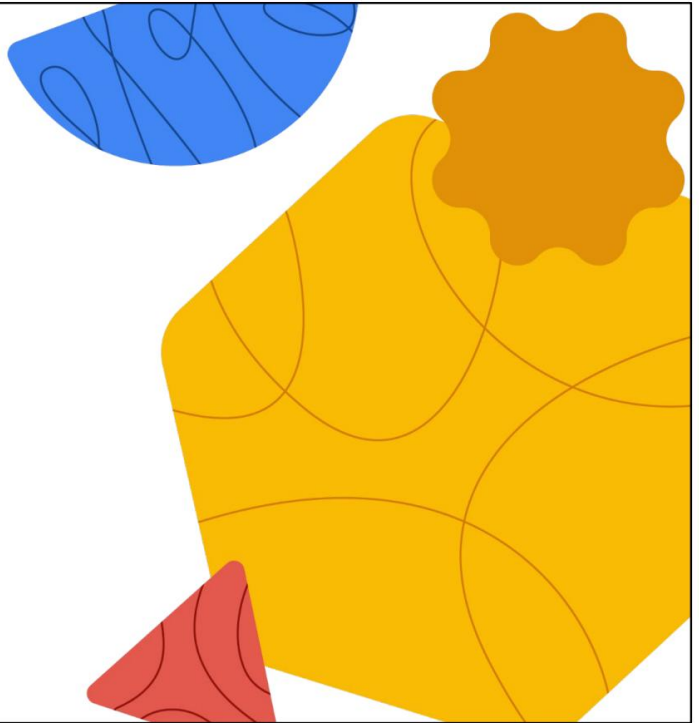




# Preparándose para su Nube profesional Ingeniero de seguridad Viaje

Libro de trabajo del curso

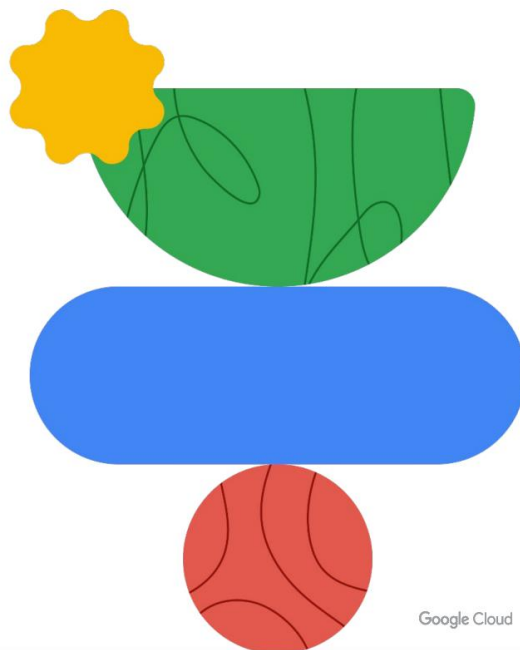


## Secciones de la guía de exámenes de certificación

- 1 Configurar el acceso
- 2 Asegurar las comunicaciones y establecer protección de límites
- 3 Garantizar la protección de datos
- 4 Gestión de operaciones
- 5 Apoyando los requisitos de cumplimiento



# Sección 1: Configurar el acceso



## 1.1 | Pregunta de diagnóstico 01

Cymbal Bank ha adquirido una empresa financiera no bancaria (NBFC). Esta NBFC utiliza Active Directory como directorio central en un servidor Windows local. Se le ha encomendado la tarea de migrar todos los usuarios y la información de los empleados de la NBFC a Cloud Identity.

¿Qué debes hacer?

- A. Ejecute Microsoft System Center Configuration Manager (SCCM) en un Instancia de Compute Engine. Deje el canal sin cifrar porque Estás en un entorno seguro de Google Cloud. Implementa Google Cloud Sincronización de directorios en la instancia de Compute Engine. Conéctese a la entorno de Windows Server local desde la instancia y migre usuarios a Cloud Identity.
- B. Ejecute Configuration Manager en una instancia de Compute Engine. Copie el archivo de configuración resultante de esta máquina en una nueva instancia de Compute Engine para mantener el entorno de producción separado del entorno de ensayo. Deje el canal sin cifrar porque se encuentra en un entorno seguro de Google Cloud. Implemente Google Cloud Directory Sync en esta nueva instancia. Conéctese al entorno local de Windows Server desde la nueva instancia y migre los usuarios a Cloud Identity.
- C. Use Cloud VPN para conectar la red local a su entorno de Google Cloud. Seleccione una Servidor Windows unido a un dominio local. En el servidor Windows unido a un dominio, ejecute Configuration Manager y Google Cloud Directory Sync. Use el canal cifrado de Cloud VPN para transferir usuarios desde Active Directory local a Cloud Identity.
- D. Seleccione un servidor Windows unido a un dominio local. Ejecute Configuration Manager en el servidor Windows unido al dominio y copie el archivo de configuración resultante en una instancia de Compute Engine. Ejecute Google Cloud Directory Sync en la instancia de Compute Engine a través de Internet y use Cloud VPN para sincronizar usuarios desde Active Directory local a Cloud Identity.



## 1.1 | Pregunta de diagnóstico 02

Cymbal Bank tiene ciertos permisos y accesos predeterminados para sus equipos de analistas, finanzas y cajeros. Estos equipos están organizados en grupos que tienen un conjunto de permisos de IAM basados en roles asignados a ellos. Después de una reciente adquisición de un banco pequeño, descubre que el banco pequeño asigna permisos directamente a sus empleados en IAM. Se le ha encomendado la tarea de aplicar la jerarquía de recursos de Cymbal Bank al banco pequeño. Los empleados necesitarán acceso a los servicios de Google Cloud.

¿Qué debes hacer?

- A. Deje todos los permisos de usuario como están en el IAM de un pequeño banco. Utilice la API de directorio en el SDK de administración de Google Workspace para Crea grupos de Google. Utiliza un script de Python para asignar usuarios a los Grupos de Google.
- B. Restablezca todos los permisos de usuario en la IAM del banco pequeño. Utilice Cloud Identity para crear grupos dinámicos para cada uno de los equipos del banco. Utilice el campo de metadatos de los grupos dinámicos para el tipo de equipo a fin de asignar usuarios a su grupo correspondiente con un script de Python.
- C. Restablezca todos los permisos de usuario en la IAM del banco pequeño. Utilice Cloud Identity para crear los grupos de Google necesarios. Actualice los grupos de Google a grupos de seguridad. Utilice un script de Python para asignar usuarios a los grupos.
- D. Restablezca todos los permisos de usuario en la IAM del banco pequeño. Utilice la API de directorio en el SDK de administración de Google Workspace para crear grupos de Google. Utilice un script de Python para asignar usuarios a los grupos.



# 1.1 Gestión de la identidad en la nube

## Cursos



### [Seguridad en Google Cloud](#)

M2: protección del acceso a Google Cloud



### [Gestión de la seguridad en Google Cloud](#)

M2: protección del acceso a Google Cloud

## Documentación

[Aprovisionamiento de cuentas de usuario de Active Directory | Gestión de identidad y acceso | Google Nube](#)

[¿Qué es Configuration Manager? - Ayuda para administradores de Google Workspace](#)

[Administrar membresías automáticamente con grupos dinámicos - Administrador de Google Workspace Ayuda](#)

[Creación y actualización de un grupo dinámico | Nube Identidad](#)

[Crear y administrar grupos mediante API - Google Ayuda para administradores del espacio de trabajo](#)

## 1.2 | Pregunta de diagnóstico 03

Cymbal Bank aprovecha los servicios de almacenamiento de Google Cloud, un clúster Apache Spark local y una aplicación web alojada en una nube de terceros. El clúster Spark y la aplicación web requieren acceso limitado a los depósitos de Cloud Storage y a una instancia de Cloud SQL durante solo unas pocas horas al día. Se le ha encomendado la tarea de compartir credenciales y minimizar el riesgo de que se vean comprometidas.

