

Laboratorio del módulo 5: Uso de CloudFront como CDN para un sitio web

Información general sobre el laboratorio

En este laboratorio, utilizarás Amazon CloudFront como red de entrega de contenido (CDN) para un sitio web almacenado en Amazon Simple Storage Service (Amazon S3).

Duración

El tiempo estimado para completar este laboratorio es de **40** minutos.

Acceso a la consola de administración de AWS

1. Para comenzar la sesión de laboratorio, elige **Start Lab** (Iniciar laboratorio) en la esquina superior derecha de la página.
 - Comienza la sesión del laboratorio.
 - En la esquina superior derecha de esta página aparece un temporizador que muestra el tiempo que queda de la sesión.

Consejo: Para actualizar la duración de la sesión en cualquier momento, vuelve a seleccionar **Start Lab** (Iniciar laboratorio) antes de que el temporizador llegue a 0:00.
2. Antes de continuar, espera hasta que el entorno de laboratorio esté listo. El entorno está listo cuando aparecen los detalles del laboratorio en el lado derecho de la página y el icono del círculo junto al enlace de **AWS** en la esquina superior izquierda pasa a ser verde.
3. Para volver a estas instrucciones, elige el enlace **Readme** (Léeme) en la esquina superior derecha.
4. Para conectarte a la consola de administración de AWS, selecciona el enlace de **AWS** situado en la esquina superior izquierda, sobre la ventana del terminal.

Se abre una nueva pestaña del navegador que te conecta a la consola de administración de AWS.

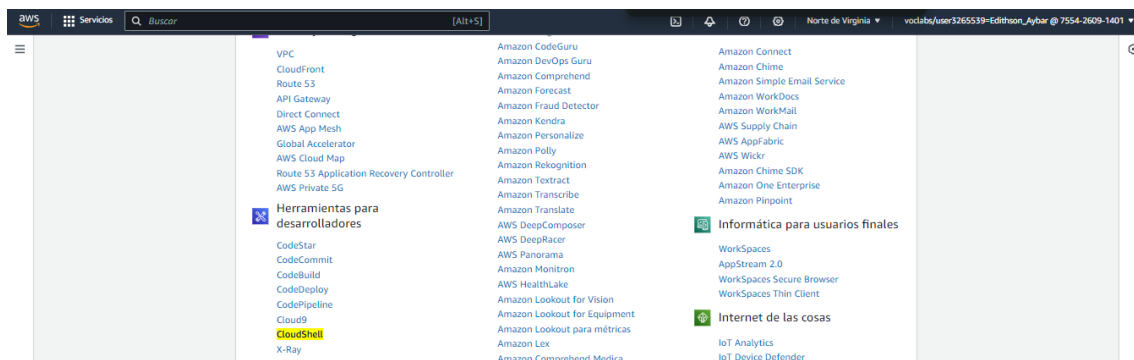
Consejo: Si no se abre una nueva pestaña del navegador, es posible que haya un banner o un icono en la parte superior del navegador con un mensaje que indique que el navegador está impidiendo que el sitio abra ventanas emergentes. Elige el banner o el icono y, a continuación, **Allow pop-ups** (Permitir elementos emergentes).

Nota: Vas a utilizar la consola en el entorno de laboratorio, por lo que no incurrirás en ningún gasto real. Sin embargo, en el mundo real, cuando se utiliza una cuenta personal o de empresa para acceder a la consola, los usuarios incurren en gastos por el uso de servicios específicos de AWS.

Tarea 1. Crear un bucket de S3 mediante AWS CLI

En esta tarea, crearás un bucket de S3 mediante la Interfaz de la línea de comandos de AWS (AWS CLI). AWS CLI es una herramienta de código abierto que puedes utilizar para interactuar con los servicios de AWS mediante comandos en tu shell de línea de comandos.

4. Elige **Servicios y Herramientas para desarrolladores** y, después, **CloudShell**.



Si aparece una ventana emergente de bienvenida, selecciona **Cerrar**.

AWS CloudShell es un shell basado en navegador que da acceso a la línea de comandos para los recursos de AWS en la región de AWS seleccionada.

