POLÍTICA DE SEGURIDAD DE LA APLICACIÓN

1. Introducción

Sistema de autenticación y autorización utilizando **Spring Security**, se controla el acceso a los recursos, cómo se gestionan los usuarios y qué permisos tiene cada rol dentro del sistema.

La aplicación utiliza una base de datos para almacenar los usuarios, roles y credenciales, el mecanismo de cifrado de contraseñas es **BCrypt**.

2. Autenticación

La autenticación se realiza mediante un **formulario de login personalizado** accesible desde la ruta **"/login"**.

Servicio personalizado de tipo **UserDetailsService** para cargar los usuarios desde la base de datos. En caso de que el usuario no exista, el sistema deniega automáticamente el acceso.

3. Gestión de Roles

En el sistema se definen los siguientes roles:
– ROLE_ADMIN
– ROLE_USER
– ROLE_MODERATOR
NOTA: Cada usuario puede tener uno o varios roles asignados.

4. Autorización

Acceso público (sin autenticación):
- / (página principal)
- /usuarios/registro (registro de nuevos usuarios)
- /css/ y /style.css** (recursos estáticos de la aplicación)

Acceso exclusivo para ROLE_ADMIN:
El rol ROLE_ADMIN dispone de permisos completos de gestión sobre las entidades del sistema. En concreto, puede:

5. Gestión de Sesión y Logout

La aplicación permite el cierre de sesión mediante un botón arriba en las plantillas.
El proceso de logout invalida la sesión activa y redirige al usuario al login.

6. Conclusión

La política de seguridad implementada garantiza que únicamente los usuarios autenticados y autorizados puedan acceder a los recursos protegidos de la aplicación, asegurando así la integridad y confidencialidad del sistema.