Prueba desarrollador front end

Parte 1: Práctica

Instrucciones:

1. Crear un proyecto de frontend utilizando HTML, CSS y JavaScript.
2. Implementar un sistema de inicio de sesión utilizando una API externa (por ejemplo, Google Sign-In, Facebook Login, GitHub Authentication, etc.).
3. Almacenar los datos del usuario en localStorage o sessionStorage.
4. Crear una interfaz de usuario para mostrar los datos del usuario autenticado.
5. Incluir una imagen personalizada en la interfaz de usuario.
6. Agregar un botón para logout.
7. Verificar si el usuario está autenticado antes de permitir acceso a ciertas secciones de la aplicación.
8. Utilizar un framework de JavaScript como React, Angular o Vue.js.
9. Utilizar una biblioteca de JavaScript para la gestión de eventos, como jQuery o EventEmitter.
10. Utilizar una biblioteca de CSS para styling, como Materialize o Bootstrap.

Parte 2: Teórica

Instrucciones:

1. Explicar brevemente el concepto de autenticación y autorización en aplicaciones web.
2. Describir el diferencial entre sessionStorage y localStorage.
3. Explicar cómo se puede utilizar una API externala para autenticar a un usuario en una aplicación web.
4. Describir el proceso de tokenización de autenticación.
5. Explicar qué es Cross-Site Request Forgery (CSRF) y cómo se puede prevenir.
6. Describir el uso de headers HTTP para controlar la autenticación y la autorización.
7. Explicar cómo se puede utilizar JSON Web Tokens (JWT) para autenticar a un usuario en una aplicación web.
8. Describir el proceso de refresh tokens.
9. Explicar qué es Single Sign-On (SSO) y cómo funciona.
10. Describir las ventajas y desventajas de utilizar una API externala para autenticar a un usuario en una aplicación web.