Desarrollo técnico Noris.

Introducción.

El siguiente documento contempla el desarrollo de un API/REST para el manejo de usuarios. Se pensó en una autenticación mediante la implementación de Jason Web Token (jwt), donde los usuarios con rol ADMIN están autorizados para tareas como:

* Crear usuarios.
* Hacer login.
* Listar los usuarios existentes.
* Eliminar usuarios existentes.

También se implementó la documentación de la api mediante Swagger utilizando el estandar de OpenApi, donde se habilitaron procedimientos de autenticación para poder habilitar las funcionalidades que requieran permisos (jwt).

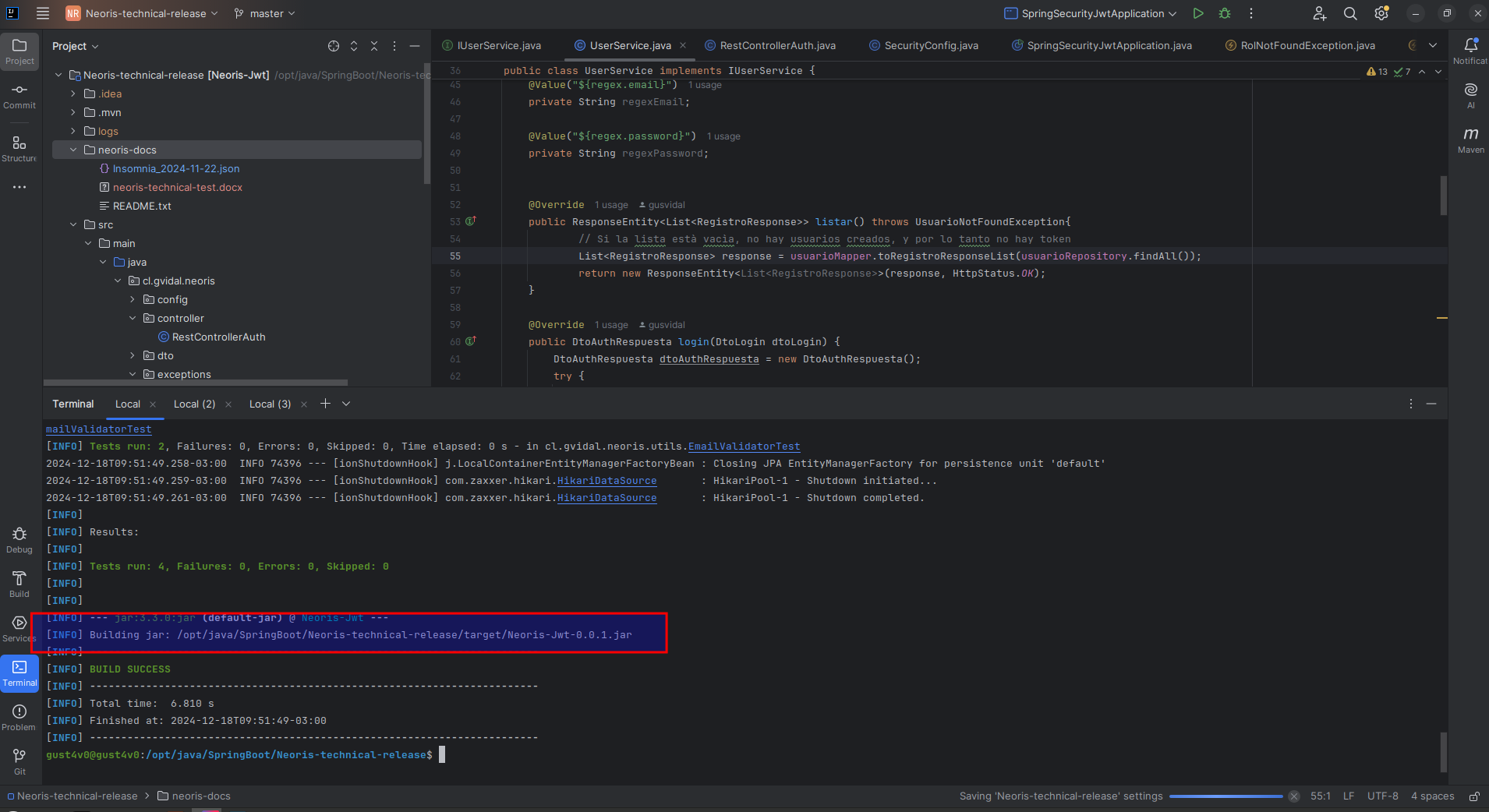
Se utilizó una base de datos en memoria (H2) para facilitar las pruebas.

Se proporciona una collection en formato json para pruebas, esta collection es posible importarla con aplicaciones como insomnia o postman, a fin de facilitar las pruebas funcionales.

Detalles del proyecto.

