustado e excessivo, ou quando – pela sua falta de fiabilidade – comprometa a finalidade determinante do tratamento.
42. O princípio da proporcionalidade constitui, igualmente, o critério determinante das decisões relativas ao tratamento de dados biométricos tomadas pelas autoridades de proteção de dados.
43. A eventual «invasão da privacidade» deve ser abordada nas duas fases do tratamento: (a)na fase do registo das características biométricas e do subsequente armazenamento no sistema e (b) na fase da identificação com o objetivo de assegurar o registo dos movimentos do trabalhador no local de trabalho.
44. A operação de captação de dados biométricos – que implica a cooperação/anuência do trabalhador através da «exposição» da respetiva parte do seu corpo (dedos, mão, olho ou rosto) para tratamento das características físicas ou morfológicas da sua identidade pessoal que se pretendem coligir para fins de identificação ou autenticação – não pode ser realizada com violação da sua identidade pessoal (art.26.º da CRP), com lesão da sua integridade física (art. 25.º n.º 1 da CRP) ou com intromissão na intimidade da vida privada (artigo 26.º da CRP).
45. Na apreciação do «grau de intromissão» importa considerar a forma como se obtêm os elementos de identificação e as finalidades que estão na base da colheita de características físicas dos trabalhadores (v.g. se representam finalidades discriminatórias).
46. Na colheita de dados biométricos – normalmente a impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina – a captação não tem qualquer implicação com a integridade física do trabalhador na medida em que a finalidade visada ou a forma como os elementos da identidade são captados não têm implicações no recato ou no pudor.

47. A simples operação de recolha, em exclusivo, para fins de controlo da assiduidade do trabalhador não afeta o direito à identidade pessoal e da intimidade da vida privada, garantidas constitucionalmente no artigo 26.º da CRP.
48. Em geral, a submissão à operação de recolha não se poderá traduzir numa discriminação ou violação do dever de respeito e dignidade do trabalhador, nem afetar o recato ou pudor que a sua condição supõe, tanto mais que a finalidade que está subjacente à captação destes dados não envolve, por princípio, qualquer discriminação ou desconfiança em relação ao próprio trabalhador.
49. Não é o dado biométrico em si mesmo que pode afetar o direito à privacidade da pessoa, mas a finalidade com que é utilizado e os riscos que apresenta para a própria pessoa (risco de discriminação ou de cruzamento com outros sistemas, consequências produzidas em razão da sua falta de fiabilidade, efeitos na sua esfera pessoal no caso de falsificação ou usurpação da característica biométrica).
50. Se justifica alertar para a aplicação, com especial pertinência, do princípio contido no artigo 13.º da Lei 67/98, que proíbe a tomada de decisões com base, exclusivamente, em tratamento automatizado.
51. O princípio da proporcionalidade "impõe que qualquer tratamento de dados pessoais, atenta a sua finalidade concreta, deva ser avaliado em termos de idoneidade e de intervenção mínima", o que envolve uma ponderação, casuística, entre a finalidade pretendida e o sacrifício ou limitação de direitos ou interesses dos trabalhadores que ela implica.
52. A utilização indevida pode ser melhor prevenida se as características biométricas não se encontrarem centralizadas numa base de dados, razão pela qual se defende, sempre que possível, o registo das características biométricas (em particular quando estiver em causa a impressão digital) em cartão que o trabalhador deve transportar.
53. A proliferação e massificação destas formas de tratamento e a possibilidade de relacionamento com outras tecnologias (v.g. videovigilância) são fatores que, em termos de proteção da privacidade, não devem ser negligenciados.

