# Especificaciones de Seguridad

1. Las contraseñas deben ser de 8 caracteres incluyendo una mayúscula , una minúscula y un numero
2. Las contraseñas se almacenan en base de datos de forma encriptada usando la función de hashing **BCRYPT** provista por Spring Security
3. Los accesos a la aplicación son a través de roles ADMIN y USER
4. El usuario de bbdd tiene solo los permisos necesarios para poder operar la aplicación
5. Se Injecta la URL de conexión de la base de datos mediante una variable de entorno , de esta manera evitamos guardar esa información dentro del código fuente y queda configurada en el servidor
6. Las querys son manejadas con JPA ,no usando queries nativas para evitar SQL Injection
7. No se muestran errores técnicos al usuario para evitar revelar información de la aplicación.
8. Se utiliza mecanismo de oauth para loguearse con Facebook a la aplicación mobile, esto es manejado automáticamente por la dependencia de Facebook
9. Se utiliza una APIKEY provista por google para utilizar las apis de google maps, esta api vincula identifica nuestra aplicación ante google