

U.C. de Projeto Integrado de

Telecomunicações

Ano Letivo: **2021/2022**

**Relatório da Fase C**

**Grupo 2**

* Catarina Neves, a93088
* Eduardo Cardoso, a89627
* José Gomes, a93083
* Luís Oliveira, a89380

01/06/2022

Universidade do Minho

Mestrado Integrado em Engenharia de Telecomunicações e Informática

Índice

[1. Introdução 5](#_Toc104888070)

[2. Trabalho Relacionado 6](#_Toc104888071)

[2.1 ESP32 WebSocket: Control ESP32 Pins 6](#_Toc104888072)

[2.2 ESP32 Robot Car Using Websockets 7](#_Toc104888073)

[3. Fases do trabalho desenvolvido 8](#_Toc104888074)

[3.1. Protocolo de comunicação 8](#_Toc104888075)

[3.2. Sistema Central 10](#_Toc104888076)

[3.2.1 Mecanismos e políticas de segurança 10](#_Toc104888077)

[3.2.1.1 Enumerados 11](#_Toc104888078)

[3.2.1.2 Configuração do protocolo HTTP 12](#_Toc104888079)

[3.2.2 Tabelas da base de dados 13](#_Toc104888080)

[3.4. Servidor *Web* 14](#_Toc104888081)

[4. Análise de resultados e testes efetuados 16](#_Toc104888082)

[5. Conclusão 18](#_Toc104888083)

[5.1. Contribuição de cada aluno 18](#_Toc104888084)

[6. Lista de referências 19](#_Toc104888085)

Índice de figuras

Figura 1 - Tarefas propostas pela fase C. 5

Figura 2 – Variação de cor da tira LED. 6

Figura 3 - Serviço web implementado pelo autor. 7

Figura 4 - Lista de componentes necessários à construção do projeto. 7

Figura 5 - Declaração da porta, do endereço e do cliente usados para a comunicação com o Sistema Central. 8

Figura 6 - Envio da trama de dados e finalização da impressão na socket, no Gateway. 8

Figura 7 - Inicialização da socket servidor no sistema. 9

Figura 8 - Estrutura da diretoria "security". 10

Figura 9 - Tarefas abordadas no parágrafo anterior. 10

Figura 10 - Habilitações da categoria administrador. 11

Figura 11 - Habilitações da categoria utilizador normal. 11

Figura 12 - Comportamento do método secure. 12

Figura 13 - Declaração da característica temporal no servidor. 13

Figura 14- População do array a ser enviado pela característica. 13

Figura 15 - Leitura do valor temporal. 13

Figura 16 - Funções de conversão da data para o formato necessário. 13

Figura 17 - Página com todas as amostras. 14

Figura 18 - Página inicial do servidor web. 14

Figura 19 - Amostras armazenadas na base de dados. 16

Figura 20 - Amostras impressas no serviço web. 16

Figura 21 - Script que efetua o parsing das amostras. 16

Figura 22 - Definição das amostras hardcoded. 17

Figura 23 - Armazenamento e impressão das amostras hardcoded. 17

Lista de siglas e acrónimos

**SQL** *Structured Query Language*

**LED** *Light Emitting Diode*

**RGB** *Red Green Blue*

**GPIO** *General Purpose Input/Output*

**IDE** *Integrated Development Environment*

**IOT** *Internet Of Things*

**HTTP** *Hypertext Transfer Protocol*

# Introdução

Serve o presente relatório como síntese do trabalho desenvolvido e implementado no decorrer desta última fase. Este contém a descrição das estratégias e algoritmos adotados pelo grupo, tal como os respetivos testes realizados. Além dos tópicos acima citados, faz-se referência a trabalhos ou projetos similares, que se enquadram na ótica deste projeto.

O relatório abordará cada etapa desta fase de forma detalhada, ou seja, será apresentada a resposta ou proposta de solução empregue pelo grupo em junção com as ferramentas que foram necessárias para a sua construção.

A figura 1 ilustra o sumário das diferentes tarefas propostas nesta fase.

