Back office Crisalis

ESPECIFICACIONES TÉCNICAS

Sprint - Deadline	**2 - 3/11/23**
Jira asociado	**SCRUM-44 (incluye SCRUM-43)**
Responsable	**Miguel Ángel Maisares**
Equipo	• Miguel Ángel Maisares • Lucas Sarfati • Javier Huebra • Matias Stewart Usher • Facundo Oliva • Koba Chajchir • Yamil Leotta
Versión	1.0

Contexto

Actualmente nuestra aplicación carece de un sistema de login robusto, se investigo el mercado y se llego a la conclusión de implementar el modulo de Spring Security junto con JWT (Json Web Token). Ambos módulos ofrecen un mecanismo de autenticación robusto y moderno para Back office Crisalis.

Objetivo

Implementar Spring Security con JWT para el sistema de login y API.

Alcance

- Sistema de login tokenizado con un tiempo valido de 1 hora.
- Validación de tokens por cada request entrante a la API.

Entregable

El entregable contiene el sevicio de login con autenticacion de token y validación por cada request a la API:

- Login de un usuario:
  POST /login

REQUEST:

```
{
   "usuario": "string",
   "password": "string"
}
```

RESPONSE:

```
{
   "token": {
      "authorities": ["string"],
      "isAdmin": boolean,
   },
   "message": "string",
   "username": "string",
}
```

- Consulta de recursos en general con su token en el header de la request:

HEADERS:

```
{
   ...,
   "Authorization": "string"
}
```