5. Copia y pega el siguiente código en un editor de texto:

```
cd ~  
aws s3api create-bucket --bucket (bucket-name) --region us-east-1
```

6. En el código que has copiado, reemplaza el nombre del bucket (**bucket-name**) por un nombre exclusivo compatible con el sistema de nombres de dominio (DNS) para el nuevo bucket.

Sigue estas pautas de nomenclatura:

- El nombre debe ser único entre todos los nombres de bucket existentes en Amazon S3.
- El nombre debe tener entre 3 y 63 caracteres.
- El nombre solo puede contener letras minúsculas, números, puntos (.) y guiones (-).
- El nombre debe empezar y terminar con una letra o un número.
- El nombre no debe tener formato de dirección IP (por ejemplo, 192.168.5.4).
- Después de crear el bucket, no podrás cambiar el nombre, así que elígelo bien.

- Elige un nombre de bucket que refleje los objetos del bucket. Esto es así porque el nombre del bucket se ve en la dirección URL del sitio web que apunta a los objetos que vas a poner en el bucket.

Consejo: A continuación se muestra un nombre de bucket de ejemplo: **mylabbucket12345**

Nota: La región **us-east-1** se ha introducido en el comando. Al crear un bucket, la práctica recomendada es elegir una región cercana para minimizar la latencia y los costes o para cumplir los requisitos normativos. Los objetos almacenados en una región nunca abandonan esa región a menos que los transfieras explícitamente a otra región.

7. Ejecuta el código actualizado en el terminal de CloudShell.

Si aparece una ventana emergente, selecciona **Pegar**.

El resultado debe tener un aspecto similar al siguiente:

```
XXXXXXXXXX
{
  "Location": "/mylabbucket12345"
}
```

```
us-east-1

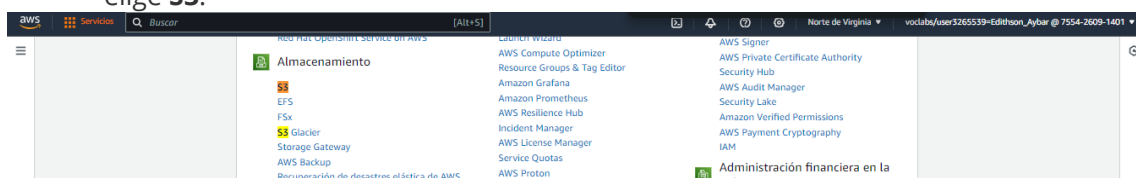
[cloudshell-user@ip-10-138-167-158 ~]$ aws s3api create-bucket --bucket contenidomodule5 --region us-east-1
{
  "Location": "/contenidomodule5"
}
[cloudshell-user@ip-10-138-167-158 ~]$
```

Nota: Al crear un bucket con este comando, el bucket está abierto al público. Te recomendamos que mantengas habilitada toda la configuración a menos que sepas que tendrás que desactivar uno o más ajustes para tu caso de uso, por ejemplo, para alojar un sitio web público.

Tarea 2. Añadir una política de bucket

En esta tarea, añadirás una política de bucket a través de AWS CLI para que el contenido esté disponible públicamente.

8. En la consola, selecciona el menú **Servicios**, localiza la sección **Almacenamiento** y elige **S3**.



9. Elige el nombre del bucket que acabas de crear.

Nombre	Región de AWS	Analizador de acceso de IAM	Fecha de creación
contenidomodule5	EE. UU. Este (Norte de Virginia) us-east-1	Ver analizador para us-east-1	22 May 2024 10:13:14 PM -05

10. Selecciona la pestaña **Permisos**. En **Bloquear acceso público (configuración del bucket)**, selecciona **Editar**. Desactiva la casilla de **Bloquear todo el acceso público**. Elige **Guardar cambios**. Confirma los cambios.

Editar el bloqueo de acceso público (configuración del bucket)

[Información](#) [Información](#)

Bloquear acceso público (configuración del bucket)

Se concede acceso público a 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 de S3, active Bloquear todo acceso público. Esta configuración se aplica en exclusiva a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo acceso público pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que sus aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a sus buckets u objetos, puede personalizar los valores de configuración individuales a continuación para que se ajusten mejor a sus necesidades específicas de almacenamiento. [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 evitará 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 concedan 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.

Cancelar

Guardar cambios

- Desplázate hasta **Propiedad del objeto** y selecciona **Editar**. Selecciona **ACL habilitadas**. Comprueba el reconocimiento y, selecciona **Guardar cambios**.

Propiedad del objeto


Controle la propiedad de los objetos escritos en este bucket desde otras cuentas de AWS y el uso de listas de control de acceso (ACL). La propiedad de los objetos determina quién puede especificar el acceso a los objetos.

☐ ACL deshabilitadas (recomendado)

Todos los objetos de este bucket son propiedad de esta cuenta. El acceso a este bucket y sus objetos se especifica solo mediante políticas.

☒ ACL habilitadas

Los objetos de este bucket pueden ser propiedad de otras cuentas de AWS. El acceso a este bucket y sus objetos se puede especificar mediante ACL.

 Recomendamos desactivar las listas de control de acceso (ACL), a menos que necesite controlar el acceso a cada objeto individualmente o que el escritor del objeto sea el propietario de los datos que carga. Utilizar una política de bucket en lugar de ACL para compartir datos con usuarios externos a la cuenta simplifica la administración de permisos y la realización de auditorías.

Habilitar las ACL desactiva la configuración forzada del propietario del bucket en cuanto a la propiedad del objeto

Una vez desactivada la configuración forzada del propietario del bucket, se restablecen las listas de control de acceso (ACL) y sus permisos asociados. El acceso a los objetos que no posee se basará en las ACL y no en la política del bucket.

☒ Reconozco que las ACL se restaurarán.


Propiedad de objetos

☒ Propietario del bucket preferido

Si los nuevos objetos escritos en este bucket especifican la ACL preconfigurada bucket-owner-full-control, son propiedad del propietario del bucket. De lo contrario, son propiedad del escritor de objetos.

☐ Escritor de objetos

El escritor de objetos sigue siendo el propietario del objeto.

 Si desea aplicar la propiedad de objetos solo para objetos nuevos, la política de bucket debe especificar que la ACL preconfigurada bucket-owner-full-control es obligatoria para las cargas de objetos. [Más información](#)

Cancelar

Guardar cambios

12. En la sección **Política del bucket**, selecciona **Editar**.

13. Para conceder acceso de lectura pública a tu sitio web, copia y pega la siguiente política del bucket en el editor de políticas.

xxxxxxxxxx

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadForGetBucketObjects",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::example-bucket/*"
      ]
    }
  ]
}
```

14. En la política, reemplaza **example-bucket** por el nombre del bucket.

15. En la parte inferior de la página, selecciona **Guardar cambios**.

Política de bucket

EditarEliminar

La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

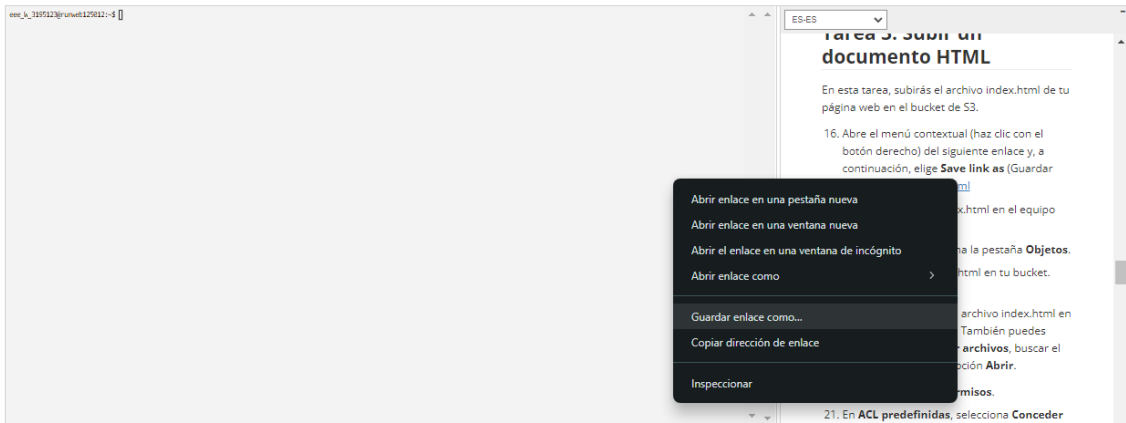
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadForGetBucketObjects",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::contenidomodule5/*"
    }
  ]
}
```