Uma imagem com texto, símbolo

Descrição gerada automaticamente

Figura 1 - Tarefas propostas pela fase C.

Nesta fase, o objetivo é a conclusão do Sistema Central, com funcionalidades mais avançadas, tais como monitorização, administração e segurança; e a aprimoração do protocolo de comunicação entre este sistema e os *gateways* (*Gateway* e Sistemas Simulados), para uma aplicação mais eficiente e fiável.

O Sistema Central recolhe a informação enviada por todos os *gateways*, que por sua vez, será armazenada na base de dados SQL. Sempre que o serviço *web* queira atualizar os dados apresentados, este faz um pedido ao gestor de serviço que, de forma encadeada, irá buscar os dados à base de dados e enviará os mesmos para o serviço *web*.

# Trabalho Relacionado

Relativamente aos trabalhos relacionados, enquadram-se os projetos seguintes que serviram de base à construção deste projeto.

## 2.1 ESP32 WebSocket: Control ESP32 Pins

Este projeto [1] demonstra a implementação de um servidor ESP32, do tipo *WebSocket,* que é responsável pelo controlo dos pinos GPIO (*General Purpose Input/Output*) de uma placa ESP32. Para além da implementação do servidor, são apresentados os passos necessários à construção de uma página *web*, que permite efetuar o controlo dos pinos referidos.

Para realizar o efeito pretendido, o autor recorreu a uma fita LED (*Light Emitting Diode)* RGB (*Red Green Blue*), cujas cores são alteradas de forma remota (através do *browser*).

O autor recorreu ao protocolo de comunicação “WebSocket”, que permite a interação entre o cliente (*web browser*)e o servidor *web* (ESP32 WebSocket), isto é, ocorre troca de informação entre a página *web* e o servidor. Desta forma, o servidor manipula os pinos, consoante os dados que são introduzidos na página *web*.

O funcionamento deste projeto pode ser ordenado de acordo com as etapas seguintes:

1. Escolher a cor pretendida através de um web *browser.*
2. Envio da informação (cor selecionada) através do protocolo WebSocket.
3. A placa ESP32 (servidor WebSocket) recebe a informação e altera a cor do LED.

É de realçar o cuidado do autor, no tratamento do conjunto de eventos associados ao protocolo aplicado, nomeadamente: conexão e desconexão.

A figura 2 ilustra o resultado pretendido, aquando da finalização o projeto.



Figura 2 – Variação de cor da tira LED.

## 2.2 ESP32 Robot Car Using Websockets

Este projeto [2], da autoria de donsky, consiste num carro robot construído com o auxílio de uma placa ESP32 e de um motor LM298, que por sua vez, é controlado através de um smartphone. Este projeto foi desenvolvido com recurso ao IDE (Integrated Development Environment) PlatformIO, uma vez que este é favorável e adequado a projetos que se enquadram no domínio da IOT (Internet Of Things).

O cerne deste projeto encontra-se na utilização do protocolo de comunicação “*WebSockets”.* O protocolo citado é essencial e preenche todos os requisitos e tópicos, que são exigidos por aplicações do ramo da IOT, devido à pouca latência oferecida pelas *websockets.*

Neste contexto, o carro *robot* desempenha o papel de servidor e o *web browser* desempenha o papel de cliente. O cliente envia um conjunto de mensagens / instruções ao servidor, sendo posteriormente respondidas por este.

A figura 3 ilustra o serviço *web,* implementado pelo autor, que é responsável pelo controlo da direção do respetivo carro.



Figura 3 - Serviço web implementado pelo autor.

A placa ESP32 atua como servidor *websocket* e o *browser* do *smartphone* atua como cliente *websocket.* As mensagens do tipo WebSockets, provenientes do *browser*, são processadas pela placa referida. Concluído o seu processamento, a placa envia mensagens de controlo para o motor LM298, com o intuito de este controlar a rotação das rodas do carro. Para além do controlo da rotação das rodas, também é possível variar a velocidade das mesmas através da modulação por largura de pulso.

