

Paso 4 AWS

Primero, créate una cuenta en AWS, una vez la tengas sigue lo siguientes pasos.

Si trabajas con Mac, abre tu terminal y ejecuta:

```
brew install awscli
```

```
aws --version
```

Si trabajas con Windows: instalar “AWS CLI v2” (MSI) y comprueba en la terminal:

```
aws --version
```

Deberías ver algo así:

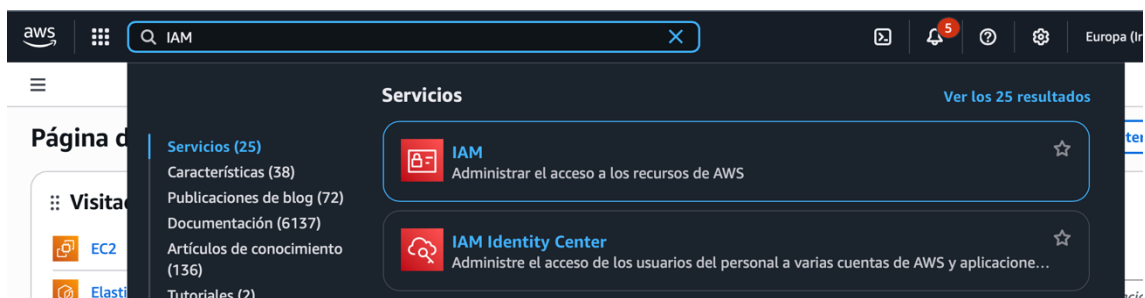
```
(base) david@MacBook-Pro-de-David ~ % aws --version
aws-cli/2.31.11 Python/3.13.7 Darwin/25.1.0 exe/arm64
(base) david@MacBook-Pro-de-David ~ %
```

Ahora vamos a configurar las credenciales en nuestro ordenador (AWS CLI), para ello ejecutamos el comando “aws configure”.

Para rellenar cada campo sigue estos campos, te dire donde podemos encontrar cada valor.

Para AWS Access Key ID:

Dentro de nuestra cuenta de AWS, en el buscador escribimos “IAM” y seleccionamos la primera opción.



En nuestro panel lateral, pulsamos en la opción “Personas”, ahí crearemos nuestro usuario. Escribimos el nombre de nuestro usuario y damos a siguiente.

IAM > Personas > Crear persona

Paso 1
● Especificar los detalles de la persona

Paso 2
○ Establecer permisos

Paso 3
○ Revisar y crear

Especificar los detalles de la persona

Detalles de la persona

Nombre de usuario

tfg-cicd-user

El nombre de usuario puede tener un máximo de 64 caracteres. Caracteres válidos: A-Z, a-z, 0-9, and + = , . @ _ - (guion)

☐ **Proporcione acceso de usuario a la consola de administración de AWS: *opcional***
In addition to console access, users with SigninLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

❗ Si está creando acceso mediante programación a través de claves de acceso o credenciales específicas de servicios para AWS CodeCommit o Amazon Keyspaces, puede generarlos después de crear este usuario de IAM. [Más información](#)

Cancelar **Siguiente**

Dejamos esta ventana como esta y pulsamos a “crear un grupo”.

IAM > Personas > Crear persona

Paso 1
● Especificar los detalles de la persona

Paso 2
● **Establecer permisos**

Paso 3
○ Revisar y crear

Establecer permisos

Agregue una persona a un grupo existente o cree uno nuevo. El uso de grupos es una práctica recomendada para administrar los permisos de usuario según las funciones laborales. [Más información](#)

Opciones de permisos

☒ **Agregar persona al grupo**
Agregue la persona a un grupo existente o cree uno nuevo. Le recomendamos que utilice grupos para administrar los permisos de usuario según las funciones laborales.

☐ **Copiar permisos**
Copie todas las suscripciones a grupos, las políticas administradas adjuntas y las políticas insertadas de una persona existente.

☐ **Adjuntar políticas directamente**
Adjunte una política administrada a una persona de manera directa. Como práctica recomendada, le sugerimos, en cambio, adjuntar políticas a un grupo. A continuación, agregue la persona al grupo adecuado.

