3. Explica cómo garantizarías la seguridad en una aplicación backend. Incluye consideraciones sobre autenticación y autorización, así como cualquier otra medida de seguridad que consideres relevante.

Soy consciente de la alta seguridad que debe haber en una aplicación, sobre todo en la parte backend, donde se llevan a cabo todas aquellas operaciones lógicas que dan o devuelven respuestas a las peticiones de usuarios o clientes.

Para garantizar la seguridad brindaría ciertas medidas que considero importantes, hablando sobre autenticación: implementaría métodos que verificarán la identidad de un usuario, dichos métodos podrían ser: política de contraseñas fuertes y seguras, posteriormente almacenar las contraseñas de forma segura utilizando algoritmos de hash seguros, tokens de autenticación que permitan mantener la sesión de un usuario activa, autenticación de dos factores y la implementación de un mecanismo seguro al momento de realizar un cierre de sesión.

En términos de autorización implementaría roles y permisos, por ejemplo, un usuario con el rol de 'administrador' tiene permisos para acceder a todas las zonas de la aplicación, y otro con el rol de ‘usuario’ tiene acceso limitado, únicamente a áreas específicas. En pocas palabras, implementaría un sistema de RBAC para asignar roles y permisos específicos a los usuarios.

Otras medidas que considero relevante es el cifrado de datos sensibles, ya sean aquellos datos que se encuentran almacenados en bases de datos; o los que están en tránsito. Así como también realizar una configuración satisfactoria de firewalls para filtrar el tráfico no autorizado y proteger la aplicación de amenazas externas.

Algo que también considero esencial es la protección contra ciberataques de inyecciones SQL, dado que existen personas (hackers) que se dedican a explotar vulnerabilidades por medio de sentencias SQL, ante esta situación utilizaría consultas parametrizadas o el uso ORM para prevenir tales ataques, no obstante, también prevenir otro tipo de ataques (como Cross-Site Scripting, Phishing) e incluso no permitir muchos intentos de inicio de sesión.

Implementar parches de seguridad, realizar pruebas de seguridad, garantizar la confidencialidad de los datos durante la transferencia implementando el protocolo SSL/TLS.

Y obviamente no me olvido de las validaciones en cada entrada de datos (principalmente en los formularios), uso de expresiones regulares, validar tipo de datos correspondientes a cada input, proporcionar buen feedback al usuario por medio de mensajes emergentes, y realizar validaciones en ambas partes del sistema Frontend y Backend; para que la data llegue 100% correcta a la Base de Datos que alojará la información de usuarios.