

Paso 4 AWS

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

Si trabajas con Mac, abre tu terminal y ejecuta:

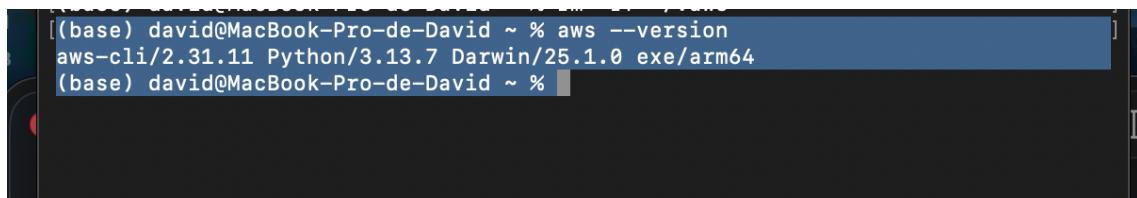
```
brew install awscli
```

```
aws --version
```

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

```
aws --version
```

Deberás ver algo así:



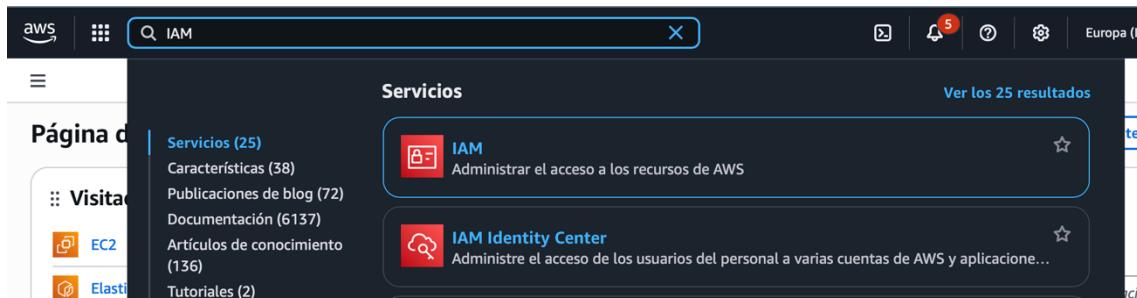
```
(base) david@MacBook-Pro-de-David ~ % aws --version
aws-cli/2.31.11 Python/3.13.7 Darwin/25.1.0 exe/arm64
(base) david@MacBook-Pro-de-David ~ %
```

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

Para llenar 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
 Especificar los detalles de la persona
 Establecer permisos
 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 Keypaces, 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
 Establecer permisos
 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
Copia 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

AmazonSSMManagedInstanceState

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](#)

Filtrar por Tipo

Buscar

Todos los tipos

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

<input type="checkbox"/>	Nombre de la política	Tipo	Usa...	Descripción
<input type="checkbox"/>	AccountManagement...	Administrada...	Ninguno	For use with accounts created through the AWS Management Con...
<input type="checkbox"/>	AdministratorAccess	Administrada...	Ninguno	Provides full access to AWS services.
<input type="checkbox"/>	AdministratorAccess...	Administrada...	Ninguno	Grants account administrative permissions.
<input type="checkbox"/>	AdministratorAccess...	Administrada...	Ninguno	Grants account administrative permissions.
<input type="checkbox"/>	AIOpsAssistantIncident...	Administrada...	Ninguno	Provides permissions required by the AIOps Assistant Incident Res...
<input type="checkbox"/>	AIOpsAssistantPolicy...	Administrada...	Ninguno	Provides ReadOnly permissions re...

[Cancelar](#)

[Crear grupo de personas](#)

Veremos algo así, después damos a siguiente.

Paso 3 Revisar y crear

tfg-cicd-group grupo de personas creado.

