


# GUÍA DE ACTIVIDADES PARA LA CONSTRUCCIÓN DE CONOCIMIENTO

NOMBRE DE LA ASIGNATURA		DESARROLLO DE SOLUCIONES EN LA NUBE – CLOUD COMPUTING						
NOMBRE DE LA ACTIVIDAD		Explorando IAM - GCP						
TIPO DE ACTIVIDAD	Sincrónica		Asincrónica	x	Individual	x	Grupal	
TEMÁTICA REQUERIDA PARA LA ACTIVIDAD			OBJETIVOS					
Tema 3. Jerarquía de recursos GCP - IAM			Utilizar Cloud IAM para restringir el acceso a funciones o recursos específicos de GCP. Utilizar la función de usuario de cuenta de servicio.					
COMPETENCIAS			INSUMOS PARA EL DESARROLLO DE LA ACTIVIDAD / REFERENCIAS BIBLIOGRÁFICAS					
• Ninguna			• Cuenta de Google Cloud Platform-GCP					
CONOCIMIENTOS PREVIOS REQUERIDOS								
Ninguna								
ESPECIFICACIONES DE LA ACTIVIDAD								
<p><b>Procedimientos:</b></p> <p>El sistema de Identity and Access Management (IAM) de Google Cloud te permite otorgar acceso detallado a recursos específicos de Google Cloud y ayuda a evitar el acceso a otros recursos. IAM te permite adoptar el principio de seguridad de privilegio mínimo, que indica que nadie debe tener más permisos que los que realmente necesita.</p> <p><b>Tarea 1: Explore la consola de IAM y explore sus funciones</b></p> <ol style="list-style-type: none"><li>1. Ingresa a la consola de Google Cloud Platform con su cuenta</li><li>2. En el <b>menú de navegación</b> () , haga clic en <b>IAM y administración &gt; IAM</b>.</li></ol>								

IAM

APRENDIZAJE

PERMISOS

HISTORIAL DE RECOMENDACIONES

Permisos para el proyecto "My First Project"

Estos permisos afectan a este proyecto y todos sus recursos. [Más información](#)

3 cuentas de servicio con funciones con una gran cantidad de privilegios de propietario o editor tienen permisos que no usan. Para mejorar la seguridad, aplica las recomendaciones a estas cuentas. [Obtén más información sobre las recomendaciones](#)

VER RECOMENDACIONES EN LA TABLA

☐ Incluir asignaciones de roles proporcionadas por Google

VER POR PRINCIPALES

VER POR ROLES

OTORGAR ACCESO

ELIMINAR ACCESO

Filtro

Ingresar el nombre o el valor de la propiedad

Tipo	Principal	Nombre	Rol	Estadísticas de seguridad	Herencia
	234845573531-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	7686/7687 permisos no usados	
	august-vine-346421@appspot.gserviceaccount.com	App Engine default service account	Editor	7687/7687 permisos no usados	
	cloud-sql-prony@august-vine-346421-iam.gserviceaccount.com	cloud-sql-prony	Administrador de Cloud SQL	106/106 permisos no usados	
	jafralee@gmail.com	jairo seane	Propietario	8708/8796 permisos no usados	

3. Haga clic en **OTORGAR ACCESO** y explore las funciones del menú desplegable. Para conocer las distintas funciones relacionadas con cada recurso, navegue por el menú **Funciones**.

Otorgar acceso a "My First Project"

Otorga a las principales acceso a este recurso y agrega roles para especificar qué acciones pueden realizar. De manera opcional, puedes agregar condiciones para otorgar acceso a las principales solo cuando se cumplan criterios específicos. [Más información sobre las condiciones de IAM](#)

Recurso

My First Project

Agregar principales

Las principales son usuarios, grupos, dominios o cuentas de servicio. [Más información sobre las principales de IAM](#)

Principales nuevas \*

Ingresar al menos una principal

Asignar funciones

Los roles se componen de conjuntos de permisos y determinan lo que la principal puede hacer con este recurso. [Más información](#)

Selecciona un rol \*

Condición de IAM (opcional)

+ AGREGAR CONDICIÓN DE IAM

+ AGREGAR OTRO ROL

GUARDAR

CANCELAR


4. Haga clic en **CANCELAR**.

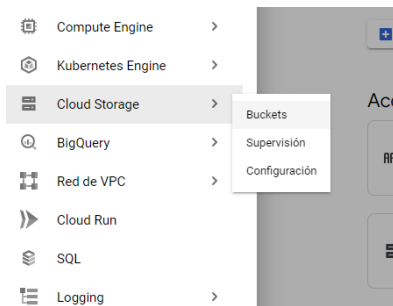
## Tarea 2: prepare un recurso para pruebas de acceso

Para esta tarea se han aprovisionado dos nombres de usuario con diferentes roles de un dominio de Cloud Identity real. Por ello, **se solicita limitarse solo a las actividades que se indiquen en esta tarea, para evitar incurrir en gastos por consumo de recursos y cumplimientos de cuotas.**

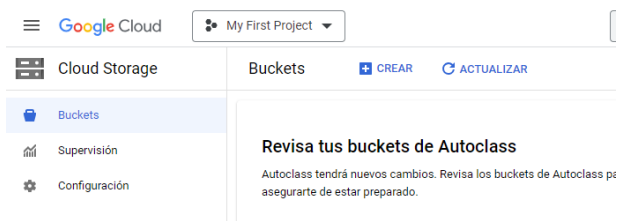
Los detalles de las cuentas aprovisionadas se indican en la siguiente tabla:

Username	Password	Roles IAM
<a href="#">usuario-iam-1@ingseosolutions.com</a>	usuarioiam12345#	Administrador de objetos de Storage Visualizador
<a href="#">usuario-iam-2@ingseosolutions.com</a>	usuarioiam12345#	Visualizador

1. Acceda a Google Cloud Console como el usuario **usuario-iam-1**
2. En el **menú de navegación** () , haga clic en **Cloud Storage > Buckets**.



3. Haga click en **Crear Bucket**



4. Especifique lo siguiente y deje las configuraciones restantes con sus valores predeterminados

Propiedad	Valor (escriba el valor o seleccione la opción como se especifica)
Nombre	Ingresa un nombre único a nivel global
Tipo de ubicación	Region: us-central1 (iowa)

✓ **Asigna un nombre a tu bucket**  
Nombre: example-js-bucket-1

• **Elige dónde almacenar tus datos**  
Esta opción define la ubicación geográfica de tus datos y afecta el costo, el rendimiento y la disponibilidad. No se puede cambiar más adelante. [Más información](#)

**Tipo de ubicación**

☐ Multi-region  
Máxima disponibilidad en el área más amplia

☐ Dual-region  
Alta disponibilidad y baja latencia en 2 regiones

☒ Region  
Latencia mínima dentro de una sola región

us-central1 (Iowa)

CONTINUAR

• **Elige una clase de almacenamiento para tus datos**  
Clase de almacenamiento predeterminada: Standard

• **Elige cómo controlar el acceso a los objetos**  
Prevención del acceso público: Activada  
Control de acceso: Uniforme

• **Elige cómo proteger los datos de objeto**  
Herramientas de protección: Ninguno  
Encriptación de datos: Administrada por Google

CREAR CANCELAR

- Haga click en **Crear**
- Haga clic en **SUBIR ARCHIVOS**.
- Suba algún archivo de texto de muestra desde su computadora local
- Una vez que se suba el archivo, haga clic en los tres puntos ubicados al final de la línea que contiene el archivo y, luego, en **Cambiar nombre**.
- Cambie el nombre del archivo a **sample.txt** y haga clic en **CAMBIAR NOMBRE**.
- Como puede observar el usuario permitió la creación de un Bucket y agregarle un archivo.**
- Acceda a Google Cloud Console como el usuario **usuario-iam-2**
- En Console, vaya al **menú de navegación** y haga clic en **Cloud Storage > Buckets** y verifique que puede visualizar el bucket creado.
- Intente crear un nuevo Bucket aplicando los pasos indicados anteriormente
- ¿Cuál fue el resultado? ¿Cuál es la razón?**


### Tarea 3: Utilice la función cuenta de servicio

#### Creacion de una cuenta de servicio

- En el **menú de navegación** () , haga clic en **IAM y administrador > Cuentas de servicio**.
- Haga clic en **CREAR CUENTA DE SERVICIO**.
- Especifique el **Nombre** de la cuenta de servicio como **read-bucket-objects**.
- Haga clic en **CREAR Y CONTINUAR**.
- Especifique la **Función** como **Cloud Storage > Visualizador de objetos de Storage**.
- Haga clic en **CONTINUAR**.

7. Haga clic en **LISTO**.

### Creacion de una VM con el usuario de cuenta de servicio

1. En el **menú de navegación** () , haga clic en **Compute Engine > Instancias de VM**.
2. Haga clic en **CREAR INSTANCIA**.
3. Especifique lo siguiente y deje la configuración restante con sus valores predeterminados:

Propiedad	Valor (escriba el valor o seleccione la opción como se especifica)
Nombre	demoiam
Región	us-central1 (iowa)
Zona	us-central1-a
Serie	E2
Tipo de máquina	e2-micro (2 vCPU, 1 GB memory)
Disco de arranque	Debian GNU/Linux 11 (bullseye)
Cuenta de servicio	read-bucket-objects

4. Haga clic en **Crear**.

### Utilice la función cuenta de servicio

En este punto, puede hacer que el usuario pruebe el acceso conectándose a través de SSH a la VM y realizando las siguientes acciones. Como propietario del proyecto, ya posee la función Usuario de cuenta de servicio. Por lo tanto, puede simular la experiencia del usuario si utiliza SSH para acceder a la VM desde Cloud Console.

1. En la vm **demoiam**, haga clic en **SSH** para iniciar una terminal y conectarse.
2. Ejecute el siguiente comando, el cual, permite mostrar una lista de las vm creadas:  
`gcloud compute instances list`
3. **¿Qué pasó? ¿Por qué?**
4. Liste el contenido del bucket que creó antes, con el siguiente comando:  
`gsutil ls gs://[YOUR_BUCKET_NAME]/`
5. **¿Qué pasó? ¿Por qué?**
6. Copie el archivo sample.txt del bucket que creó antes. Tenga en cuenta que el punto final es parte del siguiente comando. Significa copiar en “esta ubicación”:

```
gsutil cp gs://[YOUR_BUCKET_NAME]/sample.txt .
```

7. **¿Qué pasó? ¿Por qué?**

8. Puede verificar que el archivo sample.txt fue copiado con el comando **ls**

9. Para cambiar el nombre del archivo que copió, ejecute el siguiente comando:

```
mv sample.txt sample2.txt
```

10. Intente copiar el archivo al que le cambió el nombre en el bucket, ejecutando el siguiente comando:

```
gsutil cp sample2.txt gs://[YOUR_BUCKET_NAME]
```

11. **¿Qué pasó? ¿Por qué?**

Dado que se conectó a la instancia a través de SSH, puede **"actuar como la cuenta de servicio"** y utilizar prácticamente los mismos permisos.

La cuenta de servicio con la que se inició la instancia tenía la función Visualizador de objetos de almacenamiento, que permite descargar objetos de los buckets de GCS al proyecto.

Para mostrar la lista de instancias de un proyecto, debe otorgar el permiso **compute.instance.list**. Dado que la cuenta de servicio no tenía ese permiso, no se pudo mostrar la lista de instancias que se estaban ejecutando en el proyecto.

Dado que la cuenta de servicio **sí** tenía permiso para descargar objetos, pudo descargar un objeto del bucket. Pero no tenía permiso para escribir objetos, por lo que recibió el mensaje **"403: Access denied"**.

### Modificando la cuenta de servicio

1. En la ventana de **IAM** intente editar los permisos de la cuenta de servicio **read-bucket-objects** haciendo clic en el ícono de lápiz. **read-bucket-objects** actualmente tiene la función de **Visualizador de objetos de Storage**. Cambie la **Función** por **Cloud Storage > Creador de objetos de almacenamiento**.

2. Haga clic en **Guardar**.

3. Regrese a la ventana SSH de **demoiam**.

4. Para volver a copiar el archivo al que le cambió el nombre en el bucket, ejecute el siguiente comando:

```
gsutil cp sample2.txt gs://[YOUR_BUCKET_NAME]
```

5. **Esta vez, el comando se ejecutará de forma correcta, ya que la cuenta de servicio tiene los permisos correctos.**

## ¡Felicitaciones!

RECOMENDACIONES /  
OBSERVACIONES

Ninguna