Sempre que um utilizador clica nos botões de *Up, Down. Left* ou *Right,* o *smartphone* envia uma mensagem do tipo *websocket* para o robot, que por sua vez será processada pela respetiva placa.

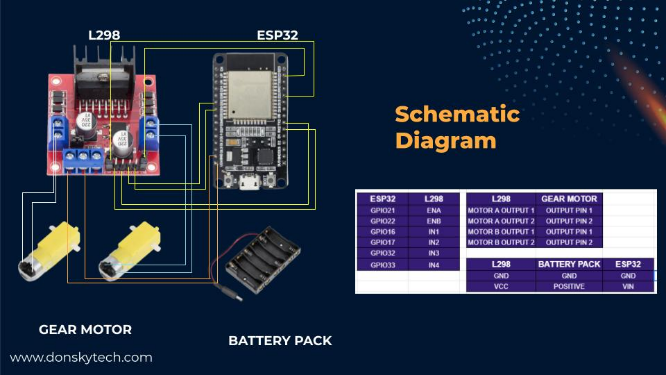
A figura 4 apresenta a listra de componentes que são necessários ao desenvolvimento deste projeto.

Figura 4 - Lista de componentes necessários à construção do projeto.

# Fases do trabalho desenvolvido

Esta secção contém todas as etapas necessárias ao desenvolvimento desta fase, que se encontram descritas pelos mecanismos, ferramentas utilizadas e algoritmos implementados pelo grupo.

## 3.1. Protocolo de comunicação

Para estabelecer a comunicação entre o Sistema Central e o *Gateway* recorreu-se ao protocolo TCP/IP, de modo a transmitir as tramas de dados recolhidas.

Para tal, o grupo declarou *sockets* do tipo servidor no Sistema Central e *sockets* do tipo cliente no *Gateway*. A partir destas, tirando partido da programação concorrente, foi estabelecida a referida ligação, que permite o bom funcionamento das interações necessárias.

Numa fase mais avançada do projeto, as tramas não irão passar só os valores obtidos pelo Sistema Sensor (e as amostras temporais), como também transportarão informação relativa ao atual funcionamento dos sensores e incluirão ordens de começo, paragem ou retoma da atividade.

A figura 5 apresenta os parâmetros necessários à implementação das *sockets* referidas e o objeto responsável pelo envio da trama e pelo estabelecimento da ligação com o Sistema Central (dentro do código do *Gateway*).

Graphical user interface, text

Description automatically generated with medium confidence

Figura 5 - Declaração da porta, do endereço e do cliente usados para a comunicação com o Sistema Central.

A figura 6 ilustra as mensagens de diagnóstico, relativas à conexão com o Sistema Central, e o envio da amostra para o mesmo.

Graphical user interface, text, application

Description automatically generated

Figura 6 - Envio da trama de dados e finalização da impressão na socket, no Gateway.

A figura 7 ilustra o código do Sistema Central, que é responsável pela inicialização e execução do servidor.

Text

Description automatically generated

Figura 7 - Inicialização da socket servidor no sistema.

## 3.2. Sistema Central

Nas subsecções seguintes serão analisadas e descritas todas as caraterísticas, funcionalidades e matérias inerentes ao Sistema Central, que foram implementadas pelo grupo.

### 3.2.1 Mecanismos e políticas de segurança

Os mecanismos de autenticação, autorização e outros recursos de segurança foram elaborados com o apoio da *framework Spring Security* [3]*.* As políticas e estratégias de segurança adotadas pelo grupo encontram-se disponíveis na diretoria “*security*”.

A diretoria referida é composta por:

* 2 enumerados, um deles é responsável pela conceção do tipo de utilizadores do sistema e o restante define o conjunto de permissões ou habilitações associadas a cada tipo de utilizador.
* 1 classe que é responsável pela encriptação da *password* dos utilizadores. É de salientar que a encriptação das *passwords* é necessária e imposta pela *Spring Security,* para a definição do serviço *web.*
* 1 classe que filtra e configura o protocolo HTTP (*Hypertext Transfer Protocol*), isto é, define quais os *websites* que um determinado tipo de utilizadores possui acesso. Em junção com a qualificação dos *websites,* esta classe é responsável pela extração do conjunto de utilizadores, que se encontram registados na base de dados.

