

## [Publish] - 2. El alojamiento de sitios web estáticos está deshabilitado en los buckets de S3

El hallazgo de seguridad "**El alojamiento de sitios web estáticos está deshabilitado en los buckets de S3**" puede parecer contradictorio, especialmente si el propósito del bucket es servir un sitio web. Sin embargo, este hallazgo promueve una arquitectura más segura y eficiente.

La función de "alojamiento de sitios web estáticos" en S3 es una característica heredada que requiere que el bucket sea público para funcionar. Como hemos discutido en otros hallazgos, hacer un bucket público expone directamente tus datos y no es la mejor práctica.

La arquitectura moderna y recomendada por AWS es:

1. Mantener el **bucket de S3 completamente privado**.
2. Utilizar **Amazon CloudFront** como la capa pública.
3. Configurar CloudFront para que acceda al bucket de S3 de forma privada a través de un **Control de Acceso de Origen (OAC)**.

Este enfoque no solo es más seguro, sino que también mejora el rendimiento al distribuir tu contenido globalmente a través de la red de borde de AWS.

### Análisis de los Buckets Reportados

Los siguientes buckets de S3 han sido identificados por tener habilitada la función de alojamiento de sitios web estáticos, lo que implica que son (o fueron) públicos.

Tipo	Nombre del Bucket	Número de Cuenta
S3	banco-imagen-gs-frontend	002670977573
S3	biometricos-frontend	002670977573
S3	biometricos-gs-frontend	002670977573

**Observación Clave:** Los nombres de estos buckets confirman su propósito como frontends de aplicaciones. Esto refuerza la recomendación de servirlos a través de CloudFront en lugar de exponerlos directamente.

## Preguntas para tu Equipo (Acción Requerida)

La acción a tomar es clara, pero la coordinación es esencial para evitar interrumpir el servicio.

1. **¿Están estos sitios web actualmente en producción?**
2. **¿Ya existe una distribución de CloudFront para estos sitios?** Si la respuesta es sí, se debe proceder a deshabilitar el alojamiento estático en S3. Si es no, el primer paso es crear y configurar la distribución de CloudFront.
3. **¿Quién es el responsable de actualizar los registros DNS** para que apunten al nuevo dominio de CloudFront una vez que esté listo?

## Consideraciones de Costo

- **Deshabilitar el Alojamiento Estático:** Esta acción es **gratuita**.
- **Implementar Amazon CloudFront:** Como se mencionó en hallazgos anteriores, usar CloudFront es a menudo **más económico** que servir contenido directamente desde S3, gracias a su nivel gratuito y tarifas de transferencia de datos más bajas. La transferencia de datos de S3 a CloudFront es gratuita.

## Conclusión sobre Costos:

Migrar de un alojamiento estático en S3 a una arquitectura con CloudFront no solo soluciona el hallazgo de seguridad sin costo directo, sino que también puede reducir tus costos operativos y mejorar el rendimiento.

## Cómo Solucionarlo: Deshabilitar el Alojamiento Estático

Una vez que hayas confirmado que el tráfico de usuarios está siendo servido a través de una distribución de CloudFront, puedes proceder a deshabilitar la configuración heredada.

1. **Navegar al Bucket de S3:**
  - Ve a la consola de **Amazon S3** y selecciona el bucket correspondiente.
2. **Editar la Configuración de Alojamiento Estático:**
  - Ve a la pestaña **Propiedades**.
  - Desplázate hasta la parte inferior, a la sección **Alojamiento de sitios web estáticos (Static website hosting)**.
  - Haz clic en **Editar**.
3. **Deshabilitar la Función:**
  - Selecciona la opción **Deshabilitar**.
  - Haz clic en **Guardar cambios**.
4. **Asegurar el Bucket (Paso Crucial):**
  - Después de deshabilitar el alojamiento estático, ve a la pestaña **Permisos**.

- Asegúrate de que el **Bloqueo de Acceso Público** esté **activado** para el bucket.
- Revisa la **Política del bucket** para asegurarte de que ya no permita el acceso público ( `"Principal": "*"`  ), excepto para la identidad de CloudFront (OAC).

#### Recomendación

Se recomienda que se adopte la arquitectura de **Amazon CloudFront + S3 privado** como el estándar para todo el alojamiento de sitios web estáticos. Para los buckets listados, el plan de acción es:

1. **Confirmar** que una distribución de CloudFront está activa y sirviendo el tráfico.
2. **Deshabilitar** la función de alojamiento de sitios web estáticos en la configuración del bucket.
3. **Verificar** que el Bloqueo de Acceso Público esté activado para asegurar que el bucket quede completamente privado.

#### Referencias

 [Get started with a CloudFront standard distribution - Amazon CloudFront](#)