Rúbrica de Evaluación: Seguridad en la Web del Hospital

Criterio de Evaluación	TL (1.5)	L (1)	ML (0.5)	NL (0)	Puntaje Máximo
Protección de Rutas con React Router DOM	Las rutas protegidas están correctamente implementadas. Solo los usuarios autenticados pueden acceder a las secciones protegidas y las rutas públicas son accesibles sin autenticación.	Las rutas están implementadas, pero algunas fallan en la protección o accesibilidad de las secciones.	Las rutas están parcialmente protegidas o presentan errores significativos en la autenticación.	No se implementa correctamente la protección de rutas con React Router DOM.	1.5
Implementación de Autenticación de Usuarios y Roles	El sistema de autenticación funciona correctamente, permitiendo el acceso basado en roles. Los roles de usuario (como doctor o	El sistema de autenticación y roles funciona, pero con errores menores en la implementación de los roles o en la asignación de accesos.	La autenticación está implementada de manera incompleta o presenta errores graves en la gestión de roles.	No se implementa un sistema de autenticación funcional ni de roles.	1.5

Criterio de Evaluación	TL (1.5)	L (1)	ML (0.5)	NL (0)	Puntaje Máximo
	administrador) restringen el acceso a las áreas correspondientes.				
Consumo de APIs Protegido con API Key y JWT	Las peticiones a la API están protegidas con **JWT**. Los datos sensibles solo se obtienen con un token válido, y se muestra un mensaje de error si el token no es válido o ha expirado.	Se utiliza JWT, pero con pequeños errores en la verificación del token o en el manejo de las solicitudes.	La protección con JWT está mal implementada o no se verifica correctamente el token en las peticiones.	No se implementa la protección de las peticiones a la API con JWT o API Key.	1.5
Prevención de Vulnerabilidades Comunes	Se implementan medidas efectivas para prevenir ataques como **Clickjacking**, **XSS**, **SQL Injection** y **DoS**, protegiendo la aplicación	Las medidas de prevención están implementadas, pero con fallos menores en alguna de las vulnerabilidades.	La prevención de vulnerabilidades es parcial o presenta errores importantes, dejando la aplicación expuesta a ataques.	No se implementan medidas de seguridad efectivas contra vulnerabilidades comunes.	1.5

Criterio de Evaluación	TL (1.5)	L (1)	ML (0.5)	NL (0)	Puntaje Máximo
	de manera adecuada.				
Encriptación de Datos en el Front-End	Los datos sensibles se encriptan correctamente antes de ser enviados a la API, protegiendo la información confidencial de los usuarios y pacientes.	Se implementa encriptación, pero con errores menores que pueden comprometer la seguridad de los datos.	La encriptación está mal implementada o solo se aplica de manera parcial a los datos sensibles.	No se implementa ninguna técnica de encriptación en los datos sensibles.	1

Interpretación de los Resultados

- **Totalmente logrado (TL)**: Los estudiantes han implementado correctamente todas las medidas de seguridad en el sistema del hospital, asegurando la protección de rutas, autenticación, consumo de APIs y previniendo vulnerabilidades.
- **Logrado (L)**: La mayoría de las medidas de seguridad están implementadas, con pequeños errores que no afectan gravemente la funcionalidad o seguridad de la aplicación.
- **Medianamente logrado (ML)**: Varias áreas de seguridad están mal implementadas o incompletas, lo que afecta la protección general de la aplicación.
- **No logrado (NL)**: No se implementan correctamente las medidas de seguridad solicitadas, dejando la aplicación vulnerable a ataques.

Puntaje total: 7 puntos.