Opciones de permisos

Agregar persona al grupo
Agregar 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)

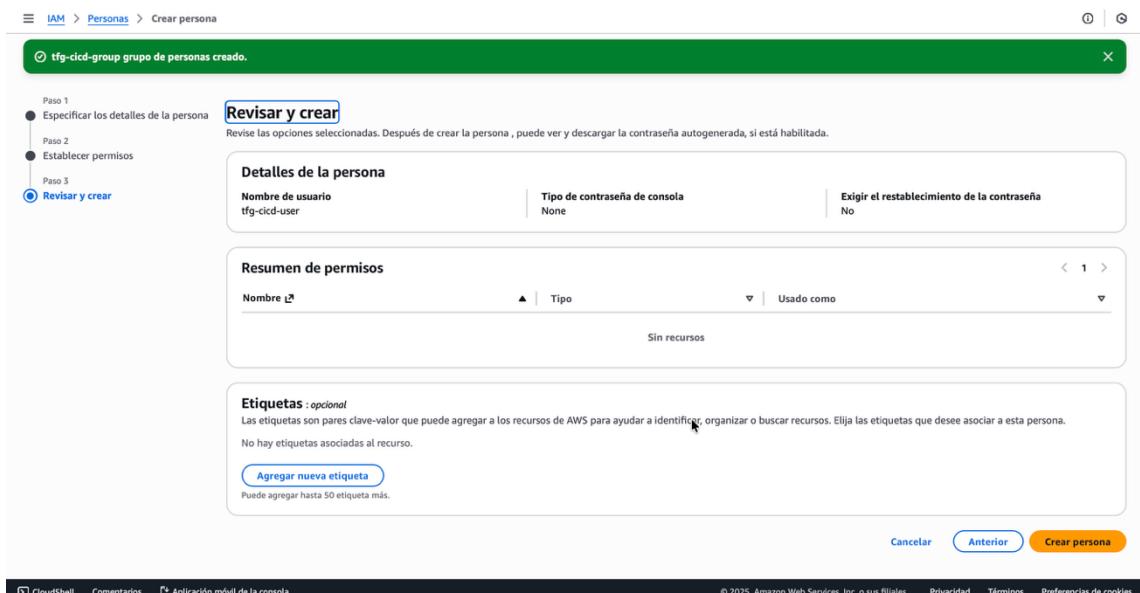
[Crear un grupo](#)

<input type="checkbox"/>	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](#)

Pulsamos a siguiente sin tocar nada en esta ventana.



