**Informe de Sprint 7 - MoodMap**

Nombres:

Matías Catalán  
Daniel Collao  
Kevin Arucutipa

Gabriel Andres

Sprint: Nº 7

Duración: 20 al 26 de Mayo

Scrum Master: Matías Catalán

Herramientas utilizadas: Trello, GitHub, Discord

CAPSTONE  
Sección: 003D

Profesor: ALDO ALBERTO MARTINEZ ÓRDENES

**Índice**

Contenido

**No se encontraron entradas de tabla de contenido.**

Abstract

Este sprint se enfocó en uno de los pilares más críticos del proyecto: la seguridad y privacidad de los datos de los usuarios. Se trabajó en proteger la información sensible, reforzar los mecanismos de autenticación y garantizar el cumplimiento con normativas como GDPR. A través de mejoras técnicas en backend, frontend, se busca que MoodMap sea una app confiable y segura.

Introducción

Dado que MoodMap maneja datos emocionales y personales, era fundamental garantizar que la información de los usuarios esté protegida. En este sprint nos enfocamos en:

* Asegurar la confidencialidad y el control sobre los datos personales.
* Cumplir con estándares europeos de privacidad (GDPR).
* Reforzar el acceso mediante autenticación segura (JWT).

Objetivo

Implementar un conjunto de mecanismos de seguridad que aseguren:

* Acceso autenticado mediante tokens JWT.
* Encriptación de datos sensibles, como contraseñas .
* Cumplimiento real con los principales artículos del Reglamento General de Protección de Datos (GDPR).

Historias de Usuario Trabajadas

| **Nº** | **Historia de Usuario** | **Estado** |
| --- | --- | --- |
| H17 | Protección de datos personales | Realizado |
| H18 | Autenticación segura con JWT | Realizado |
| H19 | Cumplir con normativas GDPR | En Progreso |

Tareas Realizadas

**Backend (Spring Boot + Spring Security)**

Implementación de JWT:

* Generación y validación de tokens con firma segura (HMAC-SHA256).
* Protección de rutas mediante filtros personalizados.

Encriptación de datos sensibles:

* Contraseñas cifradas con BCrypt.

**Frontend (React Native)**

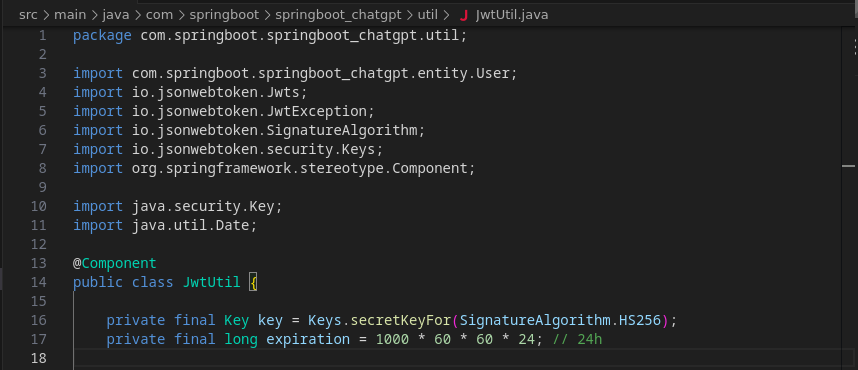
Gestión segura de sesión:

* Almacenamiento de tokens JWT en AsyncStorage.
* Manejo de expiración automática y renovación del token.