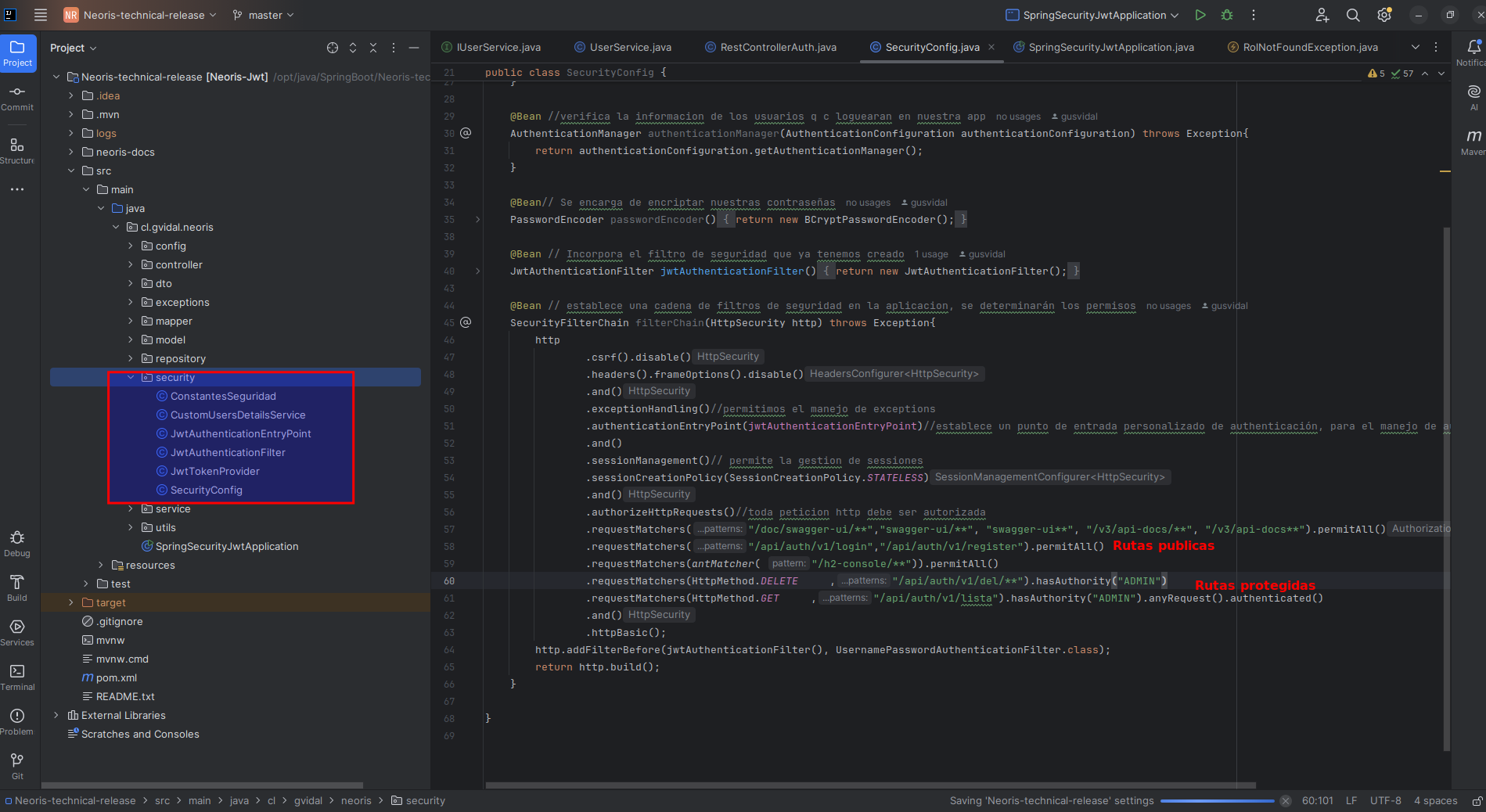
Compilación del proyecto

Al desarrollarse con maven, para compilar el proyecto utilizamos el comando “mvn clean package”, adjunto imagen del archivo jar generado.

