Universidad de Cantabria

Facultad de Ciencias

HAPI SECURITY: APLICACIÓN PARA EL ANÁLISIS DE DISPOSITIVOS IoT EN BASE A SU SEGURIDAD Y SOSTENIBILIDAD (Hapi Security: Mobile app for the analysis of IoT devices based on their security and sustainability)

Trabajo de Fin de Grado
para acceder al

GRADO EN INGENIERÍA INFORMÁTICA

Autor: Mario Ingelmo Diana

Director: Carlos Blanco Bueno

Co-Director: Juan Maria Rivas Concepcion

Julio – 2023

Índice

Resumen

Actualmente, utilizamos un gran número y variedad de dispositivos inteligentes conectados a la red (IoT) tanto en entornos domésticos como laborales, sanitarios, de transporte, etc. Aunque dichos dispositivos manejan infraestructuras críticas e información sensible, no suelen contar con un buen nivel de seguridad. Por otro lado, al ser dispositivos que están continuamente conectados, la sostenibilidad también es un aspecto importante a tener en cuenta. Este proyecto se centra en ayudar a los usuarios a mejorar la infraestructura de su entorno (hogar, oficina, etc.) mediante el uso de dispositivos más adecuados.

Para ello, en este proyecto se desarrolla una aplicación móvil (Hapi Security) que permite conocer cómo de seguro es un dispositivo IoT concreto, a qué se debe y si existen alternativas mejores. Cada dispositivo tiene asociada una calificación de seguridad (de 0 a 100) y de sostenibilidad (de A a G) y una serie de aspectos que presenta e influyen de forma positiva o negativa en dichas calificaciones. La aplicación ha sido desarrollada para Android utilizando Java y presenta funcionalidades para permitir búsquedas y filtrados de dispositivos, escanear códigos de barras, gestionar favoritos y compartir la aplicación.

Como apoyo a dicha aplicación, se desarrolla un servicio REST utilizando Spring Boot con información sobre el catálogo de dispositivos IoT (alineada con ENISA) junto con sus calificaciones de seguridad y sostenibilidad y el listado de aspectos que influyen positiva o negativamente en ellas.

Palabras clave:

Aplicación móvil, Dispositivos IoT, Seguridad, Sostenibilidad, Servicio REST, Java, Android Studio.

Abstract

Currently, we use a large number and variety of smart devices connected to the network (IoT) both in home and work environments, health, transportation, etc. Although these devices handle critical infrastructure and sensitive information, they often do not have a good level of security. On the other hand, being devices that are continuously connected, sustainability is also an important aspect to consider. This project focuses on helping users to improve the infrastructure of their environment (home, office, etc.) by using more suitable devices.

To do this, in this project a mobile application (Hapi Security) is developed that allows knowing how secure a specific IoT device is, what it is due to and if there are better alternatives. Each device is associated with a safety rating (from 0 to 100) and sustainability (from A to G) and a series of aspects that it presents and influences positively or negatively in said ratings. The application has been developed for Android using Java and presents functionalities to allow searching and filtering of devices, scanning barcodes, managing favorites, and sharing the application.

In support of said application, a REST service is developed using Spring Boot with information about the IoT device catalog (aligned with ENISA) together with its security and sustainability ratings and the list of aspects that positively or negatively influence them.

Key Words:

Mobile application, IoT devices, Security, Sustainability, REST service, Java, Android Studio.

1. Introducción

Hoy en día vivimos rodeados de dispositivos IoT, los entornos IoT desempeñan un papel cada vez más importante, estos dispositivos hacen de puente entre el mundo físico y el digital, incluyen todo tipo de funciones de computación, almacenamiento y comunicación que les permite gestionar objetos en el mundo físico y proporcionar servicios en numerosas áreas como la salud, el suministro de energía, el transporte, la automatización industrial o el hogar inteligente. Todo ello sumado a su constante conexión a Internet supone un riesgo en la seguridad de estos y en tu seguridad.

Prueba de esto es la cantidad de ataques que se detectan a dispositivos de este tipo. *Kaspersky*, conocida compañía internacional en el sector de la ciberseguridad hizo públicos los siguientes datos sobre ataques a sus honeypots (Software que imita un dispositivo IoT vulnerable) en 2021: “En el primer semestre de 2021, el número de intentos de infección totales alcanzó los 1.515.714.259, mientras que durante los seis meses anteriores fueron 639.155.942” [1]. A la vista de estos datos observamos como el aumento de los ataques, solamente en “señuelos” de la empresa *Kaspersky* casi se triplican, lo que nos da una idea general de lo que puede suponer a nivel global donde actualmente hay alrededor de 7 mil millones de dispositivos IoT conectados a la red y se estima un crecimiento hasta los 27 mil millones en 2025 [2].

A la vista de estos datos, podemos observar la gran importancia que tiene la seguridad en los dispositivos IoT. La falta de seguridad en estos dispositivos puede tener consecuencias considerables. Por un lado, sus áreas de aplicación suelen corresponder a infraestructuras críticas, en las que la interrupción o el compromiso de estos sistemas puede tener consecuencias devastadoras, que van desde interrupciones en los servicios públicos hasta riesgos para la seguridad y la vida humana. Por otro lado, recopilan y procesan grandes cantidades de datos sensibles, como información personal, datos de salud o datos empresariales confidenciales. Por lo que la falta de seguridad en estos sistemas puede resultar en fugas de datos, robo de información personal o financiera, y posibles daños a la reputación de las organizaciones. Sin embargo, su rápida evolución y adopción ha llevado a que muchos de ellos se diseñen y se lancen al mercado sin una atención adecuada a estos aspectos, generando así un gran número de vulnerabilidades que pueden ser explotadas. Además la gran variedad de dispositivos de este tipo dificulta la estandarización de unas medidas de seguridad consistentes y eficaces y lamentablemente es un aspecto al que poca gente presta atención y cuyos datos son de difícil acceso.

También es importante la sostenibilidad de estos dispositivos, tanto la eficiencia energética al estar conectados continuamente, como el proceso de fabricación de este (si es respetuoso con el medio ambiente) o la reparabilidad del dispositivo entre otros. Es un aspecto más ignorado que la seguridad, pero también es vital, puesto que puede ayudarnos a ahorrar ya sea en la factura de la luz o en reparaciones y puede ayudar a cuidar del planeta.

A la vista de la dificultad de obtener datos sobre la seguridad y sostenibilidad de estos dispositivos, ya que la cantidad de estos es enorme y abarca muchas categorías diferentes y para cada categoría muchos fabricantes, se desarrolla una aplicación móvil

(Hapi Security) donde poder consultar la seguridad de los diferentes dispositivos IoT del mercado, además de la sostenibilidad y las listas con los aspectos tanto positivos como negativos de seguridad y sostenibilidad, de manera que el usuario tenga fácil acceso a los mismos y pueda valorar diferentes opciones a la hora de comprar dispositivos IoT en materia de seguridad y sostenibilidad.

El nombre de la aplicación proviene del dios egipcio Hapi, dios encargado de la inundación anual del río Nilo, que proveía de suelo fértil para los cultivos y así de alimento al pueblo egipcio. Por eso, era considerado por muchos el dios de la seguridad, al encargarse de "proteger" a los egipcios dándoles una tierra donde cultivar y así mantener la vida y la economía.

El presente TFG se ha desarrollado en el marco del proyecto ALBA: mejora de la ciberseguridad y su sostenibilidad en Beneficio de la sociedad y de las personas, financiado por el Ministerio de Ciencia e Innovación dentro de la convocatoria de Proyectos de Transición Ecológica y Transición Digital.

1.1. Objetivo

Como objetivo principal de este proyecto se plantea el desarrollo de una aplicación móvil (llamada Hapi Security) donde los usuarios puedan consultar información sobre la seguridad y sostenibilidad de dispositivos IoT. Dicha aplicación les permitirá buscar dispositivos, observar sus calificaciones en cuanto a seguridad y sostenibilidad y a qué se deben (qué aspectos presentan que afectan positiva o negativamente en la seguridad y sostenibilidad). De esta forma, los usuarios podrán tomar decisiones más informadas a la hora de comprar un dispositivo nuevo o de reemplazar alguno de sus dispositivos actuales.

Para la consecución de dicho objetivo se plantea el desarrollo de un servicio donde almacenar y obtener los datos de los dispositivos: categorías, dispositivos, información de detalle, calificaciones de seguridad y sostenibilidad asociadas, aspectos que influyen positiva o negativamente en la seguridad y/o sostenibilidad, etc. La aplicación móvil utilizará este servicio a la vez que proporcionará funcionalidades de búsqueda, filtrado, gestión de favoritos, etc.

2. Materiales y metodología utilizada

Este apartado recoge tanto la metodología y la planificación del trabajo seguida, como las tecnologías y herramientas utilizadas.

2.1. Metodología

La metodología seguida ha sido la iterativa incremental. Esta metodología consiste en dividir el proyecto en diferentes iteraciones o ciclos. En cada iteración el producto se va actualizando de manera que se desarrolla hasta llegar a un producto final que cumpla con los requisitos y objetivos marcados [3]. Se ha elegido esta metodología porque así las funcionalidades se desarrollan de una en una, dado que en mi opinión, esto beneficia

el correcto desarrollo del producto total al pulir cada una de las funcionalidades en la iteración correspondiente y poder ir usando esas implementaciones en el desarrollo de las siguientes a esta.

