## [Publish]- 9. Asegurar que los buckets de Amazon S3 estén configurados de forma privada con Bloqueo de Acceso Público

El hallazgo de seguridad **"Asegurar que los buckets de Amazon S3 estén configurados de forma privada con Bloqueo de Acceso Público"** es un control de seguridad fundamental para tu entorno de AWS. Por defecto, todos los recursos de Amazon S3 son privados. Sin embargo, configuraciones erróneas pueden exponer tus datos accidentalmente a la internet pública, creando un riesgo de seguridad significativo.

La característica **Bloqueo de Acceso Público de S3 (S3 Block Public Access)** es un control centralizado, a nivel de cuenta o de bucket, que actúa como una poderosa salvaguarda. Te permite anular las políticas de bucket y los permisos de objetos individuales para garantizar que ningún dato sea accesible públicamente, ni ahora ni en el futuro, a menos que tengas una razón deliberada y explícita para ello.

#### Análisis de los Buckets de S3 Reportados

Se ha revisado la lista de buckets de S3 que actualmente no cumplen con este control de seguridad. Basado en sus nombres, aquí hay una evaluación inicial y preguntas para guiar nuestro plan de remediación.

| Tipo | Nombre del Bucket | Número de Cuenta | Propósito Inferido y Riesgo |
|---|---|---|---|
| S3 | `banco-imagen-gs-frontend` | 002670977573 | El sufijo "-frontend" sugiere que podría alojar activos web (imágenes, CSS, JS). **Posiblemente necesite ser público**, pero debe confirmarse. |

| | | | |
|---|---|---|---|
| S3 | `biometricos-frontend` | 002670977573 | Similar al anterior, podría contener el frontend de una aplicación de biométricos. **Posiblemente necesite ser público**. |
| S3 | `gs-novis-721225638995-installers` | 398984081329 | Probablemente almacena instaladores de software. **No debería ser público**. Exponer instaladores puede revelar versiones de software y posibles vulnerabilidades. |
| S3 | `gs-resp-sql` | 002670977573 | El nombre sugiere que contiene respaldos de bases de datos SQL. **Es crítico que este bucket sea privado**. Los respaldos públicos son una brecha de seguridad severa. |

| | | | |
|---|---|---|---|
| S3 | `gs-softfloat` | 002670977573 | El propósito no está claro, pero por precaución, **debería ser privado** hasta que se demuestre lo contrario. |

#### Preguntas para tu Equipo (Acción Requerida)

Para confirmar la configuración correcta, por favor discute lo siguiente con los dueños de las aplicaciones y la infraestructura:

1. **Para `banco-imagen-gs-frontend` y `biometricos-frontend`:** ¿Estos buckets alojan sitios web estáticos que necesitan ser accesibles directamente desde internet? Si es así, la forma correcta de exponerlos es a través de un servicio de **Amazon CloudFront**, no haciendo el bucket público directamente.
2. **Para los demás buckets (`-installers`, `-resp-sql`, `-softfloat`):** ¿Pueden confirmar que estos buckets son para uso interno únicamente y no tienen ningún requisito de acceso público?

A menos que exista un requisito de negocio confirmado y documentado para el acceso público (que debería ser manejado por CloudFront), debemos proceder a hacer privados todos los buckets listados.

#### Cómo Habilitar el Bloqueo de Acceso Público

Habilitar el Bloqueo de Acceso Público es la forma recomendada de solucionar este hallazgo. Se puede aplicar a nivel de cuenta (la mejor práctica) o en buckets individuales.

**Opción 1: Habilitar el Bloqueo de Acceso Público para toda la Cuenta de AWS (Recomendado)**

Este es el enfoque más seguro, ya que impone una postura privada por defecto para todos los buckets actuales y futuros en la cuenta.

1. Navega a la consola de **Amazon S3**.
2. En el panel de navegación izquierdo, elige **Bloquear acceso público (configuración de la cuenta)**.
3. Haz clic en **Editar**.

4. Selecciona **Bloquear todo el acceso público** y luego haz clic en **Guardar cambios**.

**Opción 2: Habilitar el Bloqueo de Acceso Público para un Bucket Individual**

Usa este método si tienes una razón específica y confirmada para dejar otros buckets en la cuenta como públicos.

1. Navega a la consola de **Amazon S3** y selecciona el bucket que deseas configurar.
2. Ve a la pestaña **Permisos**.
3. En la sección **Bloquear acceso público (configuración del bucket)**, haz clic en **Editar**.
4. Selecciona **Bloquear todo el acceso público** y luego haz clic en **Guardar cambios**.

Las cuatro configuraciones bajo "Bloquear todo el acceso público" proporcionan un control granular. Para una máxima seguridad, se recomienda **habilitar las cuatro opciones**.

#### Consideraciones de Costo

No hay **costos directos** asociados con el uso de la característica de Bloqueo de Acceso Público de Amazon S3. Es una configuración de seguridad fundamental proporcionada por AWS sin cargo adicional. Implementar este control no aumentará tu factura de AWS.

#### Recomendación

Se recomienda habilitar el **Bloqueo de Acceso Público** a **nivel de cuenta** para todas las cuentas afectadas. Esto proporciona la postura de seguridad más robusta y asegura que incluso las configuraciones erróneas accidentales a nivel de bucket no conduzcan a la exposición de datos.

Si, después de la investigación, se confirma que los buckets de "frontend" necesitan servir contenido públicamente, la solución correcta es configurar una distribución de **Amazon CloudFront** que apunte a estos buckets como origen, manteniendo los buckets mismos como privados.

Referencias

Blocking public access to your Amazon S3 storage - Amazon Simple Storage Service