

# CI/CD

En esta guía se explican algunas de las características y ventajas de GitHub Actions, por ejemplo, la CI/CD. Se trata de una combinación de dos prácticas comunes en el desarrollo de *software*: la **integración continua** (CI) y la **distribución o entrega continua** (CD).

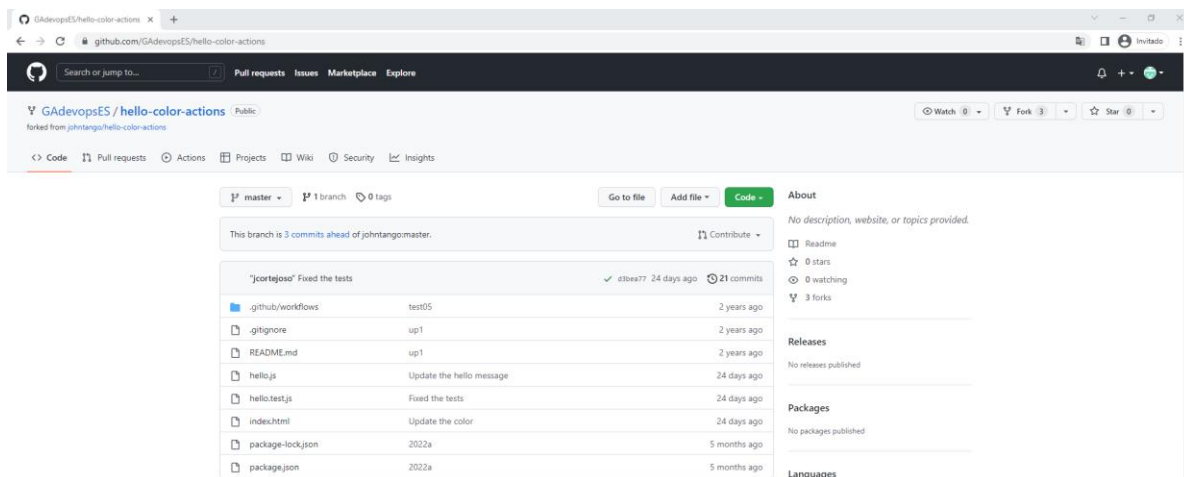
## Cambiar los colores de una página web con GitHub Actions

En esta actividad vamos a establecer una canalización de CI/CD a través de [GitHub Actions](#).

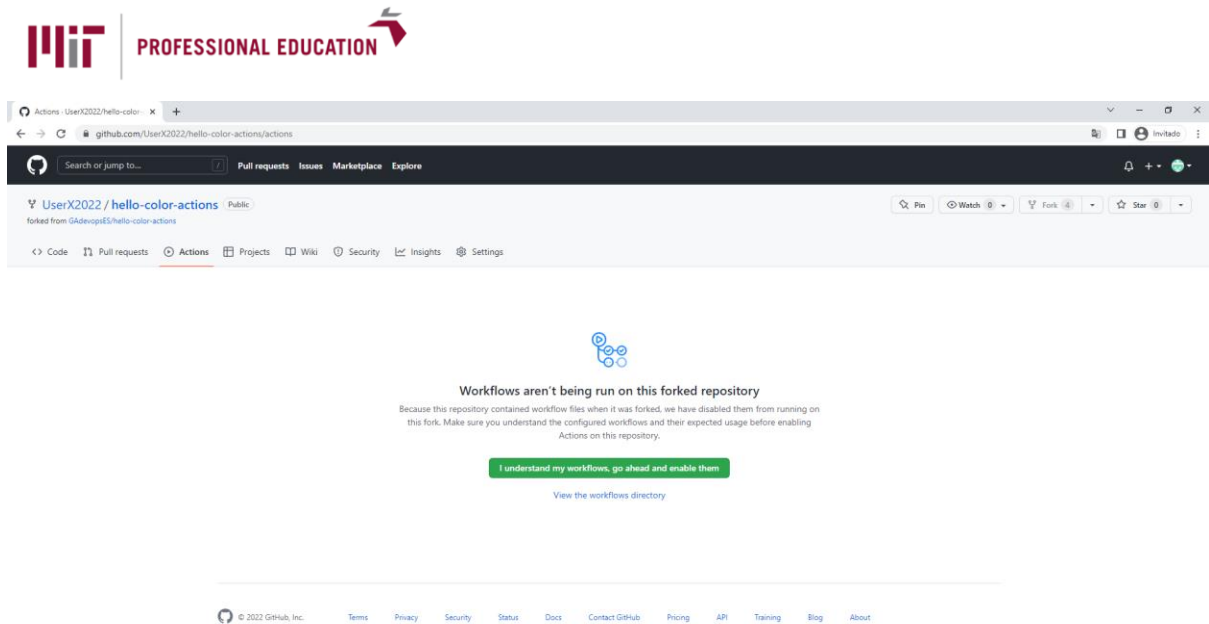
### Hacer una bifurcación del repositorio y activar GitHub Actions

En primer lugar, es necesario crear una bifurcación de [este repositorio](#). El concepto de bifurcación (en inglés "fork") significa copiar un repositorio a nuestra cuenta de Git. Es una forma habitual de colaborar con otras personas sin dejar de gestionar el acceso a los repositorios de Git.

Para crear la bifurcación en GitHub, primero vaya a la página del repositorio y haga clic en el botón "Fork". Seleccione su usuario si fuera necesario.



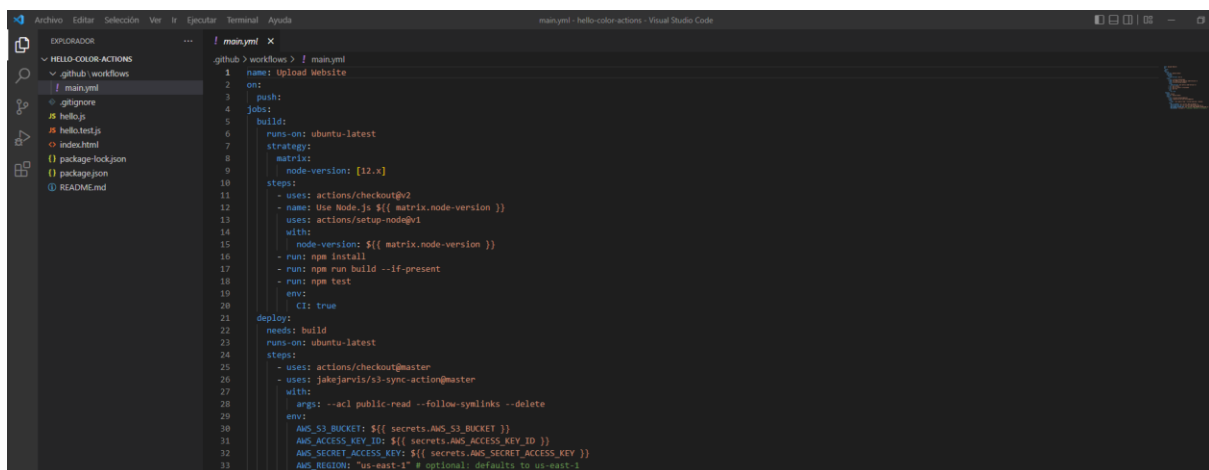
Una vez creada la bifurcación, diríjase al repositorio en GitHub. Vaya a la pestaña "Actions" y haga clic en "I understand my workflows, go ahead and enable them":



## Revisar el código

Ahora clone en Visual Studio Code el repositorio para el que hemos creado la bifurcación y ábralo. Repasemos los archivos que están en el repositorio:

- index.html: un archivo HTML para una página web. Esta página web incluye algo de código en JavaScript.
- hello.js: un archivo JavaScript que muestra el texto "Hello World" en pantalla.
- hello.test.js: un archivo JavaScript que comprueba el correcto funcionamiento del archivo hello.js.
- .GitHub\workflows\main.yml: un archivo YAML que representa nuestro flujo de trabajo de GitHub Actions con la canalización de CI/CD.



Veamos la configuración de este flujo de trabajo:

```
on:
  push:
```

Esta parte establece el momento en que se activa el flujo de trabajo. En este caso, el flujo de trabajo se ejecutará con cada evento *push* del repositorio.

```
jobs:
  build:
  deploy:
```

A este flujo de trabajo le corresponden dos *jobs* (en español, "trabajos" o "funciones"): *build* (que representa la parte de integración continua) y *deploy* (la parte de distribución continua).

```
build:
  runs-on: ubuntu-latest
  strategy:
    matrix:
      node-version: [12.x]
  steps:
    - uses: actions/checkout@v2
    - name: Use Node.js ${{ matrix.node-version }}
      uses: actions/setup-node@v1
      with:
        node-version: ${{ matrix.node-version }}
    - run: npm install
    - run: npm run build --if-present
    - run: npm test
  env:
    CI: true
```

Estos son los datos de la tarea de *build*. Hemos especificado el entorno en el que se ejecutará (la última versión de Ubuntu, "ubuntu-latest"), la versión que se usará de NodeJS (12.x) y los pasos de ejecución de este *job*. Estos pasos incluyen la descarga del código Git, la configuración de NodeJS, la creación de nuestro proyecto y la comprobación de que todo funciona correctamente.

```
deploy:
  needs: build
  runs-on: ubuntu-latest
  steps:
    - uses: actions/checkout@master
    - uses: jakejarvis/s3-sync-action@master
      with:
        args: --acl public-read --follow-symlinks --delete
  env:
    AWS_S3_BUCKET: ${ secrets.AWS_S3_BUCKET }
    AWS_ACCESS_KEY_ID: ${ secrets.AWS_ACCESS_KEY_ID }
    AWS_SECRET_ACCESS_KEY: ${ secrets.AWS_SECRET_ACCESS_KEY }
    AWS_REGION: "us-east-1" # optional: defaults to us-east-1
```

Por último, veamos el *deploy job*. Necesitaremos establecer una dependencia durante la fase de *build*. Si la fase de *build* falla, la fase de *deploy* no se ejecutará. Usaremos la siguiente acción de GitHub: `jakejarvis/S3-sync-action@master` para desplegar el código en Amazon Web Services (AWS) S3.