A figura 8 ilustra a estrutura da diretoria “*security*”*.*

Uma imagem com texto

Descrição gerada automaticamente

Figura 8 - Estrutura da diretoria "security".

Desta forma, cada utilizador possui os atributos seguintes: um *username*, uma *password*, um tipo e um conjunto de habilidades associadas a esse tipo. Tal como foi citado anteriormente, o conjunto de utilizadores aptos a interagir com o serviço *web*, encontram-se armazenados numa tabela, dentro da base de dados (tópico que será explorado na secção seguinte).

Uma imagem com texto

Descrição gerada automaticamenteA figura 9 ilustra as questões que foram abordadas no parágrafo anterior.

Figura 9 - Tarefas abordadas no parágrafo anterior.

#### 3.2.1.1 Enumerados

O grupo categorizou, diferenciou os clientes/utilizadores em duas categorias distintas: administradores ou utilizadores normais.

Cada categoria possui um conjunto de permissões ou habilitações associadas, que por consequência, terão impacto nas funcionalidades disponibilizadas pelo serviço *web*.

A figura 10 descreve a categoria “ADMIN” (administrador) e o conjunto de habilitações associadas.

Uma imagem com texto, eletrónica, disco compacto

Descrição gerada automaticamente

Figura 10 - Habilitações da categoria ADMIN.

Tal como é evidenciado na figura 10, qualquer utilizador do tipo “ADMIN” pode efetuar operações de leitura e escrita sobre as amostras, por exemplo:

* Ler as amostras que se encontram armazenadas na base de dados.
* Pesquisar por uma determinada amostra através do seu código identificador (que compõe a chave primária da tabela das amostras).
* Introdução de uma amostra na base de dados.
* Remoção de uma amostra da base de dados.

Todos os tópicos acima referidos, foram realizados com recurso a anotações, que são caraterísticas da *framework Spring Security,* que no fundo podem ser interpretadas como filtros. Nessas anotações é passado como parâmetro, a categoria de utilizador pretendida. As anotações citadas foram aplicadas sobre um conjunto de métodos intrínsecos ao protocolo HTTP (*POST, GET, PUT* e *DELETE*.), que por sua vez encontram-se disponíveis na classe *WeatherSampleController*.

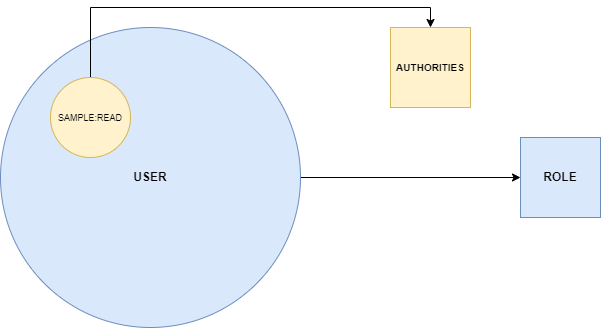
A figura 11 descreve a categoria USER (administrador) e o conjunto de habilitações correspondentes.

Figura 11 - Habilitações da categoria USER.

Em contrapartida, qualquer utilizador do tipo “USER”, apenas pode efetuar operações de leitura sobre as amostras, como é o caso da leitura da série de amostras, que se encontra armazenada na base de dados.

#### 3.2.1.2 Configuração do protocolo HTTP

A configuração do protocolo HTTP e da sua segurança, é efetuada dentro do método *configure* da classe *ApplicationSecurityConfig*. Dentro do método referido, são definidos o conjunto de *web sites* disponíveis às categorias de utilizadores, que foram descritas na subsecção anterior. Em junção com o tópico anterior*,* também são referenciados ou direcionados, os ficheiros html associados às páginas de *login* e *logout*.

