

# Resumen del workflow generado para GitHub Actions

Proyecto: tfg-cicd-aws-2526

Ramas donde corre la CI: main

¿Ejecuta en pull\_request?: sí

¿Proyecto con Node?: no

¿Incluye SonarCloud?: sí

¿Incluye deploy a AWS (ECR + EC2)?: sí

¿Usa base de datos?: sí

---

## Secrets/variables necesarios para SonarCloud

Variables necesarias para que el análisis de SonarCloud funcione dentro de la pipeline.

Uso los mismos nombres en GitHub y GitLab para no duplicar trabajo.

---

### Nombre del secret/variable: SONAR\_HOST\_URL

Ejemplo de valor: https://sonarcloud.io

¿De dónde saco este valor?: Es la URL base de mi servidor SonarCloud. En la mayoría de casos es https://sonarcloud.io.

---

### Nombre del secret/variable: SONAR\_PROJECT\_KEY

Ejemplo de valor: mi-proyecto\_en\_sonar

¿De dónde saco este valor?: En SonarCloud voy a mi proyecto, pestaña 'Administration' → 'Update key', y copio el valor exacto de 'Project key'. Ese valor es el que pego en este secret/variable.

---

### Nombre del secret/variable: SONAR\_ORGANIZATION

Ejemplo de valor: mi-organizacion

¿De dónde saco este valor?: En SonarCloud, arriba a la derecha, puedo ver el identificador de mi organización (Organization key). Copio ese valor y lo uso en este secret/variable.

---

### Nombre del secret/variable: SONAR\_TOKEN

Ejemplo de valor: Token personal de análisis

¿De dónde saco este valor?: En SonarCloud entro con mi usuario, voy a My Account → Security, creo un token nuevo y copio el valor. Ese valor es el que pego en este secret/variable.

---

## Secrets/variables necesarios para AWS (ECR + EC2)

Secrets/variables necesarios para poder hacer login en ECR, subir imágenes Docker y conectarme por SSH a la instancia EC2 donde despliego.

---

### Nombre del secret/variable: AWS\_ACCESS\_KEY\_ID

Ejemplo de valor: AKIAIOSFODNN7EXAMPLE

¿De dónde saco este valor?: En AWS Console entro a IAM → Users, selecciono mi usuario y en la pestaña 'Security credentials' creo una access key. Uso el valor de Access key ID.

---

---

**Nombre del secret/variable: AWS\_SECRET\_ACCESS\_KEY**

Ejemplo de valor: wJalrXUtnF/.../KEY

¿De dónde saco este valor?: En el mismo sitio donde creo la access key (IAM → Users → Security credentials) copio el Secret access key. Ese valor solo se muestra una vez, así que lo guardo y lo pego en este secret/variable.

---

**Nombre del secret/variable: AWS\_REGION**

Ejemplo de valor: eu-west-1

¿De dónde saco este valor?: En la esquina superior derecha de AWS Console selecciono la región en la que tengo mis recursos (por ejemplo eu-west-1) y uso ese código.

---

**Nombre del secret/variable: AWS\_ECR\_URL**

Ejemplo de valor: 490145258703.dkr.ecr.eu-west-1.amazonaws.com

¿De dónde saco este valor?: En AWS Console voy a ECR → Repositories, selecciono mi repositorio y pulso el botón 'Copy URI'. De esa URI me quedo con la parte del registry (por ejemplo 490145258703.dkr.ecr.eu-west-1.amazonaws.com).

---

**Nombre del secret/variable: ECR\_REPOSITORY**

Ejemplo de valor: tfg-cicd-aws-2526

¿De dónde saco este valor?: En AWS Console → ECR → Repositories uso el nombre exacto del repositorio Docker donde subo las imágenes (en mi caso tfg-cicd-aws-2526).

---

**Nombre del secret/variable: EC2\_HOST**

Ejemplo de valor: ec2-11-22-33-44.eu-west-1.compute.amazonaws.com

¿De dónde saco este valor?: En AWS Console voy a EC2 → Instances y copio el valor de 'Public IPv4 DNS' o 'Public IPv4 address' de la instancia donde voy a desplegar.

---

**Nombre del secret/variable: EC2\_USUARIO**

Ejemplo de valor: ubuntu

¿De dónde saco este valor?: Depende de la AMI de la instancia. Para Ubuntu el usuario por defecto es 'ubuntu' y para Amazon Linux normalmente es 'ec2-user'. Yo utilizo el que corresponde a mi máquina.

---

**Nombre del secret/variable: EC2\_LLAVE\_SSH**

Ejemplo de valor: ----BEGIN PRIVATE KEY---- ... ----END PRIVATE KEY----

¿De dónde saco este valor?: Cuando creo el par de claves de la instancia EC2, AWS me descarga un fichero .pem. Guardo ese .pem en mi equipo, le doy permisos con 'chmod 400 nombre-clave.pem' y lo abro con un editor de texto. Copio TODO el contenido de la clave privada, incluyendo las líneas '----BEGIN PRIVATE KEY----' y '----END PRIVATE KEY----', y lo pego tal cual dentro de este secret/variable.

---

**Variables necesarias para Base de Datos**

Estas variables permiten conectar la aplicación con cualquier base de datos externa (por

ejemplo RDS en AWS) o interna (un contenedor Docker).

---

**Nombre del secret/variable: DB\_ENGINE**

Ejemplo de valor: postgresql

¿De dónde saco este valor?: Motor de base de datos. Ejemplos: postgresql, mysql, mariadb, sqlserver, oracle.

---

**Nombre del secret/variable: DB\_HOST**

Ejemplo de valor: postgres-db

¿De dónde saco este valor?: Host o endpoint de la base de datos. Si usas Docker local: postgres-db. Si usas RDS: copia el endpoint desde AWS RDS.

---

**Nombre del secret/variable: DB\_PORT**

Ejemplo de valor: 5432

¿De dónde saco este valor?: Puerto de conexión. Depende del motor: PostgreSQL=5432, MySQL/MariaDB=3306, SQL Server=1433, etc.

---

**Nombre del secret/variable: DB\_NAME**

Ejemplo de valor: tfg

¿De dónde saco este valor?: Nombre de la base de datos. Lo defines al crear tu BD o lo lees del panel de RDS/gestor de BBDD.

---

**Nombre del secret/variable: DB\_USER**

Ejemplo de valor: tfg

¿De dónde saco este valor?: Usuario con permisos para conectarse a la base de datos. En RDS lo defines al crear la instancia.

---

**Nombre del secret/variable: DB\_PASSWORD**

Ejemplo de valor: \*\*\*\*\*

¿De dónde saco este valor?: Password de acceso del usuario de base de datos. No se guarda en código, solo en secrets/variables.

---

**Cómo creo los secrets en GitHub**

1. Entro en el repositorio de GitHub del proyecto.
2. Voy a Settings → Secrets and variables → Actions.
3. Pulso el botón 'New repository secret'.
4. En 'Name' escribo exactamente el nombre del secret que aparece en este documento (por ejemplo AWS\_ACCESS\_KEY\_ID, EC2\_LLAVE\_SSH, SONAR\_HOST\_URL, SONAR\_PROJECT\_KEY, SONAR\_ORGANIZATION, SONAR\_TOKEN, DB\_ENGINE, DB\_HOST, etc.).
5. En 'Secret' pego el valor real que he obtenido de AWS, SonarCloud o del proveedor de base de datos.
6. Repito estos pasos para cada uno de los secrets hasta tenerlos todos creados.