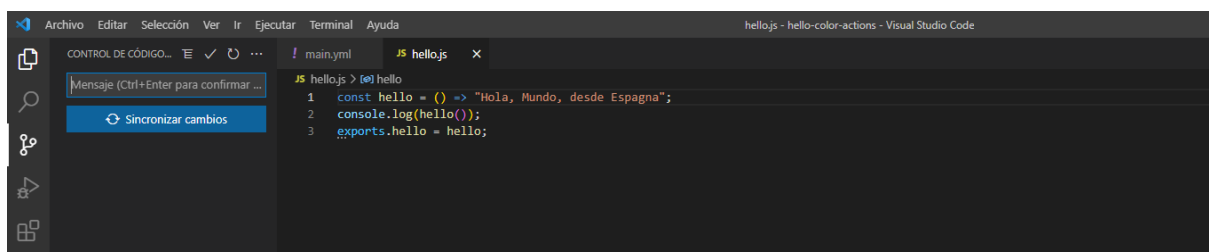
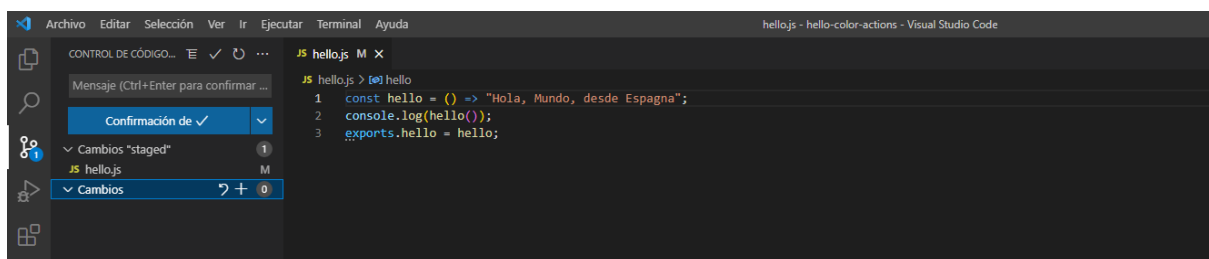
Fíjese en que este *job* necesita más información sobre las variables para poder dar acceso a AWS. Estas variables deben introducirse en GitHub Actions, en los *secrets*, en los ajustes de los repositorios. Más adelante, aprenderemos a hacerlo.

## Modificar el código

Ahora realizaremos algunos cambios en el código para confirmar que el sistema CI/CD funciona. Edite el archivo `hello.js` y modifique el mensaje "Hello World" e introduzca, por ejemplo, "Hola, Mundo, desde España" (aunque puede añadir lo que desee):



Guarde los cambios, vaya a "Control de código fuente", haga clic en "Confirmación", y envíe los cambios a GitHub a través del comando "push":



Ahora si vuelve a la pestaña de "Actions", en el repositorio bifurcado verá si el flujo de trabajo funciona correctamente o si ha fallado:

Workflow run deleted successfully.

UserX2022 / hello-color-actions Public  
forked from GAdavopsES/hello-color-actions

Code Pull requests Actions Projects Wiki Security Insights Settings

Workflows [New workflow](#)  
[All workflows](#)  
[Upload workflow](#)

All workflows  
Showing runs from all workflows

Filter workflow runs

1 workflow run	Event	Status	Branch	Actor
<b>Commit</b> Upload Website #2: Commit e401a5b pushed by UserX2022	master	Failure	3 minutes ago	35s

Para descubrir qué ha fallado, haga clic en el flujo de trabajo y luego en el *build job* fallido. Si hace clic en el texto que está al lado de las equis rojas se mostrará el registro.

Commit Upload Website #2

Summary

Jobs

- build (12.x)
- deploy

Triggered via push 3 minutes ago  
UserX2022 pushed e401a5b master

Status: Failure Total duration: 35s Artifacts: -

main.yml  
on: push

Matrix: build

1 job completed  
Show all jobs

Annotations  
1 error

build (12.x)  
Process completed with exit code 1.

Commit Upload Website #2

Summary

Jobs

- build (12.x)
- deploy

build (12.x)  
Failed 4 minutes ago in 26s

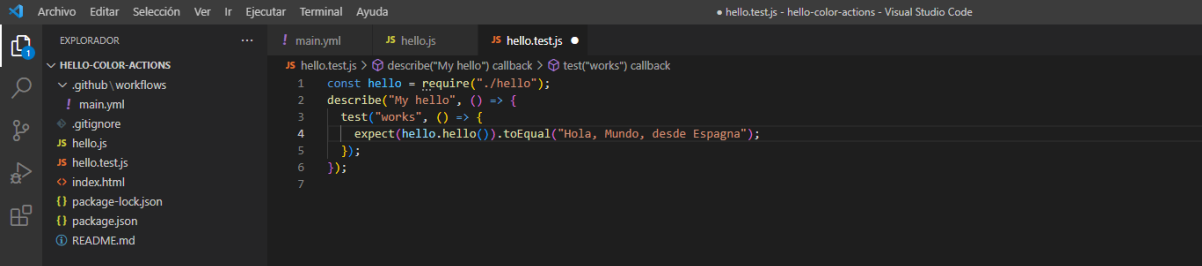
Search logs

```

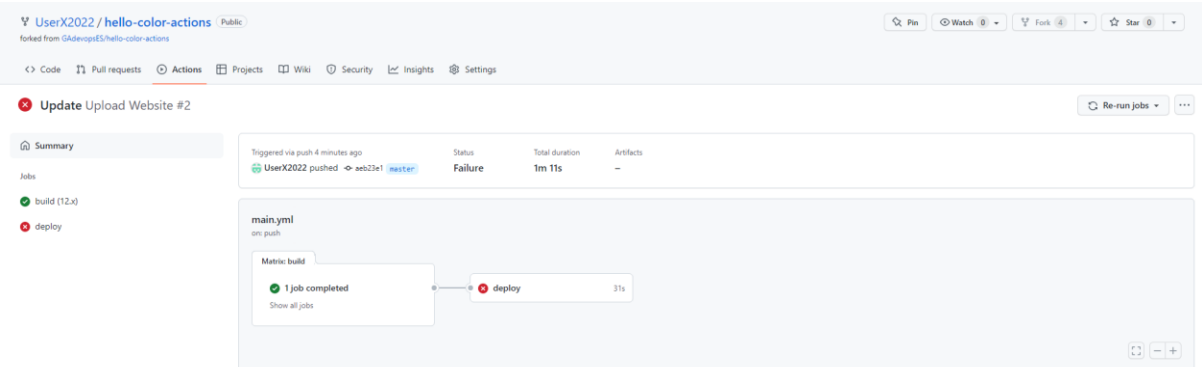
> Set up job
> Run actions/checkout@v2
> Use Node.js 12.x
> Run npm install
> Run npm run build --if-present
> Run npm test
1 Run npm test
2
3 > hello1.0.0 test /home/runner/work/hello-color-actions/hello-color-actions
4 > jest
5
6 FAIL ./hello.test.js
7   My hello
8     ✕ works (7 ms)
9
10   My hello > works
11     expect(received).toEqual(expected) // deep equality
12
13     Expected: "Hello World from Spain"
14     Received: "Hola, Mundo, desde España"
15
16   2 | describe("My hello", () => {
17     3 |   test("works", () => {
18       4 |     expect(hello.hello()).toEqual("Hello World from Spain");
19         ^
20     5 |   });
21     6 | });
22     7 |
23   at Object.canonicalize (hello.test.js:4:27)
  
```

Arreglar el código

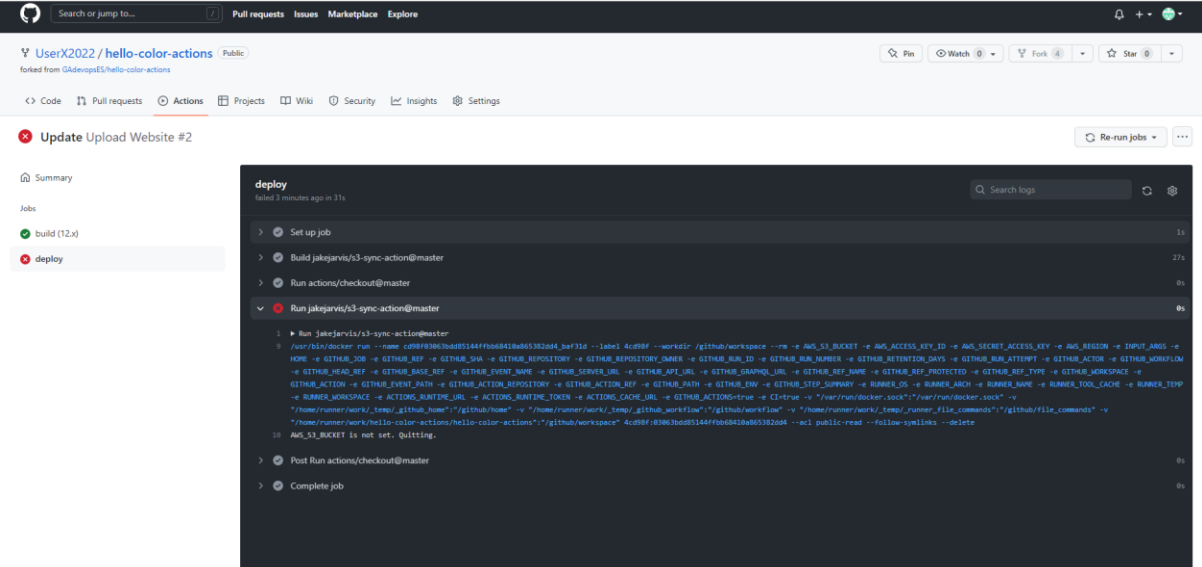
Podemos ver el error en la fase de prueba. Parece que el test está esperando a que llegue el mensaje "Hello World", pero lo hemos actualizado a "Hola, Mundo, desde España". Así que actualicemos el archivo `hello.test.js` con el nuevo mensaje:



Guarde, haga clic en "Confirmar" y sincronice los cambios. Después, compruebe de nuevo si el flujo de trabajo funciona:



Como se puede apreciar, el *build job* se ejecutó correctamente, pero el *deploy job* falló porque no le proporcionamos los *secrets* de AWS necesarios para un funcionamiento adecuado. En la siguiente sección arreglaremos este problema.



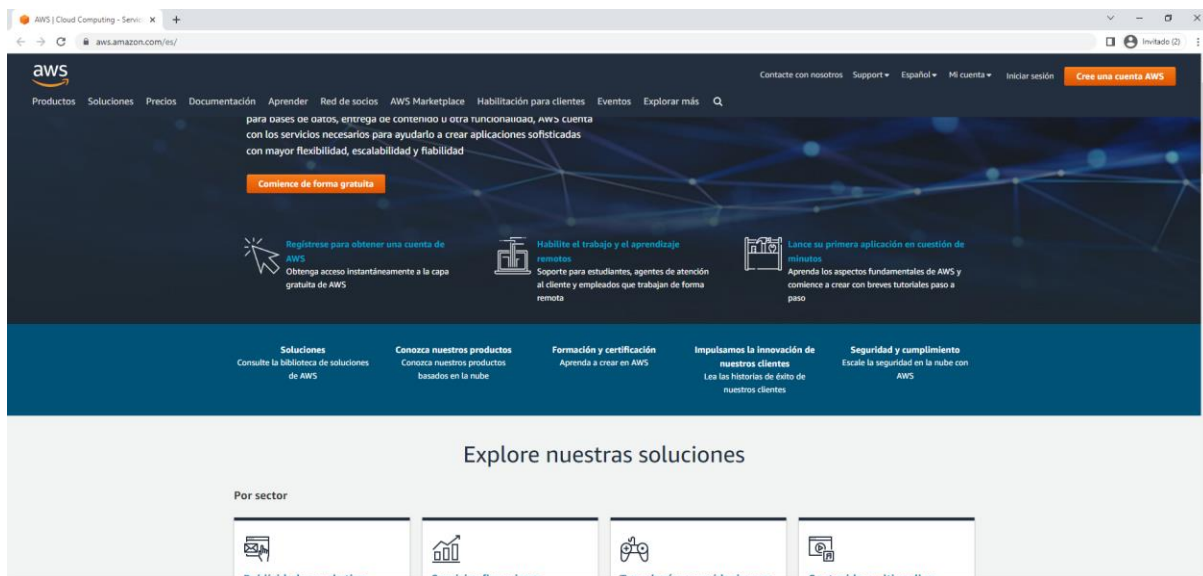
# El papel de las claves en la canalización

El *deploy job* necesita acceso a AWS S3 para que el proyecto pueda ser desplegado automáticamente durante la fase de distribución (CD). Lo primero que hay que hacer es crear una cuenta de AWS y unas credenciales que nos permitan acceder desde nuestro flujo de trabajo.