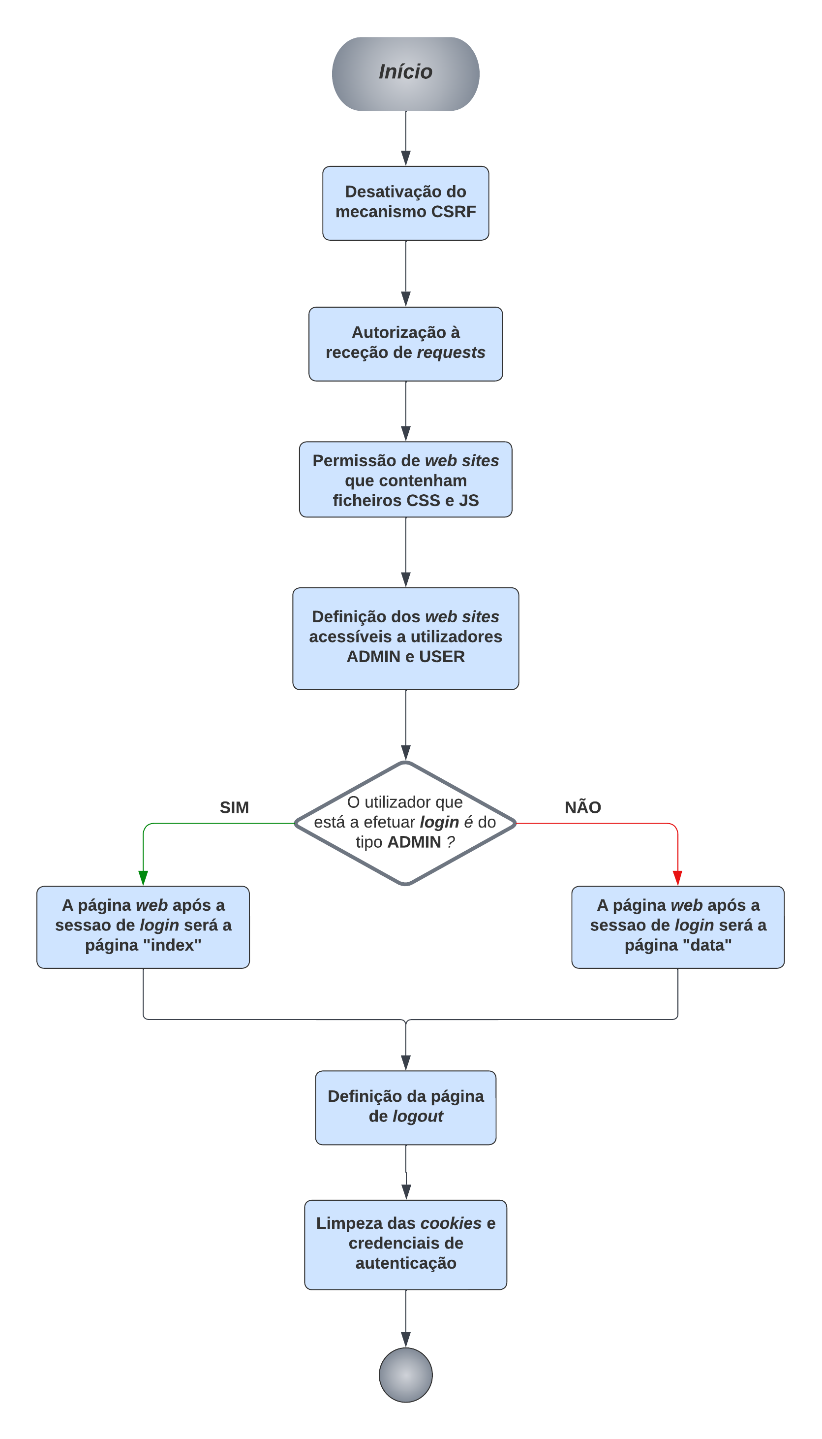
O algoritmo, que descreve o método citado, encontra-se traduzido de acordo com o fluxograma da figura 12.