Imagen 1. Representación de la metodología iterativa incremental

En este proyecto cada iteración se ha dividido en 4 partes:

- Requisitos.
- Diseño.
- Implementación.
- Pruebas.

2.2. Planificación del trabajo

La planificación de este proyecto puede dividirse en tres apartados principales: preparación previa al desarrollo, desarrollo y despliegue del software y desarrollo de la memoria del trabajo.

A continuación se añade un diagrama de Gantt con la planificación del trabajo.

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Preparación previa	**10 días**	**lun 27/02/23**	**jue 09/03/23**	
Desarrollo y despliegue	**71 días**	**jue 09/03/23**	**dom 21/05/23**	**1**
Desarrollo y despliegue del servicio	**22 días**	**jue 09/03/23**	**vie 31/03/23**	
Iteración 1. Desarrollo de la capa de repositorio	5 días	jue 09/03/23	mar 14/03/23	
Iteración 2. Desarrollo de la capa de servicio	5 días	mar 14/03/23	dom 19/03/23	4
Iteración 3. Desarrollo de la capa de controlador y configuración	7 días	dom 19/03/23	dom 26/03/23	5
Iteración 4. Pruebas y despliegue final	5 días	lun 27/03/23	vie 31/03/23	6
Desarrollo y despliegue de la aplicación	**71 días**	**jue 09/03/23**	**dom 21/05/23**	
Iteración 1. Desarrollo del menú y la sección de compartir	18 días	jue 09/03/23	lun 27/03/23	
Iteración 2. Desarrollo de la sección de buscador	14 días	sáb 01/04/23	sáb 15/04/23	7;9
Iteración 3. Desarrollo de la sección de escanear	14 días	sáb 15/04/23	sáb 29/04/23	10
Iteración 4. Desarrollo de la sección de favoritos	14 días	dom 30/04/23	dom 14/05/23	11
Iteración 5. Pruebas finales y despliegue de la aplicación	7 días	dom 14/05/23	dom 21/05/23	12
Realización de la memoria	**44 días**	**lun 22/05/23**	**jue 06/07/23**	**8**

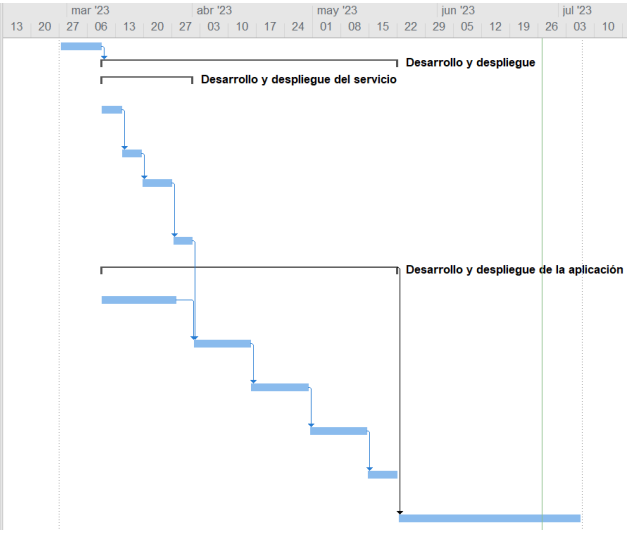

Imagen 2. Diagrama de Gantt

2.2.1. Preparación previa al desarrollo

Este apartado es clave puesto que es el inicio de todo. Que este apartado nazca con buen pie es de suma importancia, ya que se determinan los objetivos principales del proyecto y qué herramientas se van a utilizar para logarlos. Por lo que una buena elección de objetivos y herramientas ayuda en las diferentes etapas del proyecto.

Tras una pequeña reunión inicial donde intercambiamos las ideas que teníamos, pusimos en consonancia los objetivos a desarrollar para este proyecto, llegando a un acuerdo y rellenando un documento con estos, para ir revisándolos y ver que todo se completaba adecuadamente.

En otra reunión donde se siguió perfilando la idea del proyecto también se evaluaron las herramientas de desarrollo y se estableció que tecnologías utilizar para el desarrollo de las diferentes partes del proyecto. Estas se explicarán más adelante.

2.2.2. Desarrollo y despliegue del software

Este apartado corresponde con lo hablado anteriormente en la metodología. Se ha dividido en iteraciones, incluyendo cada una de las fases mencionadas anteriormente (requisitos, diseño, implementación y pruebas), para una vez finalizado todo el trabajo, realizar el despliegue final del servicio y de la aplicación móvil.

Ahora explicaré un poco más en detalle las fases en las que se divide cada iteración:

- **Requisitos:** Se establecen los objetivos a desarrollar en cada iteración del software (requisitos), estos pueden dividirse en dos:
    - **Requisitos funcionales:** Son requisitos sobre las funcionalidades que nuestro sistema deberá implementar y ofrecer a los usuarios, tales como poder buscar, filtrar, escanear, etc…
    - **Requisitos no funcionales:** Son atributos de calidad del sistema, tales como la seguridad, el rendimiento, la mantenibilidad, etc…

- **Diseño:** Se analizan los requisitos definidos anteriormente y se plantea una solución sobre cómo poder implementarlos en consonancia con los ya implementados. Esto implica generar o ampliar el diseño a alto nivel (arquitectura) así como el diseño detallado del sistema.

- **Implementación:** Basándose en el diseño creado en el apartado anterior, este es implementado en el software de manera que añada toda la funcionalidad nueva establecida en los objetivos de la iteración.

- **Pruebas:** Tras realizar la implementación del software en el apartado anterior se pasa al testeo de los cambios realizados, ya sea funcionalidad nueva o actualizada, tanto individualmente, como en conjunto. Por ello, se realizan cuatro tipos de pruebas diferentes que explicaremos más adelante: unitarias, integración, sistema y aceptación.

2.2.3. Desarrollo de la memoria.

Aunque durante las diferentes etapas de desarrollo se ha ido generando documentación del sistema, la memoria como tal se ha realizado una vez todo el software ha sido desarrollado, testeado y desplegado. Esta decisión podría haber sido completamente diferente y haberlo hecho en paralelo con el desarrollo, pero en mi caso me decanté por un desarrollo de esta posterior, para así centrar todos mis esfuerzos en el correcto desarrollo del servicio y la aplicación.

2.3. Tecnologías y Herramientas

Las tecnologías y herramientas que se han utilizado son las siguientes:

2.3.1. Git y GitHub

Git es un sistema avanzado de control de versiones (como el “control de cambios” de Microsoft Word) distribuido. Git permite “rastrear” el progreso de un proyecto a lo largo del tiempo ya que hace “capturas” del mismo a medida que evoluciona y los cambios se van registrando. Esto permite ver qué cambios se hicieron, quién los hizo y por qué, e incluso volver a versiones anteriores [4].

Por otra parte GitHub es un servidor de alojamiento en línea o repositorio remoto para albergar proyectos basados en Git que permite la colaboración entre diferentes usuarios o con uno mismo. Un repositorio es un directorio donde desarrollar un proyecto que contiene todos los archivos necesarios para el mismo [4].

Imagen 3. Logos de Git y GitHub

Se usarán tanto Git con su bash, para ir almacenando los cambios y poder llevar así un control de versiones del proyecto, como GitHub para almacenar el repositorio en la nube. Esto se realiza así por si en un futuro se añadieran más personas al proyecto, facilitar la trazabilidad y el manejo del código y los documentos. Ya que estas tecnologías son mundialmente conocidas y utilizadas.

2.3.2. Spring Boot, Maven y Java

Para el desarrollo del servicio implementado se ha tomado la decisión de utilizar Spring Boot software desarrollado por la empresa Spring y que está disponible para usarse en

Java, Kotlin o Groovy. En mi caso, al ser el lenguaje más dominado Java, se ha utilizado este, además de utilizar Maven a la hora de manejar el empaquetamiento del servicio.

Java Spring Boot (Spring Boot) es una herramienta que acelera y simplifica el desarrollo de microservicios y aplicaciones web con Spring Framework gracias a tres funciones principales:

- Configuración automática.
- Un enfoque de configuración que facilita los pasos a dar.
- La capacidad de crear aplicaciones autónomas.

Estas características, combinadas, conforman una herramienta que le permite configurar una aplicación basada en Spring con el mínimo de instalación y configuración [5].

Imagen 4. Logo de Spring Boot

Hoy en día, la mayoría de las empresas piden conocimientos sobre cómo implementar microservicios con Spring, por lo que, además de parecerme la opción más cómoda después de valorar varias aprendidas en la asignatura de *Servicios Software*, también me pareció la que más variabilidad podía otorgarme y más proyección a futuro podía tener.

2.3.3. Eclipse

Para el desarrollo del servicio mencionado anteriormente, gracias a la gran cohesión que tiene tanto con Java (es uno de los entornos más utilizados a nivel mundial para el desarrollo de software Java) como con Spring Boot y Maven, se ha decidido utilizar como entorno de desarrollo Eclipse IDE for Enterprise Java and Web Developers.