Copiar

Tarea 3. Subir un documento HTML

En esta tarea, subirás el archivo index.html de tu página web en el bucket de S3.

16. Abre el menú contextual (haz clic con el botón derecho) del siguiente enlace y, a continuación, elige **Save link as** (Guardar enlace como): [index.html](#)



17. Guarda el archivo index.html en el equipo local.
18. En la consola, selecciona la pestaña **Objetos**.
19. Carga el archivo index.html en tu bucket.
- Selecciona **Cargar**.
 - Arrastra y suelta el archivo index.html en la página de carga. También puedes seleccionar **Añadir archivos**, buscar el archivo y usar la opción **Abrir**.

Cargar

Información

Agregue los archivos y las carpetas que desea cargar en S3. Para cargar un archivo de más de 160 GB, utilice la CLI de AWS, el SDK de AWS o la API REST de Amazon S3. [Más información](#)

Arrastre y suelte aquí los archivos y carpetas que desee cargar, o seleccione **Add files** (Agregar archivos) o **Add folder** (Agregar carpeta).

Archivos y carpetas (1 Total, 64.0 B)

Eliminar

Agregar archivos

Agregar carpeta

Se cargarán todos los archivos y las carpetas de esta tabla.

Q

Buscar por nombre

< 1 >

<input type="checkbox"/>	Nombre	▼	Carpeta
<input type="checkbox"/>	index.html		-

20. Expande la sección **Permisos**.

21. En **ACL predefinidas**, selecciona **Conceder acceso de lectura público**.

Debajo de la configuración seleccionada aparece un mensaje parecido a este: **No se recomienda otorgar acceso de lectura público**.

22. Marca la casilla que aparece junto a **Entiendo que...** debajo del mensaje de advertencia.

▼ **Permisos**
Conceder acceso público y acceso a otras cuentas de AWS.

Lista de control de acceso (ACL)
Conceder permisos básicos de lectura/escritura a otras cuentas de AWS. [Más información](#)

ⓘ AWS recomienda utilizar políticas de bucket de S3 o políticas de IAM para el control de acceso. [Más información](#)

Lista de control de acceso (ACL)

☒ Elija entre ACL predefinidas

☐ Especificar permisos de ACL individuales

ACL predefinidas

☐ Privado (recomendado)
Solo el propietario del objeto tendrá acceso de lectura y escritura.

☒ Conceder acceso de lectura público
Cualquier persona del mundo podrá obtener acceso a los objetos especificados. El propietario del objeto tendrá acceso de lectura y escritura. [Más información](#)

⚠ **No se recomienda conceder acceso de lectura público**
Cualquier persona del mundo podrá obtener acceso a los objetos especificados. [Más información](#)

☒ Entiendo el riesgo de conceder acceso de lectura público a los objetos especificados.

► **Propiedades**
Especifique la clase de almacenamiento, los ajustes de cifrado, las etiquetas y mucho más.

Cancelar **Cargar**

23. En la parte inferior de la página, selecciona **Cargar**.

24. Selecciona **Cerrar**.

El archivo index.html aparece en la lista **Objetos**.