Figura 12 - Comportamento do método secure.

### 3.2.2 Tabelas da base de dados

Dentro do sistema de gerenciamento de base de dados [4], o grupo definiu 3 tabelas, que são cruciais ao correto funcionamento deste projeto. É de salientar que cada tabela representa uma determinada entidade e que existem ligações entre as mesmas.

As tabelas definidas pelo grupo foram as seguintes:

* A tabela “users”, que armazena a lista de utilizadores autorizados a interagir com o serviço *web.*
* A tabela “authorities”, que contém o conjunto de competências associadas a cada categoria de utilizador.
* A tabela “weather”, que conserva todas as amostras recebidas pelo Sistema Central.

## 3.4. Servidor *Web*

Para esta etapa, o servidor *Web* que estamos a apresentar é uma versão mais atualizada da que foi apresentada na fase B.

Uma modificação visual importante foi a substituição do submenu *Feeds* porum novo intitulado *Historical Data*, cuja função é a de adicionar uma dimensão gráfica à apresentação dos dados obtidos, com gráficos que mostram a alteração da temperatura, humidade e pressão atmosférica ao longo do tempo. Outra modificação visual importante é a adição do controlo, por parte de um utilizador com capacidades de administração, dos *gateways*, podendo estes assim fazer alterações ao estado de cada *gateway.*

Como já vimos anteriormente, também adicionamos ao nosso *Servidor Web* um protocolo de *login*, sendo essa a primeira página onde cada utilizador vai parar.

Caso o utilizador não seja administrador, este apenas terá acesso a uma página com uma tabela, que apresenta, em tempo real, o ID da amostra, o ID do *gateway* de onde origina a amostra, tal como a temperatura, humidade e pressão atmosférica recolhida pelos sensores, juntamente com o *timestamp*, como mostra a figura 25.



Figura 17 - Página com todas as amostras.

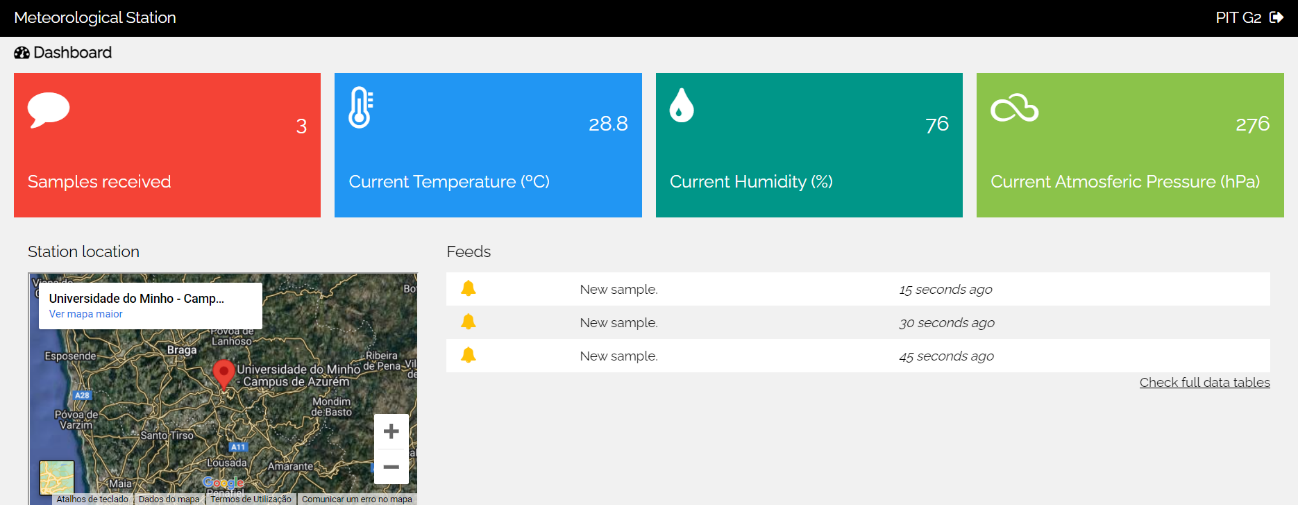


Figura 18 - Página inicial do servidor web.