## Crear una cuenta AWS y un bucket de AWS

Si ya tiene una cuenta de AWS, inicie sesión [aquí](#).

Si no la tiene, vaya a la página de [Web Services](#) de AWS y haga clic en "Cree una cuenta AWS".



## Crear un bucket de AWS

[S3](#) es el servicio de almacenamiento en la nube escalable de Amazon Web Services. Un "bucket" es un contenedor de objetos (archivos) que están almacenados en S3. Los bucket son globales y únicos, por lo que deben tener un nombre único dentro de toda la red de AWS.

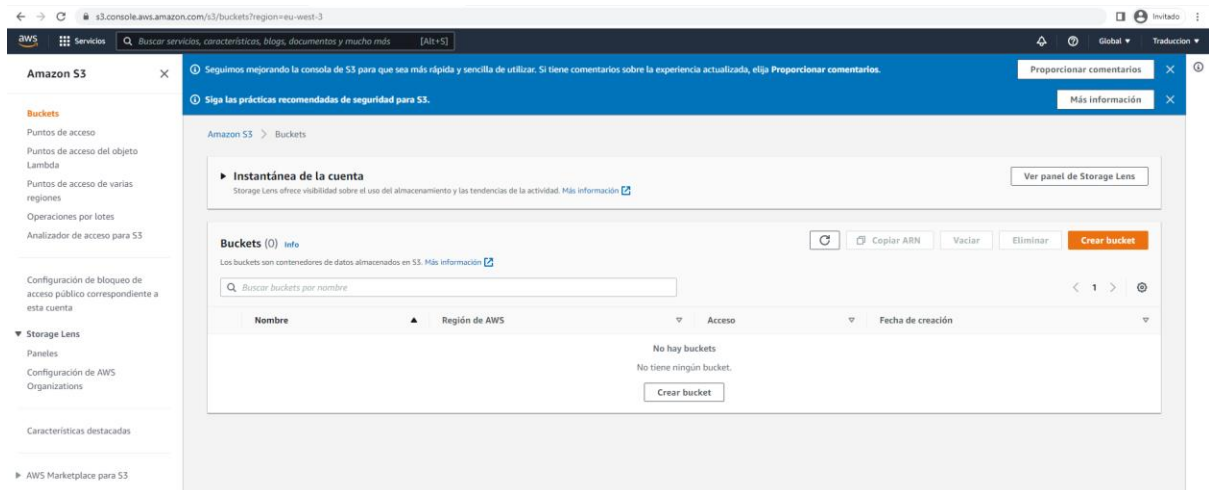
Cuando entre en la consola de AWS, vaya a la [página de servicio de S3](#) para crear un nuevo bucket. Este nuevo bucket:

- Tendrá un nombre único dentro de AWS y podrá añadirle su nombre, números, etc. Tenga en cuenta que los caracteres especiales y las mayúsculas no están permitidos. Dado que este nombre será público, le recomendamos que no incluya sus datos personales en él.

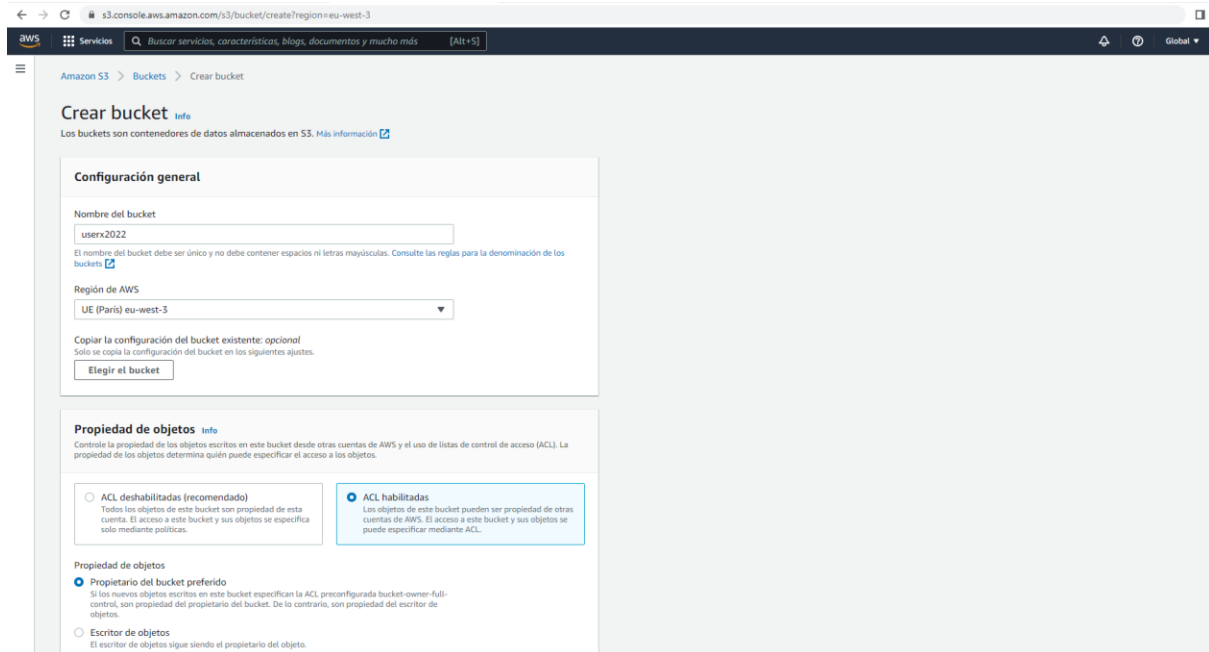
- Se configurará para ser leído por cualquier persona en internet, ya que se utilizará para almacenar nuestra página web.

Le recomendamos que elimine el bucket tras finalizar esta actividad.

Haga clic en "Crear bucket":



Ahora asígnele un nombre único al bucket, active las ACL (siglas de "access control lists", "listas de control de acceso") y permita el acceso público. Haga clic en "Crear bucket" para completar el proceso:





← → ↻ s3.console.aws.amazon.com/s3/bucket/create?region=eu-west-3

**WSS** Servicios  [Alt+S]

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)

☐ **Bloquear todo el acceso público**  
Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

☐ **Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)**  
S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y ventilará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.

☐ **Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)**  
S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.

☐ **Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas**  
S3 bloqueará las nuevas políticas de buckets y puntos de acceso que conceden acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.

☐ **Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública**  
S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.

**⚠ Desactivar el bloqueo de todo acceso público puede provocar que este bucket y los objetos que contiene se vuelvan públicos**  
AWS recomienda que active la opción para bloquear todo el acceso público, a menos que se requiera acceso público para casos de uso específicos y verificados, como el alojamiento de sitios web estáticos.

☐ Reconozco que la configuración actual puede provocar que este bucket y los objetos que contiene se vuelvan públicos.

**⚠ Debe seleccionar la casilla de verificación para seguir creando el bucket.**

← → ↻ s3.console.aws.amazon.com/s3/bucket/create?region=eu-west-3

**WSS** Servicios  [Alt+S]

Control de versiones de buckets

El control de versiones es una forma de mantener múltiples variantes de un objeto dentro del mismo bucket. Puede utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. Con el control de versiones, puede recuperarse con facilidad de las acciones involuntarias de los usuarios y de los errores en las aplicaciones. [Más información](#)

Control de versiones de buckets

☒ Desactivar

☐ Habilitar

**Etiquetas (0) - opcional**

Para realizar un seguimiento del costo del almacenamiento u otros criterios, etiquete el bucket. [Más información](#)

No hay etiquetas asociadas a este bucket.

**Cifrado predeterminado**

Cifre automáticamente los nuevos objetos almacenados en este bucket. [Más información](#)

Cifrado del lado del servidor

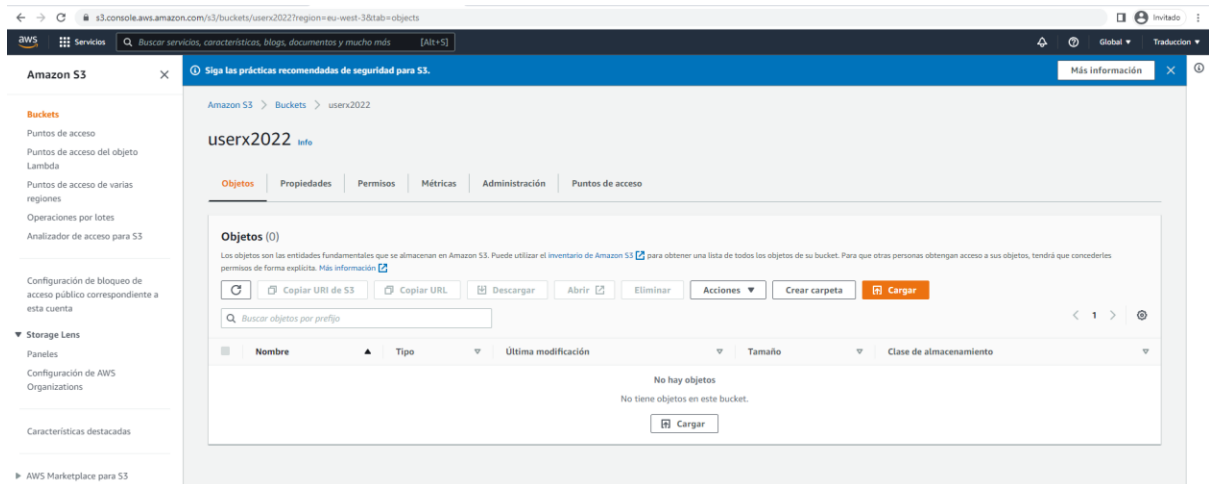
☒ Desactivar

☐ Habilitar

► Configuración avanzada

ⓘ Después de crear el bucket, puede cargar archivos y carpetas en el bucket y configurar ajustes adicionales del bucket.

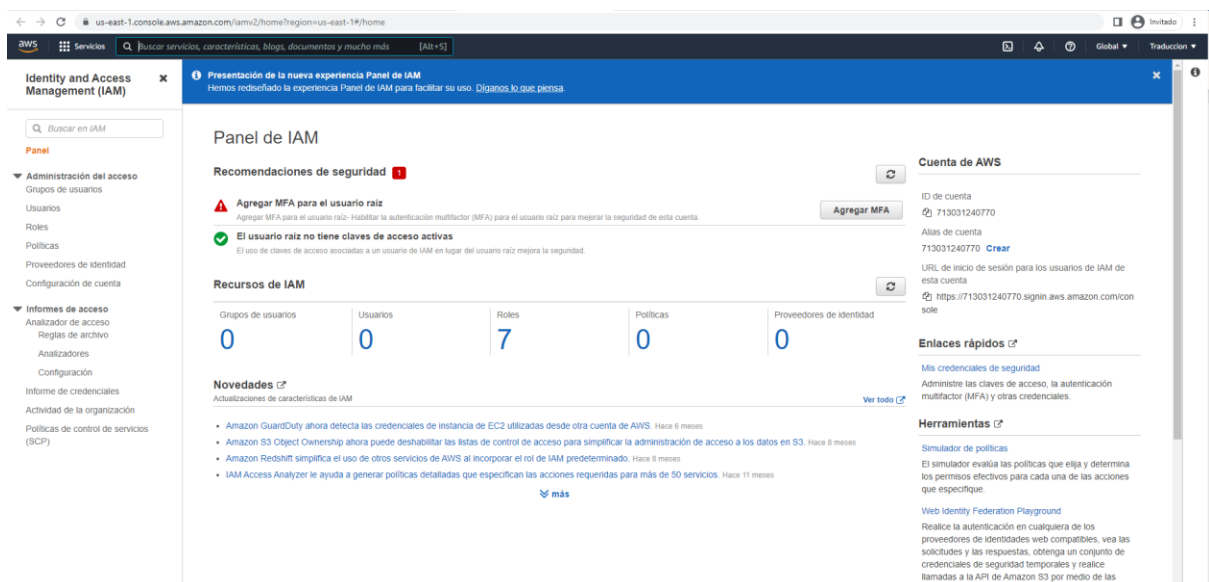
Así, hemos creado el bucket:



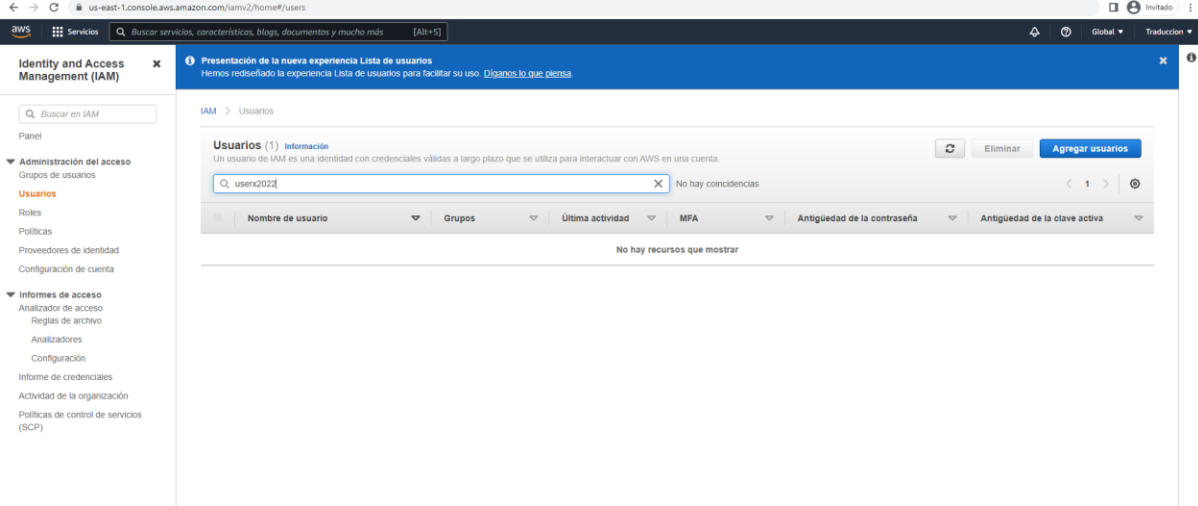
## Crear un usuario de IAM para la actividad

Es necesario crear una cuenta nueva y configurar las credenciales de acceso de AWS para ajustar nuestro GitHub Actions a ellas. IAM (Identity and Access Management) es un servicio que permite configurar el control del acceso a todos los servicios y recursos de AWS.

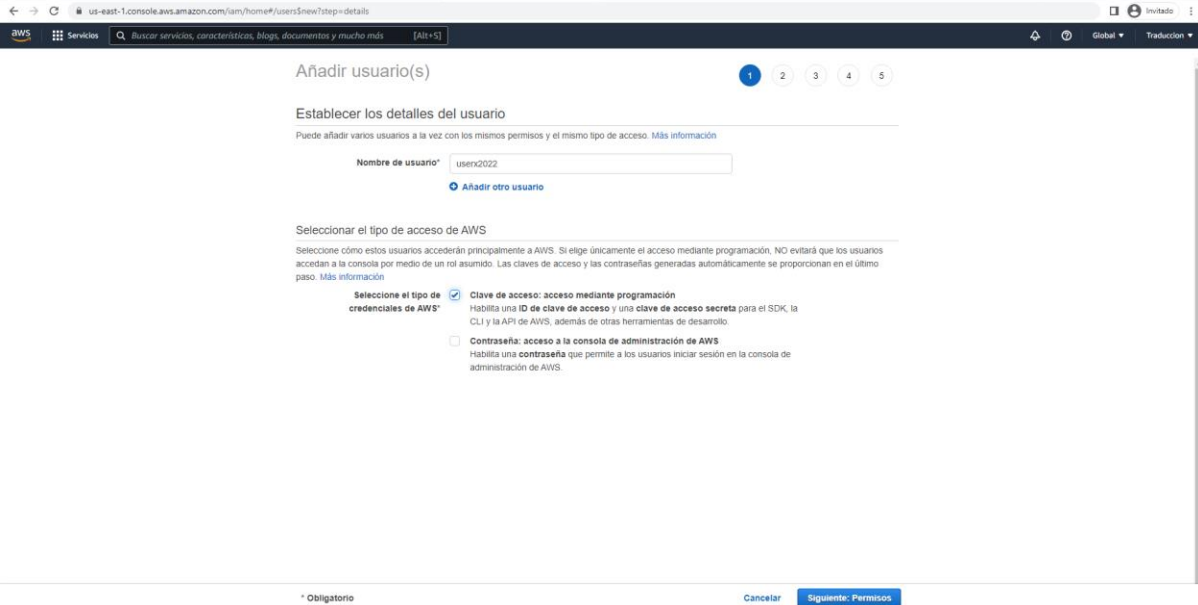
Vaya a la [AWS S3](#).



Entre en "Usuarios", en el menú izquierdo, y seleccione "Añadir usuarios":



La acción de GitHub utilizará el usuario que hemos creado, por lo que es necesario otorgarle, como veremos, un "acceso programático":



También necesita acceso para poder cargar los archivos al bucket de S3 que acabamos de crear. Para ello, añada la política "AmazonS3FullAccess" ya existente:

us-east-1.console.aws.amazon.com/iam/home#/users/new?step=review&accessKeyUserNames=uxenx2022&permissionType=policies&policies=arn:aws:iam::aws:policy%3FAmazonS3FullAccess

Añadir usuario(s)

1 2 3 4 5

### Revisar

Revise las opciones que ha elegido. Después de crear el usuario, puede ver y descargar la contraseña y la clave de acceso generadas automáticamente.

#### Detalles del usuario

<b>Nombre de usuario</b>	uxenx2022
<b>Tipo de acceso de AWS</b>	Acceso mediante programación: con una clave de acceso
<b>Límite de permisos</b>	No se ha establecido un límite de permisos

#### Resumen de permisos

Las políticas siguientes se asociarán al usuario que se muestra más arriba.

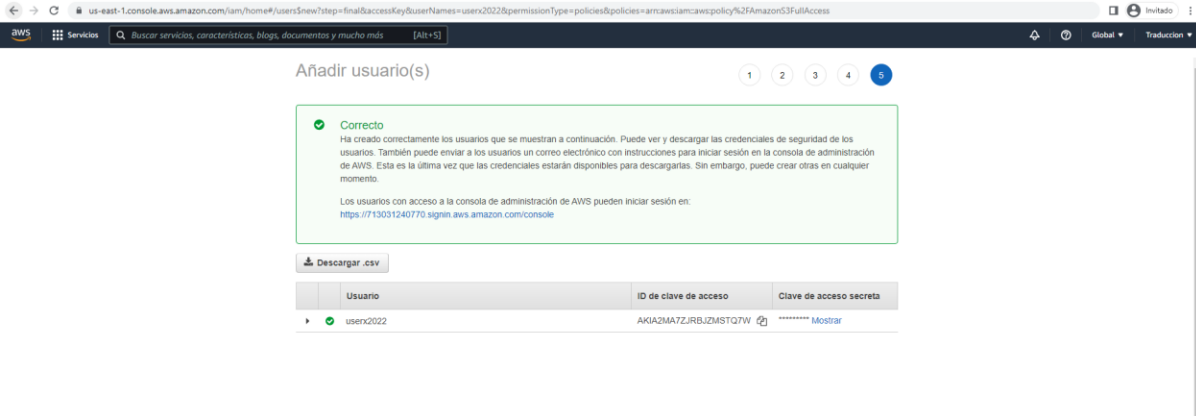
Tipo	Nombre
Política administrada	<a href="#">AmazonS3FullAccess</a>

#### Etiquetas

No se han añadido etiquetas.

Cancelar Anterior **Crear un usuario**

Cree el usuario y guárdelo a buen recaudo tanto el ID de clave de acceso como la clave de acceso secreta. Recuerde que debe hacer clic en "Mostrar" para guardar la clave correcta, y no el valor oculto ("\*\*\*\*\*"). Estos valores son secretos y no deben compartirse, considérellos contraseñas.



