

Practica 2

Principios SOLID y JWT para sesiones de *Delivereats*



PONDERACIÓN: 3

Horas Aproximadas: 8

Universidad San Carlos de Guatemala

Facultad de ingeniería.

Ingeniería en ciencias y sistemas

Contenido

Diseño de Arquitectura y Base de Datos para <i>Delivereats</i>	0
Contexto.....	2
Objetivos	2
General.....	2
específicos:.....	2
Alcance	2
Entregables.....	3
Documentación:	3
Funcionalidades:	3
Consideraciones	3
Cronograma	3
Rúbrica de Calificación	4
Valores.....	6
1. Originalidad del Trabajo	6
2. Prohibición de Copias y Plagio	6
3. Uso Responsable de Recursos Externos.....	6
4. Revisión y Detección de Plagio.....	6

Contexto

La práctica se basa en el proyecto **Delivereats**, una plataforma de delivery diseñada con arquitectura de microservicios.

En esta ocasión se le solicita que realice una demostración de sus conocimientos de programación y reglas de diseño (Principios SOLID) para la creación del registro e inicio de sesión de la plataforma.

Objetivos

General

El objetivo de la práctica es que el estudiante aplique de manera efectiva metodologías ágiles para la construcción de una aplicación mediante la entrega continua y progresiva de incrementos funcionales. A través de este enfoque iterativo, se busca que el estudiante desarrolle la capacidad de planificar, diseñar, documentar y validar componentes del sistema en pequeños ciclos, garantizando una evolución constante del proyecto, una mejor adaptación a cambios, y una gestión eficiente del tiempo y los recursos.

Implementar un sistema de gestión de identidades y acceso utilizando microservicios, aplicando principios de diseño de software para garantizar una base técnica escalable y segura.

específicos:

Que el estudiante sea capaz de:

- Desarrollar un servicio de autenticación que gestione el registro y login mediante JWT
- Asegurar la integridad de los datos sensibles mediante la encriptación de contraseñas
- Establecer comunicación técnica entre componentes utilizando el protocolo gRPC para servicios y REST para Gateway
- Garantizar la persistencia de datos y la protección de información sensible mediante contraseñas encriptadas

Alcance

La práctica abarca el desarrollo de los siguiente componentes:

- **Frontend:** Interfaz de usuario para capturar los datos
- **API Gateway:** Encargado de exponer rutas REST, validar tokens JWT, enrutar peticiones vía gRPC.
- **Auth-Service:** Responsable de la lógica de usuarios y generación de JWT y almacenamiento seguro de credenciales

Entregables

Documentación:

- Justificación de elección de framework para backend y frontend
- Explicación del manejo de uso de JWT

Funcionalidades:

- **Gestión de sesiones con JWT:** El sistema debe generar un JWT tras un login exitoso, el cual será valido para el Gateway en cada petición protegida.
- **Registro de Usuario:**
 - **Cliente:** Capacidad de crear cuentas para clientes desde el modulo principal
 - **Administrador:** Capacidad de crear cuentas de Repartidor y Restaurante desde un modulo único para administrador
- **Seguridad:** Las contraseñas deben de almacenarse siempre de forma encriptada (hasheada)
- **Consumo y comunicación:** El frontend debe consumir el API Gateway vía REST y este ultimo debe comunicarse con el Auth-Service mediante gRPC

Si el estudiante considera otra solución viable esta debe ser documentada y justificada

Despliegue inicial:

- Archivos de configuración para Docker y Docker-Compose que permitan levantar el servicio.

Consideraciones

- Se debe hacer uso de un repositorio en la nube para realizar la entrega de su práctica (Gitlab, Github, Bitbucket, etc.) con el nombre SA_PRACTICAS_CARNET y con una carpeta con el título PRACTICA2, una vez finalizada la practica el estudiante deberá de agregar el trabajo realizado al repositorio del proyecto y crear un tag con el siguiente nombre v0.2.0
- La practica se debe presentar de forma local (**NO DESPLIEGUES EN NUBE**)
- Agregar al auxiliar al repositorio de GitHub cómo colaborador: Samashoas
- Se trabajará de manera individual.
- Las copias completas/parciales serán merecedoras de una nota de 0 puntos, los responsables serán reportados al catedrático de la sección y a la Escuela de Ciencias y Sistemas.
- La práctica tiene una nota aprobatoria de 61 nota mínima para optar a trabajar en parejas **y es requisito entregarla y calificarla para tener derecho a calificación de la fase 1.**

Cronograma

Tarea	Fecha
Asignacion practica	29/01/2026
Fecha de entrega	04/02/2026
Fecha de calificación	05/02/2026, 07/02/2026

Rúbrica de Calificación

Descripción	Valor	Punteo
Interfaz de usuario funcional	5	
módulos y formularios de registro	5	
Formulario de Login y persistencia del JWT	10	
Creación de usuarios con contraseña encriptada	10	
Generación correcta del JWT tras validar credenciales	10	
Manejo de errores repetidos o credenciales invalidas	5	
API Gateway funcional	5	
Comunicación por medio de gRPC entre Gateway y Auth-service	10	

Uso de contenedores para levantar los servicios y la db	5	
Aplicación de principios SOLID	20	
Documentación	5	
Preguntas	10	

Valores

En el desarrollo de la práctica, se espera que cada estudiante demuestre honestidad académica y profesionalismo. Por lo tanto, se establecen los siguientes principios:

1. Originalidad del Trabajo

- Cada estudiante o equipo debe desarrollar su propio código y/o documentación, aplicando los conocimientos adquiridos en el curso.

2. Prohibición de Copias y Plagio

- Si se detecta la copia total o parcial del código, documentación o cualquier otro entregable, la calificación será de **0 puntos**.
- Esto incluye la reproducción de código entre compañeros, la reutilización de proyectos de semestres anteriores o el uso de código externo sin la debida referencia.

3. Uso Responsable de Recursos Externos

- El uso de bibliotecas, frameworks y ejemplos de código externos está permitido, siempre y cuando se referencian correctamente y se comprendan plenamente. (Consultar con el catedrático su política)

4. Revisión y Detección de Plagio

- Se podrán utilizar herramientas automatizadas y revisiones manuales para identificar similitudes en los proyectos.
- En caso de sospecha, el estudiante deberá justificar su código y demostrar su desarrollo individual o en equipo. Si este extremo no es comprobable la calificación será de **0 puntos**.

Al detectarse estos aspectos se informará al catedrático del curso quien realizará las acciones que considere oportunas.