# Análise de resultados e testes efetuados

De forma a retificar o funcionamento e o comportamento do Sistema Central e do protocolo de comunicação foram retiradas várias amostras, que evidenciam o funcionamento dos protocolos e mecanismos utilizados.

A figura 27 ilustra um conjunto de 10 amostras enviadas pelo Gateway para o Sistema Central, sendo armazenadas na base de dados pelo mesmo.

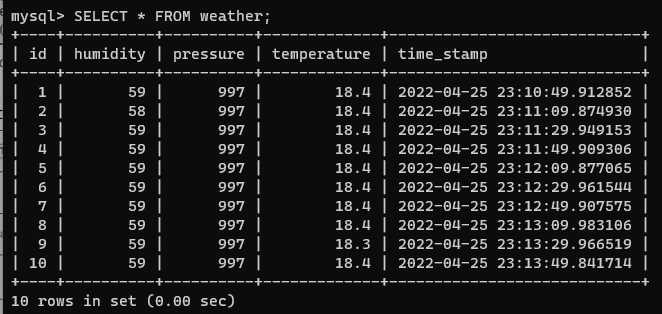


Figura 19 - Amostras armazenadas na base de dados.

A figura 28 ilustra o conjunto de 10 amostras referido, colocadas no serviço *web*.

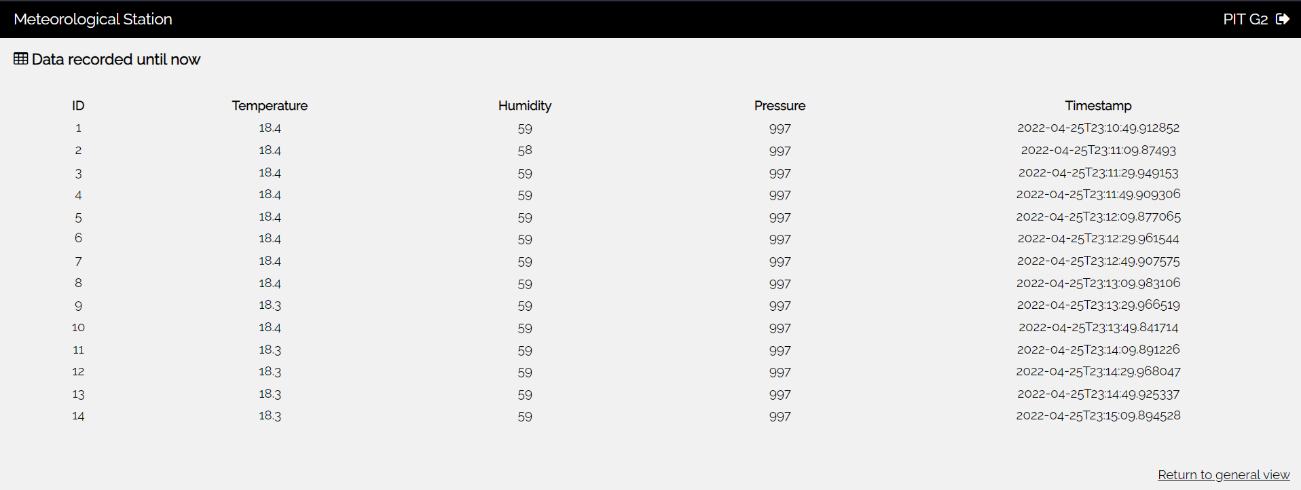


Figura 20 - Amostras impressas no serviço web.

Para se estabelecer um fio de ligação entre a base de dados e o serviço web, o grupo construiu um *script* que se encontra apresentado na figura 29.

Uma imagem com texto

Descrição gerada automaticamente

Figura 21 - Script que efetua o parsing das amostras.