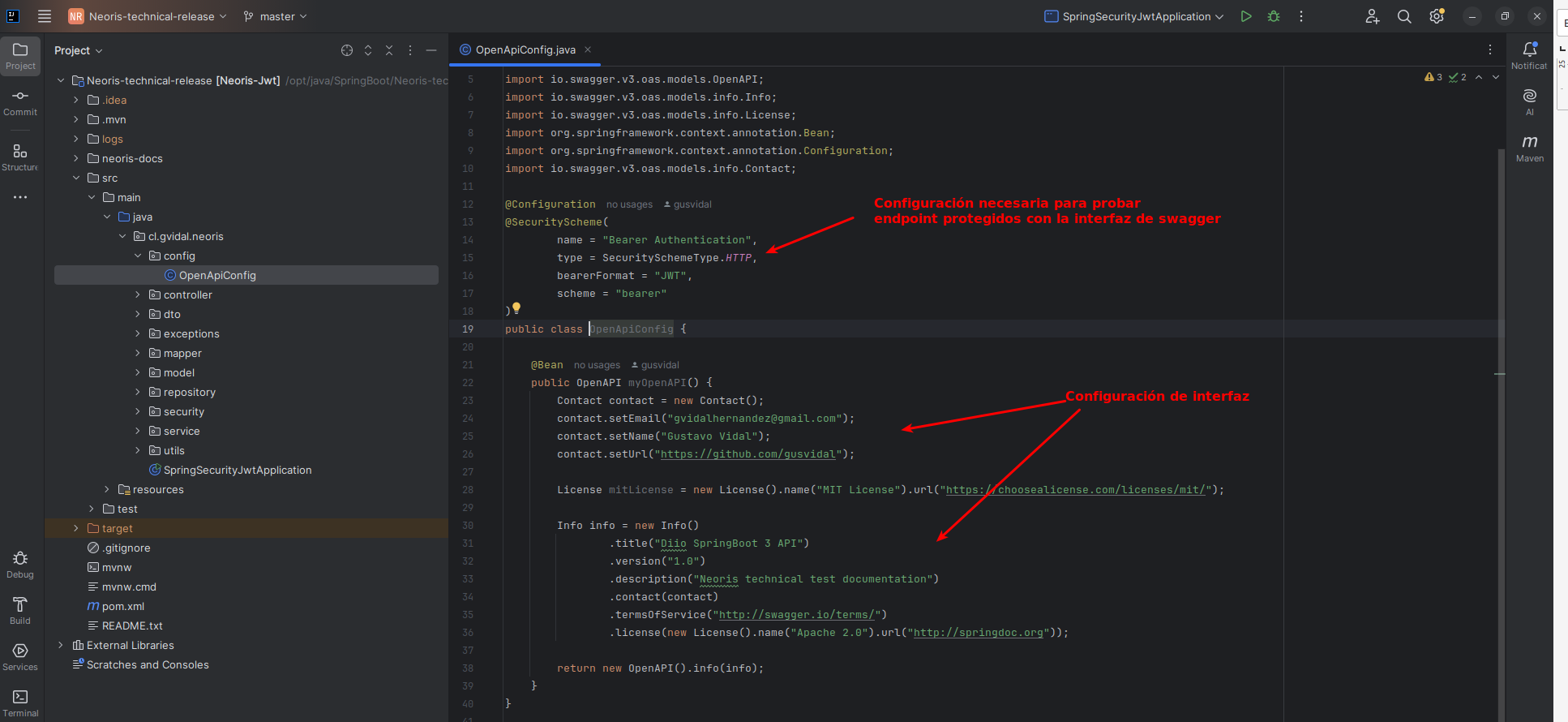


En las siguientes imágenes, se hace mención a las rutas relevantes del proyecto.

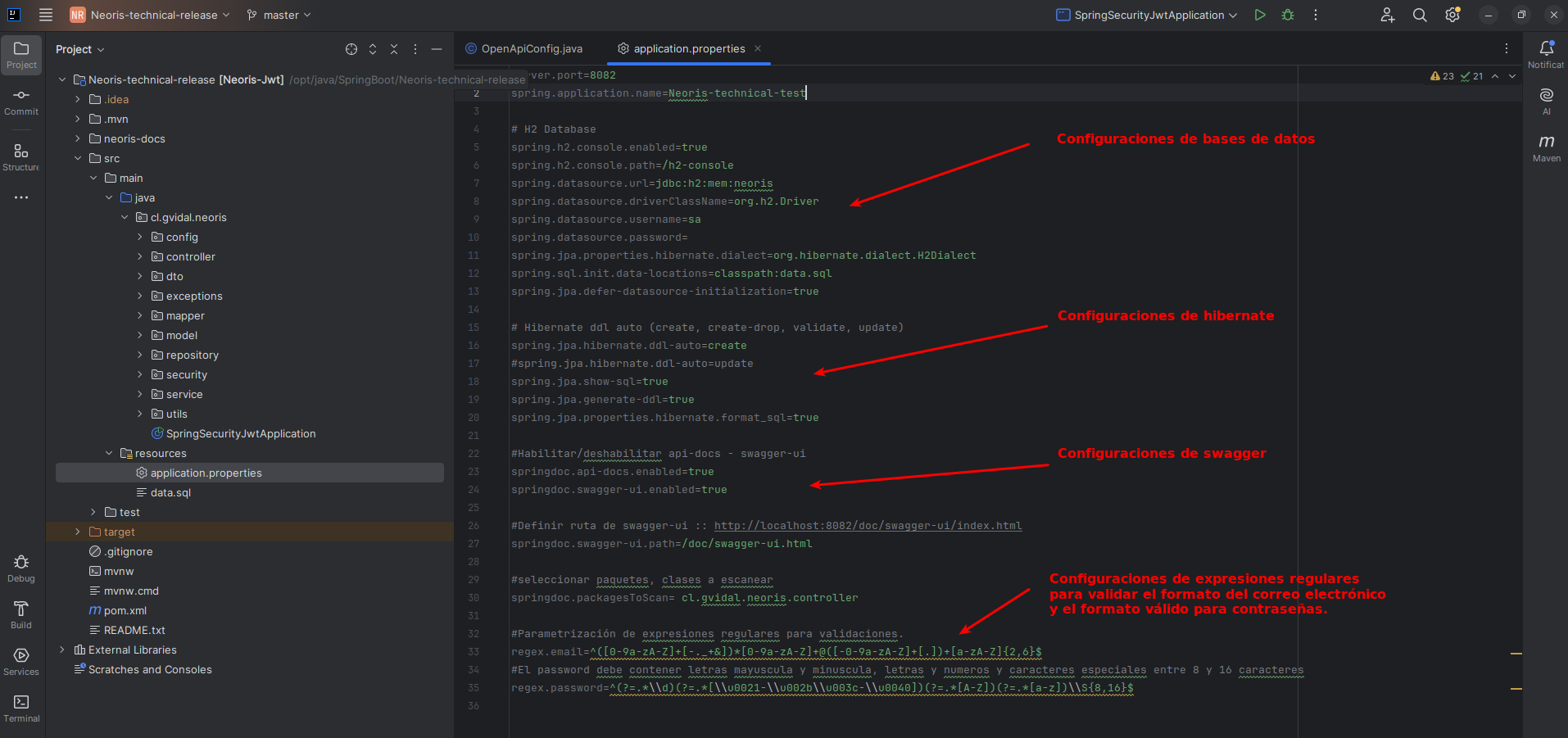
Sección de autenticación y autorización mediante jason web token, en la sección de la izquierda se muestra el directorio con la configuración de seguridad, en tanto, a la derecha se encuentran definidos los matchers necesarios para dar permisos sobre los endpoint del servicio.