GeneralController.java

```
1  package es.unican.hapisecurity.REST_TFGMarioIngelmoDiana.controllerLayer;
2
3  import java.net.URI;
32
33 @RestController
34 @RequestMapping("REST_TFGMarioIngelmoDiana")
35 public class GeneralController {
36
37     @Autowired
38     private AuthenticationManager authenticationManager;
39
40     @Autowired
41     private UserDetailsServiceImpl usuarioDetailsService;
42
43     @Autowired
44     private GestionTokens gestion;
45
46     @Autowired
47     private GeneralService servicio;
48
```

Imagen 5. Ejemplo de uso de Eclipse en el servicio implementado

2.3.4. Microsoft Azure

Microsoft Azure es una plataforma desarrollada por Microsoft compuesta por más de 200 productos y servicios en la nube [6]. Entre los servicios que ofrece encontramos desde Bases de Datos en la nube, hasta la creación de máquinas virtuales o el despliegue de aplicaciones Spring.

Imagen 6. Logo de Microsoft Azure

Gracias a estas características que ofrece y a la disponibilidad de una licencia de estudiante, se ha decidido utilizar para usar una de sus bases de datos para el servicio y poder desplegarlo en una máquina virtual, cosas que se explicarán más adelante.

2.3.5. Android Studio y Java

Android Studio es el entorno de desarrollo oficial que se usa en el desarrollo de aplicaciones Android [7]. Android Studio admite desarrollo en dos lenguajes, Java y Kotlin, en este caso se va a desarrollar la aplicación en Java, puesto que ya he desarrollado más aplicaciones Android en el mismo lenguaje y el dominio que tengo de este lenguaje es considerable a diferencia del dominio que tengo de Kotlin.

Además Android Studio ofrece todo tipo de facilidades a la hora de desarrollar aplicaciones Android, dispone de compilación flexible basada en Gradle, un emulador de dispositivos Android donde emular una gran cantidad de dispositivos con diferentes versiones de Android y otras muchas funcionalidades que son de gran ayuda.

```
@Override
public View onCreateView(LayoutInflater inflater, ViewGroup container,
                         Bundle savedInstanceState) {
    // Creo la view para la actividad principal con el xml correspondiente
    this.view = inflater.inflate(R.layout.fragment_buscador, container,  attachToRoot: false);

    if (Red.isNetworkAvailable(this.requireContext())) {
        presenter = new BuscadorPresenter( view: this, categoriaSeleccionada, String.valueOf(valorSeguridad),
    } else {
        presenter = new BuscadorPresenter( view: this, categoriaSeleccionada, String.valueOf(valorSeguridad),
    }

    this.init();
    return view;
}
```

Imagen 7. Ejemplo de uso de Android Studio en la aplicación

3. Desarrollo del servicio

Los apartados de desarrollo van a dividirse en dos: Por una parte en el punto 3 estará el desarrollo del servicio con sus respectivas partes y en el punto 4 estará el desarrollo de la aplicación con sus respectivas partes. Comenzamos con el desarrollo del servicio.

3.1. Análisis de requisitos del servicio

En este apartado se analizarán los requisitos que se han determinado para el servicio a desarrollar para la aplicación. Se analizarán tanto los requisitos funcionales como los no funcionales y también se dará una idea sobre qué se busca con el servicio.

3.1.1. Idea tras el servicio

La idea tras el servicio es la de construir y desplegar un servicio REST que dé funcionalidad a la hora de obtener los dispositivos con sus respectivos datos y características. Para esto se busca tener las siguientes características de manera resumida:

- Obtener los datos de los dispositivos o de un solo dispositivo y sus características de seguridad y sostenibilidad asociadas.
- Filtrar la lista de los dispositivos.
- Ordenar la lista de los dispositivos.
- Obtener las diferentes características o una sola de ellas.
- Crear o modificar dispositivos.
- Crear características nuevas.
- Que disponga de seguridad.

3.1.2. Requisitos funcionales

A continuación se presenta una tabla con los diferentes requisitos funcionales que se han obtenido:

ID	Descripción
RF1	El usuario podrá obtener una lista con todos los dispositivos y sus características.
RF2	El usuario podrá obtener una lista con todos los dispositivos y sus características filtrada por la categoría de los dispositivos que indique.
RF3	El usuario podrá obtener una lista con todos los dispositivos y sus características filtrada por la seguridad mínima que indique.
RF4	El usuario podrá obtener una lista con todos los dispositivos y sus características filtrada por la sostenibilidad mínima que indique.
RF5	El usuario podrá obtener una lista con todos los dispositivos y sus características filtrada por los tres parámetros de los requisitos anteriores de manera conjunta o combinados.

RF6	El usuario podrá obtener una lista con todos los dispositivos y sus características ordenada alfabéticamente, por puntuación de seguridad de mejor a peor o por puntuación de sostenibilidad de mejor a peor.
RF7	El usuario podrá obtener una lista con todos los dispositivos y sus características ordenada y filtrada por cualquiera de las opciones de los requisitos anteriores.
RF8	El usuario podrá obtener un dispositivo indicando su id.
RF9	El usuario podrá obtener una lista con todas las características de seguridad y sostenibilidad.
RF10	El usuario podrá obtener una característica indicando su id.
RF11	El usuario deberá identificarse para realizar modificaciones en los datos.
RF12	El usuario podrá obtener un token de seguridad identificándose (administrador).
RF13	El administrador podrá añadir nuevos dispositivos.
RF14	El administrador podrá modificar dispositivos ya añadidos.
RF15	El administrador podrá añadir nuevas características.

Tabla 1. Requisitos funcionales del servicio

3.1.3. Requisitos no funcionales

A continuación se presenta una tabla con los diferentes requisitos no funcionales que se han obtenido:

ID	Clasificación	Descripción
RNF1	Seguridad	El servicio deberá estar protegido utilizando JSON Web Tokens.
RNF2	Usabilidad, Mantenibilidad	El servicio deberá poder se utilizado desde otras aplicaciones que lo necesiten.
RNF3	Portabilidad	El servicio deberá estar desplegado en un entorno de acceso global.
RNF4	Fiabilidad	El servicio deberá estar disponible (en funcionamiento) cuando se realice una llamada al mismo
RNF5	Mantenibilidad	El servicio deberá poder añadir o modificar funcionalidades sin impactar en el resto del servicio.

Tabla 2. Requisitos no funcionales del servicio

3.2. Diseño del servicio

Podemos dividir el diseño del servicio en dos partes. Primero el diseño arquitectónico del servicio, con la arquitectura que se ha seguido y una explicación de cada capa y segundo el diseño del servicio REST con los recursos, URIs, métodos HTTP y códigos de respuesta HTTP.

3.2.1. Diseño arquitectónico

El servicio se ha diseñado usando la arquitectura típica de los servicios de Spring Boot, esta arquitectura está basada en capas, donde encontramos que se descompone en capa de control, capa de servicio y capa de repositorio.

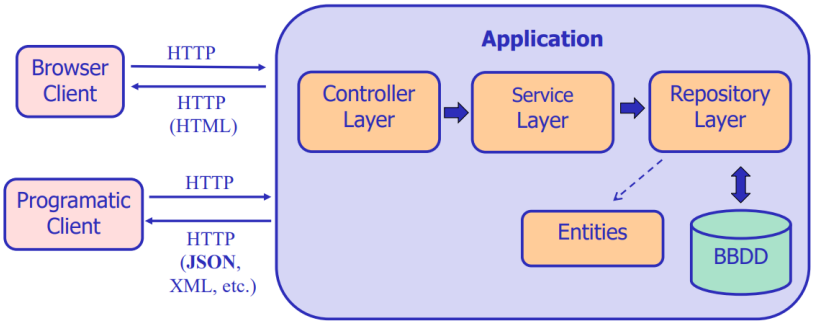

Imagen 8. Arquitectura típica de las aplicaciones Spring Boot

Viendo las capas de las que dispone el servicio, voy a explicarlas una a una para entender su funcionalidad:

- **Controller Layer:** Es la capa encargada de recibir las solicitudes HTTP y como su nombre indica, controlarlas. Esta capa puede estar formada por una o más clases anotadas con @RestController, que son las clases encargadas de, dependiendo de la URI solicitada por el cliente, procesar la petición y devolver una respuesta a este.
- **Service Layer:** Es la capa encargada de hacer de conexión entre la capa de control y la capa de repositorio. Facilita el manejo de diferentes funcionalidades desde los controladores al simplificar el código a la hora de, por ejemplo, conseguir un dispositivo, actualizarlo, etc, al no interactuar desde la capa de control directamente con el repositorio.
- **Repository Layer:** Es la capa encargada de comunicarse con la base de datos y obtener las entidades correspondientes. En este servicio se está implementando con JPA que ayuda a la hora de gestionar las entidades y la base de datos mediante anotaciones e interfaces predefinidas.