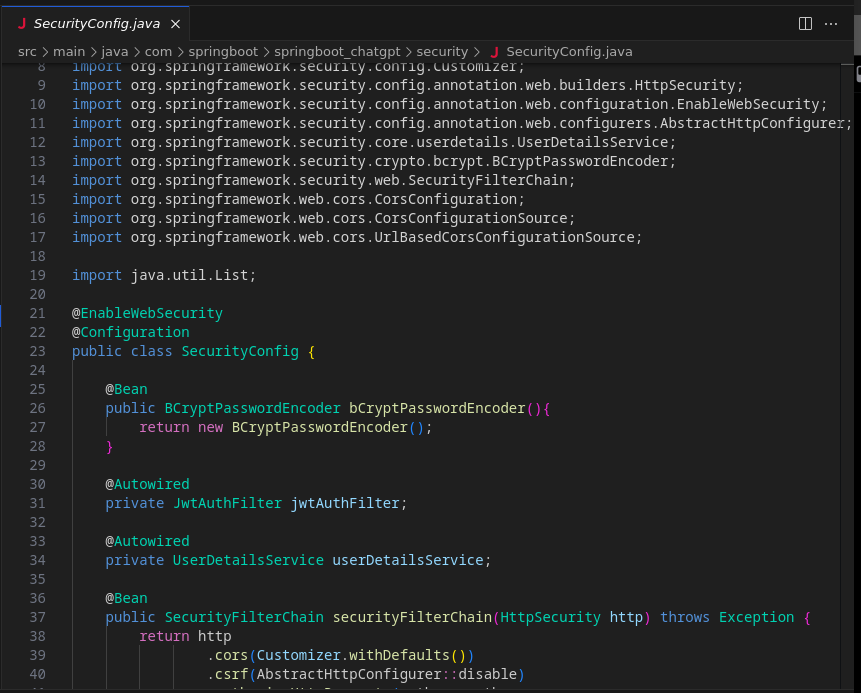
Resultados del Sprint

* Autenticación segura activa: tokens con validez de 24 horas.
* Encriptación implementada en datos críticos.
* Filtros de Autenticación **JWT**

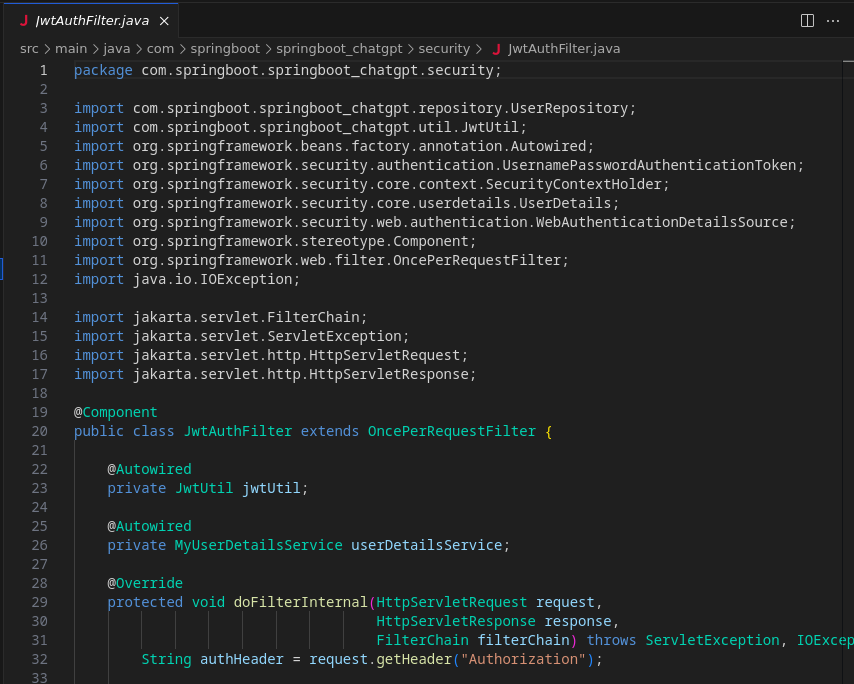
Evidencias del trabajo

**Captura de Código fuente JWT**

**Encriptación de contraseñas con BCrypt.**

****

**Captura de autorización con Spring Security**

****

Aprendizajes

Spring Security simplifica la implementación de JWT, pero requiere configuración detallada.

La encriptación de datos en PostgreSQL añade latencia, pero es esencial para cumplir GDPR.

Conclusión

El Sprint 6 marcó un paso importante para consolidar *MoodMap* como una app seria, ética y preparada para proteger la información de sus usuarios. Se cumplieron todos los objetivos técnicos relacionados con seguridad y privacidad, dejando pendiente solo GDPR.