**control de acceso por url**

En la aplicación utilizada en el curso, no tendremos diferentes perfiles de acceso para los usuarios. Sin embargo, esta característica se usa en algunas aplicaciones y podemos indicarle a Spring Security que solo los usuarios que tienen un perfil específico pueden acceder a ciertas URL.

Por ejemplo, supongamos que en nuestra aplicación tenemos un perfil de acceso llamado ADMIN, y solo los usuarios con ese perfil pueden eliminar médicos y pacientes. Podemos indicar dicha configuración a Spring Security cambiando el método securityFilterChain, en la clase SecurityConfigurations, de la siguiente manera:

@Bean

public SecurityFilterChain securityFilterChain(HttpSecurity http) throws Exception {

return http.csrf().disable()

.sessionManagement().sessionCreationPolicy(SessionCreationPolicy.STATELESS)

.and().authorizeRequests()

.antMatchers(HttpMethod.POST, "/login").permitAll()

.antMatchers(HttpMethod.DELETE, "/medicos").hasRole("ADMIN")

.antMatchers(HttpMethod.DELETE, "/pacientes").hasRole("ADMIN")

.anyRequest().authenticated()

.and().addFilterBefore(securityFilter, UsernamePasswordAuthenticationFilter.class)

.build();

}

Tenga en cuenta que se agregaron dos líneas al código anterior, indicando a Spring Security que las solicitudes de tipo DELETE de las URL /médicos y /pacientes solo pueden ser ejecutadas por usuarios autenticados y cuyo perfil de acceso es ADMIN.