Relativamente ao domínio dos sistemas simulados, o grupo definiu um conjunto de amostras *hardcoded* e armazenou-as na base de dados, com o intuito de testar as funcionalidades do repositório e a ligação com o serviço *web*.

A figura 30 ilustra os valores *hardcoded* definidos pelo grupo.

Uma imagem com texto

Descrição gerada automaticamente

Figura 22 - Definição das amostras hardcoded.

A figura 31 ilustra as amostras armazenadas na base de dados, que por sua vez encontram-se impressas no serviço *web*.

Uma imagem com texto

Descrição gerada automaticamente

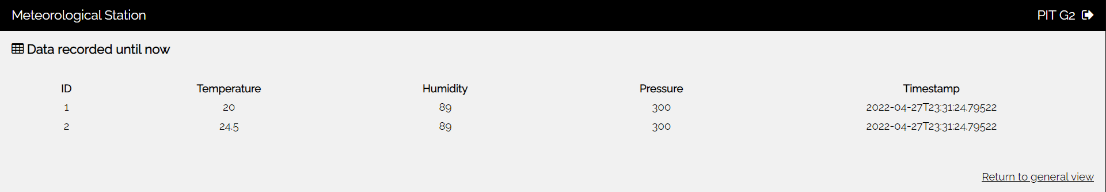


Figura 23 - Armazenamento e impressão das amostras hardcoded.

# Conclusão

Concluída esta fase, na opinião do grupo, conseguimos atingir todos os objetivos propostos. Esta fase contribuiu para o conhecimento e estudo da implementação de *Sockets*, comunicação sobre TCP/IP e sobre o desenho de Servidores *Web*, tal como comunicação bilateral utilizando o protocolo BLE.

O grupo pretende que, com o trabalho desenvolvido ao longo deste fase intermédia, ter boas fundações para completar a etapa final deste projeto com sucesso.

## 5.1. Contribuição de cada aluno

Catarina Neves

* Conceção dos algoritmos;
* Tratamento de dados, tabelas e imagens a estes relacionados;
* Transmissão de *timestamps,* sua codificação e descodificação;
* Programação e implementação da aplicação dos Sistema Sensor e *gateway*;
* Desenvolvimento do relatório;

Eduardo Cardoso

* Conceção dos algoritmos;
* Transmissão de *timestamps,* sua codificação e descodificação;
* Programação e implementação da aplicação dos Sistema Sensor e *gateway*;
* Desenvolvimento e implementação das *sockets* e comunicação TCP/IP;
* Desenvolvimento do relatório;

José Gomes

* Conceção dos algoritmos;
* Tradução das classes em diagramas;
* Implementação do Sistema Central;
* Desenvolvimento e implementação das *sockets* e comunicação TCP/IP;
* Desenvolvimento do relatório;

Luís Oliveira

* Conceção dos algoritmos;
* Desenvolvimento do *Frontend* e *Backend* do Servidor *Web*;
* Implementação do Sistema Central;
* Desenho de esquemas e gráficos;
* Desenvolvimento do relatório.

# Lista de referências

|  |  |
| --- | --- |
| [1] | SWA, “ESP32 Websocket: Control ESP32 Pins [PlatformIO],” 4 2021. [Online]. Available: https://www.survivingwithandroid.com/esp32-websocket-control-esp32-pins-platformio/. |
| [2] | donsky, “ESP32 Robot Car Using Websockets,” julho 2021. [Online]. Available: https://www.donskytech.com/esp32-robot-car-using-websockets/. |
| [3] | VMware, “Spring Security,” 2022. [Online]. Available: https://spring.io/projects/spring-security?msclkid=03ed647cc53c11ec824b0986c6465ca1. |
| [4] | R. Santos, “Random Nerd Tutorials,” 10 2020. [Online]. Available: https://randomnerdtutorials.com/esp32-websocket-server-arduino/. |
| [5] | W3Schools, “W3Schools W3.CSS,” [Online]. Available: https://www.w3schools.com/w3css/. |
| [6] | MySQL, “MYSQL,” 2022. [Online]. Available: https://www.mysql.com/. |