❗ **Iniciarse en los grupos**
Cree un grupo y seleccione políticas para adjuntarlas al grupo. Le recomendamos que utilice grupos para administrar los permisos de persona por función de trabajo, acceso a servicios de AWS o permisos personalizados. [Más información](#)

Crear un grupo

▶ **Establecer límite de permisos: *opcional***

Cancelar **Anterior** **Siguiente**

En esta venta, le ponemos un nombre al grupo y vamos a buscar y marcar estas 3 opciones:

AmazonEC2ContainerRegistryFullAccess

AmazonEC2FullAccess

AmazonSSMManagedInstanceCore

Una vez marcadas esas 3 opciones, pulsamos a “crear grupo de personas”

Crear grupo de personas

Cree un grupo de personas y seleccione políticas para adjuntarlas al grupo. Le recomendamos que utilice grupos para administrar los permisos de usuario por función de trabajo, acceso a servicios de AWS o permisos personalizados. [Más información](#)

Nombre del grupo de personas
Ingrese un nombre significativo para identificar a este grupo.

tfg-cicd-group

128 caracteres como máximo. Utilice caracteres alfanuméricos y '+=,._@-_'.

Políticas de permisos (1109)

Crear política

Buscar

Filtrar por Tipo

Todos los tipos

< 1 2 3 4 5 6 7 ... 56 >

	Nombre de la política	Tipo	Usa...	Descripción
<input type="checkbox"/>	<div><div></div><div>AccountManagem...</div></div>	Administrada ...	Ninguno	For use with accounts created thro
<input type="checkbox"/>	<div><div></div><div>AdministratorAccess</div></div>	Administrada ...	Ninguno	Provides full access to AWS servic
<input type="checkbox"/>	<div><div></div><div>AdministratorAcce...</div></div>	Administrada ...	Ninguno	Grants account administrative per
<input type="checkbox"/>	<div><div></div><div>AdministratorAcce...</div></div>	Administrada ...	Ninguno	Grants account administrative per
<input type="checkbox"/>	<div><div></div><div>AIOpsAssistantInci...</div></div>	Administrada ...	Ninguno	Provides permissions required by
<input type="checkbox"/>	<div><div></div><div>AIOpsAssistantPol...</div></div>	Administrada ...	Ninguno	Provides ReadOnly permissions re
<input type="checkbox"/>	<div><div></div><div>AIOpsAssistantAd...</div></div>	Administrada ...	Ninguno	Grants full access to Amazon AI O...

Cancelar

Crear grupo de personas

Veremos algo así, después damos a siguiente.

IAM > Personas > Crear persona

✔ tfg-cicd-group grupo de personas creado.

Paso 3

Revisar y crear

Opciones de permisos

☒ Agregar persona al grupo

Agregue la persona a un grupo existente o cree uno nuevo. Le recomendamos que utilice grupos para administrar los permisos de usuario según las funciones laborales.

☐ Copiar permisos

Copie todas las suscripciones a grupos, las políticas administradas adjuntas y las políticas insertadas de una persona existente.

☐ Adjuntar políticas directamente

Adjunte una política administrada a una persona de manera directa. Como práctica recomendada, le sugerimos, en cambio, adjuntar políticas a un grupo. A continuación, agregue la persona al grupo adecuado.

Grupos de personas (1)

Crear un grupo

Buscar

< 1 >

	Nombre del grupo	Personas	Políticas adjuntas	Creado
<input type="checkbox"/>	tfg-cicd-group	0	AmazonEC2FullAccess, Ama...	2025-12-12 (Ahora)

► Establecer límite de permisos: *opcional*

Cancelar

Anterior

Siguiente

CloudShell

Comentarios

Aplicación móvil de la consola

© 2025, Amazon Web Services, Inc. o sus filiales.

Privacidad

Términos

Preferencias de cookies

Pulsamos a siguiente sin tocar nada en esta ventana.

IAM > Personas > Crear persona

tfg-cicd-group grupo de personas creado.

Paso 1
● Especificar los detalles de la persona

Paso 2
● Establecer permisos

Paso 3
● **Revisar y crear**

Revisar y crear

Revise las opciones seleccionadas. Después de crear la persona, puede ver y descargar la contraseña autogenerada, si está habilitada.

Detalles de la persona

Nombre de usuario tfg-cicd-user	Tipo de contraseña de consola None	Exigir el restablecimiento de la contraseña No
------------------------------------	---------------------------------------	---

Resumen de permisos

Nombre Tipo Usado como

Sin recursos

Etiquetas : opcional

Las etiquetas son pares clave-valor que puede agregar a los recursos de AWS para ayudar a identificar, organizar o buscar recursos. Elija las etiquetas que desee asociar a esta persona.