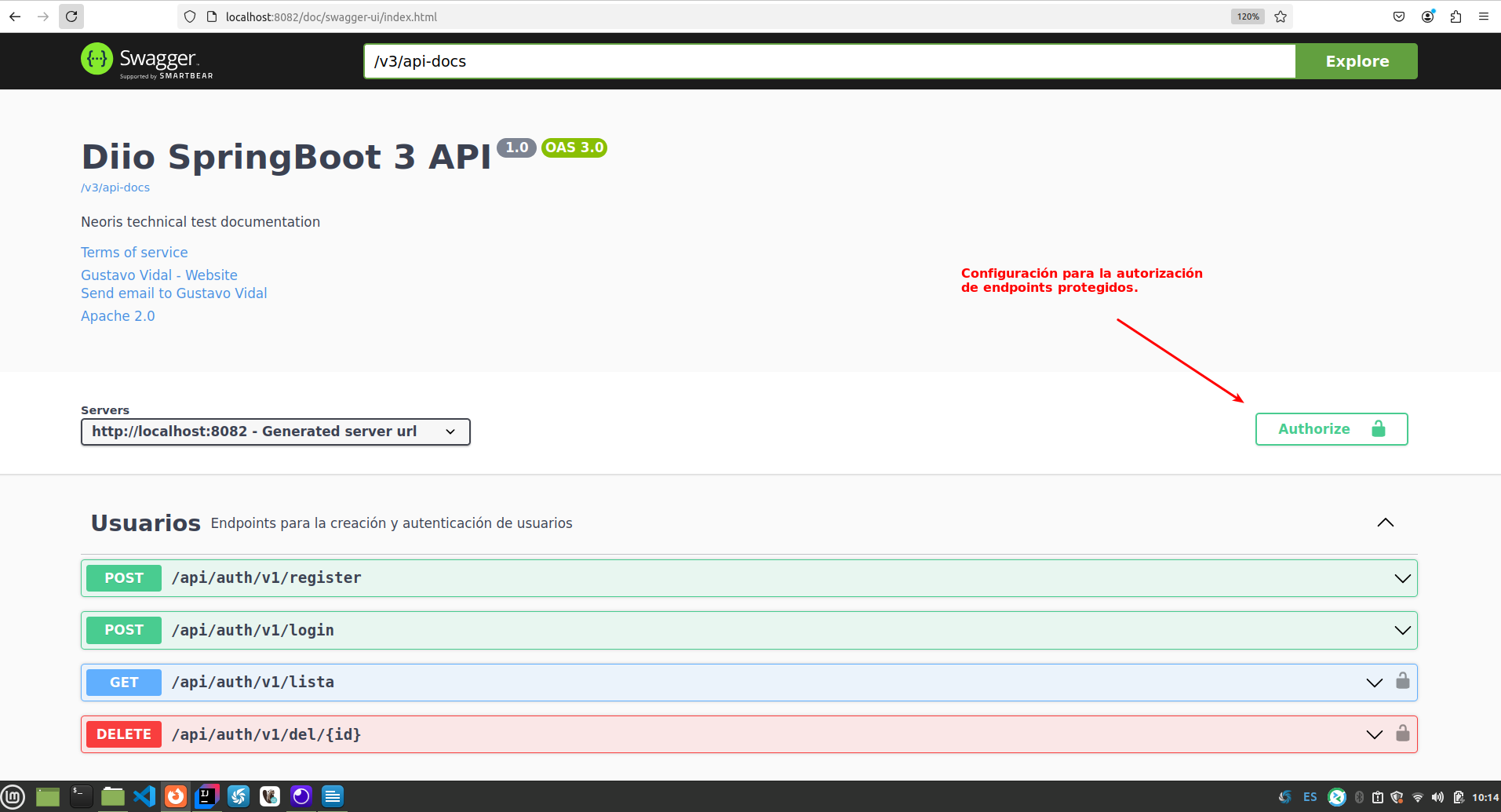
A continuación se muestra la configuración de OpenApi



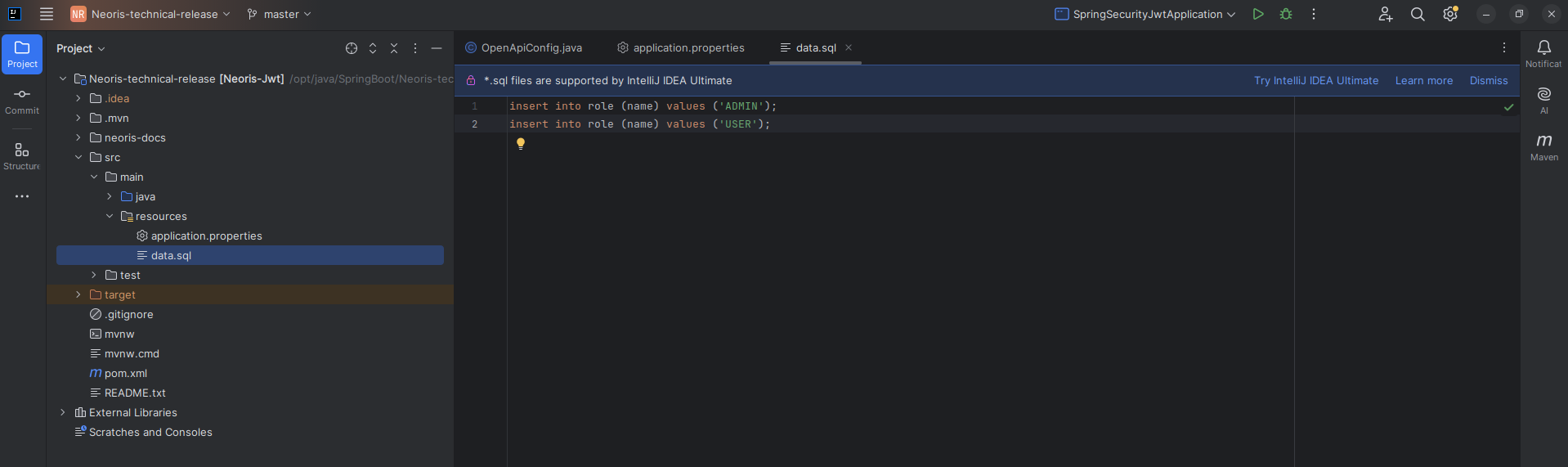
A continuación se ilustran las configuraciones realizadas para la ejecución del proyecto.