3.2.2. Diseño REST

A la vista de los requisitos, se han definido los recursos, URIs, métodos y respuestas HTTP y se ha generado el siguiente diseño REST para el servicio:

RECURSO	URI	MÉTODOS	RESPUESTAS HTTP
Token JWT	/REST_TFGMarioIngelmoDiana/token	POST	200, 400, 401, 403, 500
Lista Dispositivos	/REST_TFGMarioIngelmoDiana/dispositivos	GET - categoría - seguridad - sostenibilidad - ordenar	200, 400, 404, 500, 503
Dispositivo	/REST_TFGMarioIngelmoDiana/dispositivos/{id}	GET, PUT	200, 201, 400, 401, 403 ,404, 500, 503
Lista Características	/REST_TFGMarioIngelmoDiana/caracteristicas	GET, POST	200, 201, 400, 401, 403, 404, 500, 503

Característica	/REST_TFGMarioIngelmoDiana/ caracteristicas/{id}	GET	200, 400, 404, 500, 503

Tabla 3. Diseño REST del servicio

3.3. Implementación del servicio

Tomando como referencia el diseño tanto arquitectónico como REST del servicio, el siguiente paso es implementarlo, para ello, se ha creado un proyecto con Spring Boot Initializr con las siguientes dependencias:

- **JPA:** Esta dependencia sirve para manejar las entidades en la base de datos que se utilice en el servicio. Esto es, maneja automáticamente la base de datos mediante anotaciones, anotando las clases como entidades (@Entity) y permitiendo así su mapeo a la base de datos seleccionada, así como también a sus atributos y relaciones con otras clases.
- **Web:** Esta dependencia proporciona herramientas para desarrollar aplicaciones web en Spring Boot.
- **MySQL:** Esta dependencia sirve para implementar la base de datos del servicio en MySQL, se encarga de conectar el servicio con una base de datos MySQL local o en la nube. En mi caso, la base de datos se ha implementado en Azure, como se comentará más adelante.
- **JWT:** Esta dependencia sirve para implementar seguridad con JSON Web Tokens y así poder restringir el acceso a los usuarios a diferentes funcionalidades como modificar dispositivos, añadir características, etc.

La implementación se irá explicando por capas, siendo la última a explicar la capa de controlador donde también se comentará la implementación del diseño REST. Adicionalmente se explicará la configuración y la seguridad JWT.

3.3.1. Implementación de la repository layer

Esta capa está formada por dos entidades (Característica.java y Dispositivo.java), dos interfaces de repositorios (CaracteristicaRepository.java y DispositivoRepository.java), dos enumerados (Categoria.java y TipoOrdenar.java) y dos clases para las listas de características y dispositivos (ListaCaracteristicas.java y ListaDispositivos.java).

Cabe destacar que esta capa realiza la conexión con la base de datos, es la encargada de comunicarse con esta y realizar los cambios pertinentes u obtener los datos. Para esto se modifica el archivo application.properties de manera que escribiendo unas pocas líneas con la url de la base de datos, el usuario y la contraseña, se pueda realizar una conexión con esta.

La base de datos para este servicio ha sido implementada con una de las herramientas de Azure. Se ha creado una base de datos MySQL en Azure y se ha vinculado con el servicio, de manera que gracias a las anotaciones JPA, la base de datos, alojada en la nube, cree las tablas automáticamente y guarde valores al cargarlos. Se ha tomado esta decisión puesto que se cree que aunque pueda ser algo más lento a tenerlo de manera local en donde el servicio se despliegue, si es algo más profesional y habitual.

3.3.1.1. Entidades

Tenemos las dos entidades principales del servicio anotadas con JPA, estas entidades son las que se almacenan y se obtienen de la base de datos. Gracias a las anotaciones en las mismas, este mapeo es automático, por un lado tenemos Dispositivo.java, que representa el elemento principal del servicio, que es el dispositivo con sus diferentes datos y características asociadas:

```java
@Entity
public class Dispositivo {

    @Id
    private String id;
    private String urlImagen;
    private String nombre;
    private String marca;

    @Size(max = 750)
    private String descripcion;
    private Categoria categoria;
    private String precio;
    private int seguridad;
    private String sostenibilidad;

    @ManyToMany
    private List<Caracteristica> listaPositivaSeguridad;

    @ManyToMany
    private List<Caracteristica> listaNegativaSeguridad;

    @ManyToMany
    private List<Caracteristica> listaPositivaSostenibilidad;

    @ManyToMany
    private List<Caracteristica> listaNegativaSostenibilidad;
```

Imagen 9. Clase Dispositivo.java

Por otro lado, tenemos Característica.java, entidad que almacena las diferentes características que existen según la ENISA sobre seguridad y sostenibilidad, tanto buenas como malas. Un ejemplo de característica mala de seguridad es: Contraseñas predeterminadas débiles: Contraseñas que son fáciles de adivinar o que no se pueden cambiar fácilmente.

```java
@Entity
public class Caracteristica {

    @Id
    @GeneratedValue
    private Long id;
    private String texto;
```

Imagen 10. Clase Caracteristica.java

3.3.1.2. Interfaces de repositorio

Tenemos los dos repositorios principales que sirven de comunicación entre la base de datos y el servicio, estos extienden de JpaRepository y se indica la clase de la que va a ser repositorio y el tipo de id. Por defecto heredan todos los métodos CRUD, pero

pueden añadirse más si se cree necesario. Primero tenemos DispositivoRepository.java que representa el repositorio de los dispositivos.

```
public interface DispositivoRepository extends JpaRepository<Dispositivo, String> {

}
```

Imagen 11. Interfaz DispositivoRepository.java

También tenemos CaracteristicaRepository.java que representa el repositorio de las caracteristicas.

```
public interface CaracteristicaRepository extends JpaRepository<Caracteristica, Long> {

}
```

Imagen 12. Interfaz CaracteristicaRepository.java

3.3.1.3. Enumerados

Pasamos con los enumerados, tenemos dos diferentes, un es como se ha visto en la clase Dispositivo.java, para indicar la categoría a la que pertenece el dispositivo. De momento hay cinco categorías diferentes, pero al final del trabajo hablaremos sobre la posibilidad de ampliar esta cantidad. El enumerado tiene de nombre Categoria.java.

```
public enum Categoria {
    Asistente_Virtual, Iluminacion, Climatizacion, Electrodomesticos_Inteligentes, Limpieza
}
```

Imagen 13. Enumerado Categoria.java

El otro enumerado aunque no sea directamente de la capa de repositorio se ha añadido aquí y sirve para clasificar a la hora de ordenar, cuál de los tres métodos se quiere utilizar. El enumerado tiene de nombre TipoOrdenar.java.

```
public enum TipoOrdenar {
    Alfabetico, Seguridad, Sostenibilidad
}
```

Imagen 14. Enumerado TipoOrdenar.java

3.3.1.4. Listas

Finalmente nos encontramos con las dos listas, que aunque no se utilicen en el repositorio, al estar relacionadas directamente con las dos entidades se han colocado en esta capa. Estas listas sirven para devolver las listas de dispositivos y caracteristicas de manera más ordenada y de manera que a la hora de mapear en la aplicación resultase más sencillo. Las clases son ListaDispositivos.java y ListaCaracteristicas.java.

```
public class ListaDispositivos {

    private List<Dispositivo> dispositivos;
```

Imagen 15. Clase ListaDispositivos.java

```java
public class ListaCaracteristicas {

    private List<Caracteristica> caracteristicas;
```

Imagen 16. Clase ListaCaracteristicas.java

3.3.2. Implementación de la service layer

Esta capa está formada únicamente por una clase llamada GeneralService.java, esta clase es un servicio que sirve de puente entre la capa de control y la de repositorio, no es estrictamente necesaria y en lógicas sencillas se puede omitir, pero en este caso se ha implementado porque facilita la legibilidad y complejidad del código de la capa de control.

Con una anotación @Service se indica que es una clase de servicio que se conecta a uno o más repositorios. Los repositorios se obtienen con la anotación @Autowired y a partir de ahí se puede trabajar con normalidad llamando a los métodos de cada uno de los repositorios para realizar las operaciones pertinentes.

```java
@Service
public class GeneralService {

    @Autowired
    private DispositivoRepository repositorioDispositivos;

    @Autowired
    private CaracteristicaRepository repositorioCaracteristicas;
```

Imagen 17. Clase GeneralService.java

En el caso de este servicio se han implementado siete métodos que realizan las siguientes funciones:

El método dispositivos() coge del repositorio de dispositivos todos los dispositivos y los devuelve.

```java
public List<Dispositivo> dispositivos() {
    return repositorioDispositivos.findAll();
}
```

Imagen 18. Método dispositivos() de la clase GeneralService.java

El método dispositivoPorId(String id) coge del repositorio de dispositivos el dispositivo del que se pasa el id, si no lo encuentra, devuelve null.

```java
public Dispositivo dispositivoPorId(String id) {
    Optional<Dispositivo> dispositivoOptional = repositorioDispositivos.findById(id);
    if (dispositivoOptional.isEmpty()) {
        return null;
    }
    return dispositivoOptional.get();
}
```

Imagen 19. Método dispositivoPorId(String id) de la clase GeneralService.java

El método creaDispositivo(Dispositivo d) recibe como parámetro un dispositivo, comprueba que no exista el id del dispositivo y lo crea, si ya existe, devuelve null.

```
public Dispositivo creaDispositivo(Dispositivo d) {
    Optional<Dispositivo> optional = repositorioDispositivos.findById(d.getId());
    if (!optional.isEmpty())
        return null;
    return repositorioDispositivos.saveAndFlush(d);
}
```

Imagen 20. Método creaDispositivo(Dispositivo d) de la clase GeneralService.java

El método actualizaDispositivo(Dispositivo d) recibe como parámetro un dispositivo, comprueba que exista y lo actualiza, en caso de no existir, devuelve null.

```
public Dispositivo actualizaDispositivo(Dispositivo d) {
    Optional<Dispositivo> optional = repositorioDispositivos.findById(d.getId());
    if (optional.isEmpty())
        return null;
    return repositorioDispositivos.saveAndFlush(d);
}
```

Imagen 21. Método actualizaDispositivo(Dispositivo d) de la clase GeneralService.java

El método caracteristicas() coge del repositorio de características todas las características y las devuelve.

```
public List<Caracteristica> caracteristicas() {
    return repositorioCaracteristicas.findAll();
}
```

Imagen 22. Método caracteristicas() de la clase GeneralService.java

El método caracteristicaPorId(Long id) coge del repositorio de características la característica de la que se pasa el id, si no la encuentra, devuelve null.

```
public Caracteristica caracteristicaPorId(Long id) {
    Optional<Caracteristica> carcateristicaOptional = repositorioCaracteristicas.findById(id);
    if (carcateristicaOptional.isEmpty()) {
        return null;
    }
    return carcateristicaOptional.get();
}
```

Imagen 23. Método caracteristicaPorId(Long id) de la clase GeneralService.java

El método creaCaracteristica(Caracteristica d) recibe como parámetro una característica, comprueba que la característica no tenga id definido y la crea, si tiene id definido, devuelve null. Esto se debe a que el id de la característica es autogenerado, por lo que tiene que estar vacío.

```
public Caracteristica creaCaracteristica(Caracteristica d) {
    if (d.getId() != null)
        return null;
    return repositorioCaracteristicas.saveAndFlush(d);
}
```

Imagen 24. Método creaCaracteristica(Caracteristica d) de la clase GeneralService.java

3.3.3. Implementación de la controller layer

Esta capa está formada por un único controlador llamado GeneralController.java que es el encargado de hacer de RestController, por ello se anota la clase con @RestController indicando al servicio que esta clase es la encargada de recibir las peticiones y dependiendo del path hacer unos u otro métodos.