No hay etiquetas asociadas al recurso.

[Agregar nueva etiqueta](#)

Puede agregar hasta 50 etiqueta más.

[Cancelar](#) [Anterior](#) [Crear persona](#)

Entramos dentro de nuestra persona, es decir: tfg-cicd-user.

Identity and Access Management (IAM)

Buscar en IAM

Panel

- Administración del acceso
 - Grupos de personas
 - Personas**
 - Roles
 - Políticas
 - Proveedores de identidad
 - Configuración de cuenta
 - Administración del acceso raíz
 - nav-ivy-account-access-requests
 - Noticias
- Informes de acceso
 - Access Analyzer
 - Análisis del recurso [Noticias](#)
 - Acceso no utilizado
 - Configuración del analizador
 - Informe de credenciales
 - Actividad de la organización
 - Políticas de control de servicios
 - Políticas de control de recursos

Personas (2) Información

Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.

Buscar

<input type="checkbox"/>	Nombre de usuario	Ruta	Grupo	Última actividad	MFA	Antigüedad de	Último inicio de sesión	ID de clave
<input type="checkbox"/>	github-actions	/	0	Hace 11 días	-	-	-	Active - AKI
<input type="checkbox"/>	tfg-cicd-user	/	0	-	-	-	-	-

En esta ventana damos a “crear clave de acceso” (esta dentro del cuadro de resumen)

Identity and Access Management (IAM) > Personas > tfg-cicd-user

Resumen

ARN: [arn:aws:iam::490145258703:user/tfg-cicd-user](#)

Acceso a la consola: Desactivada

Clave de acceso 1: [Crear clave de acceso](#)

Creado: December 12, 2025, 20:05 (UTC+01:00)

Último inicio de sesión en la consola: -

Políticas de permisos (0)

Los permisos se definen mediante políticas asociadas a la persona directamente o a través de grupos.

Filtrar por Tipo: Todos los tipos

No hay recursos que mostrar

► Límite de permisos (no establecido)

▼ Generar una política basada en eventos de CloudTrail

Puede generar una nueva política basada en la actividad de acceso correspondiente a este persona. A continuación, puede personalizarla, crearla y asociarla a este rol. AWS utiliza los eventos de CloudTrail para identificar los servicios y las acciones utilizados y generar una política. [Más información](#)

CloudShell Comentarios Aplicación móvil de la consola

© 2025, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies

Marcamos la primera opción “Interfaz de línea de comandos (CLI)”, marcamos la opción de abajo y pulsamos a siguiente.

IAM > Personas > tfg-cicd-user > Crear clave de acceso

Establecer el valor de etiqueta de descripción

Paso 3

Recuperar claves de acceso

Caso de uso

☒ Interfaz de línea de comandos (CLI)

Tiene previsto utilizar esta clave de acceso para permitir que la AWS CLI obtenga acceso a su cuenta de AWS.

☐ Código local

Tiene previsto utilizar esta clave de acceso para habilitar el código de aplicación en un entorno de desarrollo local para obtener acceso a su cuenta de AWS.

☐ Aplicación ejecutada en un servicio de computación de AWS

Tiene previsto utilizar esta clave de acceso para permitir que el código de aplicación que se ejecuta en un servicio de computación de AWS como Amazon EC2, Amazon ECS o AWS Lambda obtenga acceso a su cuenta de AWS.

☐ Servicio de terceros

Tiene previsto utilizar esta clave de acceso para habilitar el acceso a una aplicación o servicio de terceros que supervise o administre sus recursos de AWS.

☐ Aplicación ejecutada fuera de AWS

Planea usar esta clave de acceso para autenticar las cargas de trabajo que se ejecutan en su centro de datos u otra infraestructura externa a AWS que necesitan acceder a sus recursos de AWS.

☐ Otros

Su caso de uso no aparece aquí.

Alternativas recomendadas

- Use AWS CLI V2 and the `aws login` command to use your existing console credentials in the CLI. [Más información](#)
- Use AWS CloudShell, a browser-based CLI, to run commands. [Más información](#)

Confirmación

☒ Entiendo la recomendación anterior y deseo proceder a la creación de una clave de acceso.

Cancelar Siguiente

Podemos poner algo en este campo o dejarlo vacío, pulsamos a “crear clave de acceso”.

