

HOJA01_AWS_03

Creación de un Bucket S3 en AWS

1. En el buscador de AWS introducimos **S3** y seleccionamos el servicio. Una vez en el menú contextual del bucket, seleccionamos *Crear bucket*.



2. Elegiremos el tipo de bucket como **Uso general** y estableceremos ***dac-archivos-javier*** como nombre:

Crear bucket Información

Los buckets son contenedores de datos almacenados en S3.

Configuración general

Región de AWS
EE.UU. Este (Norte de Virginia) us-east-1

Tipo de bucket Información

☒ **Uso general**
Recomendado para la mayoría de los casos de uso y patrones de acceso. Los buckets de uso general son del tipo de bucket de S3 original. Permiten una combinación de clases de almacenamiento que almacenan objetos de forma redundante en múltiples zonas de disponibilidad.

☐ **Directorio**
Recomendado para casos de uso de baja latencia. Estos buckets utilizan únicamente la clase de almacenamiento S3 Express One Zone, que proporciona un procesamiento más rápido de los datos dentro de una única zona de disponibilidad.

Nombre del bucket Información

dac-archivos-javier

Los nombres de los buckets deben tener entre 3 y 63 caracteres y ser únicos dentro del espacio de nombres global. Los nombres de los buckets también deben empezar y terminar con una letra o un número. Los caracteres válidos son a-z, 0-9, puntos (.) y guiones (-). [Más información](#)

Copiar la configuración del bucket existente: *opcional*
Solo se copia la configuración del bucket en los siguientes ajustes.

Elegir el bucket

Formato: s3://bucket/prefijo

3. Seleccionamos **ACL deshabilitadas** en **Propiedad de objetos**, de forma que todos los objetos del bucket pertenezcan a la cuenta de AWS que lo ha creado.

Propiedad de objetos Información

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.

Propiedad del objeto

☒ **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.

Propiedad del objeto

Aplicada al propietario del bucket

4. En **Configuración de bloqueo de acceso público** desbloqueamos todas las opciones, permitiendo el acceso público (no recomendable en producción, pero este bucket se usará para aprendizaje):

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 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.

⚠ 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.

5. Desactivamos el **Control de versiones** para este bucket:

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

6. Establecemos el **Cifrado predeterminado** mediante *claves administradas de Amazon S3*:

Cifrado predeterminado [Información](#)

El cifrado del lado del servidor se aplica automáticamente a los nuevos objetos almacenados en este bucket.

Tipo de cifrado [Información](#)

Proteja sus objetos con dos capas de cifrado independientes. Para obtener más información sobre los precios, consulte [DSSE-KMS pricing](#) (Precios de DSSE-KMS) en la pestaña **Storage** (Almacenamiento) de la [página de precios de Amazon S3](#).

☒ Cifrado del servidor con claves administradas de Amazon S3 (SSE-S3)
☐ Cifrado del servidor con claves de AWS Key Management Service (SSE-KMS)
☐ Cifrado de doble capa del servidor con claves de AWS Key Management Service (DSSE-KMS)

Clave de bucket

El uso de una clave de bucket de S3 para SSE-KMS reduce los costos de cifrado al reducir las llamadas a AWS KMS. Las claves de bucket de S3 no son compatibles con DSSE-KMS. [Más información](#)

☐ Desactivar
☒ Habilitar

7. Finalmente, hacemos clic en *Crear bucket*:

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

[Cancelar](#) [Crear bucket](#)

Buckets de uso general [Todas las regiones de AWS](#)

Buckets de directorio

Buckets de uso general (1) [Información](#) [Recargar](#) [Copiar ARN](#) [Vaciar](#) [Eliminar](#) [Crear bucket](#)

Los buckets son contenedores de datos almacenados en S3.

Buscar buckets por nombre

Nombre	Región de AWS	Fecha de creación
<input type="radio"/> dac-archivos-javier	EE.UU. Este (Norte de Virginia) us-east-1	23 Sep 2025 2:03:36 PM CEST

Instantánea de la cuenta [Información](#)

Actualizado a diario

[Ver panel](#)

Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de actividad.

Resumen de acceso externo: nuevo

Actualizado a diario

[Información](#)

Los resultados de acceso externo le ayudan a identificar los permisos de los buckets que permiten el acceso público o desde otras cuentas de AWS.

Cargar ficheros

Desde dentro del bucket, cargamos los ficheros (o carpeta que los contiene) relativos a las películas.

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, los 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 (10 total, 1.3 MB)
Se cargarán todos los archivos y las carpetas de esta tabla.