54. A CNPD alerta os responsáveis para a necessidade de cumprirem certos princípios de proteção de dados e informa que irá considerar os seguintes aspetos no momento da apreciação dos tratamentos de dados biométricos para controlo de acessos e de assiduidade:

I. O tratamento de dados biométricos, porque estamos perante dados pessoais, deve respeitar todas as condições estabelecidas na Lei 67/98, nomeadamente:

a) O tratamento deve ser feito com respeito pela reserva da vida privada (artigo 2.º) e para finalidades determinadas, explícitas e legítimas (art. 5.º n.º 1 al. b);

b) Os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade e proporcionados aos objetivos que se pretendem atingir (art. 5.º n.º 1 al. c);

c) O responsável só pode proceder ao tratamento se, de acordo com a natureza dos dados (artigo 6.º e 7.º), estiverem preenchidas as «condições de legitimidade»;
d) O responsável deve fazer a notificação destes tratamentos à CNPD (art. 27.º n.º 1).
e) O responsável deve assegurar o direito de informação em relação à existência de tratamento, dados pessoais tratados, finalidades e entidades a quem os dados podem ser transmitidos (cf. artigo 10.º);
f) O responsável não pode utilizar os dados biométricos para finalidade diversa da determinante da recolha (artigo 5.º n.º 1 alínea b) da Lei 67/98);
g) Aos titulares dos dados deve ser assegurado o direito de acesso, retificação ou oposição, nos termos dos artigos 11.º e 12.º alínea a).

II. No requerimento de notificação devem ser indicadas, com detalhe, as características do sistema biométrico, as condições de tratamento e outras condições que permitam à CNPD apreciar o pedido em termos de necessidade e de proporcionalidade. Deverão ser indicados, nomeadamente:
a) A capacidade do sistema e o número de trabalhadores abrangidos;
b) Forma como é armazenada ou gravada a característica biométrica;
c) Taxas de falsas rejeições ou de falsas aceitações do sistema;
d) Formas como foi ou vai ser assegurado o direito de informação aos trabalhadores;
e) Especificação do tipo de relacionamento com outros tratamentos (v.g. gestão de pessoal ou de remunerações);
f) Junção de declaração do fabricante, comprovativa de que as chaves dos algoritmos não são cedidas e de que os sistemas não permitem a reversão.

III. A preocupação primordial em relação à utilização de dados biométricos passa pela ponderação, no caso concreto, da idoneidade e da necessidade daquele meio e da conformidade dos motivos apresentados com o princípio da proporcionalidade.

IV. A finalidade do tratamento insere-se no âmbito do exercício de poderes de controlo conferidos legalmente ao responsável do tratamento, correspondendo a uma «atividade legítima».

V. O controlo de acessos e de assiduidade com recurso a dados biométricos apresenta-se como um meio adequado por corresponder a uma «finalidade legítima», razão pela qual esse controlo terá que ser enquadrado na previsão do artigo 6.º al. e) da Lei 67/98.

VI. A CNPD deverá verificar, numa ponderação dos interesses em presença e em cada caso concreto, se «não prevalecem os interesses ou os direitos liberdades e garantias dos titulares dos dados» sobre o «interesse legítimo» invocado pelo responsável.

VII. A recolha de dados biométricos – normalmente a impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina – não tem qualquer

implicação com a integridade física do trabalhador, não afetando, igualmente, o seu direito à identidade pessoal e à intimidade da vida privada, garantidos constitucionalmente no artigo 26.º da CRP.

VIII. Em geral, a operação de recolha e comparação das características biométricas não constitui fator de discriminação ou violação do dever de respeito, nem afeta o recato ou pudor do trabalhador.

IX. Se a inserção das características biométricas em cartão que o trabalhador traz consigo tem a vantagem de sossegar o trabalhador em relação ao não fornecimento da sua característica biométrica à entidade empregadora e de lhe permitir um controlo sobre a utilização dos seus dados biométricos, a verdade é que tem o inconveniente de exigir que o trabalhador tenha sempre o cartão consigo, obrigando o responsável a produzir novo cartão em caso de extravio ou mau estado de conservação.

X. Não estando afastados riscos efetivos de falsificação ou «apropriação» das características biométricas, aspeto que tem consequências imprevisíveis para os titulares nomeadamente se caminharmos para a utilização generalizada destes meios, a CNPD seguirá com atenção os novos desenvolvimentos tecnológicos.