☰ IAM > Personas > tfg-cicd-user > Crear clave de acceso

Paso 1
● Prácticas recomendadas y alternativas para la clave de acceso

Paso 2 - *opcional*
● Establecer el valor de etiqueta de descripción

Paso 3
○ Recuperar claves de acceso

Establecer el valor de etiqueta de descripción - *opcional* [Información](#)

La descripción de esta clave de acceso se adjuntará a esta persona como una etiqueta y se mostrará junto con la clave de acceso.

Valor de etiqueta de descripción
Describe el objetivo de esta clave de acceso y dónde se utilizará. Una buena descripción lo ayudará a rotar esta clave de acceso con confianza más adelante.

Máximo de 256 caracteres. Los caracteres permitidos son letras, números, espacios representables en UTF-8 y: _ . : / = + - @

[Cancelar](#) [Anterior](#) [Crear clave de acceso](#)

En esta ventana, descargamos el archivo .csv y te recomiendo guardar la clave de acceso y la clave de acceso secreta en algún fichero para tenerlo a mano para cuando nos haga falta.

☰ IAM > Personas > tfg-cicd-user > Crear clave de acceso

✔ Este es el único momento en el que se puede ver o descargar la clave de acceso secreta. No podrá recuperarla posteriormente. Sin embargo, puede crear una nueva clave de acceso en cualquier momento.

Paso 1
● Prácticas recomendadas y alternativas para la clave de acceso

Paso 2 - *opcional*
● Establecer el valor de etiqueta de descripción

Paso 3
● Recuperar claves de acceso

Recuperar claves de acceso [Información](#)

Clave de acceso
Si pierde u olvida la clave de acceso secreta, no podrá recuperarla. En su lugar, cree una nueva clave de acceso y deje inactiva la antigua.

Clave de acceso | Clave de acceso secreta

[Mostrar](#)

Prácticas recomendadas para la clave de acceso

- Nunca almacene la clave de acceso en texto plano, en un repositorio de código o en el código.
- Desactive o elimine la clave de acceso cuando ya no sea necesaria.
- Habilite los permisos con privilegios mínimos.
- Rote con regularidad las claves de acceso.

Para obtener más información sobre cómo administrar las claves de acceso, consulte las [prácticas recomendadas para administrar las claves de acceso de AWS](#).

[Descargar archivo.csv](#) [Listo](#)

Ya tenemos la clave creada.

The screenshot shows the AWS IAM console for a user named 'tf-g-cicd-user'. The left sidebar contains navigation links for Identity and Access Management (IAM), including sections for Administration and Access, and Reports. The main content area shows the user's details under the 'Security Credentials' tab. Key information includes the ARN 'arn:aws:iam::490145258703:user:tf-g-cicd-user', console access status 'Desactivada', and two access keys. The 'Inicio de sesión en la consola' section shows a console login link and a disabled console password. The 'Autenticación multifactor (MFA) (0)' section indicates no MFA devices are currently assigned.

En grupos de personas necesitamos asegurarnos de que este nuestro usuario agregado, si no agrégalo, tienes que ver esto

The screenshot shows the AWS IAM console for a group named 'tf-g-cicd-group'. A green notification banner at the top indicates that one person has been added to the group. The main content area shows the group's details under the 'Personas (1)' tab. The 'Personas de este grupo (1)' section lists the group member 'tf-g-cicd-user' with columns for Name, Groups, Last Activity, and Creation Time.

vamos a rellenar las variables de nuestro “aws configure”.

AWS Access Key ID [None]: aquí escribimos la clave de acceso que acabamos de crear, tiene que ser algo así “AKIAXXXXXXXXXXXXXXXXXX”

AWS Secret Access Key [None]: escribimos la clave secreta que hemos creado.

En la siguiente captura aparecen las 2 claves anteriores.

☰ IAM > Personas > tfg-cicd-user > Crear clave de acceso

✓ Este es el único momento en el que se puede ver o descargar la clave de acceso secreta. No podrá recuperarla posteriormente. Sin embargo, puede crear una nueva clave de acceso en cualquier momento.

Paso 1
● Prácticas recomendadas y alternativas para la clave de acceso

Paso 2 - *opcional*
● Establecer el valor de etiqueta de descripción

Paso 3
● **Recuperar claves de acceso**

Recuperar claves de acceso [Información](#)

Clave de acceso

Si pierde u olvida la clave de acceso secreta, no podrá recuperarla. En su lugar, cree una nueva clave de acceso y deje inactiva la antigua.