El path general para todas las direcciones en este controlador se añade con la anotación @RequestMapping y se ha utilizado como se puede ver en la Tabla 3 “REST_TFGMarioIngelmoDiana”.

En este controlador se obtienen con la anotación @Autowired tanto el servicio comentado en la capa anterior (GeneralService.java) como otras tres clases que se explicarán en el apartado siguiente de seguridad. Por esto, el método getToken, aunque pertenezca al controlador, se mencionará y explicará en el siguiente punto.

```
@RestController
@RequestMapping("REST_TFGMarioIngelmoDiana")
public class GeneralController {

    @Autowired
    private AuthenticationManager authenticationManager;

    @Autowired
    private UserDetailsServiceImpl usuarioDetailsService;

    @Autowired
    private GestionTokens gestion;

    @Autowired
    private GeneralService servicio;
```

Imagen 25. Clase GeneralController.java

Este controlador, para cumplir con lo especificado en la Tabla 3, dispone de siete métodos para cubrir todas las peticiones que se han definido, en este apartado se explicarán seis de ellas, dejando para después el POST de getToken():

El método getDispositivos(Varios request params) se encarga de gestionar las peticiones GET con el path “REST_TFGMarioIngelmoDiana/dispositivos” y conseguir todos los dispositivos del servicio, filtrando por categoría, seguridad y sostenibilidad si se indica y ordenando en caso de solicitarse. En caso de no haber dispositivos devuelve un NOT FOUND.

```java
@GetMapping("/dispositivos")
public ResponseEntity<ListaDispositivos> getDispositivos(
        @RequestParam(value = "categoria", required = false) String categoria,
        @RequestParam(value = "seguridad", required = false) String seguridad,
        @RequestParam(value = "sostenibilidad", required = false) String sostenibilidad,
        @RequestParam(value = "ordenar", required = false) String ordenar) {
    List<Dispositivo> dispositivos = servicio.dispositivos();
    if (dispositivos.isEmpty()) {
        return ResponseEntity.notFound().build();
    }
    if (categoria != null && !categoria.equals("Todas")) {
        dispositivos = dispositivos.stream().filter(d -> d.getCategoria() == Categoria.valueOf(categoria))
                .collect(Collectors.toList());
    }
    if (seguridad != null && Integer.valueOf(seguridad) >= 0 && Integer.valueOf(seguridad) <= 100) {
        dispositivos = dispositivos.stream().filter(d -> d.getSeguridad() >= Integer.valueOf(seguridad))
                .collect(Collectors.toList());
    }
    if (sostenibilidad != null) {
        dispositivos = dispositivos.stream()
                .filter(d -> d.getSostenibilidad().matches("[A-" + sostenibilidad.toUpperCase() + "]"))
                .collect(Collectors.toList());
    }
    if (ordenar != null && (ordenar.equals("Alfabetico") || ordenar.equals("Seguridad") || ordenar.equals("Sostenibilidad"))) {
        switch (TipoOrdenar.valueOf(ordenar)) {
        case Alfabetico:
            dispositivos = dispositivos.stream().sorted(Comparator.comparing(Dispositivo::getNombre, String.CASE_INSENSITIVE_ORDER)).collect(Collectors.toList());
            break;
        case Seguridad:
            dispositivos = dispositivos.stream().sorted(Comparator.comparingInt(Dispositivo::getSeguridad).reversed()).collect(Collectors.toList());
            break;
        case Sostenibilidad:
            dispositivos = dispositivos.stream().sorted(Comparator.comparing(Dispositivo::getSostenibilidad)).collect(Collectors.toList());
            break;
        default:
            break;
        }
    }
    return ResponseEntity.ok(new ListaDispositivos(dispositivos));
}
```

Imagen 26. Método getDispositivos(…) de la clase GeneralController.java

El método getDispositivo(@PathVariable String id) se encarga de gestionar las peticiones GET con el path “REST_TFGMarioIngelmoDiana/dispositivos/{id}” y conseguir el dispositivo cuyo id se pasa en el path, devolviendo NOT FOUND si no existe ningún dispositivo con ese id.

```java
@GetMapping("/dispositivos/{id}")
public ResponseEntity<ListaDispositivos> getDispositivo(@PathVariable String id) {
    Dispositivo d = servicio.dispositivoPorId(id);
    if (d == null) {
        return ResponseEntity.notFound().build();
    }
    List<Dispositivo> dispositivos = new LinkedList<Dispositivo>();
    dispositivos.add(d);
    return ResponseEntity.ok(new ListaDispositivos(dispositivos));
}
```

Imagen 27. Método getDispositivo(@PathVariable String id) de la clase GeneralController.java

De la misma manera que los dos métodos anteriores, tenemos lo mismo para las características, el método getCaracteristicas() se encarga de gestionar las peticiones GET con el path “REST_TFGMarioIngelmoDiana/ caracteristicas” y el método getCaracteristica(@PathVariable String id) se encarga de gestionar las peticiones GET con el path “REST_TFGMarioIngelmoDiana/caracteristicas/{id}”.

```java
@GetMapping("/caracteristicas")
public ResponseEntity<ListaCaracteristicas> getCaracteristicas() {
    List<Caracteristica> caracteristicas = servicio.caracteristicas();
    if (caracteristicas.isEmpty()) {
        return ResponseEntity.notFound().build();
    }
    return ResponseEntity.ok(new ListaCaracteristicas(caracteristicas));
}
```

Imagen 28. Método getCaracteristicas() de la clase GeneralController.java

```java
@GetMapping("/caracteristicas/{id}")
public ResponseEntity<Caracteristica> getCaracteristica(@PathVariable String id) {
    Caracteristica c = servicio.caracteristicaPorId(Long.valueOf(id));
    if (c == null) {
        return ResponseEntity.notFound().build();
    }
    return ResponseEntity.ok(c);
}
```

Imagen 29. Método getCaracteristica(@PathVariable String id) de la clase GeneralController.java

El método creaOReemplazaDispositivo(@PathVariable String id, @RequestBody Dispositivo d) se encarga de gestionar las peticiones PUT con el path "REST_TFGMarioIngelmoDiana/dispositivos/{id}" y de crear o actualizar el dispositivo cuyo id se pasa en el path, en caso de que los ids no coincidan o que no se pueda crear o actualizar se devolverá un CONFLICT.

```java
@GetMapping("/caracteristicas/{id}")
public ResponseEntity<Caracteristica> getCaracteristica(@PathVariable String id) {
    Caracteristica c = servicio.caracteristicaPorId(Long.valueOf(id));
    if (c == null) {
        return ResponseEntity.notFound().build();
    }
    return ResponseEntity.ok(c);
}
```

Imagen 30. Método creaOReemplazaDispositivo(@PathVariable String id, @RequestBody Dispositivo d) de la clase GeneralController.java

Y finalmente el método creaCaracteristica(@RequestBody Caracteristica c) se encarga de gestionar las peticiones POST con el path "REST_TFGMarioIngelmoDiana/caracteristicas" y de crear una nueva característica, en caso de que no se pueda crear, se devolverá un CONFLICT.

```java
@PostMapping("/caracteristicas")
public ResponseEntity<Caracteristica> creaCaracteristica(@RequestBody Caracteristica c) {
    Caracteristica creado = servicio.creaCaracteristica(c);
    if (creado == null)
        return ResponseEntity.status(HttpStatus.CONFLICT).build();
    URI location = ServletUriComponentsBuilder.fromCurrentRequest().build().toUri();
    return ResponseEntity.created(location).body(creado);
}
```

Imagen 31. Método creaCaracteristica(@RequestBody Caracteristica c) de la clase GeneralController.java

3.3.4. Implementación de la seguridad y la configuración

Para implementar la seguridad se va a utilizar JSON Web Tokens (JWT), JWT es un estándar abierto que define un mecanismo para el intercambio seguro de información en forma de objetos JSON. La información es verificable y confiable porque está digitalmente firmada, además pueden ser firmados usando una llave pública o privada secreta [8]. Todo esto convierte a JWT en una forma muy completa y buena para implementar la seguridad en el servicio y poner un filtro de autorización en las funcionalidades deseadas.

