

**FIAP**

**Faculdade de Informática e Administração Paulista**

# **Challenge Softtek Sprint 2**

Diego Xavier Lourenço — RM556415

Edilberto Cunha de Moraes — RM554365

Leandro Jun Sakai Takara — RM558441

Luciana Aparecida de Almeida — RM554667

Misael Souza Marcelino — RM554568

# Entrega - Softmind Backend

## 1. Organização por Camadas e Módulos

O projeto segue **arquitetura em camadas (Layered Architecture)**, garantindo separação de responsabilidades e manutenção facilitada.

- **Camada de Entidades (Entities / Documents)**  
Representa os objetos de domínio e documentos do MongoDB.  
Ex.: `User`, `Employee`, `Survey`, `Answer`.
- **Camada de DTOs (Data Transfer Objects)**  
Estruturas para transportar dados entre backend e frontend.  
Ex.: `LoginRequestDto`, `LoginResponseDto`, `SurveyCreateDto`.
- **Camada de Repositórios (Repositories)**  
Interface com o banco de dados MongoDB (Spring Data).  
Ex.: `UserRepository`, `SurveyRepository`.
- **Camada de Serviços (Services)**  
Contém a lógica de negócio.  
Ex.: `UserService`, `EmployeeService`, `AuthService`.
- **Camada de Controladores (Controllers / Resources)**  
Expõe endpoints REST da API.  
Ex.: `AuthController`, `SurveyController`.

## 2. Estratégia de Segurança e Controle de Acesso

- **Autenticação baseada em JWT (JSON Web Token).**
- **Perfis de acesso:**
  - **ADMIN** → Criação de pesquisas, gestão de funcionários.
  - **USER** → Responder pesquisas.
- **Spring Security** configurado para interceptar requisições e validar o token.
- **Claims extras no JWT:** Nome do colaborador, perfil de acesso.
- **Política de expiração:** Tokens expira em 24h.

### 3. Especificações dos Endpoints Chave (Contrato da API)

#### Autenticação

- **POST** /auth/login
  - Request: { "username": "string", "password": "string" }
  - Response: { "token": "string", "username": "string", "name": "string" }

#### Pesquisas

- **POST** /survey (ADMIN)
  - Cria nova pesquisa.
  - Request: SurveyCreateDto.
- **GET** /survey/{id}
  - Retorna os detalhes de uma pesquisa por ID.
- **POST** /survey/{id}/answer (USER)
  - Registra uma resposta.
  - Request:

```
{
  "answers": [
    { "questionText": "string", "response": "string" }
  ],
  "participationDate": "2025-10-01T22:56:49.244Z"
}
```

## 4. Modelo de Dados e Exceções

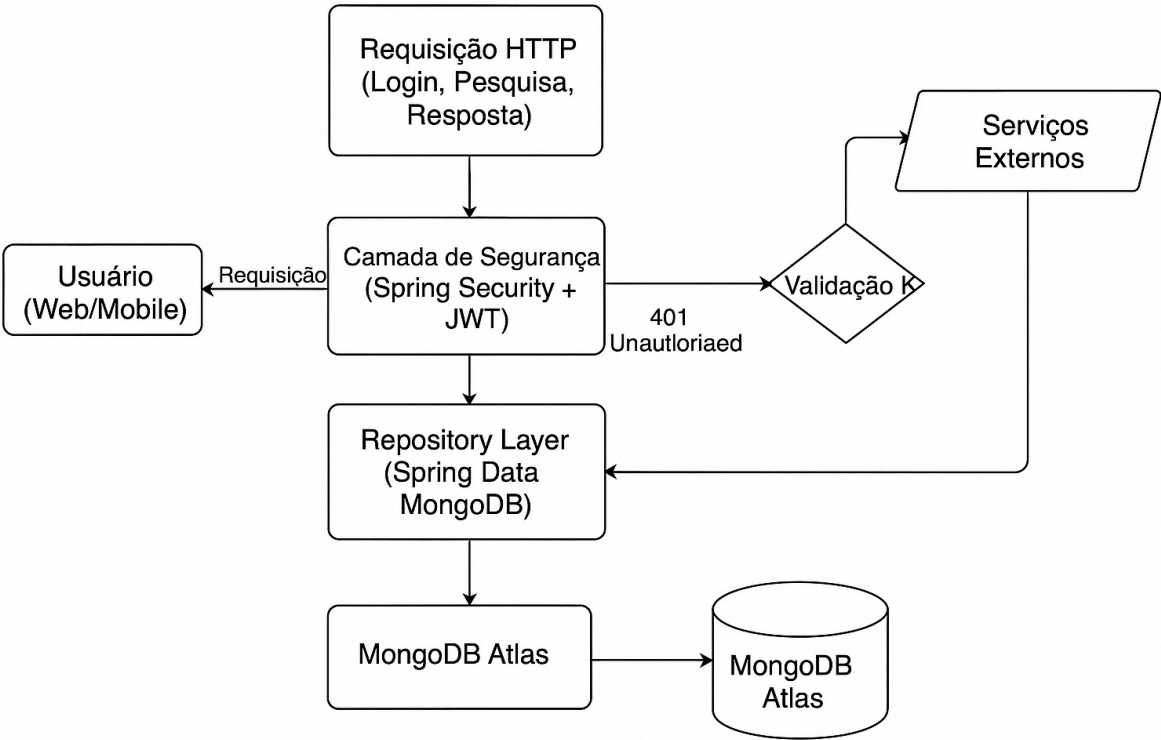
### Documentos principais no MongoDB:

- **User**
  - id, username, password, role, employeeId.
- **Survey**
  - id, title, questions[], createdBy.
- **Survey Response**
  - id, surveyId, userId, answers[], participationDate.
- **Employee**
  - id, companyId[], name, email, role(Cargo), sector, permission.

### Exceções tratadas:

- **AuthenticationException** → Login inválido.
- **NotFoundException** → Usuário ou pesquisa não encontrados.
- **Validation Exception** → Dados inválidos no request.

5. Diagrama de Arquitetura do Back-end



5.1. Estrutura em Camadas

Camada	Componentes Chave	Responsabilidade
Apresentação	Contróllers (AuthController, SurveyController, etc.) e DTOs	Interface com o funcionário (HTTP/JSON). Recebe DTOs e retorna DTOs, tratando as exceções de forma amigável (GlobalExceptionHandler).
Lógica de Negócio	Services (UserService, SupportService, etc.)	Aplica as regras de negócio complexas, validações e orquestração de dados.
Infraestrutura /Persistência	Repositories (UserRepository, SupportRepository)	Abstração do acesso aos dados. Interage com o MongoDB via Spring Data.
Segurança (Transversal)	Configs (SecurityConfig), Filters (JwtAuthenticationFilter), Services (JwtService)	Gerência autenticação, autorização, criptografia de senha e CORS.

6. Estratégia de Autenticação e Controle de Acesso

6.1. A segurança é implementada pelo Spring Security e JWT, seguindo um fluxo stateless.

Aspecto	Implementação	Artefatos e Código
---------	---------------	--------------------

Mecanismo Central	JSON Web Tokens (JWT)	JwtService (Geração e Validação), JwtAuthenticationFilter (Filtro).
Criptografia de Senha	BCrypt	BCryptPasswordEncoder (Bean em SecurityConfig). Usado em UserService e AuthController.
Política de Sessão	Stateless	sessionCreationPolicy (SessionCreationPolicy.STATELESS) em SecurityConfig.
Fluxo de Autenticação	O AuthController.login usa o AuthenticationManager para validar a senha. O JwtService gera o token, incluindo a Claim extra name do funcionário.	
Controle de Acesso	Autorização Baseada em Roles	Anotações @PreAuthorize("hasRole('ADMIN')") ou hasAnyRole('EMPLOYEE').
Roles Definidas	ADMIN e EMPLOYEE	Enum Permission. O User mapeia o Enum para GrantedAuthority (ex: ROLE_ADMIN).

## 6.2. Estratégia de Autenticação e Controle de Acesso

1. Usuário envia credenciais para `/auth/login`.
2. Sistema autentica com `AuthenticationManager`.
3. Gera JWT com claims (usuário, role, nome).
4. Token é enviado no header `Authorization: Bearer <token>`.
5. Spring Security intercepta chamadas → valida token → injeta usuário autenticado no contexto.
6. Controllers verificam roles via `@PreAuthorize`.

## 7. Modelo de Dados NoSQL Utilizado (MongoDB)

O MongoDB é o banco de dados principal, com coleções representando as entidades de domínio, identificadas pela anotação @Document.