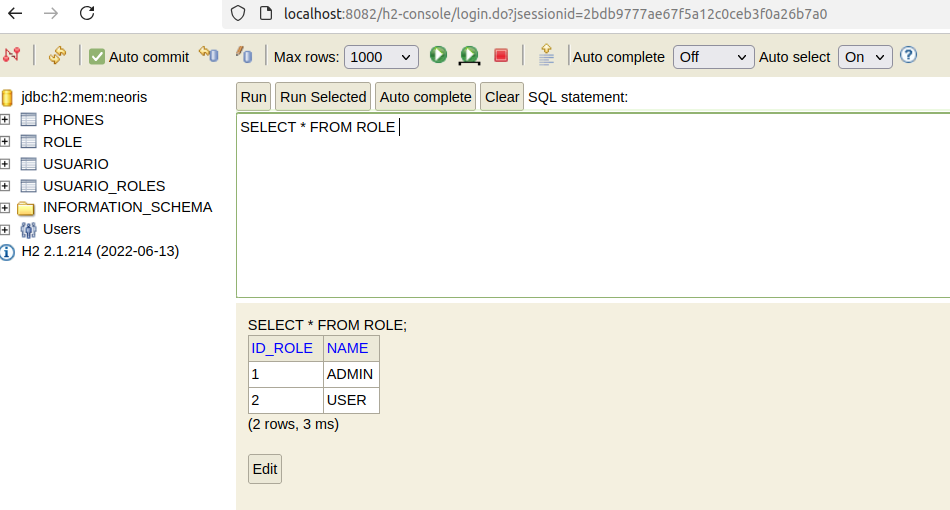


En la siguiente imagen, se puede apreciar Swagger en ejecución.



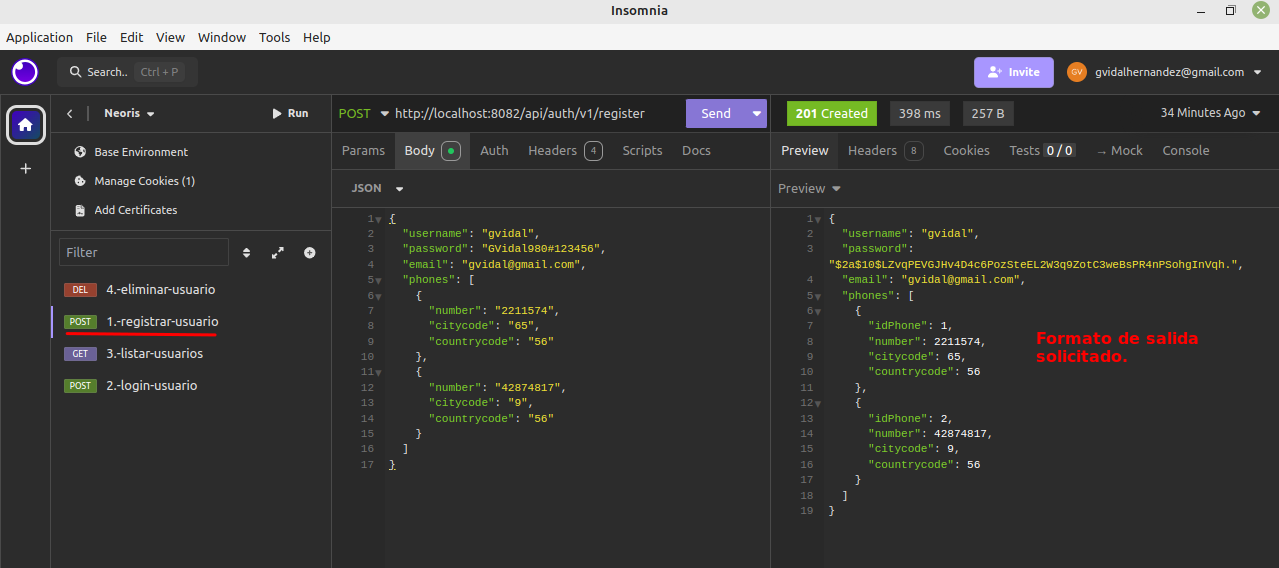
Para facilitar las pruebas, se crean objetos de datos de bases de datos, y se poblan las tablas con datos mínimos para la correcta ejecución de la API al momento de iniciar la aplicación.