Añadir usuario(s)

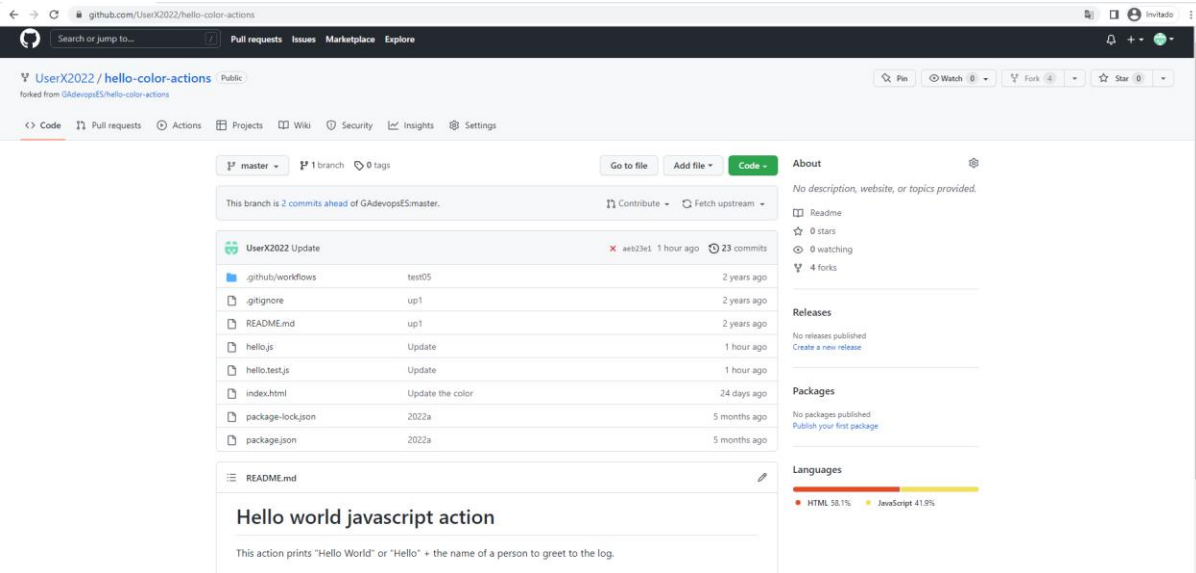
**Correcto**  
Ha creado correctamente los usuarios que se muestran a continuación. Puede ver y descargar las credenciales de seguridad de los usuarios. También puede enviar a los usuarios un correo electrónico con instrucciones para iniciar sesión en la consola de administración de AWS. Esta es la última vez que las credenciales estarán disponibles para descargarlas. Sin embargo, puede crear otras en cualquier momento.  
Los usuarios con acceso a la consola de administración de AWS pueden iniciar sesión en:  
<https://713031240770.signin.aws.amazon.com/console>

Descargar .csv

Usuario	ID de clave de acceso	Clave de acceso secreta
userx2022	AKIAZMATZJRBZJMSTQ7W	*****Mostrar

## Configure su repositorio de GitHub con los parámetros de AWS

Ahora disponemos de los parámetros necesarios para configurar los *secrets* que antes nos hacían falta en nuestro repositorio de GitHub. Vuelva a la pestaña de "Settings" de su repositorio de GitHub bifurcado:



github.com/UserX2022/hello-color-actions

UserX2022 / hello-color-actions Public

This branch is 2 commits ahead of G4devops5/master.

Go to file Add file Code About

Contribute Fetch upstream

UserX2022 Update x 4623e1 1 hour ago 23 commits

- .github/workflows test05 2 years ago
- .gitignore up1 2 years ago
- README.md up1 2 years ago
- hello.js Update 1 hour ago
- hello.test.js Update 1 hour ago
- index.html Update the color 24 days ago
- package-lock.json 2022a 5 months ago
- package.json 2022a 5 months ago

README.md

### Hello world javascript action

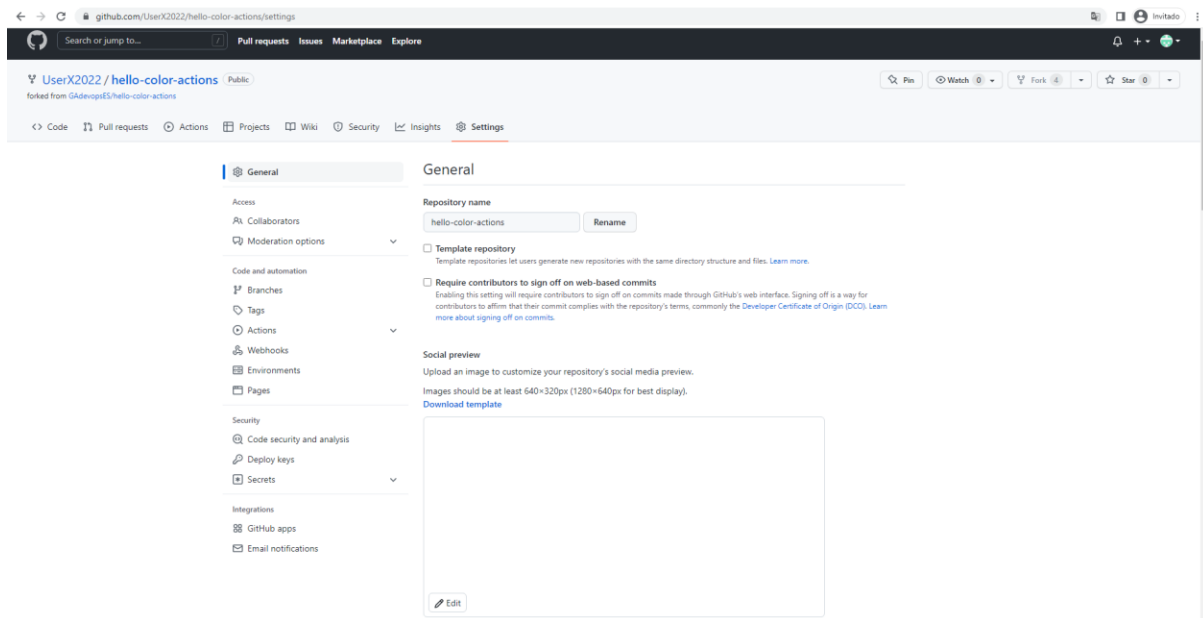
This action prints "Hello World" or "Hello" + the name of a person to greet to the log.

About: No description, website, or topics provided.

Releases: No releases published. Create a new release.

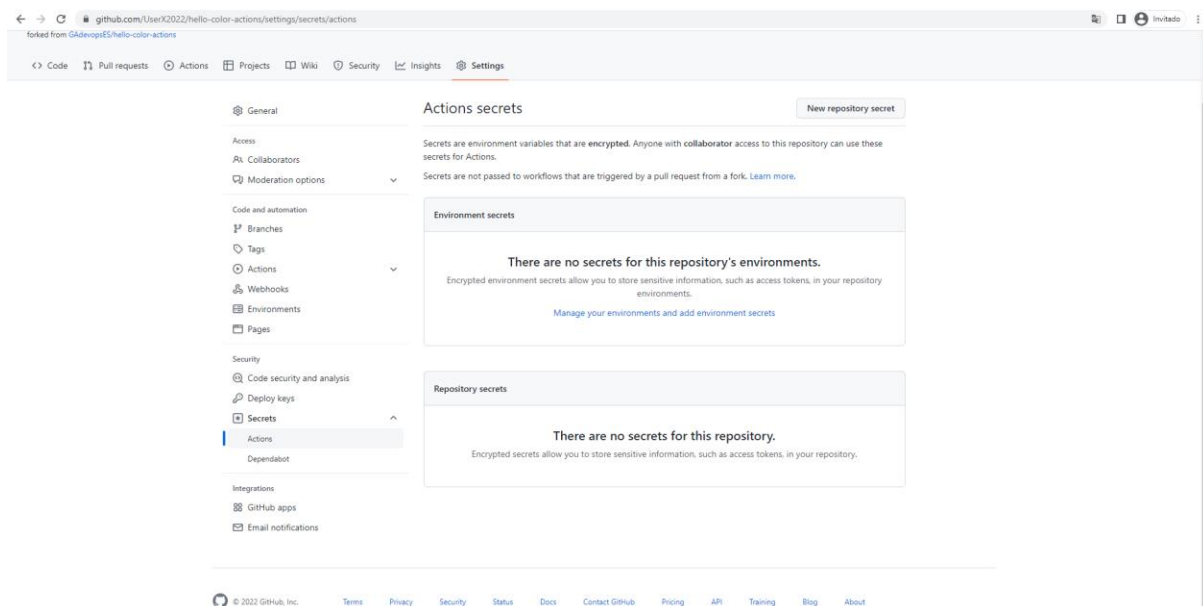
Packages: No packages published. Publish your first package.

Languages: HTML 58.1%, JavaScript 41.9%



The screenshot shows the GitHub repository settings page for 'UserX2022 / hello-color-actions'. The left sidebar contains a menu with categories: General, Access, Code and automation, Security, and Integrations. The 'Settings' tab is selected. The main content area is titled 'General' and includes sections for Repository name, Template repository, Require contributors to sign off on web-based commits, Social preview, and a large empty box for a social media preview image with an 'Edit' button.

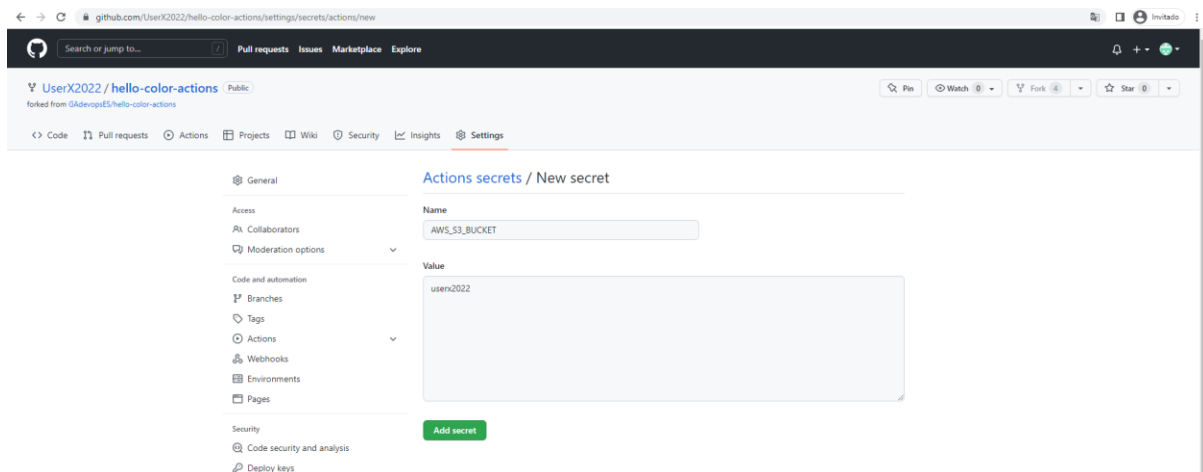
En el menú de la izquierda, haga clic en "Secrets", "Actions", y "New repository secret":



The screenshot shows the GitHub repository settings page for 'UserX2022 / hello-color-actions' with the 'Secrets' tab selected in the left sidebar. The main content area is titled 'Actions secrets' and includes a 'New repository secret' button. It contains two sections: 'Environment secrets' and 'Repository secrets', both of which currently show 'There are no secrets for this repository's environments' and 'There are no secrets for this repository.' respectively, with links to manage or add secrets.

Aquí debemos añadir los siguientes secretos:

1. **AWS\_S3\_BUCKET**: El nombre del bucket que hemos creado.



The screenshot shows the GitHub Actions secrets page for the repository 'UserX2022/hello-color-actions'. The 'Actions secrets / New secret' form is displayed. The 'Name' field is filled with 'AWS\_S3\_BUCKET' and the 'Value' field is filled with 'usens2022'. The 'Add secret' button is visible at the bottom right of the form.