<input type="checkbox"/>	Nombre	Carpeta	Tipo	Tamaño
<input type="checkbox"/>	1.jpg	películas/	image/jpeg	92.1 KB
<input type="checkbox"/>	10.jpg	películas/	image/jpeg	101.7 KB
<input type="checkbox"/>	2.jpg	películas/	image/jpeg	119.5 KB
<input type="checkbox"/>	3.jpg	películas/	image/jpeg	150.3 KB
<input type="checkbox"/>	4.jpg	películas/	image/jpeg	222.6 KB
<input type="checkbox"/>	5.jpg	películas/	image/jpeg	119.7 KB
<input type="checkbox"/>	6.jpg	películas/	image/jpeg	131.7 KB
<input type="checkbox"/>	7.jpg	películas/	image/jpeg	102.2 KB
<input type="checkbox"/>	8.jpg	películas/	image/jpeg	95.8 KB
<input type="checkbox"/>	9.jpg	películas/	image/jpeg	167.6 KB

[Eliminar](#) [Agregar archivos](#) [Agregar carpeta](#)

Destino información

Destino
[s3://dac-archivos-javier](#)

► **Detalles del destino**
Los ajustes del bucket que afectan a los objetos nuevos almacenados en el destino especificado.

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

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

[Cancelar](#) [Cargar](#)

Se ha realizado la carga correctamente
Para obtener más información, consulte la tabla Archivos y carpetas.

Cargar: estado [Cerrar](#)

Después de salir de esta página, la siguiente información ya no estará disponible.

Uso de las imágenes del Bucket en nuestra Base de Datos

1. Comprobamos que el acceso público esté desactivado en la pestaña Permisos

dac-archivos-javier Información

Objetos | Metadatos | Propiedades | Permisos | Métricas | Administración | Puntos de acceso

Objetos (1)

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](#)

Buscar objetos por prefijo

Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
películas/	Carpeta	-	-	-

Bloquear acceso público (configuración del bucket)

[Editar](#)

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

Desactivado

▼ Configuración de bloqueo de acceso público individual para este bucket

- ☐ 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.

2. Si probamos a acceder a la URL de uno de los objetos subidos, nos da el siguiente error:

películas/ [Copiar URI de S3](#)

Objetos | Propiedades

URL de objeto copiada

Objetos (1/10)

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](#)

Buscar objetos por prefijo

Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
1.jpg	jpg	23 Sep 2025 2:06:30 PM CEST	92.1 KB	Estándar
10.jpg	jpg	23 Sep 2025 2:06:30 PM CEST	101.7 KB	Estándar

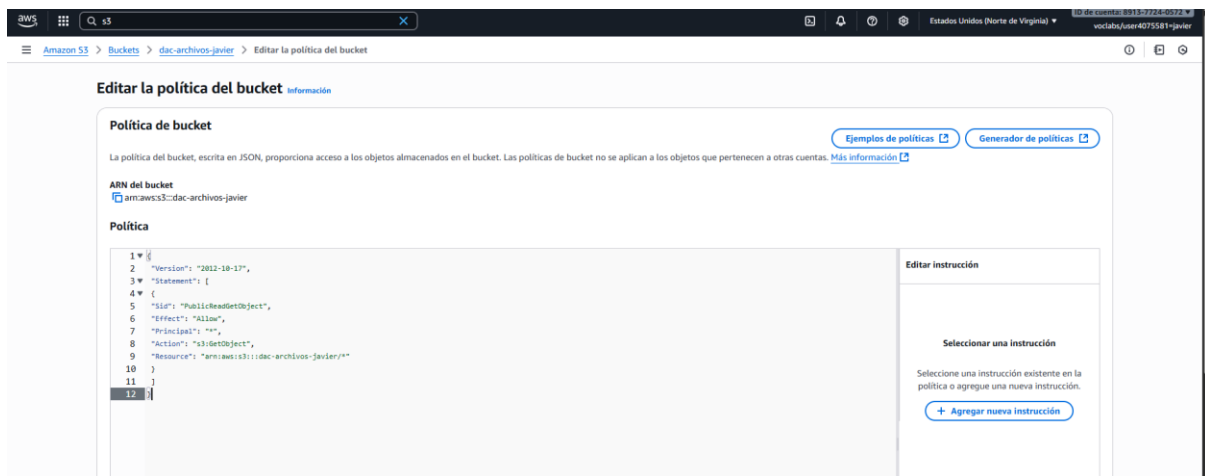
← → ↺ **dac-archivos-javier.s3.us-east-1.amazonaws.com/películas/1.jpg**

Documentación | Cursos | Recursos | DAW

This XML file does not appear to have any style information associated with it. The document tree is shown below.