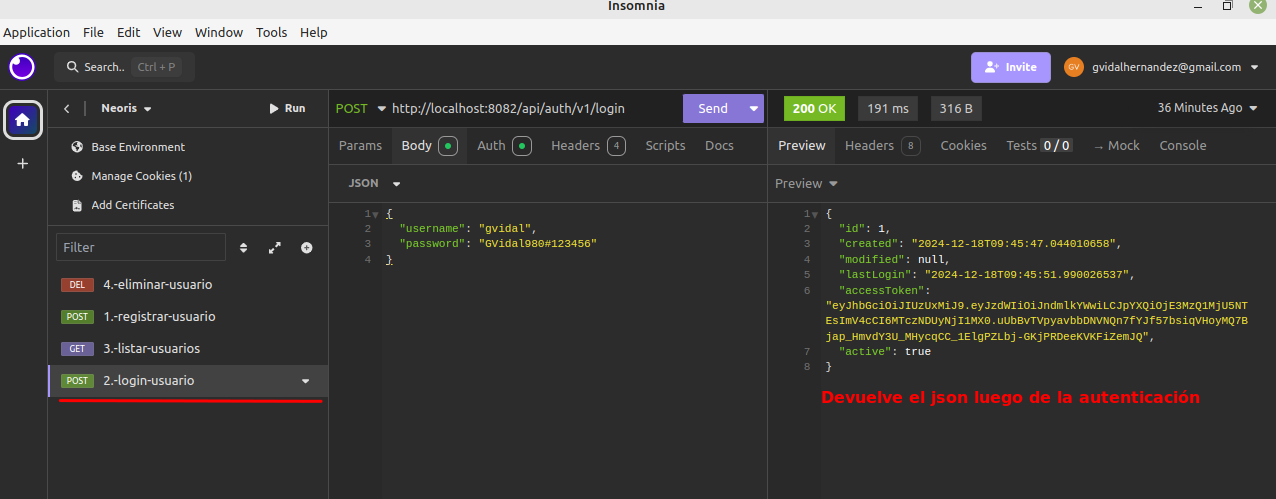


En cuanto a las pruebas funcionales, se adjunta un archivo readme.txt donde se disponen los endpoint y los json de entrada para poder realizar las pruebas funcionales del proyecto.

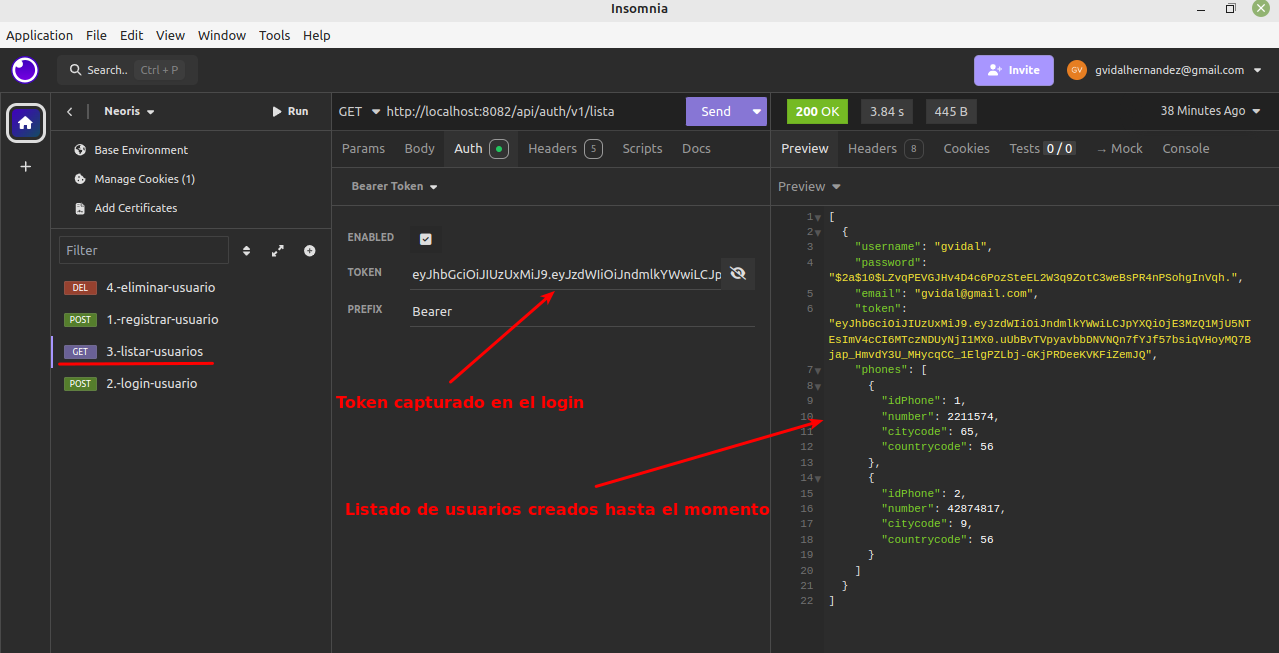
1.- Crear usuario, esto creará un usuario en la base de datos



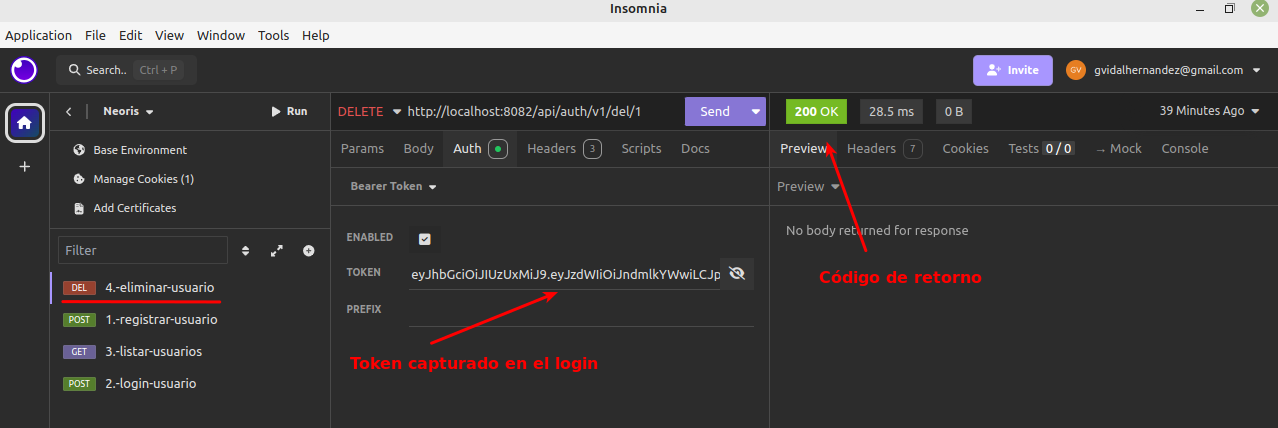
2.- Login de usuario, esto realizará el proceso de login, creando el token.



