


 **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.

Resumen

Destino
s3://s3josebelchi



Realizado correctamente
 1 archivo, 590.0 B (100.00%)


Con errores
 0 archivos, 0 B (0%)

Archivos y carpetas

Configuración

Archivos y carpetas (1 total, 590.0 B)

 1 

Nombre	Carpeta	Tipo	Tamaño	Estado	Error
index_JoseBelchi.html	-	text/html	590.0 B	 Realizado correctamente	-

Editar el bloqueo de acceso público (configuración del bucket) [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](#)

arn:aws:s3::s3josebelchi

Política

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3::s3josebelchi/*"  
10    }  
11  ]  
12 }
```

Editar instrucción
Statement1[Eliminar](#)

Agregar acciones

Elegir un servicio

🔍 Filtrar servicios

Incluido

[S3](#)

Disponible

[AI Operations](#)[AMP](#)[API Gateway](#)[API Gateway V2](#)[ARC Zonal Shift](#)[ASC](#)

Esta página ha sido creada por **Jose Belchí**