¿Qué debes hacer?

- A. Cree una cuenta de servicio con la información adecuada Permisos. Autenticar el clúster Spark y la aplicación web como solicitudes directas y compartir la clave de la cuenta de servicio.
- B. Cree una cuenta de servicio con los permisos adecuados. Haga que Spark El clúster y la aplicación web se autentican como solicitudes delegadas y comparten la credencial de cuenta de servicio de corta duración como JWT.
- C. Cree una cuenta de servicio con los permisos adecuados. Autentique el Spark Cluster y la aplicación web como una solicitud delegada y comparten la clave de la cuenta de servicio.
- D. Cree una cuenta de servicio con los permisos adecuados. Haga que Spark El clúster y la aplicación web se autentican como una solicitud directa y comparten las credenciales de la cuenta de servicio de corta duración como tokens XML.



## 1.2 | Pregunta de diagnóstico 04

Recientemente, Cymbal Bank descubrió un uso indebido de la clave de cuenta de servicio en uno de los equipos durante una auditoría de seguridad. Como medida de precaución, en el futuro no desea que ningún equipo de su organización genere nuevas claves de cuenta de servicio externas. También desea restringir el uso de cada nueva cuenta de servicio a su proyecto asociado.

¿Qué debes hacer?

- A. Navegue hasta Políticas organizacionales en el Consola de Google Cloud. Seleccione su organización. Seleccione
1. Cree una cuenta de servicio con el nombre de usuario y contraseña. Personalice la **propiedad** aplicada y configure la aplicación como "Activada". Haga clic en Guardar. Repita el proceso para `iam.disableCrossProjectServiceAccountUsage`.
- B. Ejecute el comando `gcloud resource-manager org-policies enable-enforce` con las restricciones `iam.disableServiceAccountKeyCreation` y `iam.disableCrossProjectServiceAccountUsage` y los ID de proyecto a los que desea que se apliquen las restricciones.
- C. Vaya a Políticas organizativas en Google Cloud Console. Seleccione su organización. Seleccione `iam.disableServiceAccountKeyCreation`. En Implementación de políticas, seleccione Fusionar con el elemento principal. Haga clic en Guardar. Repita el proceso para `iam.disableCrossProjectServiceAccountLienRemoval`.
- D. Ejecute el comando `gcloud resource-manager org-policies allow` con el valor booleano restricciones `iam.disableServiceAccountKeyCreation` y `iam.disableCrossProjectServiceAccountUsage` con ID de organización.





## 1.2 Gestión de cuentas de servicio

### Cursos



#### [Seguridad en Google Cloud](#)

- Gestión de identidad y acceso M3 (SOY)
  - M5 Protección de Compute Engine: Técnicas y mejores prácticas • M8
- Protección de Kubernetes: técnicas y mejores prácticas



#### [Gestión de la seguridad en Google Cloud](#)

- Gestión de identidad y acceso M3 (SOY)

#### [Prácticas recomendadas de seguridad en Google Cloud](#)

- M1 Protección del motor de cómputo: Técnicas y mejores prácticas • M4
- Protección de Google Kubernetes Motor: Técnicas y Mejores Prácticas

### Insignias de habilidad



Nube de Google

[Implementar la nube](#)  
[Fundamentos de seguridad en Google Cloud](#)

### Documentación


[Creación de una cuenta de servicio de corta duración](#)  
[credenciales](#) | [Documentación de IAM](#)

[Restringir el uso de cuentas de servicio](#) | [Recurso](#)  
[Documentación del administrador](#) | [Google Cloud](#)

## 1.3 Pregunta de diagnóstico 05

Cymbal Bank publica sus API a través de Apigee. Cymbal Bank ha adquirido recientemente ABC Corp, que utiliza un proveedor de identidad externo. Se le ha encomendado la tarea de conectar el proveedor de identidad de ABC Corp a Apigee para el inicio de sesión único (SSO). Debe configurar el SSO para que Google sea el proveedor de servicios. También desea supervisar y registrar actividades de alto riesgo.

¿Cuáles dos opciones seleccionarías para habilitar SSO?

- 
- A. Utilice openssl para generar archivos públicos y Claves privadas. Almacene la clave pública en un Certificado X.509 y cifrar mediante RSA o DSA para SAML. Inicie sesión en la consola de administración de Google y, en Seguridad, cargue el certificado.
  - B. Utilice openssl para generar una clave privada. Almacene la clave privada en un archivo X.509 Certificado y encriptelo con AES o DES para SAML. Inicie sesión en la consola de administración de Google Workspace y cargue el certificado.
  - C. Utilice openssl para generar claves públicas y privadas. Almacene la clave privada en un certificado X.509 y encripte con AES o DES para SAML. Inicie sesión en la consola de administración de Google y, en Seguridad, cargue el certificado.
  - D. Revise los resultados del mapeo de red y asigne perfiles SSO a los usuarios requeridos.
  - E. Revise los resultados del mapeo de red y asigne perfiles SAML a los requeridos. usuarios.

## 1.3 | Pregunta de diagnóstico 06



Usted es administrador del equipo de desarrollo móvil de Cymbal Bank. Desea controlar durante cuánto tiempo los distintos usuarios pueden acceder a la consola de Google Cloud, al SDK de Cloud y a cualquier aplicación que requiera autorización de usuario para ámbitos de Google Cloud sin tener que volver a autenticarse. Más específicamente, desea que los usuarios con privilegios elevados (propietarios de proyectos y administradores de facturación) se vuelvan a autenticar con más frecuencia que los usuarios normales a nivel de la organización. administrador de facturación.

¿Qué debes hacer?

- A. Abra todos los proyectos de Google Cloud que pertenecen a Equipo de desarrollo móvil de Cymbal Bank. Busque la configuración de control de sesión de Google Cloud de cada proyecto y configure una política de reautenticación que requiera la reautenticación. Elija la frecuencia de reautenticación en la lista desplegable.
- B. En la consola de administración, seleccione Control de sesión de Google Cloud y configure una política de reautenticación que requiera reautenticación. Elija la frecuencia de reautenticación en la lista desplegable.
- C. Cree una función personalizada para los propietarios de proyectos y los administradores de facturación a nivel de la organización en la consola de Google Cloud. Agregue la función reautenticación requerida Permiso para esta función. Asignar esta función a cada propietario de proyecto y
- D. Cree una función personalizada para los propietarios de proyectos y los administradores de facturación a nivel de la organización en la consola de Google Cloud. Agregue la función reautenticación requerida Permiso para esta función. Cree un grupo de Google que contenga a todos los administradores de facturación y propietarios de proyectos. Aplique la función personalizada al grupo.

# 1.3 Gestión de la autenticación

## Cursos



[Seguridad en Google Cloud](#)

M3 Identidad y acceso  
Gestión (IAM)



[Gestión de la seguridad en Google Cloud](#)

M3 Identidad y acceso  
Gestión (IAM)

## Documentación

[Descripción general de SAML | Apigee X | Google Cloud](#)

[Configurar el inicio de sesión único para Google administrado](#)

[Cuentas que utilizan proveedores de identidad de terceros -](#)

[Ayuda para administradores de Google Workspace](#)

[Asignar un perfil SSO a unidades organizativas o grupos -](#)

[Ayuda para administradores de Google Workspace](#)

[Resultados de mapeo de red - Google Workspace](#)

[Ayuda de administración](#)

[Creación y gestión de roles personalizados | IAM](#)

[Documentación](#)

[Comprensión de los roles personalizados de IAM | IAM](#)

[Documentación | Google Cloud](#)

[Descripción de los roles | Documentación de IAM](#)

## 1.4 Pregunta de diagnóstico 07



La jerarquía organizativa de Cymbal Bank divide la organización en departamentos. El departamento de ingeniería tiene una carpeta de "equipo de productos". Esta carpeta contiene carpetas para cada uno de los productos del banco. Cada carpeta de producto contiene un proyecto de Google Cloud, pero se pueden agregar más. Cada proyecto contiene una implementación de App Engine.

Cymbal Bank ha contratado a un nuevo gerente técnico de productos y a un nuevo desarrollador web. El gerente técnico de productos debe poder interactuar con todos los servicios de los proyectos que se transfieren a la carpeta del Departamento de Ingeniería y gestionarlos. El desarrollador web necesita acceso de solo lectura a las configuraciones y ajustes de App Engine para un producto específico.

- A. Asignar el rol de Editor de Proyecto en Cada proyecto individual a la Gerente técnico de producto. Asignar el rol de Editor de Proyecto en cada proyecto individual para el desarrollador web.
- B. Asignar el rol de Propietario del proyecto en cada proyecto individual al Gerente técnico de productos. Asignar el rol de Implementador de App Engine al desarrollador web en cada proyecto individual.
- C. Asigne el rol de Editor de proyectos en el nivel de carpeta del Departamento de ingeniería al gerente técnico de productos. Asigne el rol de Implementador de App Engine en el nivel de carpeta del producto específico al desarrollador web.
- D. Asigne el rol de Editor de proyectos en el nivel de carpeta del Departamento de ingeniería al gerente técnico de productos. Cree un rol personalizado en la carpeta del producto a la que el desarrollador web necesita acceder. Agregue los permisos `appengine.versions.create` y `appengine.versions.delete` a ese rol y asígnelo al desarrollador web.

¿Cómo debe asignar los roles de los nuevos empleados a su jerarquía siguiendo los principios del mínimo privilegio?

## 1.4 Pregunta de diagnóstico 08



La jerarquía organizativa de Cymbal Bank divide la organización en departamentos. El departamento de ingeniería tiene una carpeta de "equipo de productos". Esta carpeta contiene carpetas para cada uno de los productos del banco.

Una carpeta titulada "analytics" contiene un proyecto de Google Cloud que contiene una implementación de App Engine y una instancia de Cloud SQL.

Un equipo necesita acceso específico a este proyecto. El líder del equipo necesita acceso administrativo completo a App Engine y Cloud SQL. Un desarrollador debe poder configurar y administrar todos los aspectos de las implementaciones de App Engine. También hay un revisor de código que puede revisar periódicamente el código fuente de App Engine implementado sin realizar ningún cambio.

¿Qué tipos de permisos proporcionarías a cada uno de estos usuarios?

- A. Cree roles personalizados para los tres tipos de usuarios en el nivel de carpeta "analíticas". Para el líder del equipo, Proporcione todos los permisos de `appengine.*` y `cloudsql.*`. Para el desarrollador, proporcione `appengine.applications.*` y permisos `appengine.instances.*`. Para el revisor de código, proporcione los permisos `appengine.instances.*`.
- B. Asigne los roles básicos de "Administrador de App Engine" y "Administrador de Cloud SQL" al líder del equipo. Asigna el rol de "Administrador de App Engine" al desarrollador. Asigna el rol de "Visor de código de App Engine" al revisor de código. Asigna todos estos permisos en el nivel del proyecto de análisis.
- C. Cree roles personalizados para los tres tipos de usuarios en el nivel de proyecto. Para el líder del equipo, proporcione todos los permisos `appengine.*` y `cloudsql.*`. Para el desarrollador, proporcione los permisos `appengine.applications.*` y `appengine.instances.*`. Para el revisor de código, proporcione los permisos `appengine.instances.*`.
- D. Asignar el rol básico de "Editor" al líder del equipo. Crear un rol personalizado para el desarrollador. Proporcionar todos los permisos de `appengine.*` al desarrollador. Proporcionar el rol predefinido "Visor de código de App Engine" al revisor de código. Asignar todos estos permisos en el nivel de la carpeta "analytics".

# 1.4 | Gestión e implementación de controles de autorización

## Cursos



[Seguridad en Google Cloud](#)

M3 Identidad y acceso  
Gestión (IAM)



[Gestión de la seguridad en Google Cloud](#)

M3 Identidad y acceso  
Gestión (IAM)

## Insignias de habilidad



## Documentación

[Control de acceso para proyectos con IAM | Recurso](#)  
[Documentación del administrador | Google Cloud](#)

[Control de acceso para organizaciones con IAM |](#)  
[Documentación del Administrador de recursos | Google](#)  
[Nube](#)

[Control de acceso a carpetas con IAM | Recurso](#)  
[Documentación del administrador | Google Cloud](#)

[Descripción de los roles | Documentación de IAM](#)


[Descripción general de Access Content Manager](#)

[Descripción general del administrador de acceso privilegiado](#)

## 1.5 | Pregunta de diagnóstico 09

Cymbal Bank se divide en departamentos independientes, cada uno de los cuales se divide en equipos y cada equipo trabaja en un producto específico que requiere recursos de Google Cloud para su desarrollo.

¿Cómo diseñarías una jerarquía organizativa de Google Cloud para que se adapte mejor a la estructura organizativa y las necesidades de Cymbal Bank?

- 
- A. Cree un nodo de organización. En el Nodo de organización, crear departamento carpetas. Bajo cada Departamento, crea Carpetas de productos. En cada producto, crea carpetas de equipos. En la carpeta de equipos, agrega proyectos.
  - B. Cree un nodo de organización. En el nodo de organización, cree Carpetas de departamento. Cree carpetas de productos en cada departamento. Agregue proyectos a las carpetas de productos.
  - C. Cree un nodo de organización. En el nodo de organización, cree Carpetas de departamento. Cree carpetas de Teams en cada departamento. Agregue proyectos a las carpetas de Teams.
  - D. Cree un nodo de organización. En el nodo de organización, cree Carpetas de departamento. En cada departamento, crea una carpeta de equipos. En cada equipo, crea carpetas de productos. Agregue proyectos a las carpetas de productos.



## 1.5 | Pregunta de diagnóstico 10



Cymbal Bank cuenta con un equipo de desarrolladores y administradores que trabajan en diferentes conjuntos de recursos de Google Cloud. Los administradores del banco deberían poder acceder a los puertos seriales en las instancias de Compute Engine y crear cuentas de servicio. Los desarrolladores solo deberían poder acceder a los puertos seriales.

¿Cómo diseñaría la jerarquía de la organización para proporcionar el acceso requerido?

- A. Denegar el acceso al puerto serie y la creación de una cuenta de servicio en el Nivel de organización. Cree una carpeta 'admin' y configure las opciones obligatorias: falso para restricciones/compute.disableSerialPortAccess. Cree una nueva carpeta 'dev' dentro de la carpeta 'admin' y configure enforced: false para las restricciones/iam.disableServiceAccountCreation. Otorgue a los desarrolladores acceso a la carpeta 'dev' y a los administradores acceso a la carpeta 'admin'.
- B. Denegar el acceso al puerto serie y la creación de cuentas de servicio a nivel de la organización. Crear una carpeta "dev" y configurar enforced: false para limitations/compute.disableSerialPortAccess. Crear una nueva carpeta "admin" dentro de la carpeta "dev" y configurar enforced: false para limitations/iam.disableServiceAccountCreation. Dar a los desarrolladores acceso a la carpeta "dev" y a los administradores acceso a la carpeta "admin".
- C. Denegar el acceso al puerto serie y la creación de cuentas de servicio en el nivel de la organización. Crear una carpeta "dev" y establecer enforced: true para las restricciones/compute.disableSerialPortAccess y enforced: true para las restricciones/iam.disableServiceAccountCreation. Crear una nueva carpeta "admin" dentro de la carpeta "dev" y establecer enforced: false para las restricciones/iam.disableServiceAccountCreation. Dar a los desarrolladores acceso a la carpeta "dev" y a los administradores acceso a la carpeta "admin".
- D. Permitir el acceso al puerto serie y la creación de cuentas de servicio en el nivel de la organización. Crear una carpeta "dev" y configurar enforced: true para las restricciones/iam.disableServiceAccountCreation. Crear otra carpeta "admin" que herede de la carpeta principal dentro del nodo de la organización. Dar a los desarrolladores acceso a la carpeta "dev" y a los administradores acceso a la carpeta "admin".

# 1.5 Definición de la jerarquía de recursos

## Cursos



[Seguridad en Google Cloud](#)

M3 Identidad y acceso  
Gestión (IAM)

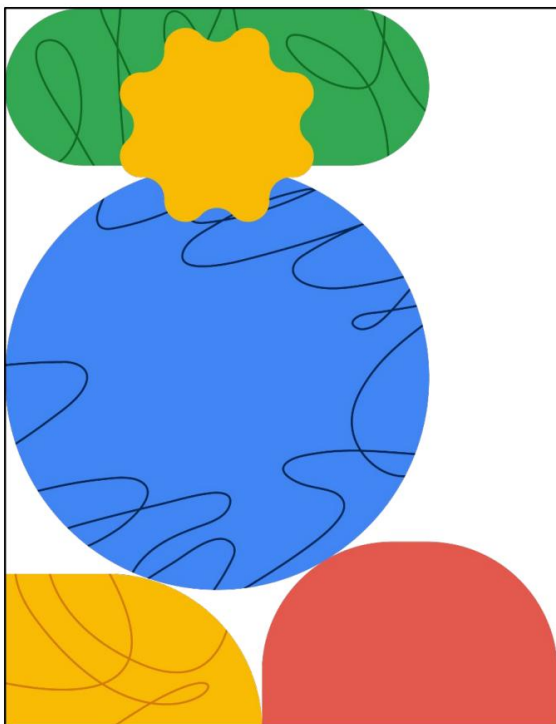


[Gestión de la seguridad en Google Cloud](#)

M3 Identidad y acceso  
Gestión (IAM)

## Documentación

- [Comprender la evaluación jerárquica | Recurso](#)
- [Documentación del administrador | Google Cloud](#)
- [Creación y gestión de organizaciones |](#)
- [Documentación del Administrador de recursos | Google](#)
- [Nube](#)
- [Mejores prácticas para organizaciones empresariales |](#)
- [Documentación | Google Cloud](#)



## Sección 2: Protección de las comunicaciones y establecimiento de protección de límites

## 2.1 Pregunta de diagnóstico 01

Cymbal Bank ha publicado una API que los equipos internos utilizarán a través del balanceador de carga de aplicaciones. Debe limitar el uso de la API a 200 llamadas por hora. Cualquier uso excesivo debe informar a los usuarios que los servidores están ocupados.

¿Qué comando gcloud ejecutarías para limitar el equilibrio de carga para la especificación dada?

A. gcloud computing security-policies reglas crear prioridad --security-policy sec-policy --src-ip-ranges=source-range --acción=acelerador --conteo-umbral-límite-de-velocidad=200 --intervalo-umbral-límite-de-velocidad-sec=3600 --acción-conforme=permitir --exceed-action=denegar-429 --enforce-on-key=ENCABEZADO HTTP

B. gcloud computing security-policies reglas crear prioridad --security-policy sec-policy --src-ip-ranges=rango-de-origen --acción=acelerador --umbral-límite-de-velocidad-conteo=200 --umbral-límite-de-velocidad-intervalo-sec=60 --acción-de-conformidad=denegar --exceed-action=denegar-404 --enforce-on-key=ENCABEZADO HTTP

C. Las reglas de políticas de seguridad de gcloud computing crean prioridad --security-policy sec-policy --src-ip-ranges=rango-de-origen --action=prohibición-basada-en-tasa --umbral-límite-de-velocidad-conteo=200 --umbral-límite-de-velocidad-intervalo-sec=3600 --acción-de-conformidad=denegar --exceed-action=denegar-403 --enforce-on-key=ENCABEZADO HTTP

D. Las reglas de políticas de seguridad de gcloud computing crean prioridad --security-policy sec-policy --src-ip-ranges="<rango de origen>" --action=rate-based-ban --conteo-umbral-límite-de-velocidad=200 --intervalo-umbral-límite-de-velocidad-sec=3600 --acción-conforme=permitir --exceed-action=denegar-500 --enforce-on-key=IP



## 2.1 Pregunta de diagnóstico 02



Cymbal Bank está lanzando una nueva aplicación de gestión de préstamos que utiliza un grupo de instancias administradas por Compute Engine. Los usuarios externos se conectarán a la aplicación mediante un nombre de dominio o una dirección IP protegida con TLS 1.2.

Un balanceador de carga ya aloja esta aplicación y conserva la dirección IP de origen. Usted tiene la tarea de configurar el certificado SSL para este balanceador de carga.

¿Qué debes hacer?

- A. Cree un certificado SSL administrado por Google. Adjunte un certificado SSL global. dirección IP externa dinámica al balanceador de carga de aplicaciones interno. Valide que un mapa de URL existente enrute el servicio entrante al backend de su grupo de instancias administradas. Cargue su certificado y cree un proxy HTTPS que enrute a su mapa de URL. Cree una regla de reenvío global que enrute las solicitudes entrantes al proxy.
- B. Cree un certificado SSL administrado por Google. Adjunte una dirección IP externa estática global a la dirección IP global. Balanceador de carga de aplicaciones externo. Valide que un mapa de URL existente enrute el servicio entrante al backend de su grupo de instancias administradas. Cargue su certificado y cree un proxy HTTPS que enrute a su mapa de URL. Cree una regla de reenvío global que enrute las solicitudes entrantes al proxy.
- C. Importe un certificado SSL autogestionado. Adjunte una dirección IP externa estática global al certificado externo. Balanceador de carga de red proxy. Valide que un mapa de URL existente enrute el servicio entrante al backend de su grupo de instancias administradas. Cargue su certificado y cree un proxy TCP que enrute a su mapa de URL. Cree una regla de reenvío global que enrute las solicitudes entrantes al proxy.
- D. Importe un certificado SSL autogestionado. Adjunte una dirección IP externa estática global al certificado externo. Balanceador de carga de red proxy. Valide que un mapa de URL existente enrute el servicio entrante al backend de su grupo de instancias administradas. Cargue su certificado y cree un proxy SSL que enrute a su mapa de URL. Cree una regla de reenvío global que enrute las solicitudes entrantes al proxy.

## 2.1 Pregunta de diagnóstico 03



Su organización tiene un sitio web que se ejecuta en Compute Engine. Esta instancia solo tiene una dirección IP privada. Debe proporcionar acceso SSH a un desarrollador local que depurará el sitio web desde el servidor autorizado.

Ubicación únicamente en las instalaciones.

¿Cómo habilitar esto?

- A. Configure una VPN en la nube. Configure un túnel sin cifrar hacia uno de los hosts de la red. Cree reglas de firewall de salida o de entrada. Utilice la dirección IP privada para iniciar sesión con un comando `gcloud ssh`.
- B. Utilice el proxy SOCKS a través de SSH. Configure un túnel SSH hacia uno de los hosts de la red. Cree el proxy SOCKS en el lado del cliente.
- C. Utilice el firewall de la VPC predeterminada. Abra el puerto 22 para el protocolo TCP mediante la consola de Google Cloud.
- D. Utilice un proxy con reconocimiento de identidad (IAP). Configure el reenvío TCP de IAP creando reglas de firewall de entrada en el puerto 22 para TCP usando el comando `gcloud`.

# 2.1 | Diseño y configuración de la seguridad perimetral

## Cursos



### Redes en Google Cloud • M3

Supervisión y registro de redes • M9 Control de acceso a redes VPC • M11 Equilibrio de carga híbrido y gestión de tráfico

### Seguridad en Google Cloud

- M4 Configuración de VPC para aislamiento y seguridad
- M7 Seguridad de aplicaciones: técnicas y mejores prácticas • M8 Protección de Google Kubernetes Engine: técnicas y mejores prácticas
- M9 Protección contra ataques DDoS



### Redes en Google Cloud: conceptos básicos •

Monitoreo y registro de red M3

### Redes en Google Cloud: seguridad de la red • M2

Control de acceso a redes VPC

### Redes en Google Cloud: equilibrio de carga

• Equilibrio de carga híbrido M1 y gestión de tráfico

### Gestión de la seguridad en Google Cloud

• M4 Configuración de VPC para aislamiento y seguridad

### Prácticas recomendadas de seguridad en Google Cloud

- M3 Seguridad de aplicaciones: técnicas y mejores prácticas • M4 Protección de Google Kubernetes Engine: técnicas y mejores prácticas

### Mitigación de vulnerabilidades de seguridad en Google

Cloud • M1 Protección contra ataques DDoS

## Insignias de habilidad



Nube de Google

[Construir y proteger](#)  
[Redes en](#)  
[Nube de Google](#)



Nube de Google

[Implementar la nube](#)  
[Fundamentos de seguridad](#)  
[en Google Cloud](#)

## Documentación

[Descripción general de Cloud NGFW](#)

[Actualización de reglas de políticas de seguridad de gcloud computing | Documentación del SDK de la nube](#)

[Políticas de seguridad de gcloud computing | SDK de la nube Documentación](#)

[Configuración del balanceador de carga de aplicaciones clásico con un backend de grupo de instancias administradas | Cargar](#)

[Equilibrio | Google Cloud](#)

[Uso de certificados SSL administrados por Google | Cargar](#)  
[Equilibrio](#)

[Uso de IAP para reenvío TCP | Con reconocimiento de identidad Proxy | Nube de Google](#)

[Conexión segura a instancias de VM | Computación](#)  
[Documentación del motor | Google Cloud](#)

## 2.2 Pregunta de diagnóstico 04

Recientemente se unió a Cymbal Bank como ingeniero de la nube. Creó una red VPC personalizada y seleccionó usar el modo de creación de subred automática y nada más. La red predeterminada aún existe en su proyecto. Crea una nueva instancia de máquina virtual Linux y selecciona la VPC personalizada como interfaz de red. Intenta conectarse a su instancia mediante SSH, pero recibe un error de "conexión fallida".

¿Qué respuesta explica mejor por qué no puedes acceder mediante SSH a la instancia?

A. Deberías haber eliminado la red predeterminada.

Cuando tiene varias VPC en su proyecto, Compute Engine no puede permitirle conectarse porque los rangos de IP superpuestos impiden que la API establezca una conexión raíz.

B. Debería haber utilizado la red predeterminada al configurar su instancia.

Si bien las redes personalizadas admiten la creación de instancias, solo deben usarse para la comunicación interna.

C. Debería haber utilizado el modo de creación de subredes personalizado. Dado que la VPC

predeterminada aún existe, el modo automático creó subredes en las mismas regiones, lo que generó direcciones IP superpuestas.

D. No configuró ninguna regla de firewall en su red VPC personalizada. Si bien la VPC predeterminada viene con una regla de firewall predefinida que permite el tráfico SSH, estas reglas deben agregarse a cualquier VPC personalizada.





## 2.2 Pregunta de diagnóstico 05



Cymbal Bank necesita conectar su base de datos MongoDB de empleados a una nueva aplicación web de recursos humanos en la misma red. Tanto la base de datos como la aplicación se escalan automáticamente con la ayuda de plantillas de instancia. Como administrador de seguridad y editor de proyectos, se le ha encomendado la tarea de permitir que la aplicación lea el puerto 27017 en la base de datos.

¿Qué debes hacer?

A. Cree cuentas de servicio para la aplicación y la base de datos. Cree una regla de firewall utilizando:

```
gcloud calculate firewall-rules create ALLOW_MONGO_DB --network
nombre-de-red --allow
TCP:27017 --source-
service-accounts cuenta-de-servicio-de-aplicación-web --target-service-
accounts cuenta-de-servicio-de-base-de-datos
```

B. Cree cuentas de servicio para la aplicación y la base de datos. Cree una regla de firewall utilizando:

```
gcloud calculate firewall-rules create ALLOW_MONGO_DB --network
nombre-de-red --allow
ICMP:27017 --source-
service-accounts cuenta-de-servicio-de-aplicación-web
--target-service-accounts cuenta-de-servicio-de-base-de-datos
```

C. Cree una cuenta de usuario para el administrador de la base de datos y una cuenta de servicio para la aplicación. Cree una regla de firewall utilizando:

```
gcloud calculate firewall-rules create ALLOW_MONGO_DB --network
nombre-de-red --allow
TCP:27017 --source-
service-accounts cuenta-de-servicio-de-aplicación-web --target-service-
accounts cuenta-de-usuario-de-administración-de-base-de-datos
```

D. Cree cuentas de usuario para la aplicación y la base de datos. Cree una regla de firewall utilizando:

```
gcloud calculate firewall-rules create ALLOW_MONGO_DB --network
nombre-de-red --deny UDP:27017
--source-service-
accounts cuenta-de-usuario-de-aplicación-web --target-service-accounts
cuenta-de-usuario-de-administrador-de-base-de-datos
```

## 2.2 Pregunta de diagnóstico 06



Cymbal Bank ha diseñado una aplicación para detectar fraudes con tarjetas de crédito que analizará información confidencial. La aplicación que se ejecuta en una instancia de Compute Engine está alojada en una nueva subred en una VPC existente. Varios equipos que tienen acceso a otras máquinas virtuales en la misma VPC deben acceder a la máquina virtual. Debe configurar el acceso para que las máquinas virtuales no autorizadas o los usuarios de Internet no puedan acceder a la máquina virtual de detección de fraudes.

¿Qué debes hacer?

A. Utilice el aislamiento de subred. Cree una cuenta de servicio para la máquina virtual de detección de fraudes.

Cree una cuenta de servicio para todas las instancias de Compute Engine de los equipos que Accederá a la máquina virtual de detección de fraudes. Cree una nueva regla de firewall usando:

```
gcloud calculate firewall-rules create ACCESS_FRAUD_ENGINE --network <nombre de la red> --allow TCP:80 --source-service-accounts <una cuenta de servicio para todos los equipos> --target-service-accounts <cuenta de servicio del motor de detección de fraude>
```

B. Utilice el filtrado de destino. Cree dos etiquetas llamadas "app" y "data". Asigne la etiqueta "app" a la instancia de Compute Engine que aloja la aplicación de detección de fraude (origen) y asigne la etiqueta "data" a las otras instancias de Compute Engine (destino). Cree una regla de firewall para permitir toda la comunicación de entrada en esta etiqueta.

C. Utilice el aislamiento de subred. Cree una cuenta de servicio para el motor de detección de fraudes. Cree cuentas de servicio para cada una de las instancias de Compute Engine de los equipos que accederán al motor. Agregue una regla de firewall mediante lo siguiente:

```
gcloud calculate firewall-rules create ACCESS_FRAUD_ENGINE --network <nombre de la red> --allow TCP:80 --source-service-accounts <lista de cuentas de servicio> --target-service-accounts <cuenta de servicio del motor de detección de fraude>
```

D. Utilice el filtrado de destino. Cree una etiqueta llamada "aplicación" y asígnela tanto al origen como al destino. Cree una regla de firewall para Permitir toda comunicación de ingreso en esta etiqueta.

2.2

Configuración de la segmentación de límites

Cursos



Redes en Google Cloud •  
Fundamentos de redes VPC M1 • Uso compartido de redes VPC M2 • Supervisión y registro de redes M3 • Enrutamiento y direccionamiento de redes M4 • Control de acceso a redes VPC M9

Seguridad en Google Cloud  
• M4 Configuración de VPC para aislamiento y seguridad  
• M5 Protección de Compute Engine  
• M8 Protección de Google Kubernetes Engine



Redes en Google Cloud: conceptos básicos •  
Fundamentos de redes VPC M1 • Redes VPC compartidas M2 • Monitoreo y registro de redes M3

Redes en Google Cloud: enrutamiento y direccionamiento •  
Enrutamiento y direccionamiento de red M1

Redes en Google Cloud: seguridad de la red • M2  
Control de acceso a redes VPC

Gestión de la seguridad en Google Cloud  
• M4 Configuración de VPC para aislamiento y seguridad

Prácticas recomendadas de seguridad en Google Cloud • M1 Protección de Compute Engine • M4 Protección de Google Kubernetes Engine

Insignias de habilidad



Documentación

- [Descripción general de las zonas DNS | Google Cloud](#)
- [Uso de reglas de firewall | VPC | Google Cloud](#)
- [Mejores prácticas y arquitecturas de referencia para Diseño de VPC](#)
- [Mejores prácticas y arquitecturas de referencia para Diseño de VPC](#)
- [Mejores prácticas para proteger cuentas de servicio | Documentación de IAM](#)

## 2.3 Pregunta de diagnóstico 07



Los datos de los solicitantes de préstamos de Cymbal Bank residen en una VPC compartida. Un equipo de análisis crediticio utiliza una herramienta CRM alojada en el entorno estándar de App Engine. Debe proporcionar a los analistas crediticios acceso a estos datos. Quiere que el equipo de análisis crediticio se haga cargo de los cargos.

¿Qué debes hacer?

- A. Agregue reglas de firewall de salida para permitir puertos TCP y UDP para App Engine entorno estándar en la red VPC compartida. Cree un conector del lado del cliente en el proyecto de servicio o un conector del lado del servidor en el proyecto host que utiliza el rango de IP o el ID del proyecto de la VPC de destino. Verifique que el conector esté en estado LISTO. Cree una regla de salida en la red VPC compartida para permitir que el conector use etiquetas de red o rangos de IP.
- B. Agregue reglas de firewall de salida para permitir puertos SSH o RDP para el entorno estándar de App Engine en la red de VPC compartida. Cree un conector del lado del cliente en el proyecto de servicio utilizando el rango de IP de la VPC de destino. Verifique que el conector esté en estado LISTO. Cree una regla de salida en la red de VPC compartida para permitir el conector utilizando etiquetas de red o rangos de IP.
- C. Agregue reglas de firewall de entrada para permitir rangos de NAT y Health Check para el entorno estándar de App Engine en el Red VPC compartida. Cree un conector del lado del cliente en el proyecto de servicio utilizando el ID del proyecto VPC compartido. Verifique que el conector esté en estado LISTO. Cree una regla de ingreso en la red VPC compartida para permitir el uso del conector mediante etiquetas de red o rangos de IP.
- D. Agregue reglas de firewall de entrada para permitir rangos de comprobación de estado y NAT para el entorno estándar de App Engine en la red de VPC compartida. Cree un conector del lado del servidor en el proyecto host utilizando el ID del proyecto de VPC compartida. Verifique que el conector esté en estado LISTO. Cree una regla de entrada en la red de VPC compartida para permitir el conector utilizando etiquetas de red o rangos de IP.

## 2.3 Pregunta de diagnóstico 08



La API de detalles de clientes de Cymbal Bank se ejecuta en una instancia de Compute Engine con solo una dirección IP interna. La nueva sucursal de Cymbal Bank está ubicada fuera de los puntos de presencia (PoP) de Google Cloud y requiere una forma de baja latencia para que sus aplicaciones locales consuman la API sin exponer las solicitudes a Internet pública.

¿Qué solución recomendarías?

- A. Utilice una red de distribución de contenido (CDN). Establezca un emparejamiento directo con uno de los PoP habilitados para el borde de Google cercanos.
- B. Utilizar el emparejamiento de operadores. Utilizar un proveedor de servicios para acceder a su infraestructura de nivel empresarial y conectarse al entorno de Google Cloud.
- C. Utilice Partner Interconnect. Utilice un proveedor de servicios para acceder a su infraestructura de nivel empresarial para conectarse a Google Cloud.
- D. Utilice interconexión dedicada. Establezca un emparejamiento directo con uno de PoP habilitados para edge cercano de Google.

## 2.3 Pregunta de diagnóstico 09



Una agencia de auditoría externa debe realizar una revisión única del uso de Google Cloud por parte de Cymbal Bank. Los auditores deben poder acceder a una VPC predeterminada que contenga instancias de BigQuery, Cloud Storage y Compute Engine donde se almacena toda la información de uso. Se le ha encomendado la tarea de habilitar el acceso desde su entorno local, que ya tiene una VPN configurada.

¿Qué debes hacer?

- A. Utilice un túnel VPN en la nube. Utilice su proveedor de DNS para crear zonas y registros DNS para `private.googleapis.com`. Conecte el proveedor de DNS a su red local. Transmita la solicitud desde el entorno local. Utilice un firewall definido por software para administrar las solicitudes entrantes y salientes.
- B. Utilice Partner Interconnect. Configure un túnel cifrado en las instalaciones del auditor. Entorno. Utilice Cloud DNS para crear zonas DNS y registros A para `private.googleapis.com`.
- C. Utilice un túnel VPN en la nube. Utilice Cloud DNS para crear zonas y registros DNS para `*.googleapis.com`. Configure el enrutamiento local con Cloud Router. Utilice los anuncios de ruta personalizados de Cloud Router para anunciar rutas para destinos de Google Cloud.
- D. Utilice una interconexión dedicada. Configure una VLAN en el entorno local del auditor. Utilice Cloud DNS para crear zonas y registros DNS para `restrict.googleapis.com` y `private.googleapis.com`. Configure el enrutamiento local con Cloud Router. Agregue rutas estáticas personalizadas en la VPC para conectarse individualmente a instancias de BigQuery, Cloud Storage y Compute Engine.

## 2.3 Pregunta diagnóstica 10



Un portal de comercio electrónico utiliza Google Kubernetes Engine para implementar su motor de recomendaciones en contenedores Docker. Esta instancia de clúster no tiene una dirección IP externa. Necesitas proporcionar acceso a Internet a los pods del clúster de Kubernetes. ¿Qué configuración agregarías?

¿Qué debes hacer?

- A. Cloud DNS, rango de direcciones IP primarias de subred para nodos y rango de direcciones IP secundarias de subred para pods y servicios en el clúster
- B. Cloud VPN, rango de direcciones IP secundarias de subred para nodos y rango de direcciones IP secundarias de subred para pods y servicios en el clúster
- C. Balanceador de carga de Nginx, rango de direcciones IP secundarias de subred para nodos y rango de direcciones IP secundarias de subred para pods y servicios en el clúster
- D. Puerta de enlace NAT en la nube, rango de direcciones IP principales de subred para nodos y rango de direcciones IP secundarias de subred para pods y servicios en el clúster

2.3

# Establecer conectividad privada

## Cursos



[Redes en Google Cloud • Redes](#)

VPC compartidas M2 • Opciones de conexión privada M5 • Opciones de conectividad M13 • VPN en la nube M14

[Seguridad en Google Cloud](#)

• M4 Configuración de VPC para aislamiento y seguridad • M5 Protección de Compute Engine: técnicas y Mejores prácticas



[Redes en Google Cloud: conceptos básicos •](#)

Redes VPC compartidas M2

[Redes en Google Cloud: nube híbrida y multicloud](#) • Opciones de conectividad M1 • VPN en la nube M2

[Gestión de la seguridad en Google Cloud](#)

• M4 Configuración de VPC para aislamiento y seguridad

[Prácticas recomendadas de seguridad en](#)

Google Cloud • M1 Asegurando Compute Engine: Técnicas y Mejores prácticas

## Insignias de habilidad



Nube de Google

[Construir y proteger](#)

[Redes en](#)

[Nube de Google](#)



Nube de Google

[Implementar la nube](#)

[Fundamentos de seguridad](#)

[en Google Cloud](#)

## Documentación

[Configuración del acceso a VPC sin servidor | Google Nube](#)

[Descripción general de los controles de servicio de VPC | Google Nube](#)

[Elegir un producto de conectividad de red | Nube de Google](#)

[Acceso privado a Google | VPC](#)

[Administrar zonas | DNS en la nube](#)

[Acceso privado a Google para hosts locales | VPC](#)

[Simplificando la red en la nube para las empresas: Google anuncia Cloud NAT y más | Google](#)

[Río sobre la nube](#)

[Ejemplo de configuración de GKE | NAT en la nube](#)

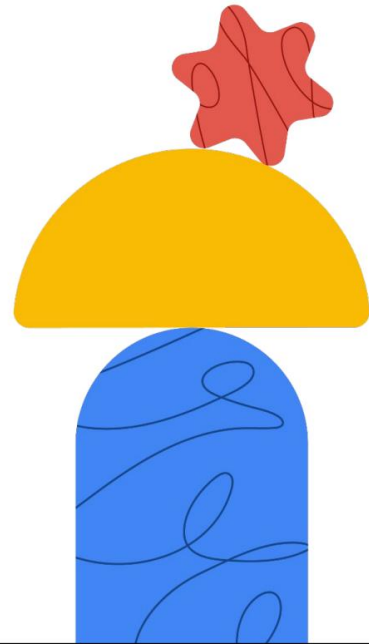
[Descripción general de NAT en la nube](#)



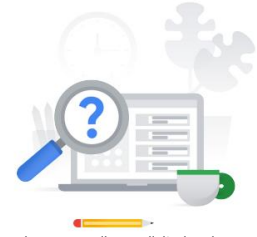


## Sección 3:

### Garantizar la protección de datos



## 3.1 Pregunta de diagnóstico 01 Discusión



Cymbal Bank ha contratado a un equipo de analistas de datos para analizar copias escaneadas de solicitudes de préstamos. Como se trata de un equipo externo, Cymbal Bank no desea compartir el nombre, el sexo, el número de teléfono ni los números de tarjetas de crédito que aparecen en las copias escaneadas. Se le ha encomendado la tarea de ocultar esta información de identificación personal y, al mismo tiempo, minimizar la latencia.

¿Qué debes hacer?

- A. Utilice la API de prevención de pérdida de datos (DLP) en la nube para realizar solicitudes de eliminación de imágenes. Proporcione su ID de proyecto, los tipos de información integrados y las copias escaneadas cuando realice las solicitudes.
- B. Utilice la API Cloud Vision para realizar el reconocimiento óptico de códigos (OCR) a partir de imágenes escaneadas. Redacte el texto utilizando la API Cloud Natural Language con expresiones regulares.
- C. Utilice la API Cloud Vision para realizar el reconocimiento de código óptico (OCR) a partir de imágenes escaneadas. Redacte el texto utilizando la API Cloud Data Loss Prevention (DLP) con expresiones regulares.
- D. Utilice la API de Cloud Vision para realizar la extracción de texto de los documentos escaneados. Redacte el texto utilizando la API Cloud Natural Language con expresiones regulares.

## 3.1 Pregunta de diagnóstico 02 Discusión



Cymbal Bank necesita predecir estadísticamente los días en que los clientes demoran los pagos de préstamos y tarjetas de crédito. Cymbal Bank no desea compartir las fechas exactas en las que un cliente incumplió o realizó un pago con los analistas de datos. Además, debe ocultar el nombre del cliente y la dirección de correo electrónico del cliente.

tipo, que podría ser corporativo o minorista.

¿Cómo proporcionar la información adecuada a los analistas de datos?

- A. Generalice todas las fechas a año y mes mediante la clasificación. Utilice el infoType integrado para el nombre del cliente. Utilice un infoType personalizado para el tipo de cliente con un diccionario personalizado.
- B. Generalizar todas las fechas a año y mes con clasificación. Utilizar el infoType integrado para el nombre del cliente. Utilizar un infoType personalizado para el tipo de cliente con expresión regular.
- C. Generalizar todas las fechas a año y mes con cambio de fecha. Utilizar un infoType predefinido para el nombre del cliente. Utilizar un infoType personalizado para el tipo de cliente con un diccionario personalizado.
- D. Generalizar todas las fechas a año y mes con cambio de fecha. Utilizar un infoType predefinido para el nombre del cliente. Utilizar un infoType personalizado para el tipo de cliente con expresión regular.

## 3.1 Pregunta de diagnóstico 03 Discusión



Cymbal Bank almacena información de los clientes en una tabla de BigQuery llamada "Información", que pertenece al conjunto de datos "Clientes". Varios departamentos de Cymbal Bank, incluidos los de préstamos, tarjetas de crédito y comercio, acceden a la tabla de información. Aunque la fuente de datos sigue siendo la misma, cada departamento necesita leer y analizar clientes y atributos de clientes por separado. Quiere una forma rentable de configurar el acceso departamental a BigQuery para proporcionar un rendimiento óptimo.

¿Qué debes hacer?

