

# Documento de Requerimientos - Sistema de Alerta y Visualización de Sismos

## 1. Introducción

Este documento describe los requerimientos para un sistema web de autenticación y gestión de usuarios desarrollado con Spring Boot, que proporciona funcionalidades de registro, inicio de sesión y administración de usuarios.

## 2. Objetivos Principales

- Implementar un sistema seguro de autenticación y autorización
- Permitir el registro de nuevos usuarios
- Gestionar diferentes roles de usuario
- Proporcionar funcionalidades de administración de sistema
- Proteger los recursos y endpoints según los roles de usuario

## 3. Funcionalidades del Sistema

### 3.1 Registro de Usuarios

- Los usuarios pueden registrarse proporcionando:
  - Nombre de usuario único
  - Correo electrónico válido
  - Contraseña (con confirmación)
- Validación de contraseñas (coincidir, longitud mínima)
- Asignación automática del rol "USER" al registrarse
- Encriptación de contraseñas antes de almacenarlas

### 3.2 Inicio de Sesión

- Autenticación mediante nombre de usuario y contraseña
- Manejo de credenciales incorrectas
- Redireccionamiento basado en roles:
  - Usuarios con rol USER acceden a páginas de usuario
  - Usuarios con rol ADMIN acceden a páginas de administración
- Control de sesiones

### 3.3 Gestión de Perfiles

- Usuarios pueden ver y actualizar:

- Nombre de usuario
  - Correo electrónico
- Visualización de rol actual
- No se permite cambiar contraseña desde el perfil

### **3.4 Administración de Usuarios (Solo ADMIN)**

- Listar todos los usuarios del sistema
- Editar información de usuarios
- Cambiar roles de usuarios (USER/ADMIN)
- Eliminar usuarios

## **4. Reglas y Restricciones de Roles**

### **4.1 Rol USER**

- Acceso a:
  - Página de inicio
  - Perfil de usuario
  - Cerrar sesión
- No puede acceder a funciones administrativas

### **4.2 Rol ADMIN**

- Acceso a todas las funcionalidades de USER
- Acceso adicional a:
  - Gestión de usuarios
  - Ver lista completa de usuarios
  - Editar y eliminar usuarios
  - Cambiar roles de usuarios

## **5. Seguridad**

- Protección contra ataques CSRF
- Encriptación de contraseñas con BCrypt
- Restricción de acceso a endpoints basada en roles
- Manejo de sesiones seguro
- Protección contra inyección de SQL
- Validación de entradas de usuario

## **6. Restricciones Técnicas**

- Desarrollado con Spring Boot
- Autenticación mediante Spring Security
- Persistencia de datos con JPA/Hibernate

- Base de datos MySQL
- Frontend con Thymeleaf y Bootstrap

## **7. Casos de Uso Principales**

1. Registro de nuevo usuario
2. Inicio de sesión
3. Actualización de perfil
4. Administración de usuarios
5. Cierre de sesión