Coleção (Entities)	Propósito	Chaves/Campos Relevantes
tb_employee	Cadastro e permissionamento para registro de pesquisa	id, name, email, password, role, permission, sector
gs_tb_surveys	Cadastro de tipo de pesquisa	id, companyId, title, description, questions[ text, type, options[ ] ], active
gs_tb_survey_response	Armazenar as respostas enviadas pelos funcionários	id, surveyId, answers[ questionText, response ], participationDate
gs_tb_participations	Contabilizar a participação e o engajamento.	id, employeeId, surveyId, participationDate,
gs_tb_daily_moods	Armazenar o sentimento diário	id, employeeId, companyId, emoji, feeling
gs_tb_companies	Registro geral da empresa	id, name, cnpj, phone, email, status

## 8. Especificações dos Endpoints (Rotas da API REST)

As especificações são baseadas no contrato da API documentado pelo Swagger, organizado por Tags de Acesso.

Administração			
PUT	/supports/{id}	Atualiza um ponto de apoio existente	🔒
DELETE	/supports/{id}	Deleta um ponto de apoio	🔒
GET	/employees/{id}	Busca funcionário por ID	🔒
PUT	/employees/{id}	Atualiza dados de um funcionário	🔒
DELETE	/employees/{id}	Remove um funcionário	🔒
POST	/surveys	Cria uma nova pesquisa	🔒
POST	/surveys/{id}/activate	Ativa uma pesquisa já criada	🔒
GET	/supports	Lista todos os pontos de apoio	🔒
POST	/supports	Cria um novo ponto de apoio	🔒
GET	/employees	Lista todos os funcionários	🔒
POST	/employees	Cria um novo funcionário	🔒
GET	/surveys/{id}	Busca uma pesquisa pelo ID	🔒
GET	/surveys/{companyId}	Lista todas as pesquisas de uma empresa	🔒
GET	/reports	Resumo semanal de bem-estar	🔒
GET	/reports/pdf	Exportar relatório semanal em PDF	🔒
GET	/employees/{email}	Busca funcionário por e-mail	🔒
Funcionários			
POST	/mood/daily/recommendations	Registra humor diário e retorna recomendações de filmes	🔒
POST	/employees/responses/daily	Enviar respostas diárias (anônimas)	🔒
GET	/surveys/daily	Pesquisa diária para o colaborador	🔒
GET	/supports/support-list	Lista todos os pontos de apoio	🔒
Autenticação			
POST	/auth/reset-password	Redefine a senha.	🔒
POST	/auth/register/admin	Registra um novo administrador	🔒
Login			
POST	/auth/login	Login do usuário	🔒



### 8.1. Tag: Autenticação (Login)

As rotas de Autenticação são públicas, permitindo o acesso sem token.

Rota	Método	Descrição
/auth/login	POST	Login do usuário
/auth/register/admin	POST	Registra um novo administrador
/auth/reset-password	POST	Redefine a senha

### 8.2. Tag: Administração

As rotas nesta seção são destinadas ao Painel de Administração e, em sua maioria, requerem a permissão ADMIN.

Rota	Método	Descrição
/reports/pdf	GET	Exportar relatório semanal em PDF
/reports	GET	Resumo semanal de bem-estar
/supports	GET	Lista todos os pontos de apoio.
/supports	POST	Cria um novo ponto de apoio.
/supports/{id}	PUT	Atualiza um ponto de apoio existente.
/supports/{id}	DELETE	Remove um ponto de apoio.
/surveys	POST	Cria uma nova pesquisa
/surveys/{id}	GET	Busca uma pesquisa pelo ID
/surveys/{id}/activate	POST	Ativa uma pesquisa já criada
/surveys/{companyID}	GET	Lista todas as pesquisas de uma empresa
/employees	GET	Lista todos os funcionários.
/employees	POST	Cria um novo funcionário.
/employees/{id}	PUT	Atualiza dados de um funcionário.
/employees/{id}	DELETE	Remove um funcionário
/employees/{id}	GET	Busca Funcionário por ID
/employees/{email}	GET	Busca funcionário por e-mail.

### 8.3. Tag: Funcionários

As rotas nesta seção são destinadas ao uso pelo Aplicativo Mobile (Funcionários) e requerem a permissão EMPLOYEE.

Rota	Método	Descrição
/employees/responses/daily	POST	Envia a resposta diária de uma pesquisa.
/mood/daily/recommendations	POST	Registra humor diário e retorna recomendações de filmes
/supports/support-list	GET	Lista todos os pontos de apoio
/surveys/daily	GET	Pesquisa diária para o colaborador