XI. A utilização de sistemas com deficientes graus de desempenho (v.g. uma elevada taxa de falsas aceitações ou de falsas rejeições) pode comprometer a finalidade do tratamento – o controlo de entradas e saídas – e criar dificuldades acrescidas ao trabalhador, que se refletem no exercício dos seus direitos, tal como estão delineados na Lei 67/98.

XII. Se houver este risco, deve entender-se que o sistema não reúne as condições legais para desempenhar as finalidades de controlo uma vez que, para além de a informação se encontrar desatualizada, é um fator de grande instabilidade e de falta de confiança no sistema, colocando aos trabalhadores grandes dificuldades de prova em relação à comprovação da «falsa entrada» que lhes foi atribuída pelo sistema.

XIII. Se isso acontecer, o tratamento das características físicas intrínsecas do trabalhador contribui, nessas circunstâncias, para violar os princípios da qualidade dos dados e, em particular, o princípio da atualização, subjacentes à previsão do artigo 5.º da Lei 67/98.

XIV. Este aspeto, que é uma «condição de licitude do tratamento», condicionará o sentido da decisão da CNPD.

XV. Neste quadro, apresentam-se como bastante problemáticas as consequências jurídicas da utilização destas tecnologias uma vez que a «prova biométrica» tem vindo, cada vez mais, a ser questionada em face da reconhecida impossibilidade destes sistemas serem 100 por cento fiáveis.

XVI. Por isso, impõe-se que o responsável do tratamento não encare, sem qualquer flexibilidade, a introdução destes novos sistemas como instrumentos «infalíveis»

em termos de reconhecimento, devendo abordar com realismo as situações em que o trabalhador questiona a sua eficácia.

XVII. Os fornecedores de equipamentos biométricos, que devem ser chamados pelos responsáveis dos tratamentos a detalhar as suas características, podem vir a ser envolvidos e ter um papel ativo na apresentação de soluções mais seguras que impeçam a utilização de dados para outras finalidades ou que reforcem, de forma efetiva, a privacidade dos titulares dos dados.

XVIII. Na linha do que já dispõe o artigo 17.º n.º 4 do Código do Trabalho, deve ser reconhecido ao trabalhador o «controlo sobre o tratamento dos seus dados pessoais» colocando ao seu alcance mecanismos para verificar – no momento da sua identificação/autenticação – se o sistema fez o seu reconhecimento (ou se fez um «falso reconhecimento»).

XIX. Para obviar aos perigos decorrentes da falta de performance e eficácia no desempenho do sistema – que deve ser testado, na prática, durante um período experimental adequado – será desejável que, no momento da validação/identificação do trabalhador pelo sistema, haja mecanismos de «validação» adicional que permitam um maior rigor no reconhecimento ou autenticação (por exemplo, um écran junto ao sensor que forneça o nome da pessoa ou n.º de funcionário que acabou de ser identificada, a digitação prévia do n.º de empregado a que se seguirá a apresentação da característica biométrica perante o sensor).

XX. A utilização para finalidade não determinante da recolha carece, necessariamente, de autorização prévia da CNPD, nos termos dos artigos 23.º n.º 1 al. c) e 28.º n.º 1 al. d) da Lei 67/98.

XXI. Os dados pessoais recolhidos não podem ser comunicados a terceiros.

XXII. Os dados biométricos serão obrigatoriamente eliminados no momento da transferência do trabalhador para outro local de trabalho ou no caso da cessação do contrato de trabalho.

XXIII. A CNPD considera que, pelo menos numa primeira fase, as autorizações podem vir a ser dadas por um período experimental.

XXIV. Decorrido esse «período experimental» a CNPD fará uma avaliação destas tecnologias, podendo vir a fazer alterações, motivadas pela necessidade de observância de princípios de proteção de dados, em função das circunstâncias, condições de funcionamento e de desempenho dos sistemas biométricos.

XXV. Os trabalhadores e os seus representantes são convidados a estar atentos ao funcionamento do sistema e a canalizar os elementos úteis para a avaliação da CNPD.

26 de Fevereiro de 2004