Clave de acceso	Clave de acceso secreta
<input type="text" value="AKIAXEHPDTHCTCKBT7UG"/>	<input type="password" value="*****"/> Mostrar

Prácticas recomendadas para la clave de acceso

- Nunca almacene la clave de acceso en texto plano, en un repositorio de código o en el código.
- Desactive o elimine la clave de acceso cuando ya no sea necesaria.
- Habilite los permisos con privilegios mínimos.
- Rote con regularidad las claves de acceso.

Para obtener más información sobre cómo administrar las claves de acceso, consulte las [prácticas recomendadas para administrar las claves de acceso de AWS](#).

[Descargar archivo.csv](#) [Listo](#)

Default region name [None]: por defecto te recomiendo que pongas esta “eu-west-1”

Default output format [None]: por defecto pon esta “json”

Con estos 4 campos ya tenemos configuradas las credenciales en nuestro ordenador:

AWS Access Key ID: captura anterior

AWS Secret Access Key: captura anterior

Default region name: eu-west-1

Default output format: json

Para comprobar que lo hemos hecho bien, vamos a ejecutar el siguiente comando para ver si nos reconoce con nuestras credenciales.

El comando es el siguiente: `aws sts get-caller-identity`

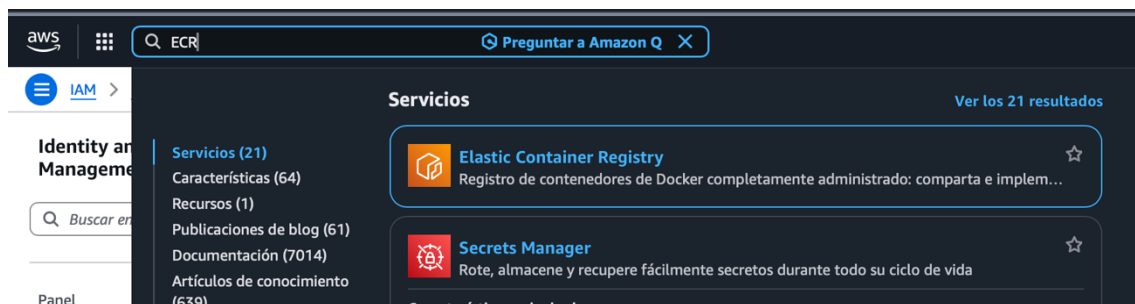
Si nos devuelve algo como en la captura siguiente, significa que nos reconoce.

De aquí quédate con el valor del campo “Account”, ya que luego vamos a crear su variable secreta en Git.

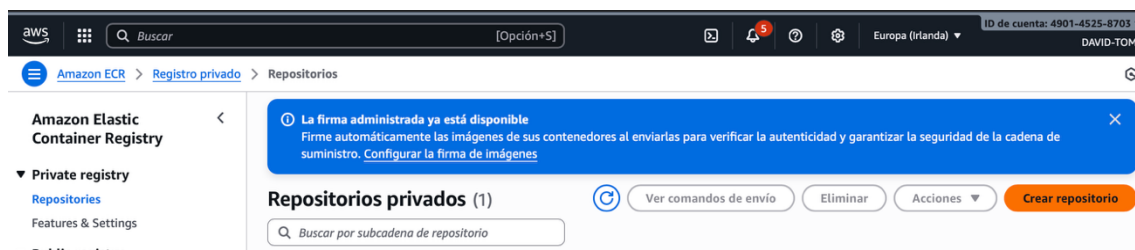

```
((base) david@MacBook-Pro-de-David ~ % aws sts get-caller-identity
{
  "UserId": "AIDAXEHXPDT43ZQNV3XI",
  "Account": "490145258703",
  "Arn": "arn:aws:iam::490145258703:user/tfg-cicd-user"
}
(base) david@MacBook-Pro-de-David ~ %
```

Crea el repositorio en ECR

En nuestra cuenta de AWS, en el buscador escribimos “ECR” y pulsamos a la opción “Elastic Container Registry”.



Creamos un repositorio nuevo.



En esta ventana solo le vamos a poner un nombre descriptivo a nuestro repositorio y dejamos todo lo demás como está. Pulsamos a crear.