Search or jump to... Pull requests Issues Marketplace Explore

UserX2022/hello-color-actions Public

forked from G4devopsES/hello-color-actions

Code Pull requests Actions Projects Wiki Security Insights Settings

General Actions secrets / New secret

Access

Collaborators

Moderation options

Code and automation

Branches

Tags

Actions

Webhooks

Environments

Pages

Security

Code security and analysis

Deploy keys

Name

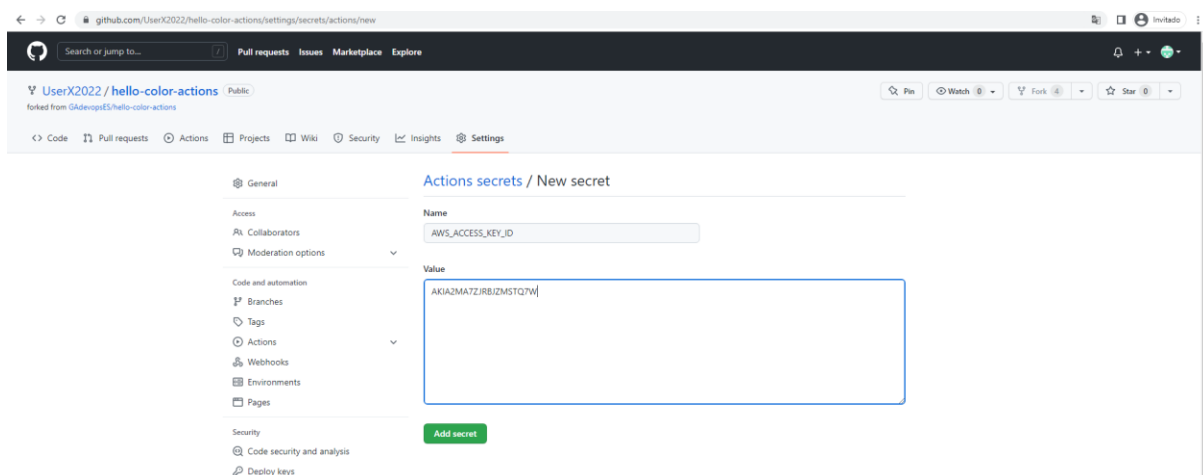
AWS\_S3\_BUCKET

Value

usens2022

Add secret

2. **AWS\_ACCESS\_KEY\_ID**: La ID de clave de acceso para el usuario de IAM que hemos creado.



The screenshot shows the GitHub Actions secrets page for the repository 'UserX2022/hello-color-actions'. The 'Actions secrets / New secret' form is displayed. The 'Name' field is filled with 'AWS\_ACCESS\_KEY\_ID' and the 'Value' field is filled with 'AKIA2MA7ZJRBIZMSTQ7W'. The 'Add secret' button is visible at the bottom right of the form.

Search or jump to... Pull requests Issues Marketplace Explore

UserX2022/hello-color-actions Public

forked from G4devopsES/hello-color-actions

Code Pull requests Actions Projects Wiki Security Insights Settings

General Actions secrets / New secret

Access

Collaborators

Moderation options

Code and automation

Branches

Tags

Actions

Webhooks

Environments

Pages

Security

Code security and analysis

Deploy keys

Name

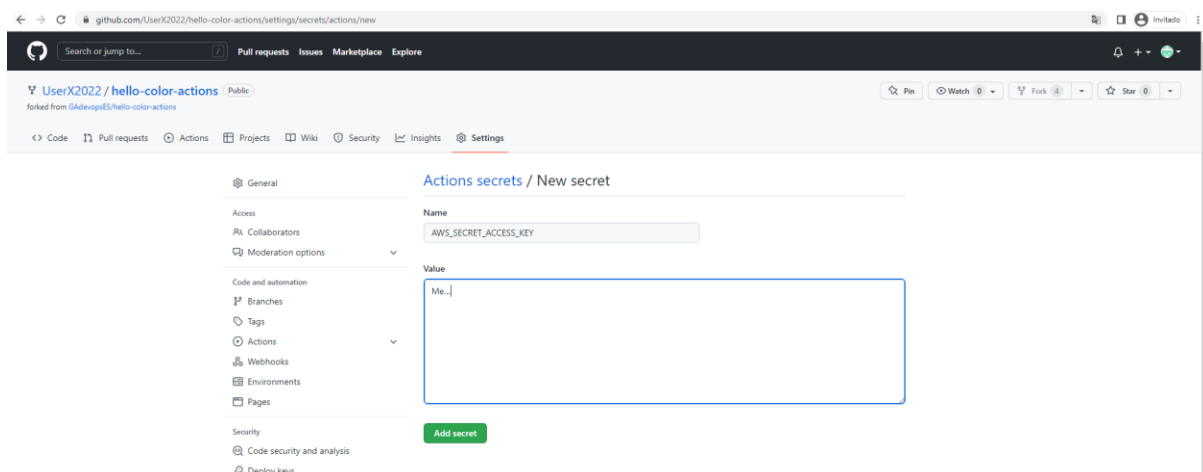
AWS\_ACCESS\_KEY\_ID

Value

AKIA2MA7ZJRBIZMSTQ7W

Add secret

3. **AWS\_SECRET\_ACCESS\_KEY**: La clave de acceso secreta para el usuario de IAM que hemos creado.



The screenshot shows the GitHub Actions secrets page for the repository 'UserX2022/hello-color-actions'. The 'Actions secrets / New secret' form is displayed. The 'Name' field is filled with 'AWS\_SECRET\_ACCESS\_KEY' and the 'Value' field is filled with 'Me...'. The 'Add secret' button is visible at the bottom right of the form.

Search or jump to... Pull requests Issues Marketplace Explore

UserX2022/hello-color-actions Public

forked from G4devopsES/hello-color-actions

Code Pull requests Actions Projects Wiki Security Insights Settings

General Actions secrets / New secret

Access

Collaborators

Moderation options

Code and automation

Branches

Tags

Actions

Webhooks

Environments

Pages

Security

Code security and analysis

Deploy keys

Name

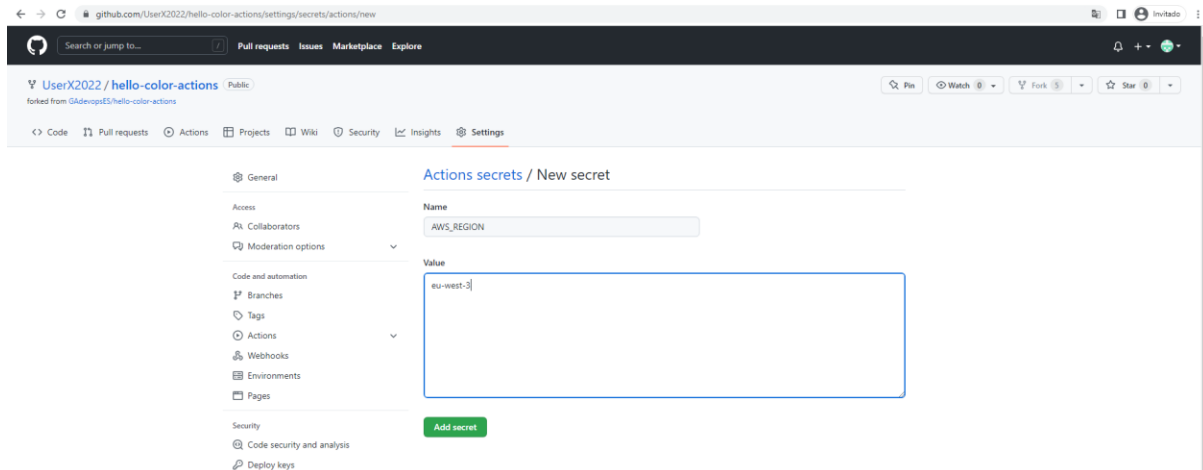
AWS\_SECRET\_ACCESS\_KEY

Value

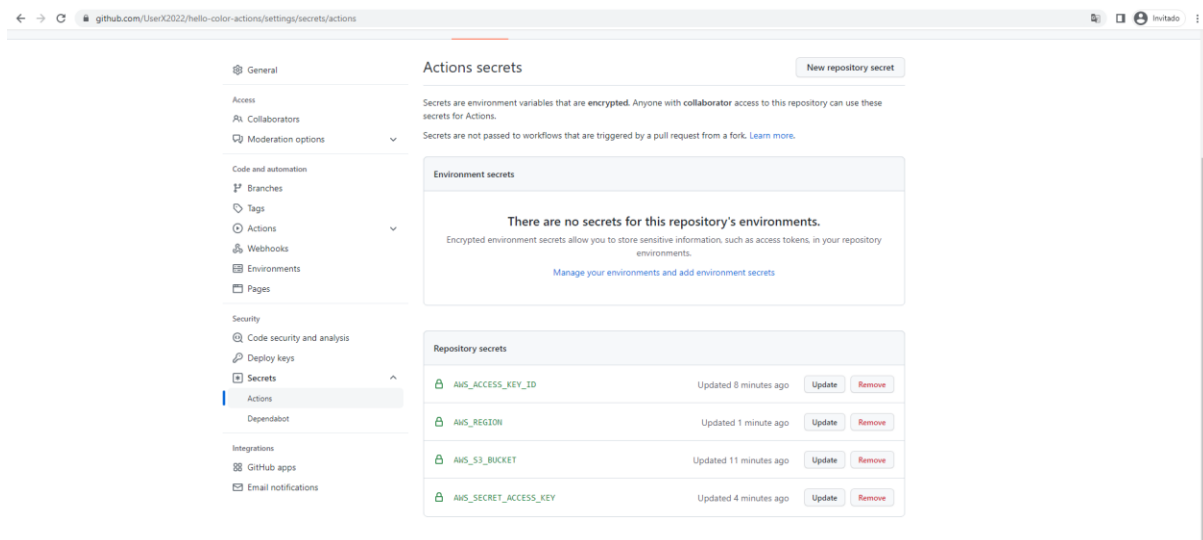
Me...

Add secret

4. **AWS\_REGION**: Seleccione la región de AWS que aparezca en la pestaña "Buckets" de la consola S3. En este caso, "eu-west-3".



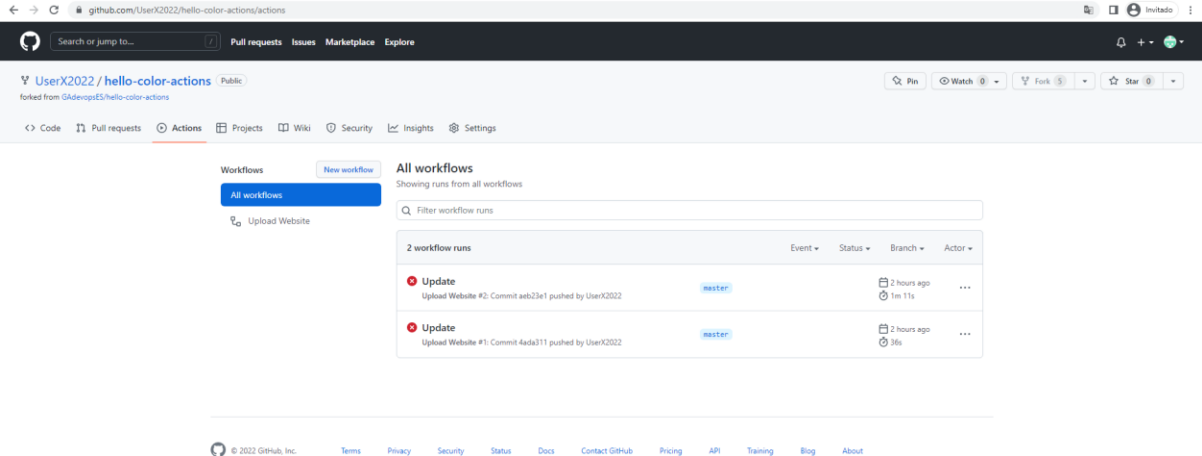
Ahora verá que se han creado los cuatro secretos del repositorio:



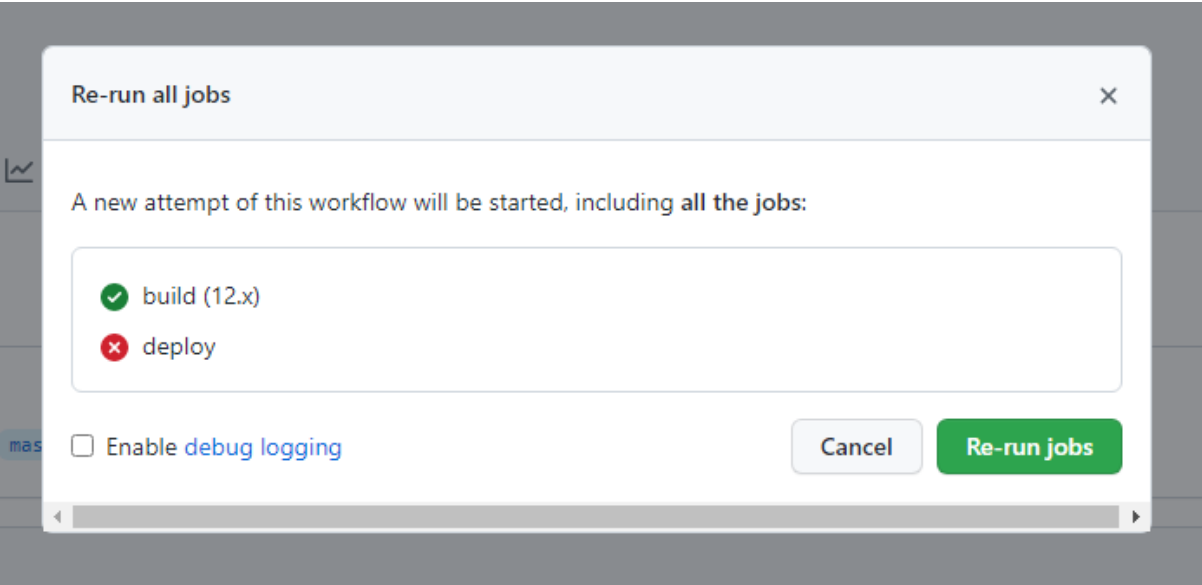
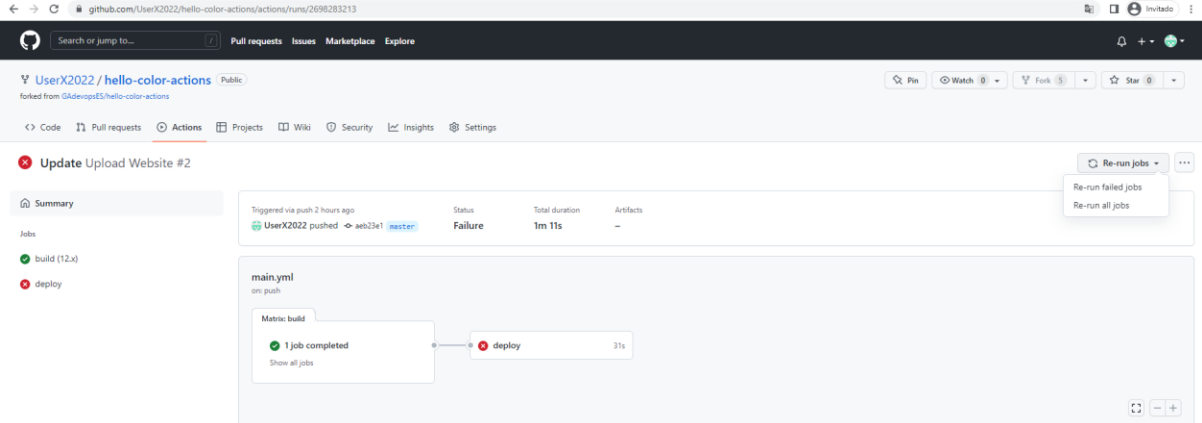
Volver a ejecutar el flujo de trabajo de GitHub

Diríjase a la pestaña "Actions" en el repositorio bifurcado. Verá una lista de las anteriores veces que se ha ejecutado.

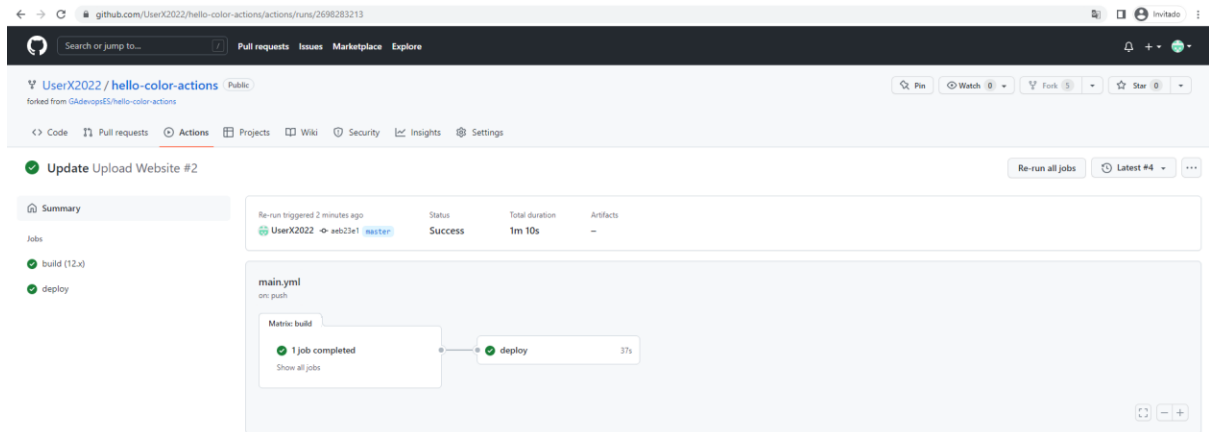




Vaya al último flujo de trabajo. En la página de ejecución puede volver a ejecutar los *jobs*. Haga clic en "Re-run jobs" y después en "Re-run all jobs":



Si todo va según lo previsto, los dos *jobs* del flujo de trabajo deberían ejecutarse correctamente:



Update Upload Website #2

Re-run triggered 2 minutes ago  
UserX2022 @arb23e1 master Success 1m 10s

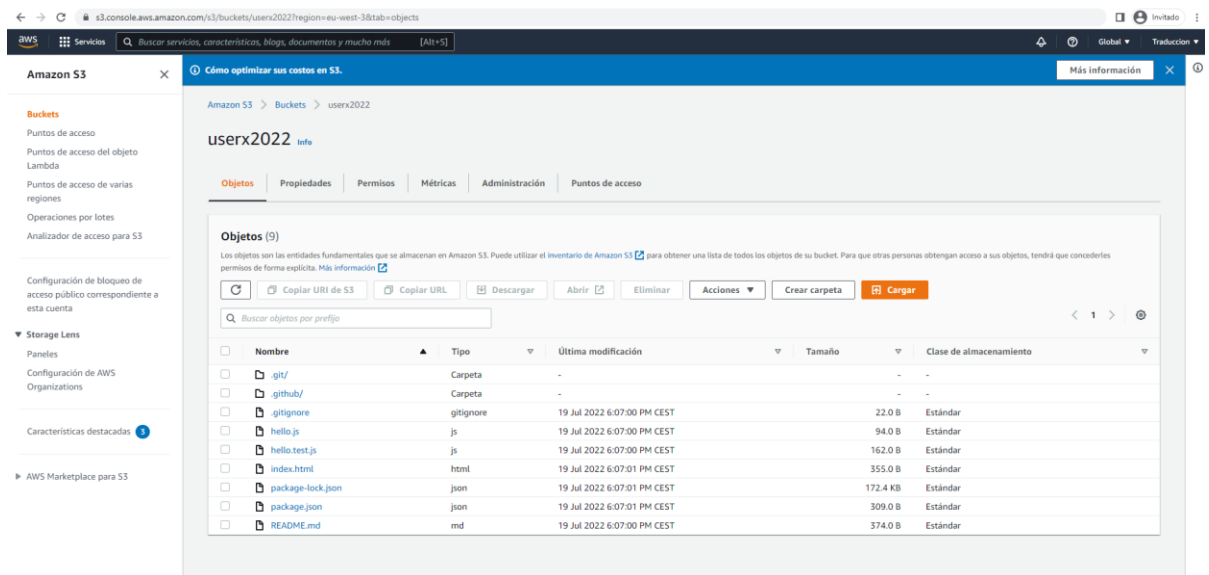
main.yml  
on: push

Matrix build

1 job completed  
Show all jobs

deploy 37s

Si vuelve a su bucket de S3, verá que el *deploy job* (fase de CD) ha desplegado apropiadamente los archivos en el bucket:



Amazon S3

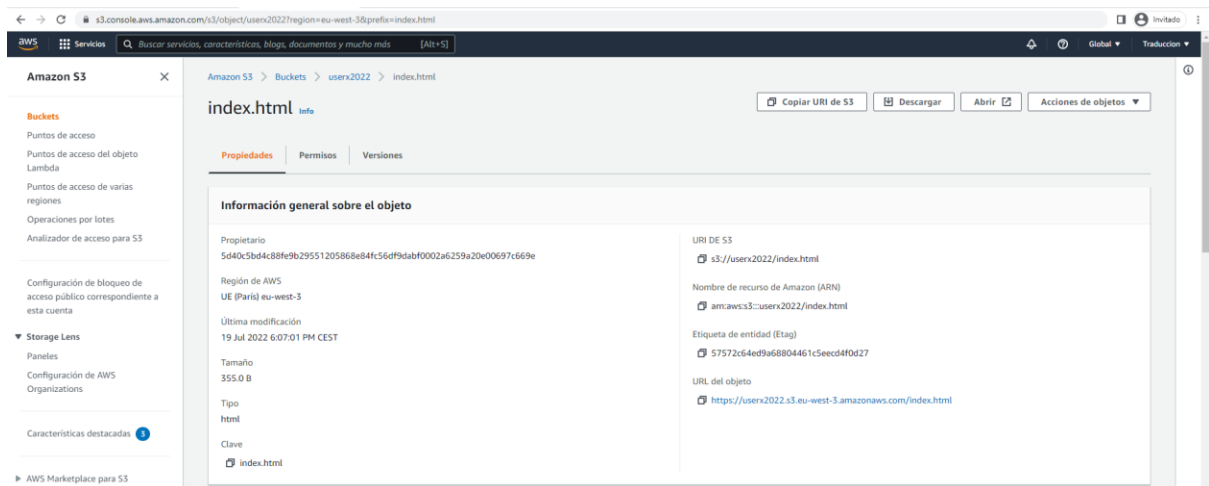
Buckets

userx2022

Objetos (9)

Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
git/	Carpeta	-	-	-
.github/	Carpeta	-	-	-
.gitignore	gitignore	19 Jul 2022 6:07:00 PM CEST	22.0 B	Estándar
hello.js	js	19 Jul 2022 6:07:00 PM CEST	94.0 B	Estándar
hello.test.js	js	19 Jul 2022 6:07:00 PM CEST	162.0 B	Estándar
index.html	html	19 Jul 2022 6:07:01 PM CEST	355.0 B	Estándar
package-lock.json	json	19 Jul 2022 6:07:01 PM CEST	172.4 KB	Estándar
package.json	json	19 Jul 2022 6:07:01 PM CEST	309.0 B	Estándar
README.md	md	19 Jul 2022 6:07:00 PM CEST	374.0 B	Estándar

Haga clic en el archivo `index.html` y después en la URL debajo de "URL de objeto":



index.html

Propiedades

Información general sobre el objeto

Propietario: 5d40c5b4c88fe9b2951205868e84fc56df9dabf0002a6259a20e00697c669e

Región de AWS: UE (Paris) eu-west-3

Última modificación: 19 Jul 2022 6:07:01 PM CEST

Tamaño: 355.0 B

Tipo: html

Clave: index.html

URI DE S3: s3://userx2022/index.html

Nombre de recurso de Amazon (ARN): aws:s3::userx2022/index.html

Etiqueta de entidad (ETag): 57572c64ed9a68804461c5eecd4f0d27

URL del objeto: https://userx2022.s3.eu-west-3.amazonaws.com/index.html

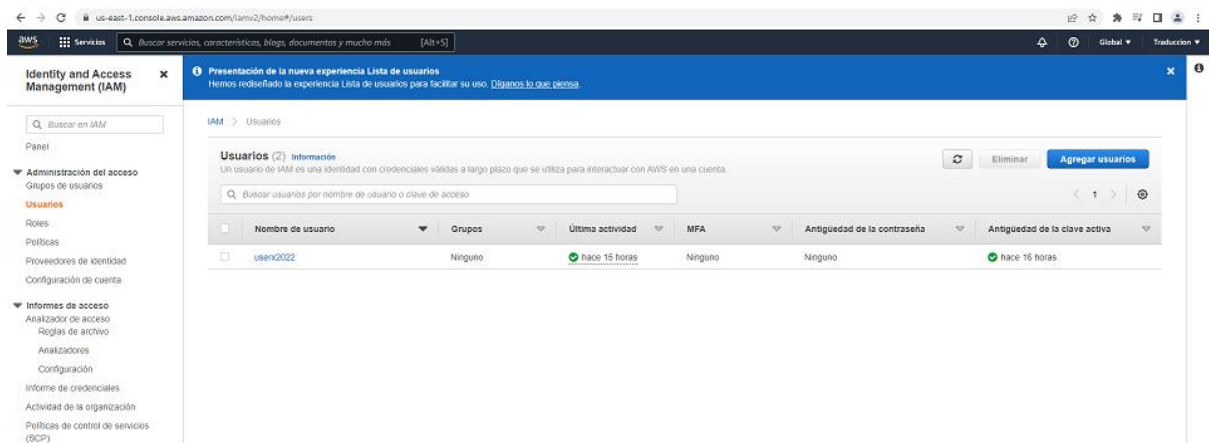


Cada vez que actualice la página se cargará con un fondo de un color distinto:

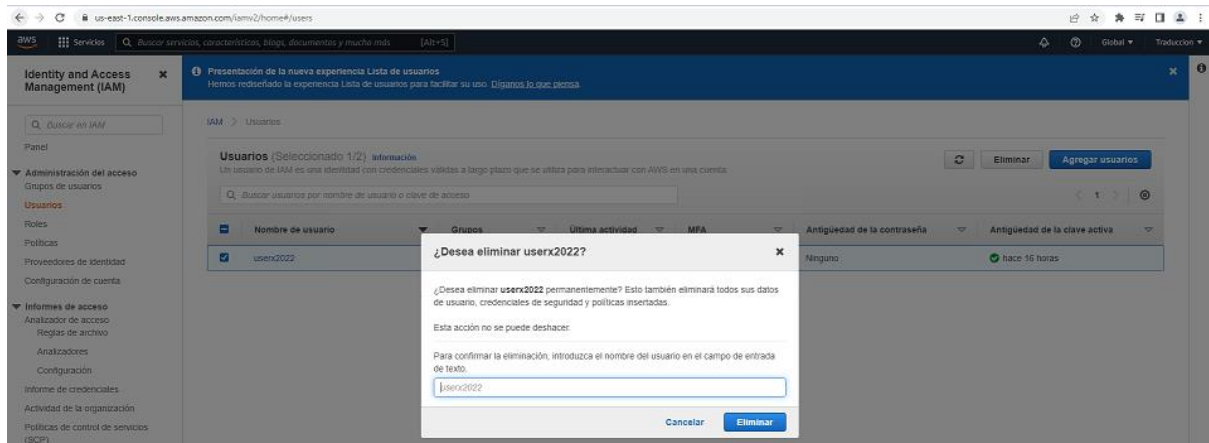


## Borrar la cuenta de IAM

Para borrar la cuenta de IAM, vuelva a [AWS IAM](#) y entre en la página "Usuarios".



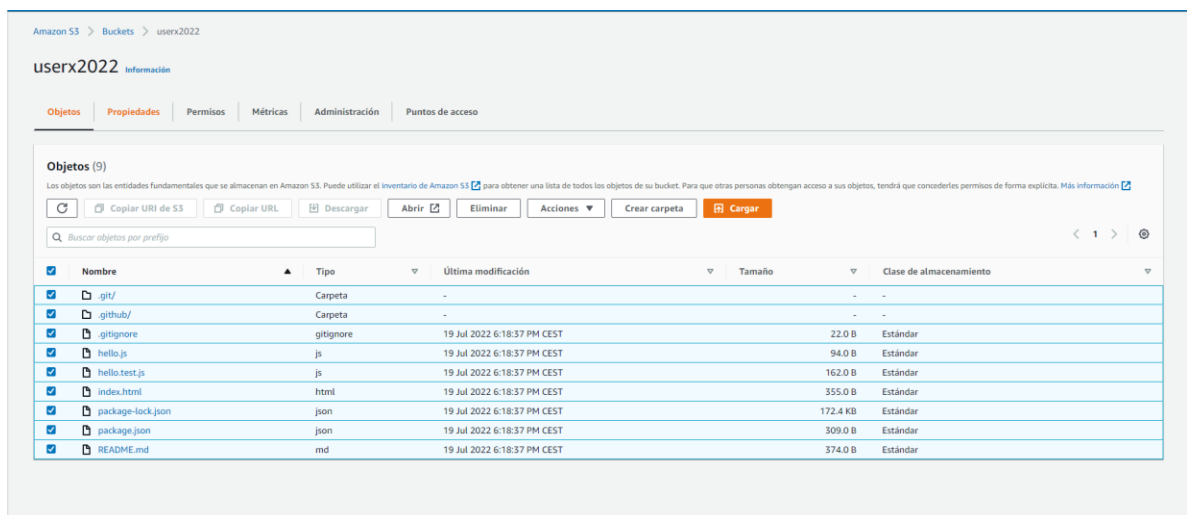
Seleccione su usuario y haga clic en el botón gris "Eliminar":




Introduzca el nombre de usuario para confirmar la eliminación (en este caso, el nombre de usuario es "userx2022"). Por último, haga clic en el botón "Eliminar" para confirmar.

## Borrar el bucket de S3

Vaya a la página correspondiente a su bucket de S3 AWS. Para borrar un bucket, primero hay que eliminar todos los objetos (archivos y carpetas) que estén dentro de este. Seleccione todos los archivos del bucket y haga clic en "Eliminar".




Escriba "Eliminar de forma permanente" en la caja de texto para confirmar la eliminación de los archivos y haga clic en "Eliminar objetos":


**Servicios**

[Alt+S]

Amazon S3 > Buckets > userx2022 > Eliminar objetos

## Eliminar objetos Información












- La eliminación de los objetos especificados no se puede deshacer.
- Los objetos dentro de las carpetas especificadas (prefijos) se eliminarán. Los objetos agregados a estas carpetas mientras la acción de eliminación del objeto esté en curso podrían eliminarse.

[Más información](#)

### Objetos especificados

< 1 >

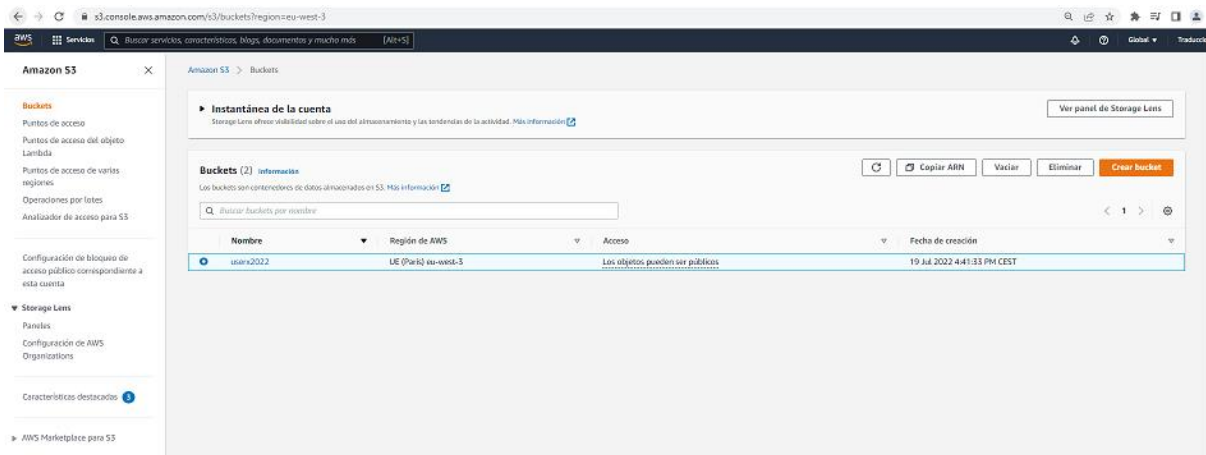
Nombre	Tipo	Última modificación	Tamaño
 .git/	Carpeta	-	-
 .github/	Carpeta	-	-
 .gitignore	gitignore	19 Jul 2022 6:18:37 PM CEST	22.0 B
 hello.js	js	19 Jul 2022 6:18:37 PM CEST	94.0 B
 hello.test.js	js	19 Jul 2022 6:18:37 PM CEST	162.0 B
 index.html	html	19 Jul 2022 6:18:37 PM CEST	355.0 B
 package-lock.json	json	19 Jul 2022 6:18:37 PM CEST	172.4 KB
 package.json	json	19 Jul 2022 6:18:37 PM CEST	309.0 B
 README.md	md	19 Jul 2022 6:18:37 PM CEST	374.0 B

### ¿Eliminar objetos permanentemente?

Para confirmar la eliminación, escriba *eliminar de forma permanente* en el campo de entrada de texto.

Cancelar
Eliminar objetos

Vuelva a la página con la lista de los bucket de S3 y seleccione su bucket. Ahora seleccione "Eliminar":



Escriba el nombre del bucket y haga clic en el botón "Eliminar bucket" para confirmar.