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

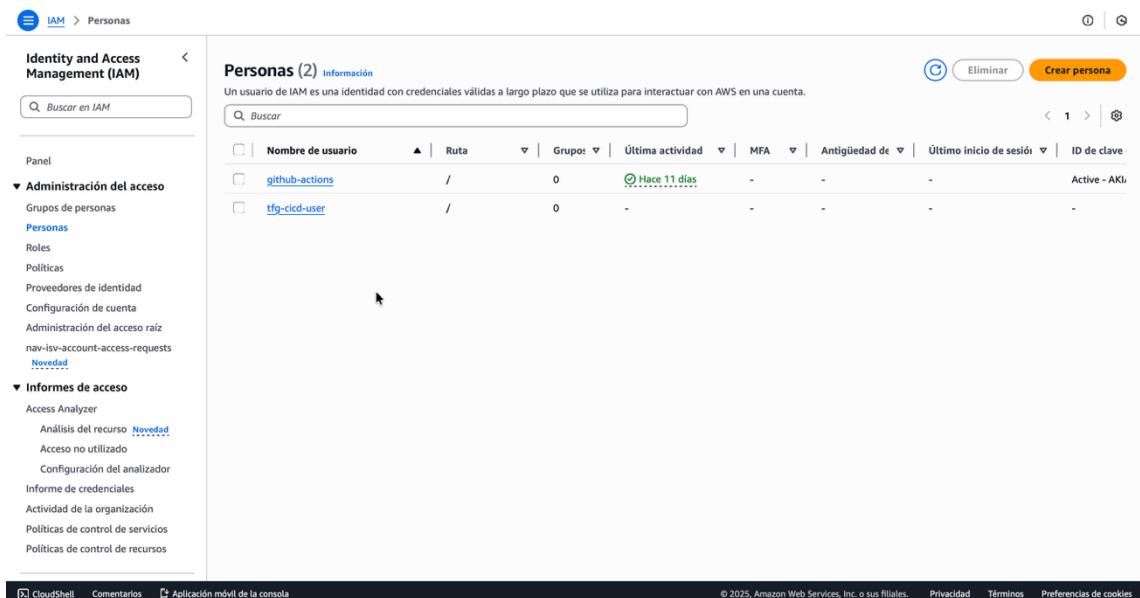
Nombre	Tipo	Usado como
Sin recursos		

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 deseé asociar a esta persona.
No hay etiquetas asociadas al recurso.

[Agregar nueva etiqueta](#)
Puede agregar hasta 50 etiquetas más.

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

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



Identity and Access Management (IAM)

Buscar en IAM

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.

Nombre de usuario	Ruta	Grupos	Última actividad	MFA	Antigüedad de	Último inicio de sesión	ID de clave
github-actions	/	0	Hace 11 días	-	-	-	Active - AKI
tfg-cicd-user	/	0	-	-	-	-	-

[Crear persona](#)

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

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

The screenshot shows the AWS IAM 'tfg-cicd-user' Information page. At the top, there's a search bar and a 'Resumen' (Summary) section with details like ARN, Creation Date, and Access to the console status. Below the summary is a 'Permisos' (Permissions) tab, which lists 'Políticas de permisos (0)' and a note about defining permissions via groups. There's also a 'Límite de permisos (no establecido)' (Unlimited permissions) section. The left sidebar includes sections for Identity and Access Management (IAM), Administration of access, and Reports.

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

The screenshot shows the 'Crear clave de acceso' (Create access key) wizard, Step 3: 'Caso de uso' (Use case). It lists several options: 'Interfaz de línea de comandos (CLI)' (selected), 'Código local', 'Aplicación ejecutada en un servicio de computación de AWS', 'Servicio de terceros', 'Aplicación ejecutada fuera de AWS', and 'Otros'. Below the options is a 'Alternativas recomendadas' (Recommended alternatives) section with two bullet points: 'Use AWS CLI V2 and the aws login command to use your existing console credentials in the CLI.' and 'Use AWS CloudShell, a browser-based CLI, to run commands.' A 'Confirmación' (Confirmation) section at the bottom contains a checked checkbox for accepting the recommendation and a 'Siguiente' (Next) button.

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

Screenshot of the AWS IAM 'Create access key' process, Step 2: Set key description. The 'Description value' field is empty. Buttons at the bottom are 'Cancelar', 'Anterior', and '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.

Screenshot of the AWS IAM 'Recuperar claves de acceso' process, Step 3: Download access key. The secret key is shown as a masked string. Buttons at the bottom are 'Descargar archivo.csv' and 'Listo'.

Ya tenemos la clave creada.

The screenshot shows the IAM User Details page for 'tfg-cicd-user'. Key details include:

- ARN: arn:aws:iam::490145258703:user/tfg-cicd-user
- Acceso a la consola: Desactivada
- Creado: December 12, 2025, 20:05 (UTC+01:00)
- Último inicio de sesión en la consola: -
- Clave de acceso 1: AKIAKEHXPDTHTCKBT7UG - Active
Nunca usado. Creado hoy.
- Clave de acceso 2: Crear clave de acceso

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

The screenshot shows the Groups page for 'tfg-cicd-group'. Key details include:

- Nombre del grupo de personas: tfg-cicd-group
- Hora de creación: December 12, 2025, 20:01 (UTC+01:00)
- ARN: arn:aws:iam::490145258703:group/tfg-cicd-group

Under the 'Personas' tab, it shows:

Nombre de usuario	Grupos	Última acti...	Hora de cre...
tfg-cicd-user	1	Ninguno	hace 57 minutos

vamos a llenar 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 “AKIAXXXXXXXXXXXXXX”

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

En la siguiente captura aparecen las 2 claves anteriores.