Crear repositorio privado

Configuración general

Nombre del repositorio

Introduzca un nombre conciso. Los repositorios admiten espacios de nombres, que puede usar para agrupar repositorios similares.

490145258703.dkr.ecr.eu-west-1.amazonaws.com/tfg-cicd-prueba1-ecr

20 de 256 caracteres máximo (2 mínimo). El nombre debe comenzar con una letra y solo puede contener letras minúsculas, números y caracteres especiales _-./.

Configuración de etiquetas de imagen

Información

Mutabilidad de la etiqueta de imagen

Elija la configuración de mutabilidad de las etiquetas.

☒ Mutable

Las etiquetas de imagen se pueden sobrescribir.

☐ Immutable

Las etiquetas de imagen no se pueden sobrescribir.

Exclusiones de etiquetas mutables

Las etiquetas que coincidan con estos filtros serán inmutables (no se podrán sobrescribir). El uso de comodines (*) coincidirá con cero o más caracteres de la etiqueta de la imagen.

Agregar filtro

Los filtros únicamente deben contener letras, números y caracteres especiales {_,^*}. Cada filtro está limitado a 128 caracteres, 2 comodines (*) y puede agregar hasta 5 filtros en la lista de exclusiones.

Ya la tenemos creada.

<input type="radio"/>	tfg-cicd-prueba1-ecr	490145258703.dkr.ecr.eu-west-1.amazonaws.com/tfg-cicd-prueba1-ecr	12 de diciembre de 2025, 20:41:40 (UTC+01)	Mutable	AES-256
-----------------------	----------------------	---	--	---------	---------

Vamos a crear nuestras nuevas variables secretas en nuestro Github, en este paso crearemos:

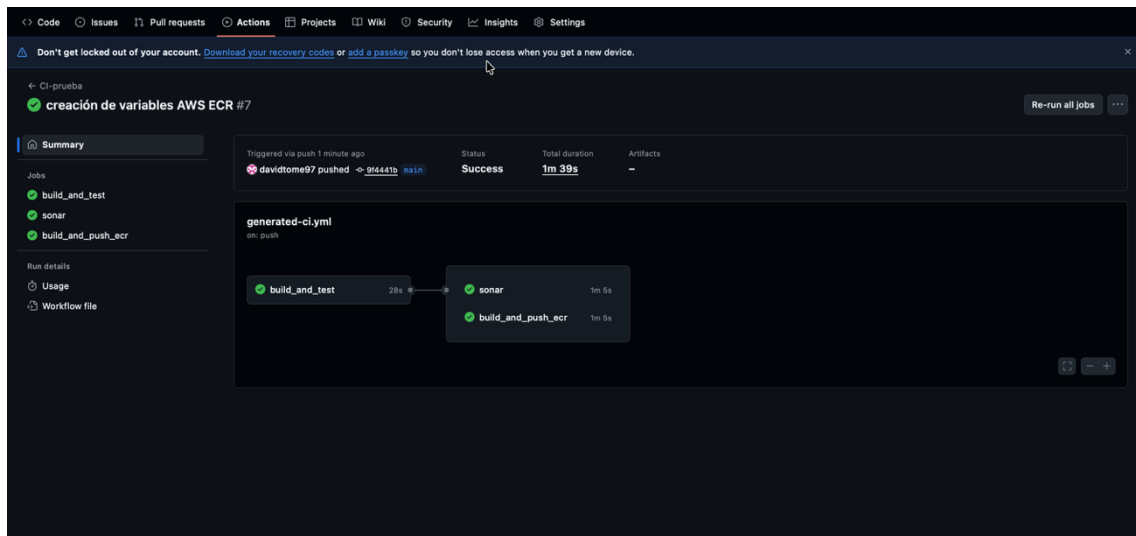
- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_REGION = eu-west-1
- AWS_ACCOUNT_ID = 490145258703
- ECR_REPOSITORY = tfg-cicd-prueba1-ecr

Una vez creadas, hay que hacer otro commit. (puede fallar por las comillas, escribirlas de nuevo)

`git commit --allow-empty -m "creación de variables AWS ECR"`

`git push`

En nuestro repositorio de Github en la ventana de actions deberíamos ver esto en verde.



Ahora vamos a probar nuestro paso 4 en la aplicación para ver si funciona correctamente.

En el paso 4, escribimos nuestro nombre del repositorio: "tfg-cicd-prueba1-ecr"