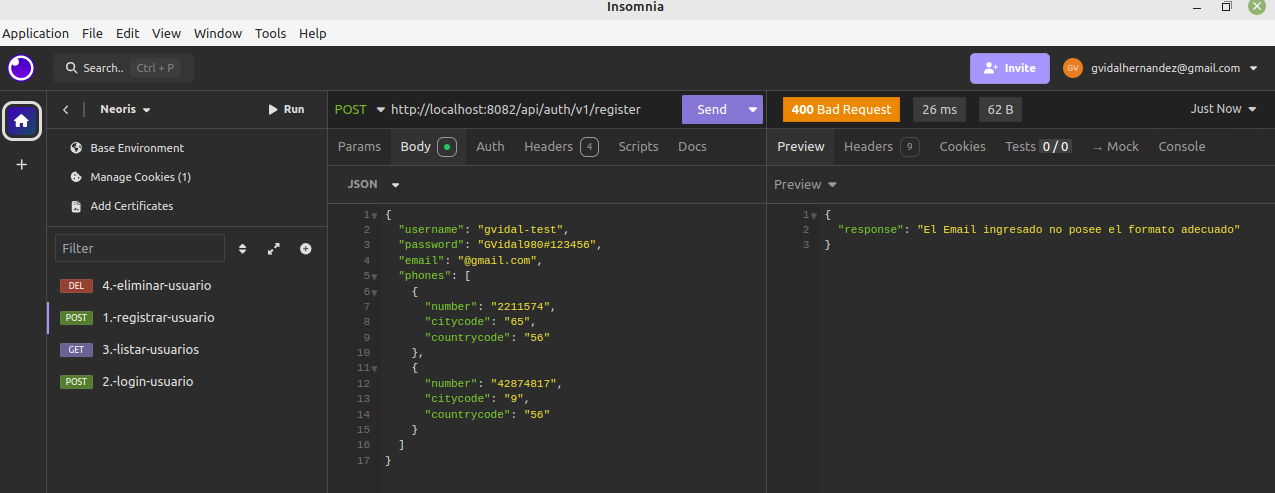
3.- Listar usuarios, este endpoint devuelve una lista de los usuarios presentes en la base de datos.

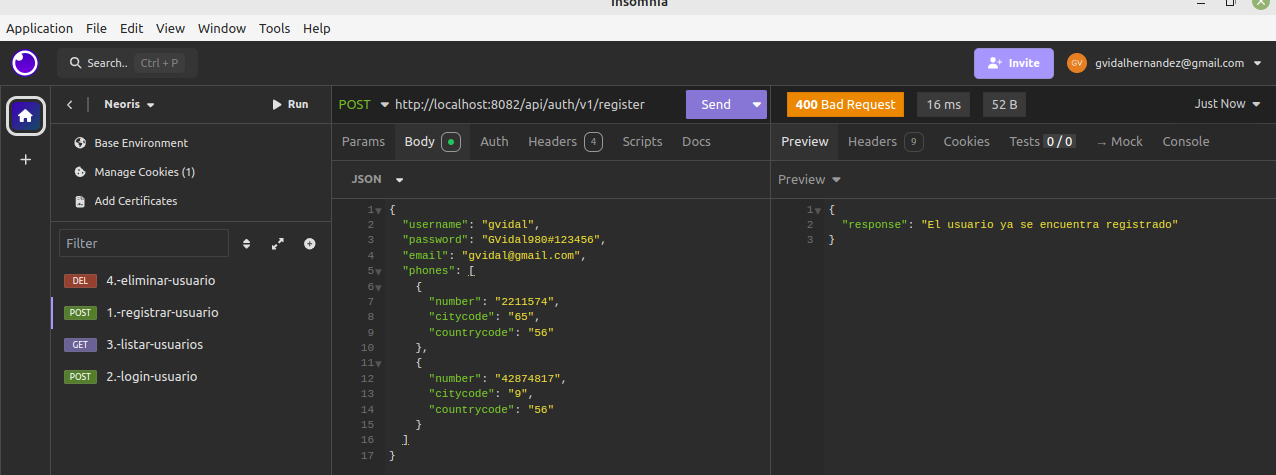


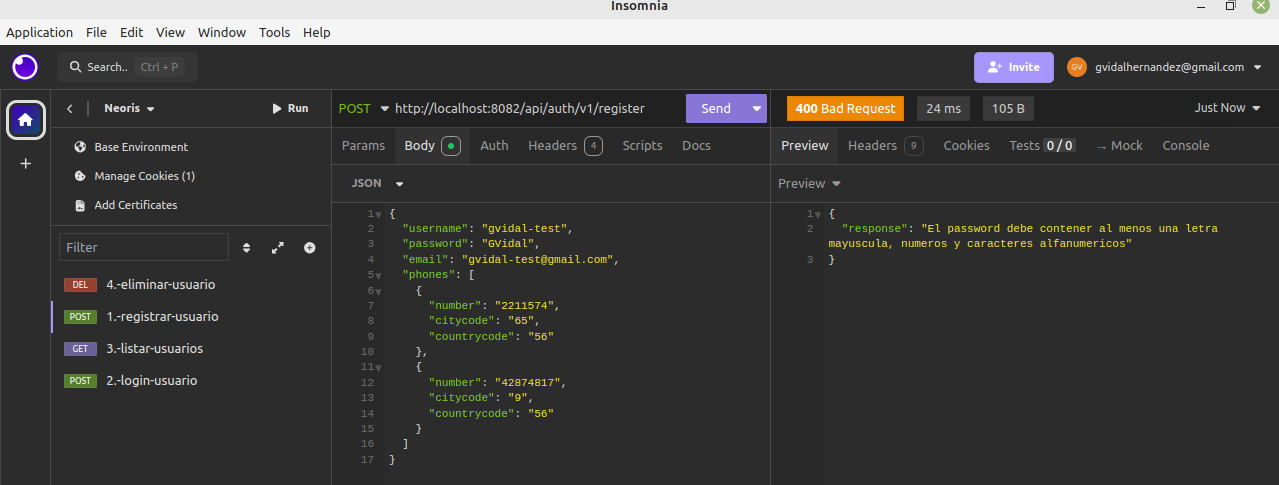
4.- Eliminar usuario, esto elimina un usuario específico, el cual debe ser individualizado mediante el id en el endpoint.