Para ello se necesitan cubrir los siguientes pasos: 1. Verificar al usuario mediante sus credenciales. 2. Crear y devolver el token JWT. 3. Validar el token introducido por el usuario y aprobar la operación o denegarla.

Se han creado una serie de clases, con diferentes funcionalidades para cubrir esos pasos:

Primero se ha añadido en el controlador (GeneralController.java) un método getToken(@RequestBody Credenciales c) que se encarga de gestionar las llamadas POST al path “REST_TFGMarioIngelmoDiana/token”, recoge las credenciales del usuario (usuario y clave), autentica al mismo, lo carga, genera el token y lo devuelve, estos pasos se explicarán a continuación.

```
@PostMapping("/token")
public ResponseEntity<String> getToken(@RequestBody Credenciales c) {
    if (c == null) {
        return ResponseEntity.status(HttpStatus.BAD_REQUEST).build();
    } else {
        authenticationManager.authenticate(new UsernamePasswordAuthenticationToken(c.getUsuario(), c.getClave()));
        usuarioDetailsService.loadUserByUsername(c.getUsuario());
        String token = gestion.generaToken(c.getUsuario(), c.getClave());
        if (token == null) {
            return ResponseEntity.status(HttpStatus.BAD_REQUEST).build();
        } else {
            return ResponseEntity.ok(token);
        }
    }
}
```

Imagen 32. Método getToken(@RequestBody Credenciales c) de la clase GeneralController.java

Una vez las credenciales se han recogido, es necesario autenticar al usuario, esto se hace de manera automática utilizando el AuthenticationManager de la dependencia de seguridad de Spring. Después se carga el usuario, esto se hace con un @Service que implementa UserDetailsService, otra clase de la dependencia de seguridad de Spring.

Y finalmente se genera el token, para esto se ha creado un clase GestionTokens.java que es un @Service que sirve para generar y para validar un token. En este caso, se genera el token mediante el nombre y contraseña que había en las credenciales que el usuario ha pasado en el método POST. Se comprueba que el nombre y contraseña coincidan y una vez verificado se firma la llave y se crea el token dándole una validez de 15 minutos. Una vez hecho esto, se devuelve al usuario.

```
public String generaToken(String nombre, String contra) {
    String token = null;
    if (nombre.equals(NOMBRE) && contra.equals(CONTRA)) {
        Key signingKey = new SecretKeySpec(DatatypeConverter.parseBase64Binary(SECRET_KEY),
                SignatureAlgorithm.HS256.getJcaName());
        keyGenerada = signingKey;
        Calendar cal = Calendar.getInstance();
        cal.add(Calendar.MINUTE, 15);
        Date date = cal.getTime();
        JwtBuilder builder = Jwts.builder().setSubject(NOMBRE).setExpiration(date).signWith(signingKey,
                SignatureAlgorithm.HS256);

        token = builder.compact();
    }
    return token;
}
```

Imagen 33. Método generaToken(String nombre, String contra)de la clase GestionTokens.java

Una vez el usuario obtiene su token, lo introduce en la siguiente petición que realice y se verificará si: 1. Su petición necesita autorización (las peticiones GET no las necesitan y el POST del token tampoco). 2. El token es válido.

Para comprobar todo lo mencionado hay que configurar el servicio de manera que lo personalicemos y ofrezca la funcionalidad que nosotros queremos, si este paso no es realizado, el servicio solicitará el token para cualquier petición a este.

Primero configuramos la seguridad web, para esto añadimos la clase WebSecurityConfig.java con la anotación @Configuration para que al lanzar el servicio, este la detecte como una configuración propia y la aplique. En esta clase, se crea un @Bean que se encargará de deshabilitar el csrf, para así permitir el uso de tokens JWT, también se encargará de autorizar determinadas llamadas sin autenticación y de aplicar una configuración de cors personalizada añadiendo un filtro propio y así poder solicitar recursos restringidos por la seguridad, que se explicará a continuación.

```
@Bean
SecurityFilterChain web(HttpSecurity http) throws Exception {
    http.csrf().disable()
            .authorizeHttpRequests((authorize) -> authorize.requestMatchers("/REST_TFGMarioIngelmoDiana/token")
                    .permitAll().requestMatchers(HttpMethod.GET, "/**").permitAll()
                    .requestMatchers(HttpMethod.POST, "/**").hasRole("ADMIN").requestMatchers(HttpMethod.PUT, "/**")
                    .hasRole("ADMIN").requestMatchers(HttpMethod.DELETE, "/**").hasRole("ADMIN").anyRequest()
                    .authenticated())
            .cors(withDefaults()).addFilterBefore(jwtRequestFilter, UsernamePasswordAuthenticationFilter.class)
            .sessionManagement((session) -> session.sessionCreationPolicy(SessionCreationPolicy.STATELESS));

    return http.build();
}
```

Imagen 34. Bean de la clase WebSecurityConfig.java para la configuración de la seguridad

El filtro propio (JwtRequestFilter,java) es el encargado de gestionar la obtención del token (lee la cabecera Authorization), también se encarga de saltar el proceso de autorización si la petición es GET o es el POST para conseguir el token y también valida el token una vez obtenido.

```
public boolean validaToken(String token) {
    try {
        Jwts.parserBuilder().setSigningKey(keyGenerada).build().parseClaimsJws(token);
        return true;
    } catch (JwtException e) {
        System.out.println("El token está mal");
    }
    return false;
}
```

Imagen 35. Método validaToken(String token)de la clase GestionTokens.java

Finalmente, para que las peticiones puedan hacerse desde cualquier dirección, hay que habilitar en el cors diferentes orígenes, métodos, etc. Esto se hace con la clase CorsConfig.java anotada con @Configuration y con un @Bean que se encarga de la configuración personalizada del cors.

```
@Bean
CorsConfigurationSource corsConfigurationSource() {
    CorsConfiguration configuration = new CorsConfiguration();
    configuration.setAllowedOrigins(Arrays.asList("*"));
    configuration.setAllowedMethods(Arrays.asList("*"));
    configuration.setAllowedHeaders(Arrays.asList("*"));
    UrlBasedCorsConfigurationSource source = new UrlBasedCorsConfigurationSource();
    source.registerCorsConfiguration("/**", configuration);
    return source;
}
```

Imagen 36. Bean de la clase CorsConfig.java para la configuración del cors

3.4. Pruebas del servicio

Este apartado es uno de los puntos a tratar en el trabajo futuro. Se han realizado pruebas al servicio, pero no tantas como se querría y esto ha sido debido a la extensión del proyecto completo.

Se han realizado pruebas para probar cada una de las funcionalidades básicas del servicio, esto es, cada una de las peticiones que se pueden realizar al servicio, se han probado tanto casos de éxito a la hora de recuperar los dispositivos, como casos de error, por ejemplo que un id de un dispositivo no exista. También se ha probado que la seguridad con JWT funcione correctamente, se ha comprobado a generar el token con un usuario registrado y con uno sin registrar y se ha comprobado que en el segundo de los casos no genera el token y devuelve el fallo deseado. También se ha comprobado que el tiempo de validez del token es funcional (15 minutos) y que los métodos indicados, funcionan solo cuando se mete un token válido.

3.5. Despliegue del servicio

Para el despliegue del servicio se ha utilizado Microsoft Azure, se ha creado un grupo de recursos donde también se ha añadido la base de datos que utiliza el servicio. Una vez terminado el servicio, este es empaquetado, primero se prueba su funcionamiento en local y después se despliega.

Para el despliegue se ha creado una máquina virtual Linux con Ubuntu 20.04, también se ha creado una interfaz de red y se ha reservado una ip pública, asociándola a la máquina virtual, de manera que, a través de esa ip, se pueda acceder al servicio a través del puerto 8080, ya que, una vez pasado a la máquina y ejecutado, el servicio queda desplegado en ese puerto, haciendo así que siempre que la máquina virtual esté activa, el servicio esté disponible en la siguiente dirección: “http://51.137.100.222:8080/”. Pudiendo así hacer peticiones como el GET de los dispositivos en la siguiente dirección: “http://51.137.100.222:8080/REST_TFGMarioIngelmoDiana/dispositivos”.

Para agilizar el procedimiento a la hora de arrancar la máquina virtual y que no sea necesario acceder a esta y arrancarlo manualmente, se ha creado un servicio que se encarga de arrancar el servicio automáticamente al iniciar.

```
[Unit]
Description=Servicio para arrancar el jar
After=network.target

[Service]
ExecStart=/usr/bin/java -jar /home/azureuser/REST_TFGMarioIngelmoDiana.jar

[Install]
WantedBy=default.target
```

Imagen 37. Servicio en la máquina virtual para el despliegue automático del servicio REST

4. Desarrollo de la aplicación

En este apartado se explicarán los diferentes apartados que ha tenido el desarrollo de la aplicación Android, desde el análisis de requisitos hasta la finalización de esta.

4.1. Análisis de requisitos de la aplicación

Se van a analizar tanto la idea tras la aplicación, como los pasos iniciales que se dieron en cuanto al diseño (mockups) y también los requisitos, tanto funcionales como no funcionales. Dando una idea global de la aplicación y que se busca con su desarrollo.

4.1.1. Idea tras la aplicación

La idea a la hora de desarrollar la aplicación es darle al usuario una manera de poder comprobar y comparar la seguridad y sostenibilidad de diferentes dispositivos IoT que pueda tener por casa o pueda estar interesado en adquirir.