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 checked="" type="text"/> AKIAIEHXPDTHTCKBT7UG	<input type="text"/> ***** <input checked="" type="button"/> 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”.

The screenshot shows the AWS search interface. In the top navigation bar, there is a search bar with the text 'ECR'. Below the search bar, the results are displayed under the heading 'Servicios'. The first result is 'Elastic Container Registry', which is highlighted with a blue border. To its right, there is a brief description: 'Registro de contenedores de Docker completamente administrado: comparta e implemente...' and a star icon for favoritizing. Below this, another service, 'Secrets Manager', is listed with its description and a star icon. On the left side of the search results, there is a sidebar with links to 'Identity and Management', 'Buscar en', and 'Panel'.

Creamos un repositorio nuevo.

The screenshot shows the 'Amazon ECR' interface. At the top, there is a header with the account ID '4901-4525-8703' and the region 'Europa (Irlanda)'. Below the header, the path 'Amazon ECR > Registro privado > Repositorios' is visible. On the left, there is a sidebar with sections for 'Amazon Elastic Container Registry', 'Private registry', 'Repositories', 'Features & Settings', and 'Public repositories'. The main area is titled 'Repositorios privados (1)' and contains a message: 'La firma administrada ya está disponible. Fírmese automáticamente las imágenes de sus contenedores al enviarlas para verificar la autenticidad y garantizar la seguridad de la cadena de suministro. Configurar la firma de imágenes'. Below this message, there is a button labeled 'Crear repositorio' and other buttons for 'Ver comandos de envío', 'Eliminar', and 'Acciones'.

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/

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.

 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:

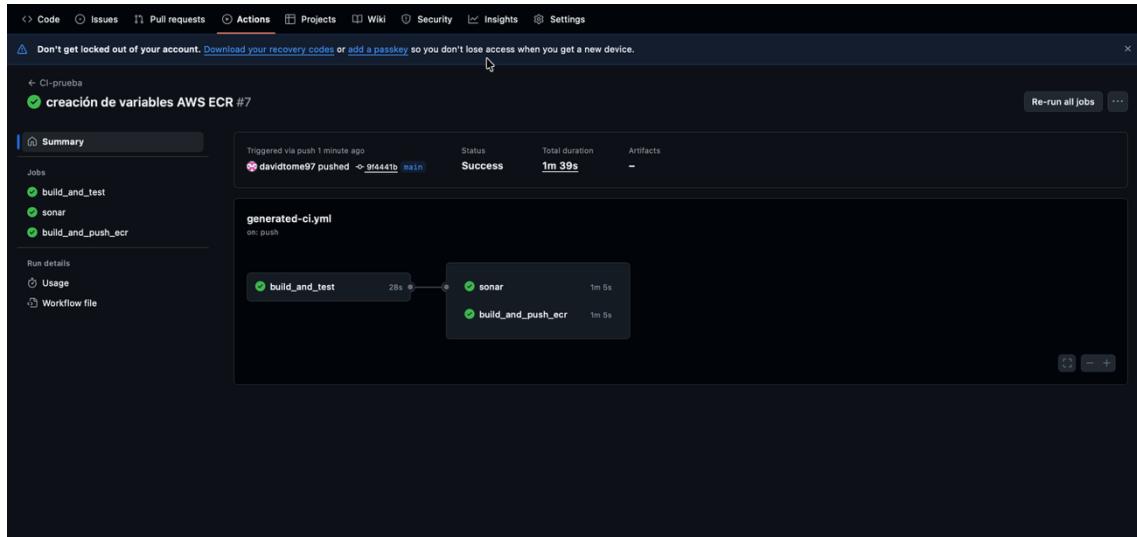
- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_REGION = eu-west-1
- AWS_ACCOUNT_ID = 490145258703
- ECR_REPOSITORY = tfg-cicd-prueba1-ecr

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"