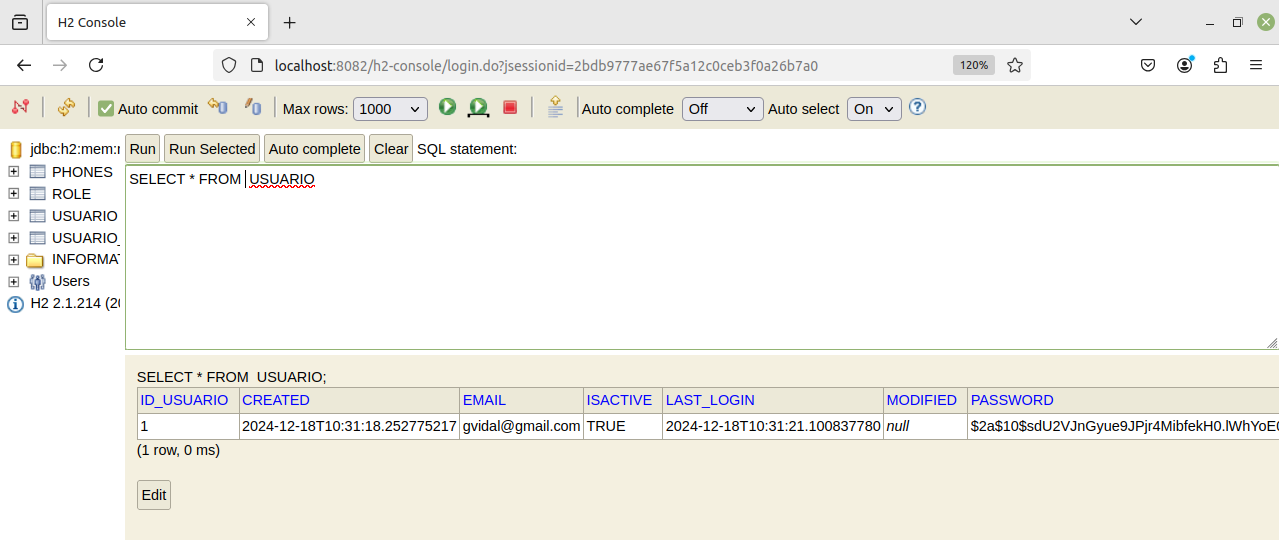
A continuación, se ilustran las validaciones de formato de correo y password.

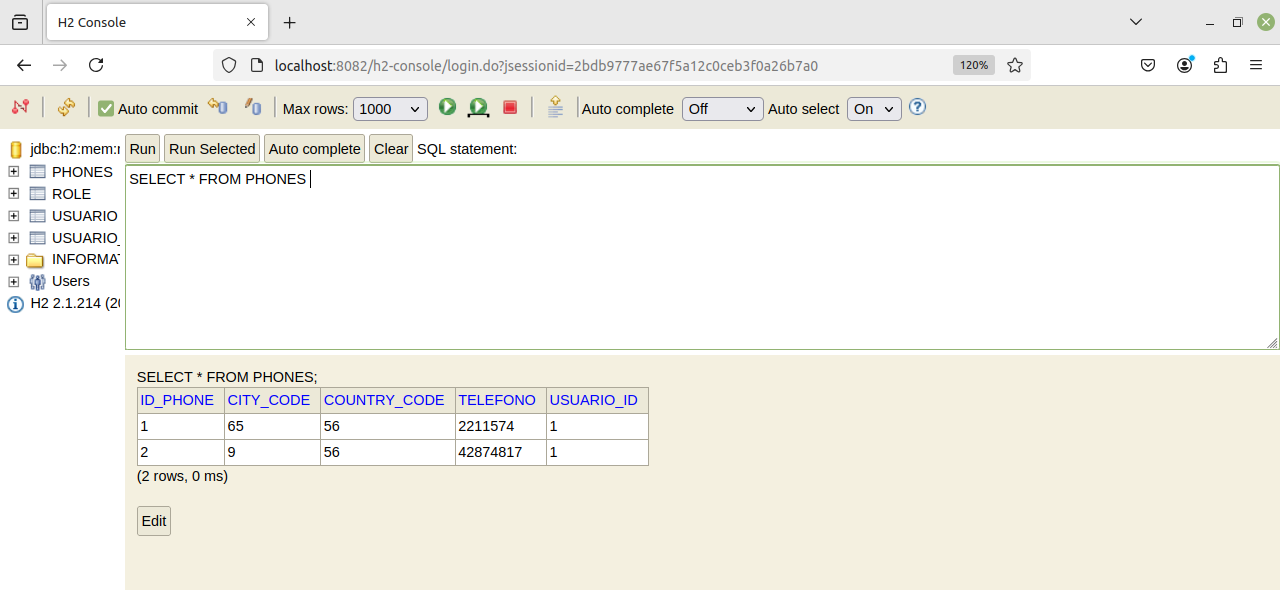






A continuación se muestran los datos persistidos en H2





Por último, adjunto un diagrama de secuencia de la solución.