Hoy en día la seguridad es algo muy importante, pero también es algo a lo que mucha gente no presta la atención suficiente, ya sea porque no le interesa o porque los datos son difíciles de conseguir. Por ejemplo, cuando vas a comprar un dispositivo de este estilo siempre tienes las mismas características: color, tamaño, precio, almacenamiento, ram, consumo, etc. Pero pocas veces o ninguna encuentras características relacionadas con la seguridad y la sostenibilidad, por esto se ha decidido desarrollar la aplicación.

Para hacer la experiencia más cómoda y sencilla al usuario se han propuesto unos objetivos básicos que se explican de manera resumida:

- Disponer de filtros y de un buscador de dispositivos.
- Disponer de una sección de favoritos donde guardar los dispositivos favoritos.
- Disponer de un escáner donde escanear los códigos de barras de los productos y acceder a sus características.
- Disponer de una interfaz donde mostrar las características del dispositivo más en detalle.
- Disponer de una interfaz moderna y amigable con el usuario.

Para mostrar las ideas principales que se manejaban y cuál era la idea sobre el diseño se van a presentar unos mockups realizados a mano alzada para luego compararlos con el diseño final de la aplicación.

Primero tenemos el mockup de lo que iba a ser la sección principal de la aplicación, con el filtro y el buscador, que una vez buscado por nombre, mostrase una lista de resultados coincidentes tanto con el filtro como con el texto del buscador.

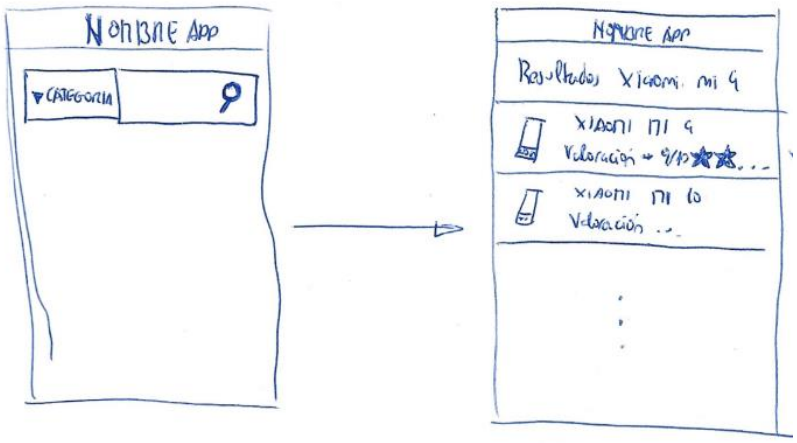

Imagen 38. Mockup de la idea sobre la sección principal

También tenemos el mockup sobre lo que sería la sección donde se mostrase un dispositivo específico en detalle al ser seleccionado.

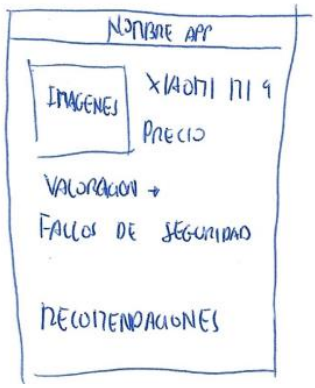

Imagen 39. Mockup de la idea sobre la sección del detalle de un dispositivo

Aunque la versión final difiere en ciertos aspectos de estos mockups, estos sirven para mostrar cuál era el enfoque inicial y poder comprobar cómo, durante el desarrollo de la aplicación, ciertos aspectos han ido cambiando, mientras que otros se han mantenido.

4.1.2. Requisitos funcionales

A continuación se presenta una tabla con los diferentes requisitos funcionales que se han obtenido:

ID	Descripción
RF1	La aplicación dispondrá de menú lateral de navegación.
RF2	La aplicación dispondrá de una sección de buscador.
RF3	La aplicación dispondrá de una sección de escanear.
RF4	La aplicación dispondrá de una sección de favoritos.
RF5	La aplicación dispondrá de una sección de compartir.
RF6	La sección de buscador se abrirá por defecto al abrir la aplicación.
RF7	La sección de buscador mostrará una lista con todos los dispositivos ordenados por orden alfabético al abrirse.

RF8	La sección de buscador dispondrá de un botón de filtros donde establecer la categoría, la seguridad y sostenibilidad mínimas y la forma de ordenar la lista de dispositivos.
RF9	La sección de buscador dispondrá de un buscador de texto que filtrará los resultados en función al texto coincidente con el nombre o la marca de los dispositivos.
RF10	La lista resumen de dispositivos mostrará la imagen, nombre, marca, seguridad y sostenibilidad del dispositivo.
RF11	Se abrirá una vista detalle del dispositivo al pinchar sobre este.
RF12	La vista en detalle de un dispositivo tendrá un botón en forma de estrella donde añadir o eliminar un dispositivo de favoritos.
RF13	La vista en detalle de un dispositivo mostrará imagen, nombre, marca, categoría, precio, puntuación de seguridad, puntuación de sostenibilidad, descripción, lista con las características de seguridad positivas y negativas y lista con las características de sostenibilidad positivas y negativas del dispositivo.
RF14	La sección de escáner permitirá escanear códigos de barras y abrir la vista en detalle del dispositivo en cuestión.
RF15	La sección de favoritos mostrará una lista resumen con los dispositivos que se hayan añadido a favoritos.
RF16	La sección de compartir tendrá un botón desde donde compartir, mediante diferentes medios, un mensaje para invitar al uso de la aplicación.
RF17	En la sección superior del menú lateral, se mostrará el logo y nombre de la aplicación, así como el nombre del desarrollador.

Tabla 4. Requisitos funcionales de la aplicación

4.1.3. Requisitos no funcionales

A continuación se presenta una tabla con los diferentes requisitos no funcionales que se han obtenido:

ID	Clasificación	Descripción
RNF1	Portabilidad	La aplicación podrá utilizarse en cualquier dispositivo Android con una versión superior a la API 28 (Android Pie 9.0).
RNF2	Portabilidad	La aplicación dispondrá de un instalador apk de manera que su instalación sea sencilla.
RNF3	Mantenibilidad	La aplicación estará modularizada de manera que cambios en una sección principal no afecten a otra.
RNF4	Fiabilidad	La aplicación mostrará mensajes de error en caso de no poder obtener datos del servicio.
RNF5	Usabilidad	La aplicación dispondrá de una interfaz amigable con el usuario, que facilite su uso.
RNF6	Rendimiento	El tamaño del archivo apk para instalar la aplicación no superará los 100 MB.
RNF7	Rendimiento, Compatibilidad	La aplicación deberá coexistir con el resto de las aplicaciones del sistema Android, de manera que no consuma en exceso ni RAM ni CPU, permitiendo así, el uso de otras aplicaciones si esta está activa.

Tabla 5. Requisitos no funcionales de la aplicación

4.2. Diseño de la aplicación

Se va a dividir el diseño de la aplicación en dos partes. Primero se va a explicar el diseño del logotipo de la aplicación de manera resumida, para finalmente, explicar el patrón de diseño utilizado y el diseño arquitectónico realizado.

4.2.1. Diseño del logotipo

Para el diseño del logotipo de la aplicación se ha tomado como referencia una imagen del dios Hapi en blanco y negro, dios que como ya se mencionó anteriormente da nombre a esta aplicación. Y se ha añadido un candado sobre su mano que da la clave sobre la seguridad y alrededor una circunferencia con el nombre de la aplicación.

Imagen 40. Logotipo de la aplicación

4.2.2. Diseño arquitectónico

Para el diseño de la aplicación se ha utilizado el patrón Modelo-Vista-Presentador (MVP), patrón utilizado en el desarrollo de aplicaciones Android que facilita la puesta en práctica de la interfaz de usuario y reduce la complejidad al modularizar el código. Este patrón de diseño consiste en tres partes [9]:

- **Modelo:** El modelo se encarga del acceso a los datos que se van a utilizar en la aplicación, ya sea una base de datos, una memoria caché o una API rest, en este caso, se encarga de la conexión con el servicio desarrollado para la obtención de los datos del dispositivo y también de gestionar la base de datos para los favoritos.
- **Vista:** La vista se encarga de la gestión de la interfaz de usuario, de lo que se le muestra y lo que puede hacer el usuario pulsando en la pantalla del dispositivo. Muestra las diferentes actividades y los diferentes fragmentos, con sus respectivos componentes.
- **Presentador:** El presentador se encarga de hacer de puente entre el modelo y la vista. Se encarga de transmitir al modelo las peticiones que el usuario pide a través de la vista, ya sea obtener datos, almacenar en favoritos, etc, y se encarga de devolver a la vista esos datos que pide al modelo. Permitiendo separar la interfaz de usuario de la lógica de la aplicación.

A la vista de este patrón y con la funcionalidad que debe tener la aplicación, la parte de interfaces de usuario se ha dividido en tres actividades y cuatro fragmentos que se utilizarán en una de las actividades.

Las actividades son dos, una es el menú inicial que dispone del menú lateral de navegación y es la actividad que desplegará cada uno de los cuatro fragmentos, que corresponden a las secciones de buscador, escanear, favoritos y compartir. La otra actividad es la encargada de mostrar los datos de cada dispositivo en detalle.