Tarea 4. Probar el sitio web

25. Selecciona la pestaña **Propiedades** y desplázate a la sección **Alojamiento de sitios web estáticos**.

26. Selecciona **Editar**.

27. Selecciona **Habilitar**.

28. En el cuadro de texto **Documento de índice**, introduce "index.html".

Editar alojamiento de sitios web estáticos

Alojamiento de sitios web estáticos

Utilice este bucket para alojar un sitio web o redirigir solicitudes. [Más información](#)

Alojamiento de sitios web estáticos

- ☐ Desactivar
☒ Habilitar

Tipo de alojamiento

- ☒ Alojamiento de un sitio web estático
Utilice el punto de enlace del bucket como dirección web. [Más información](#)
- ☐ Redirigir las solicitudes de un objeto
Redirija las solicitudes a otro bucket o dominio. [Más información](#)

Para que sus clientes puedan obtener acceso al contenido en el punto de enlace del sitio web, debe hacer que todo el contenido sea legible públicamente. Para ello, puede editar la configuración Bloquear acceso público de S3 del bucket. Para obtener más información, consulte [Utilizar Bloquear acceso público de Amazon S3](#)

Documento de índice

Especifique la página predeterminada o de inicio del sitio web.

index.html

Documento de error - opcional

Esto se devuelve cuando se produce un error.

error.html

Reglas de redireccionamiento: opcionales

Redirija las reglas, escritas en JSON, para redirigir automáticamente las solicitudes de páginas web de contenido específico. [Más información](#)

29. Selecciona **Guardar cambios**.

30. Desplázate de nuevo hacia abajo hasta la sección **Alojamiento de sitios web estáticos** y copia la URL del **Punto de enlace de sitio web del bucket** en el portapapeles.

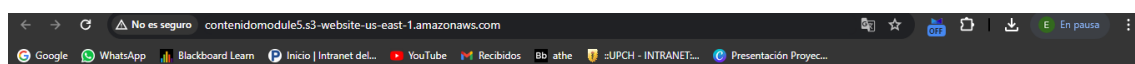
Alojamiento de sitios web estáticos [Editar](#)

Utilice este bucket para alojar un sitio web o redirigir solicitudes. [Más información](#)

Alojamiento de sitios web estáticos
Habilitada
Tipo de alojamiento
Alojamiento de bucket
Punto de enlace de sitio web del bucket
Al configurar su bucket como sitio web estático, el sitio web estará disponible en el punto de enlace del sitio web específico de la región de AWS del bucket. [Más información](#)
<http://contenidomodule5.s3-website-us-east-1.amazonaws.com>

31. Abre una nueva pestaña en el navegador web, pega la URL que acabas de copiar y pulsa **Intro**.

Debería abrirse la página web **Hello World**. Has alojado correctamente un sitio web estático mediante un bucket de S3.

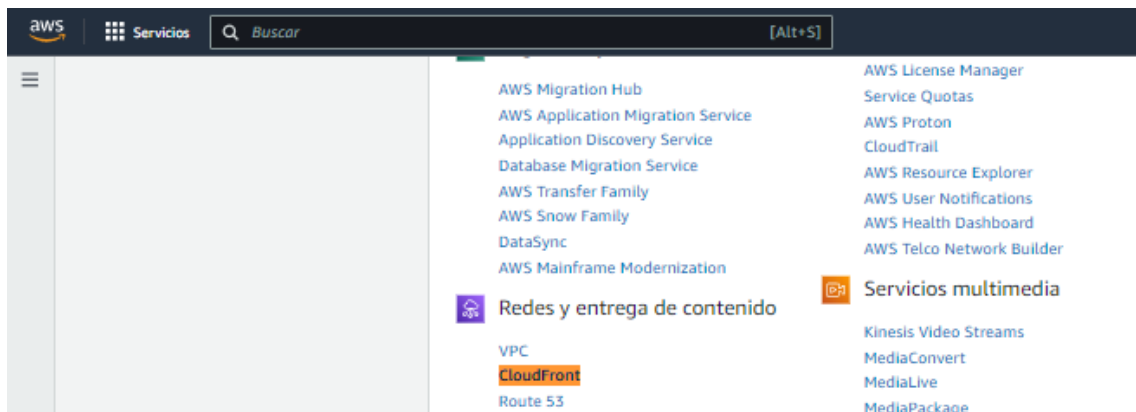


Hello World. Take me to your leader.