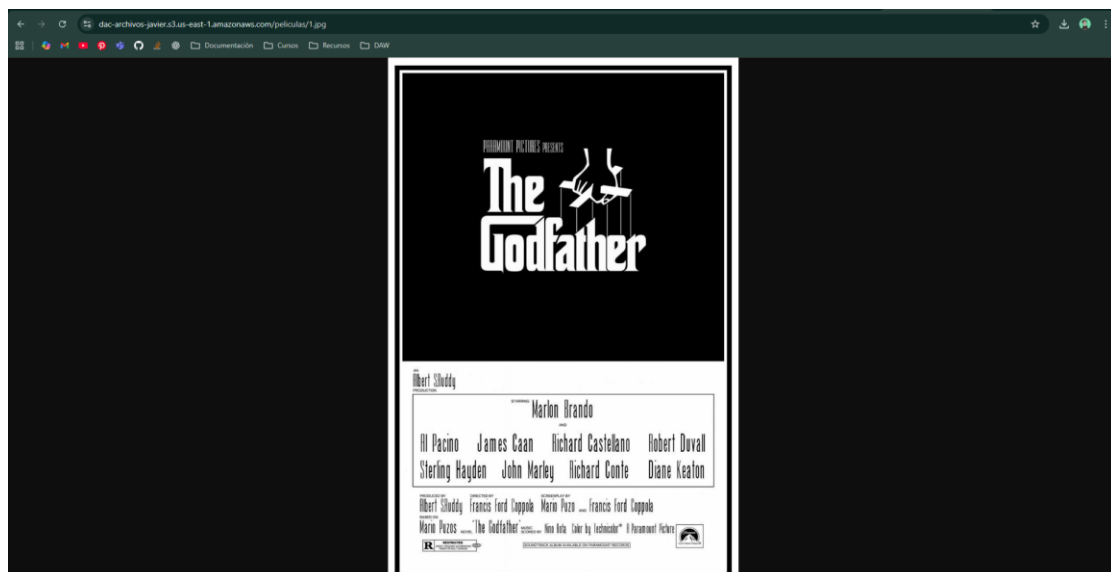
```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>M7K2SV8WB60BBYPJ</RequestId>
  <HostId>081Lfm0Qrwx8TqaWcZawVWrfX215ZbZrHxUmkVFUE7s/KN6YIhrY9Ie7rkcvTyt50avrX8Nqozs=</HostId>
</Error>
```

Para evitar dicho error, debemos añadir una nueva **política de bucket** (desde la pestaña **Permisos**):



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

Una vez añadida la política, deberíamos ser capaces de ver las imágenes desde la URL del objeto del bucket:



- Desde la terminal de nuestra instancia EC2, editaremos el fichero `/var/www/html/cine/index.php` para que la etiqueta `` apunte a las imágenes subidas a nuestro bucket S3:

```
ubuntu@ip-172-31-18-19: ~
ubuntu@ip-172-31-18-19:~$ sudo nano /var/www/html/cine/index.php
ubuntu@ip-172-31-18-19:~$ |
```

```
GNU nano 7.2 /var/www/html/cine/index.php
<?php
include("conexion.php");

try {
    $sql = "SELECT * FROM peliculas";
    $stmt = $conexion->query($sql);
    $peliculas = $stmt->fetchAll(PDO::FETCH_ASSOC);
} catch (PDOException $e) {
    die("Error al obtener datos: " . $e->getMessage());
}
?>

<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <title>Listado de Películas</title>
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css">
</head>
<body class="p-4">
    <div class="container">
        <h1 class="mb-4">Listado de Películas</h1>
        <table class="table table-striped table-bordered">
            <thead class="table-dark">
                <tr>
                    <th>ID</th>
                    <th>Título</th>
                    <th>Director</th>
                    <th>Año</th>
                    <th>Género</th>
                    <th>Imagen</th>
                </tr>
            </thead>
            <tbody>
                <?php foreach ($peliculas as $fila) { ?>
                    <tr>
                        <td><?= htmlspecialchars($fila["id"]) ?></td>
                        <td><?= htmlspecialchars($fila["titulo"]) ?></td>
                        <td><?= htmlspecialchars($fila["director"]) ?></td>
                        <td><?= htmlspecialchars($fila["anio"]) ?></td>
                        <td><?= htmlspecialchars($fila["genero"]) ?></td>
                        <td>
                            "
                                class="img-thumbnail rounded"
                                width="100">
                        </td>
                    </tr>
                </tbody>
            </table>
        </div>
    </body>
</html>
```

Al estar dentro de una carpeta dentro del contenedor s3, habrá que indicarlo en la ruta `src`:





`src = https://TU-BUCKET.s3.us-east-1.amazonaws.com/CARPETA/<?= htmlspecialchars($fila['id']) ?>.jpg`

```
<td>
    <img
        src=https://TU-BUCKET.s3.us-east-1.amazonaws.com/NOMBRE-CARPETA/<?=
        htmlspecialchars($fila['id']) ?>.jpg
        alt="Poster de <?= htmlspecialchars($fila['titulo']) ?>"
        class="img-thumbnail rounded"
        width="100"
    >
</td>
```

4. Una vez realizados los pasos anteriores, al acceder a http://IP_MAQUINA_EC2/cine/, deberíamos ser capaces de ver las imágenes en nuestra web:



Listado de Películas

ID	Título	Director	Año	Género	Imagen
1	El padrino	Francis Ford Coppola	1972	Crimen	
2	El padrino. Parte II	Francis Ford Coppola	1974	Crimen	
3	Doce hombres sin piedad	Sidney Lumet	1957	Drama judicial	
4	La lista de Schindler	Steven Spielberg	1993	Drama histórico	
5	Luces de la ciudad	Charles Chaplin	1931	Comedia romántica	