Cada actividad y fragmento contará con su clase view y su clase presenter, excepto la sección de compartir, que al tener una lógica muy simple que no necesita de datos se ha implementado directamente, al igual que el menú inicial que gestiona la navegación y el despliegue de los diferentes fragmentos y tampoco necesita datos.

A continuación se presentan tanto el diagrama con la arquitectura final de la aplicación como el diagrama con el dominio de la aplicación con sus clases y sus relaciones.

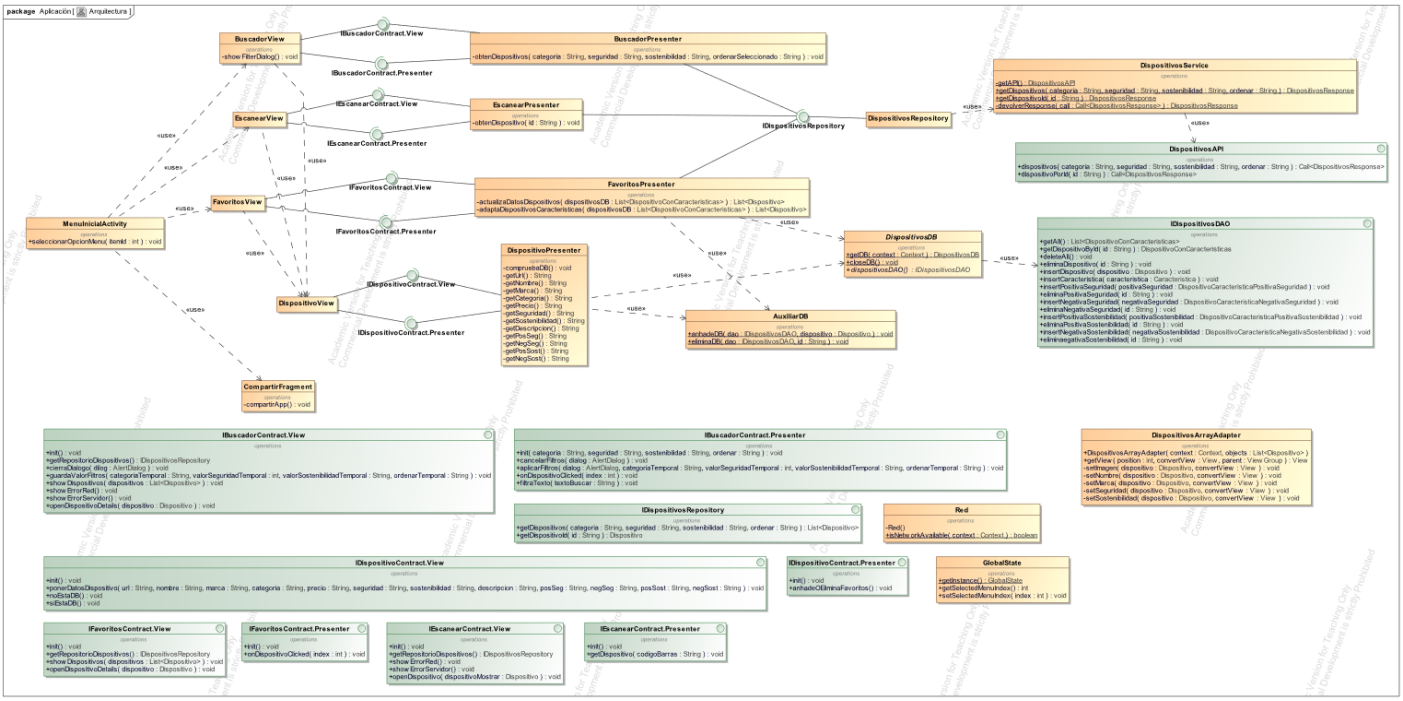

Imagen 40. Diagrama con la arquitectura de la aplicación

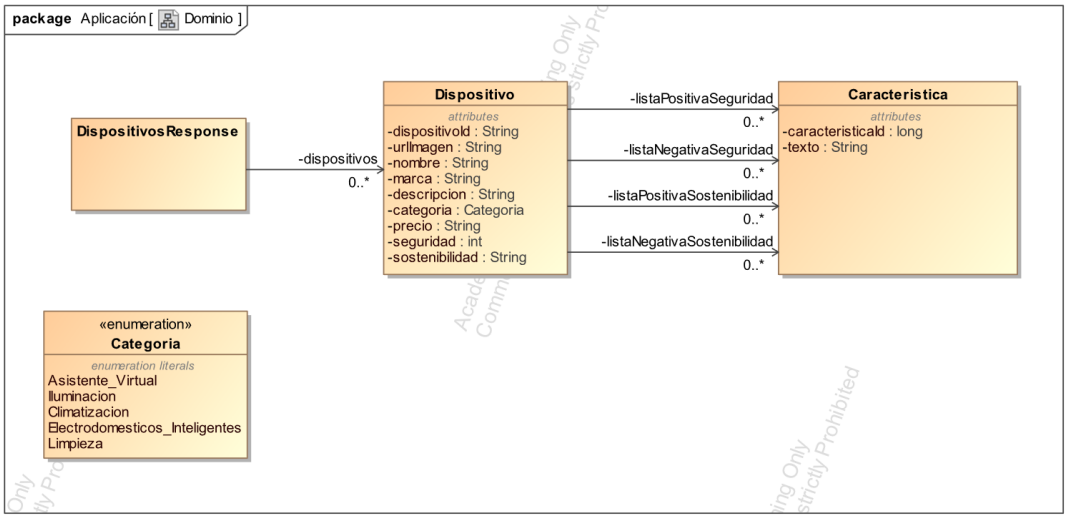

Imagen 41. Diagrama con el dominio de la aplicación

También se añade el diagrama con el dominio, pero añadiendo como se mapea en la base de datos que se usa para los favoritos. Esto se realiza así puesto que el dominio normal no se admite con las relaciones que tiene utilizando Room, hay que mapearlo de esta manera de forma que el dispositivo vaya embebido en otra clase y las relaciones a las características sean unidas mediante tablas intermedias.

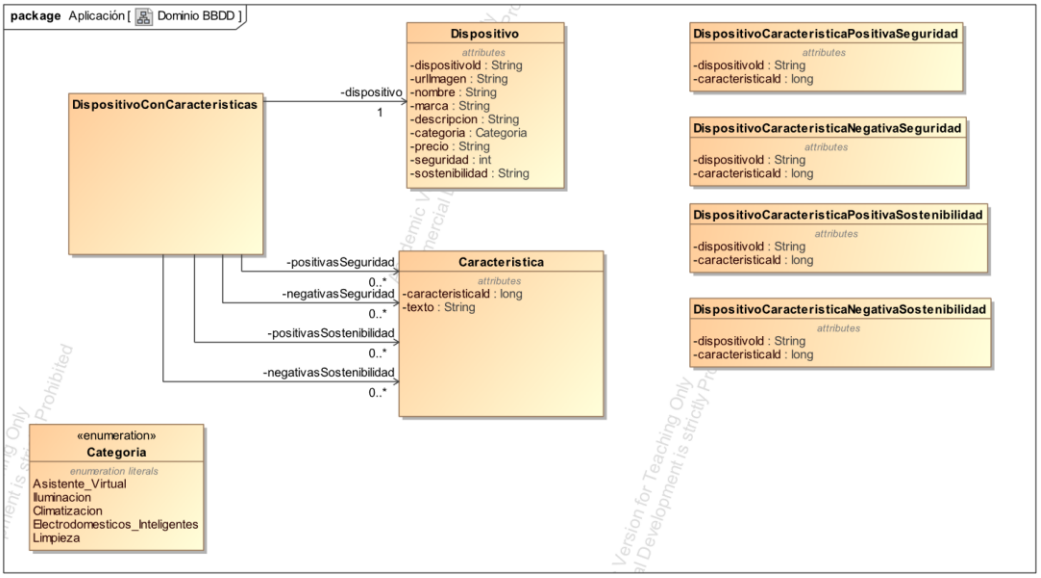

Imagen 42. Diagrama con el dominio de la aplicación para la BBDD

4.3. Implementación de la aplicación

4.4. Pruebas de la aplicación

5. Conclusiones y trabajo futuro

Trabajo futuro: Ampliar la base de datos, ampliar las categorías que se cubren, hacer que la seguridad y sostenibilidad sean auto calculados dependiendo de un baremo con un dato en las caracteristicas, eliminar dispositivos, modificar o eliminar caracteristicas.

BIBLIOGRAFIA

[1] https://www.kaspersky.es/about/press-releases/2021_el-numero-de-ataques-a-dispositivos-iot-se-duplica-en-un-ano

[2] https://dplnews.com/numero-de-dispositivos-iot-conectados-alcanzara-22-mil-millones-para-2025/#:~:text=El%20experto%20particip%C3%B3%20en%20el,millones%20de%20dispositivos%20IoT%20conectados

[3] https://proyectosagiles.org/desarrollo-iterativo-incremental/

[4] Astigarraga, J., & Cruz-Alonso, V. (2022). ¡ Se puede entender cómo funcionan Git y GitHub!. Ecosistemas, 31(1), 2332-2332.

[5] https://www.ibm.com/es-es/topics/java-spring-boot#%C2%BFQu%C3%A9+es+Java+Spring+Boot%3F

[6] https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure/

[7] https://developer.android.com/studio/intro?hl=es-419

[8] https://jwt.io/introduction

[9] https://keepcoding.io/blog/que-es-el-modelo-vista-presentador/