Requerimientos funcionales

Autenticación y Autorización

1. Registro de Usuarios : La aplicación debe permitir a los usuarios registrarse proporcionando un nombre de usuario, contraseña y correo electrónico.

2. Inicio de Sesión : Los usuarios deben poder iniciar sesión utilizando sus credenciales (nombre de usuario/correo electrónico y contraseña).

3. Recuperación de Contraseña : La aplicación debe proporcionar una opción para recuperar la contraseña mediante correo electrónico.

4. Roles y Permisos : Los usuarios deben tener diferentes roles (administrador, usuario estándar, etc.) con distintos niveles de acceso a las funcionalidades.

Gestión de Contenidos

5. Creación de Contenidos : Los usuarios autorizados deben poder crear nuevos contenidos (artículos, publicaciones, productos, etc.).

6. Edición de Contenidos : Los usuarios deben poder editar contenidos existentes.

7. Eliminación de Contenidos : Los usuarios autorizados deben poder eliminar contenidos.

8. Visualización de Contenidos : Los contenidos deben ser accesibles y visibles para los usuarios según sus permisos.

Interacción del Usuario

9. Comentarios y Valoraciones : Los usuarios deben poder dejar comentarios y valoraciones en los contenidos.

10. Búsqueda : La aplicación debe permitir a los usuarios buscar contenidos utilizando palabras clave.

11. Notificaciones : Los usuarios deben recibir notificaciones sobre eventos relevantes (nuevos comentarios, respuestas, actualizaciones de contenido, etc.).

Integración con Servicios Externos

12. Integración con Redes Sociales : Los usuarios deben poder compartir contenidos en redes sociales.

13. Pagos en Línea : Si aplica, la aplicación debe integrar una pasarela de pagos para permitir transacciones en línea.

14. APIs : La aplicación debe ofrecer APIs para la integración con otros sistemas y servicios.

Seguridad

15. Protección contra Inyección de SQL : La aplicación debe estar protegida contra ataques de inyección de SQL.

16. Protección contra CSRF y XSS : La aplicación debe estar protegida contra ataques Cross-Site Request Forgery (CSRF) y Cross-Site Scripting (XSS).

17. Cifrado de Datos Sensibles : La información sensible (contraseñas, datos de tarjetas de crédito, etc.) debe estar cifrada.

Rendimiento y Escalabilidad

18. Rendimiento Óptimo : La aplicación debe cargar rápidamente y manejar un alto volumen de usuarios simultáneos sin degradar el rendimiento.

19. Escalabilidad : La arquitectura de la aplicación debe permitir su escalado horizontal y vertical para manejar el crecimiento del tráfico y los datos.

Mantenimiento y Actualización

20. Facilidad de Mantenimiento : El código de la aplicación debe estar bien documentado y estructurado para facilitar el mantenimiento y la actualización.

21. Actualizaciones Automatizadas : La aplicación debe permitir la implementación de actualizaciones de forma automatizada con mínimo tiempo de inactividad.

Experiencia de Usuario (UX)

22. Interfaz Intuitiva : La interfaz de usuario debe ser intuitiva y fácil de usar.

23. Responsive Design : La aplicación debe ser accesible y usable en dispositivos de diferentes tamaños de pantalla (móviles, tabletas, escritorios).