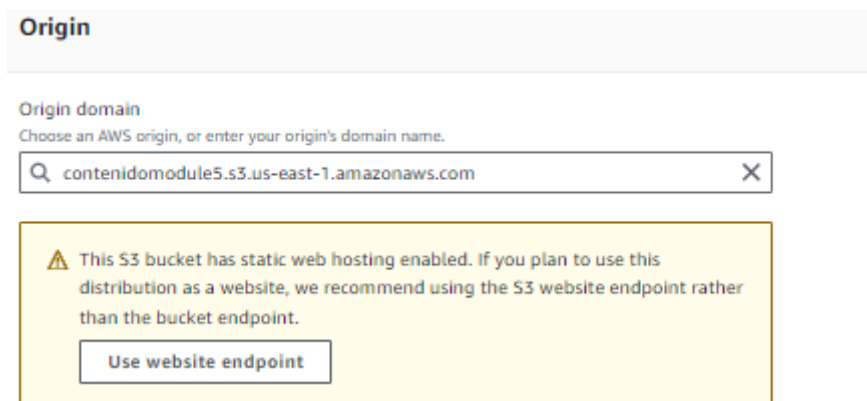
Tarea 5. Crear una distribución de CloudFront para servir al sitio web

En esta tarea, crearás una distribución de Amazon CloudFront para servir al sitio web.

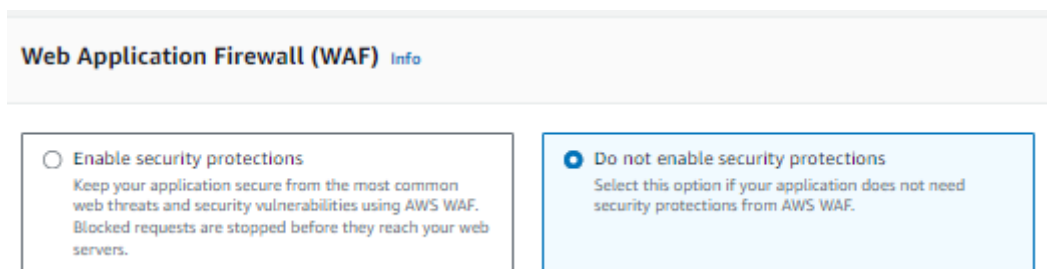
32. Selecciona el menú **Servicios**, localiza la sección **Redes y entrega de contenido** y selecciona **CloudFront**.



33. Selecciona **Crear una distribución de CloudFront**.
34. En la sección **Origen**, selecciona el cuadro de texto que aparece junto a **Dominio de origen** y selecciona el punto de enlace de tu bucket de S3.



35. Para **Viewer Protocol Policy** (Política de protocolo de visor), asegúrate de que **HTTP y HTTPS** estén seleccionados. En **Web Application Firewall (WAF)**, selecciona **Do not enable security protections** (No habilitar protecciones de seguridad).



36. Desplázate hasta la parte inferior de la página y selecciona **Crear distribución**.

Se muestra una nueva distribución de CloudFront en la lista de distribuciones. El **Estado** será *Implementando* hasta que el sitio web se haya distribuido. Puede tardar hasta 20 minutos.

Cuando el **Estado** sea *Habilitado*, puedes probar la distribución.

Distribuciones (0) Información										Actualizar	Permitir	Desactivar	Borrar	Crear distribución
Q Buscar todas las distribuciones														
	IDENTIFICACIÓN	Descripc...	Tipo	Nombre...	Nombre...	Orígenes	Estado	Última ...						
<input type="checkbox"/>	E2PSOV05HHNZ8C	-	Producción	d3oagi0cb...	-	contenidomodul	Activado	23 de may...						

37. Copia el valor de **Nombre de dominio** de la distribución y guárdalo en un editor de texto para utilizarlo en un paso posterior.

38. Crea un nuevo archivo HTML para probar la distribución.

- Busca y descarga una imagen de Internet.
- Navega hasta el bucket de S3 y carga el archivo de imagen en el bucket, asegurándote de otorgar acceso público tal como lo hiciste al subir el archivo HTML antes en este laboratorio.

