

# TALLER\_AWS

## NextDigital

## En primer lugar crearemos el Bucket en S3.

The screenshot shows the 'Crear bucket' (Create Bucket) page in the AWS Management Console. The top navigation bar includes the AWS logo, a search bar, and account information (ID de cuenta: 4775-0080-8805, Estados Unidos (Norte de Virginia)). The main content area is titled 'Configuración general' (General Configuration). It includes sections for 'Región de AWS' (Region), 'Tipo de bucket' (Bucket Type), 'Nombre del bucket' (Bucket Name), 'Copiar la configuración del bucket existente' (Optional), and 'Propiedad de objetos' (Object Ownership). The 'Configuración de bloqueo de acceso público para este bucket' (Public Access Locking Configuration) section is also visible at the bottom. The page has a light gray background with blue highlights for selected options.

**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](#)  
upm-next-digital-bucket

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

**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

**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 bloquera los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitara 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.

[CloudShell](#) [Comentarios](#) © 2026, Amazon Web Services, Inc. o sus filiales. [Privacidad](#) [Términos](#) [Preferencias de cookies](#)

### 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 - opcional

Puede usar etiquetas de bucket para analizar los permisos de un bucket, además de administrarlos y especificarlos. [Más información ↗](#)

- ⓘ Puede usar las API s3>ListTagsForResource, s3:TagResource y s3:UntagResource para administrar las etiquetas en los buckets de uso general de S3 para el control de acceso, además de la asignación de costos y la organización de los recursos. Para garantizar una transición fluida, proporcione permisos para realizar las acciones s3>ListTagsForResource, s3:TagResource y s3:UntagResource. [Más información ↗](#)

No hay etiquetas asociadas a este bucket.

[Agregar nueva etiqueta](#)

Puede agregar hasta 50 etiquetas.

### 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

### ▶ Configuración avanzada

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

[Cancelar](#)

[Create bucket](#)

Luego de haberlo creado, nos meteremos dentro del Bucket y cargaremos un archivo con extensión HTML. En mi caso subiré uno de ejemplo llamada TallerAWS.html que contiene la siguiente frase: Práctica final del taller de AWS. Ejemplo de sitio web estático.

The screenshot shows the AWS S3 'Upload' interface. At the top, the navigation bar includes the AWS logo, a search bar with 'Buscar', and account information: 'ID de cuenta: 4775-0080-8805' and 'voclabs/user4809956-Yujian\_Chen'. Below the navigation bar, the breadcrumb trail shows 'Amazon S3 > Buckets > upm-next-digital-bucket > Cargar'. The main area is titled 'Cargar' with a 'Información' link. A note says '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.' followed by a 'Más información' link. A dashed blue box indicates where files can be dropped or selected. Below this is a table titled 'Archivos y carpetas (1 total, 65.0 B)'. The table has columns: Nombre, Carpeta, Tipo, and Tamaño. It lists one item: 'TallerAWS.html' under 'Nombre', '-' under 'Carpeta', 'text/html' under 'Tipo', and '65.0 B' under 'Tamaño'. Buttons for 'Eliminar', 'Agregar archivos', and 'Agregar carpeta' are at the top right of the table. The 'Destino' section shows the destination as 's3://upm-next-digital-bucket'. Under 'Detalles del destino', it says 'Los ajustes del bucket que afectan a los objetos nuevos almacenados en el destino especificado.' Below this are sections for 'Permisos' (with a note about public access) and 'Propiedades' (with a note about storage class). At the bottom right are 'Cancelar' and 'Cargar' buttons.

Luego después haremos cambios en los permisos del Bucket para que tenga acceso todo el público y confirmaremos la acción y seguiremos en añadir una política bucket

proveniente de un pastebin que usamos en el propio taller.

The screenshot shows the AWS S3 console with the path: Amazon S3 > Buckets > upm-next-digital-bucket > Editar el bloqueo de acceso público (configuración del bucket). The main content area is titled "Editar el bloqueo de acceso público (configuración del bucket)".

**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

**Editar el bloqueo de acceso público (configuración del bucket)** X

Actualizar la configuración de bloqueo de acceso público de este bucket afectará a este bucket y a todos los objetos que contiene. Esto puede provocar que algunos objetos se vuelvan públicos.

Para confirmar la configuración, ingrese **confirmar** en el campo.

[Cancelar](#) [Confirmar](#)

The screenshot shows the AWS S3 Bucket Policy Editor. The left sidebar contains navigation links for Buckets, Security and Access Management, and Storage Lens. The main area is titled "Editar la política del bucket" (Edit bucket policy) and displays the following JSON policy:

```
1 Version: "2012-10-17",
2 Statement: [
3     {
4         Sid: "PublicReadGetObject",
5         Effect: "Allow",
6         Principal: "*",
7         Action: [
8             "s3:GetObject"
9         ],
10        ],
11       Resource: [
12           "arn:aws:s3:::upm-next-digital-bucket/*"
13       ]
14   }
15 ]
16 ]
```

The policy grants public read access to all objects in the bucket. The ARN of the bucket is listed as `arn:aws:s3:::upm-next-digital-bucket`. There are buttons for "Agregar nueva instrucción" (Add new instruction) and "Añadir" (Add). A link to "Ejemplos de políticas" (Policy examples) is also present.

Y por último editaremos para que pueda alojar sitios webs estáticos en S3

The screenshot shows the AWS S3 console interface for editing static website hosting settings. The left sidebar contains navigation links for Amazon S3, Buckets, and various security and management options. The main content area is titled "Editar alojamiento de sitios web estáticos" and includes sections for "Alojamiento de sitios web estáticos" (with a note about using the bucket as a website endpoint), "Tipo de alojamiento" (set to "Alojar un sitio web estático"), and "Documento de índice" (set to "index.html"). A callout box provides information about enabling public access. Below these are fields for "Documento de error - opcional" (set to "error.html") and "Reglas de redirección" (an empty JSON editor). The bottom of the screen shows standard AWS footer links.

Sitio web estático desplegado:

