

Rubrica de Evaluación 1 (Métodos/Técnicas de Ingeniería de Software)

1. Despliegue automatizado de la WebApp (20%)

- **Descripción:** El proyecto debe ser configurado para desplegarse utilizando pipelines de CI/CD en Jenkins. El pipeline debe incluir la obtención del código fuente desde el repositorio de GitHub, la ejecución de pruebas unitarias para el backend, la creación de imágenes Docker para el frontend y backend, y su carga en DockerHub. Teniendo las imágenes en Docker Hub, se debe desplegar localmente la aplicación web (en forma manual sin Jenkins) utilizando Docker Compose para orquestar y configurar los servicios necesarios tales como la base de datos, las réplicas del backend/frontend y los balanceadores de carga respectivos. Al final la aplicación debe quedar desplegada y funcionando correctamente desde contenedores.

2. WebApp funciona desde contenedores con todas las Épicas (25%)

- **Descripción:** La aplicación web debe estar desplegada y funcionando desde sus respectivos contenedores y debe ser accesible desde un navegador web. Además, todas las Épicas deben estar completamente implementadas y funcionar como se describe en el proyecto, permitiendo a los usuarios realizar todas las funcionalidades del proyecto.

3. Código fuente del Proyecto implementa todas las Épicas (20%)

- **Descripción:** El código fuente, disponible en el repositorio de GitHub, debe incluir la implementación completa de **todas** las Épicas especificadas. Cada épica debe estar representada en el código mediante funcionalidades específicas en el frontend y backend, cumpliendo con las descripciones y objetivos establecidos en el proyecto. *Nota: El código fuente del backend debe estar estructurado siguiendo estrictamente una arquitectura por capas. Además, debe estar escrito en inglés.*

4. Cobertura de pruebas (15%)

- **Descripción:** El proyecto debe incluir pruebas unitarias en el backend, alcanzando una cobertura de al menos el 90% a nivel de líneas de código (en la capa de lógica de negocio [servicios]).

5. Autenticación y Autorización (20%)

- **Descripción:** El sistema debe implementar un mecanismo de autenticación y autorización usando una herramienta IAM (*Identity and Access Management*) para garantizar el acceso seguro a las funcionalidades, donde la autenticación se realizará mediante un proceso de inicio de sesión con usuario y contraseña, y la autorización se gestionará a través de roles de usuario (por ejemplo, Administrador y Empleado), asegurando que cada usuario solo pueda acceder a las funcionalidades y operaciones permitidas según su perfil.

NOTA: Dado que hay problemas con Azure, no es obligatorio desplegar en la nube. Se acepta realizar el despliegue en sus computadores locales.