CUE: SECURIZACIÓN MEDIANTE JWT IMPLEMENTACIÓN EN EXPRESS

DRILLING: CONSTRUCCIÓN DE UNA API RESTFUL CON JWT PARTE II

Para resolver este ejercicio, anteriormente debe haber revisado la lectura y los videos del CUE: Securización Mediante Jwt Implementación en Express.

EJERCICIO:

Partiendo del REBOUND EXERCISE del CUE, que fue adecuado para el modelo de usuarios y libros, ahora adecúelo con la finalidad de que permita la autenticación con JWT:

- Cree un middleware para la autenticación con JWT.
- Adecue las siguientes rutas que sean validadas por medio del token generado para los usuarios registrados, y que una vez iniciada la sesión, se genera un token con duración de 30 minutos, donde pueden manipular la gestión de libros respectivamente.
- Verifique con Postman cada una de las rutas con el token de usuario respectivo en las protegidas.
- Finalmente, verifique el token generado en el login con un tiempo de expiración de 120 segundos, y que al transcurrir los 120 segundos, efectivamente emite un error avisando que el token expiró y ya no es válido.
- Los endpoint tienen la siguiente estructura:

Ruta	Verbo HTTP	Descripción	Token JWT
/api/registro	POST	Registro de usuarios.	
/api/login	POST	Inicio de sesión (email y contraseña).	Genera Token
/api/libros	GET	Listado de todos los libros.	Autorizado Token
/api/libros/:isbn	GET	Datos del libro según isbn.	Autorizado Token
/api/libros	POST	Ingreso de un libro.	Autorizado Token
/api/libros/:isbn	PUT	Actualización del libro según isbn.	Autorizado Token
/api/libros/:isbn	DELETE	Eliminación del libro según isbn.	Autorizado Token