Objetos (2) Información							Actualizar	Copiar URI de S3	Copiar URL	Descargar	Abrir	Eliminar	Acciones	Crear carpeta	Cargar
Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el inventario de Amazon S3 para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. Más información															
Q Buscar objetos por prefijo															
	Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento										
<input type="checkbox"/>	index.html	html	22 May 2024 10:25:33 PM -05	64.0 B	Estándar										
<input type="checkbox"/>	mio.jpg	jpg	22 May 2024 10:39:47 PM -05	64.5 KB	Estándar										

- Crea un nuevo archivo de texto con el Bloc de notas y copia en él el siguiente texto:

```
XXXXXXXXXX
<html>
  <head>My CloudFront Test</head>
  <body>
    <p>My test content goes here.</p>
    <p>
  </body>
</html>
```

- Reemplaza **domain-name** por el nombre de dominio que copiaste antes para la distribución de CloudFront.
- Reemplaza **object-name** por el nombre del archivo de imagen que cargaste en el bucket de S3.

La línea de código editada debe tener un aspecto similar al siguiente:

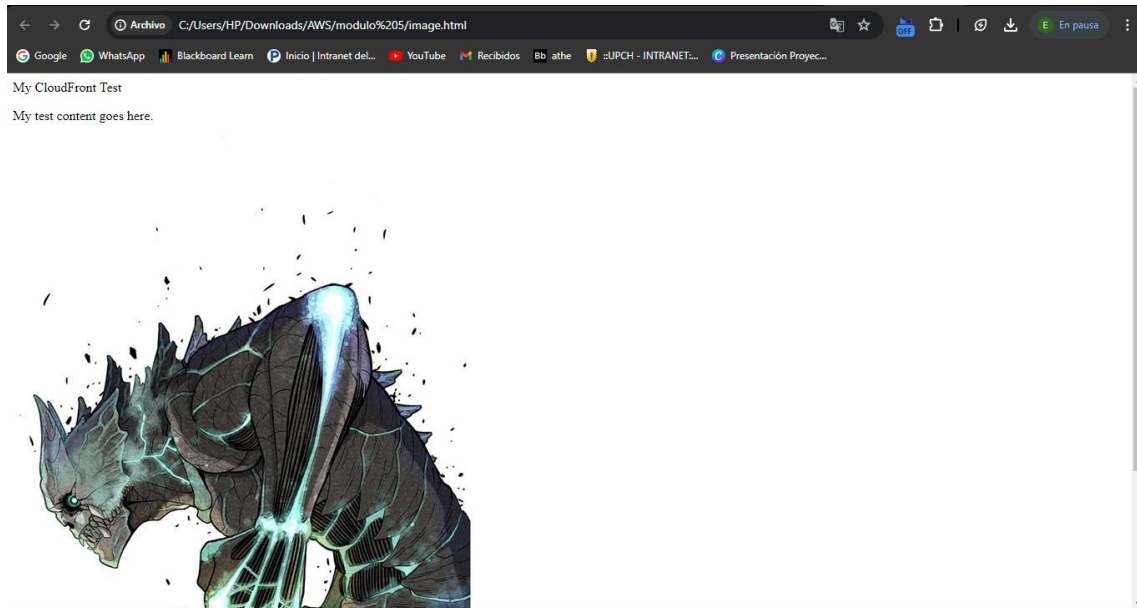
```
XXXXXXXXXX
<p>
```

- Guarda el archivo de texto con extensión HTML.

```
<html>
  <head>My CloudFront Test</head>
  <body>
    <p>My test content goes here.</p>
    <p>
  </body>
</html>
```

39. Utiliza un navegador de Internet para abrir el archivo HTML que acabas de crear.

Si se muestra la imagen que cargaste, la distribución de CloudFront se realizó correctamente. Si no es así, repite el laboratorio.



Laboratorio completado

¡Enhorabuena! Has completado el laboratorio.

40. Cierra la sesión de la consola de administración de AWS.

- En la esquina superior derecha, selecciona tu nombre de usuario, que comienza por **voclabs/user**.
- Selecciona **Cerrar sesión**.

41. Selecciona **Finalizar laboratorio** en la parte superior de esta página y, a continuación, selecciona **Sí** para confirmar que quieres dar por concluido el laboratorio.