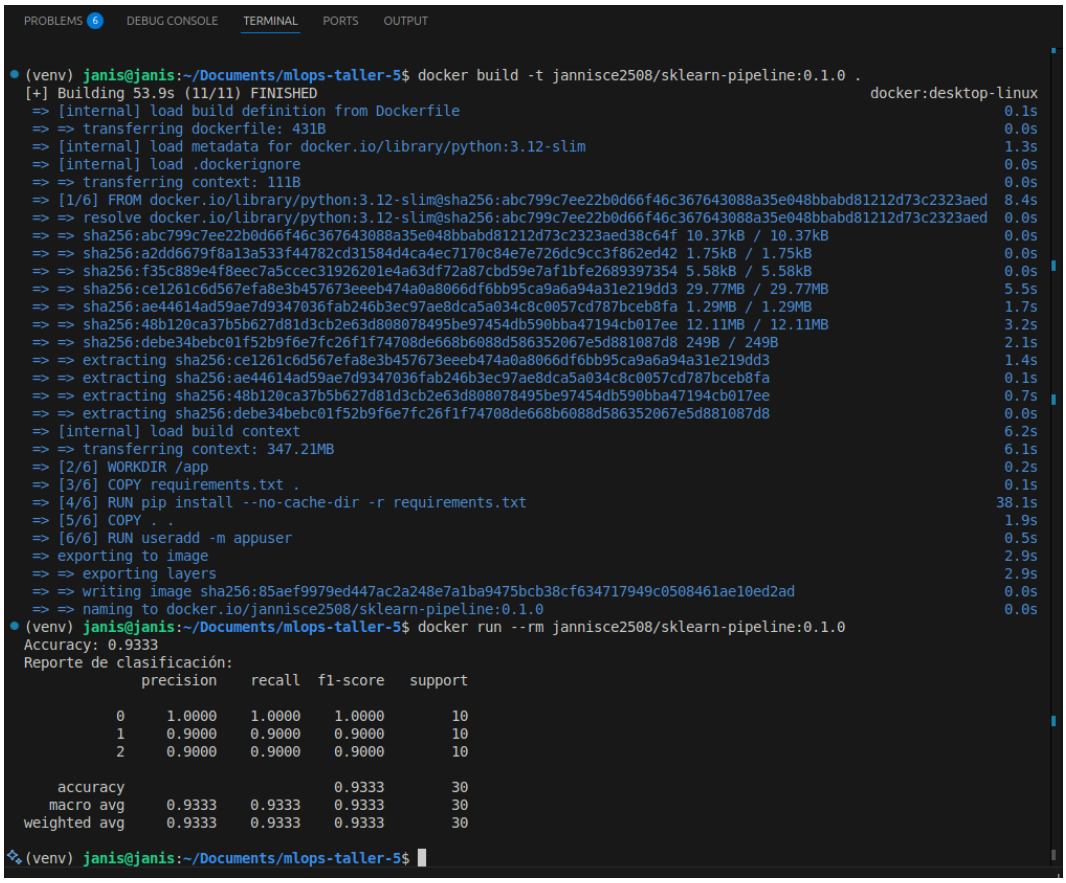
Taller 5

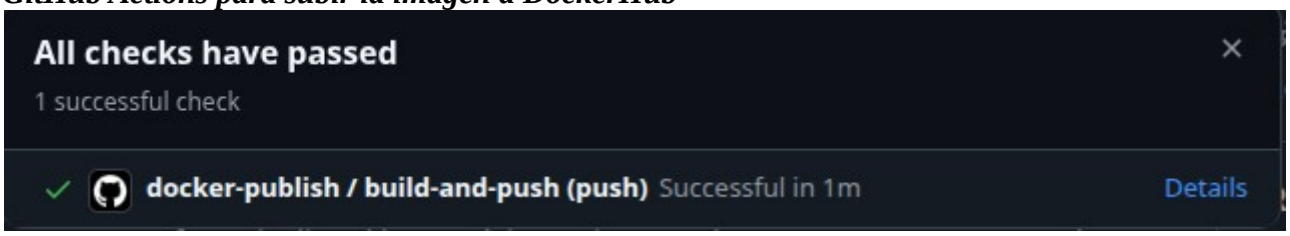
Link a repositorio de GitHub con código de la imagen de Docker.

https://github.com/JaniMariQuesiRami/mlops-taller-5

Capturas de pantalla con terminal mostrando ejecución exitosa del pipeline de scikit-learn adentro de la imagen de Docker.



GitHub Actions para subir la imagen a DockerHub



Link a Docker Hub de la imagen generada.

https://hub.docker.com/r/jannisce2508/sklearn-pipeline

Link a Documentación de Docker con comando(s) para compartir una imagen.

Guardar una imagen.
Usa docker image save para exportar una imagen a un archivo .tar. Conserva capas y tags. Útil para compartir sin usar un registro. Ejemplo conceptual: “guarda <dockerhub_username>/<image_name>:<tag> en <archivo>.tar y compártelo por cualquier medio”.
https://docs.docker.com/reference/cli/docker/image/save/

Cargar una imagen.
Usa docker image load para importar una imagen desde un .tar o desde STDIN. Restaura la imagen con sus tags y queda lista para ejecutar.
https://docs.docker.com/reference/cli/docker/image/load/

Conclusiones del ejercicio comparando estrategias que conocen para hacer portátil su código (paquetes de Python, pickles, Docker, etc)

Para portar código hay tres enfoques con roles distintos. Empaquetar como **paquete de Python** facilita reutilizar funciones y pipelines. Requiere recrear el entorno y fijar versiones. Funciona bien dentro del ecosistema Python. **Pickles/joblib** solo mueven el estado del modelo. Son frágiles a versiones y a veces inseguros. No resuelven dependencias del sistema ni de Python. No son un artefacto de despliegue por sí solos. **Docker** congela sistema, Python y librerías con el código. Ejecuta igual en cualquier host con Docker. Pesa más y exige gestionar imágenes, pero entrega reproducibilidad y trazabilidad. Recomendación práctica: código como paquete + dependencias fijadas + contenedor para ejecutar. Exporta el modelo (pickle/ONNX) como artefacto de build, no como mecanismo de portabilidad principal. Para compartir sin registro usa `docker save/load`. En resumen: paquetes portan API, pickles portan estado, Docker porta el runtime completo.