- A. Cree conjuntos de datos separados para cada departamento.
  - Cree vistas para cada conjunto de datos por separado.
  - Autorizar a estas vistas para acceder a la fuente
  - Conjunto de datos. Comparta los conjuntos de datos con los departamentos.
  - Proporcione la función `bigquery.dataViewer` a los usuarios requeridos de cada departamento.
- B. Cree un conjunto de datos autorizado en el panel Explorador de BigQuery. Escriba los metadatos de la tabla Clientes en un archivo JSON y edite el archivo para agregar el ID de proyecto y el ID de conjunto de datos de cada departamento. Proporcione el rol `bigquery.user` a los usuarios requeridos de cada departamento.
- C. Proteja los datos con clasificación. Abra la página Taxonomías del Catálogo de datos en el Consola de Google Cloud. Cree etiquetas de políticas para las columnas y filas obligatorias. Proporcione la función `bigquery.user` a los usuarios obligatorios de cada departamento. Proporcione acceso a las etiquetas de políticas a cada departamento por separado.
- D. Cree conjuntos de datos independientes para cada departamento. Cree funciones autorizadas en cada conjunto de datos para realizar las agregaciones necesarias. Escriba los datos transformados en tablas nuevas para cada departamento por separado. Proporcione la función `bigquery.dataViewer` a los usuarios necesarios de cada departamento.

## 3.1 Pregunta de diagnóstico 04 Discusión



Cymbal Bank tiene una instancia de Cloud SQL que debe compartirse con una agencia externa. A los desarrolladores de la agencia se les asignarán roles y permisos a través de un grupo de Google en Identity and Access Management (IAM). La agencia externa tiene un contrato anual y necesitará una cadena de conexión, un nombre de usuario y una contraseña para conectarse a la base de datos.

¿Cómo configurarías el acceso del grupo?

- A. Utilice Secret Manager. Utilice el atributo de duración para establecer el período de vencimiento en un año. Agregue la función `secretmanager.secretAccessor` para el grupo que contiene desarrolladores externos.
- B. Utilice el servicio de administración de claves en la nube. Utilice la dirección IP de destino y los atributos de puerto para proporcionar acceso a los desarrolladores de la agencia externa. Elimine el acceso de IAM después de un año y rote las claves compartidas. Agregue la función `cloudkms.cryptoKeyEncryptorDecryptor` para el grupo que contiene a los desarrolladores externos.
- C. Utilice el Administrador de secretos. Utilice el atributo de recurso para establecer un par clave-valor con la clave como Duración y valores como período de vencimiento dentro de un año. Agregue el rol `secretmanager.viewer` para el grupo que contiene desarrolladores externos.
- D. Utilice Secret Manager para la cadena de conexión y el nombre de usuario, y utilice Cloud Key Management Service para la contraseña. Utilice etiquetas para establecer el período de vencimiento en la marca de tiempo dentro de un año. Agregue los roles `secretmanager.secretVersionManager` y `secretmanager.secretAccessor` para el grupo que contiene desarrolladores externos.

# 3.1 | Protección de datos confidenciales y prevención de pérdida de datos

## Cursos



### Seguridad en Google Cloud

- M6 Protección de datos en la nube:  
Técnicas y mejores prácticas • Seguridad de aplicaciones M7:  
Técnicas y mejores prácticas • Contenido relacionado con M10  
Vulnerabilidades: Técnicas y Mejores prácticas



### Prácticas recomendadas de seguridad en Google Cloud

- M2 Protección de datos en la nube: técnicas y mejores prácticas
- Seguridad de aplicaciones M3: técnicas y mejores prácticas

### Mitigación de vulnerabilidades de seguridad en Nube de Google

- Vulnerabilidades relacionadas con el contenido de M2:  
Técnicas y mejores prácticas

## Documentación

- [Inspección y redacción de imágenes | Pérdida de datos](#)
- [Documentación de prevención | Google Cloud](#)
- [Cómo eliminar datos confidenciales de las imágenes | Datos](#)
- [Documentación de prevención de pérdidas | Google Cloud](#)
- [Referencia del detector InfoType | Pérdida de datos](#)
- [Documentación de prevención | Google Cloud](#)
- [Pseudonimización | Prevención de pérdida de datos](#)
- [Documentación | Google Cloud](#)
- [Vistas autorizadas | BigQuery | Google Cloud](#)
- [Conjuntos de datos autorizados | BigQuery | Google Cloud](#)
- [Compartir entre perímetros con puentes | VPC](#)
- [Controles de servicio | Google Cloud](#)
- [Creación de un puente perimetral | Servicio VPC](#)
- [Controles | Google Cloud](#)
- [Acceso contextual con reglas de ingreso | VPC](#)
- [Controles de servicio | Google Cloud](#)
- [Preguntas frecuentes | IAM](#)
- [Documentación](#)
- [Control de acceso con IAM | Secret Manager](#)
- [Documentación | Google Cloud](#)

## 3.2 | Pregunta de diagnóstico 05 Discusión



Cymbal Bank calcula los incentivos de los empleados mensualmente para el departamento de ventas y trimestralmente para el departamento de marketing. Los incentivos se liberan con el salario del mes siguiente. Los documentos de desempeño de los empleados se almacenan como hojas de cálculo, que se conservan durante al menos un año para su auditoría. Desea configurar el almacenamiento más rentable para este escenario.

¿Qué debes hacer?

- A. Importe las hojas de cálculo a BigQuery y cree tablas separadas para Ventas y Marketing. Establezca las reglas de caducidad de la tabla en 365 días para ambas tablas. Cree trabajos programados para ejecutarse cada trimestre para Marketing y cada mes para Ventas.
- B. Cargue las hojas de cálculo en Cloud Storage. Seleccione la clase de almacenamiento Nearline para el departamento de ventas y Coldline para el departamento de marketing. Use reglas de administración del ciclo de vida de objetos para configurar la clase de almacenamiento como Archival después de 365 días. Procese los datos en BigQuery con trabajos que se ejecutan mensualmente para ventas y trimestralmente para marketing.
- C. Importe las hojas de cálculo a Cloud SQL y cree tablas separadas para Ventas y Marketing. Para la caducidad de la tabla, establezca 365 días para ambas tablas. Utilice procedimientos almacenados para calcular los incentivos. Utilice trabajos cron de App Engine para ejecutar procedimientos almacenados mensualmente para Ventas y trimestralmente para Marketing.
- D. Importe las hojas de cálculo a Cloud Storage y cree tablas NoSQL. Utilice trabajos cron de App Engine para ejecutarlos mensualmente para Ventas y trimestralmente para Marketing. Utilice un trabajo independiente para eliminar los datos después de un año.

## 3.2 | Pregunta de diagnóstico 06 Discusión



Cymbal Bank utiliza Google Kubernetes Engine (GKE) para implementar sus contenedores Docker. Desea cifrar el disco de arranque de un clúster que ejecuta una imagen personalizada para que el banco controle la rotación de claves. Los clústeres de GKE también generarán hasta 1024 caracteres aleatorios que se utilizarán con las claves con contenedores Docker.

¿Qué pasos tomaría para aplicar la configuración de cifrado con una capa de seguridad de hardware dedicada?

- A. En la consola de Google Cloud, navegue hasta Google Kubernetes Engine. Seleccione su clúster y el nodo de arranque dentro del clúster. Habilite el cifrado administrado por el cliente. Use Cloud HSM para generar bytes aleatorios y brindar una capa adicional de seguridad.
- B. Cree un nuevo clúster de GKE con cifrado administrado por el cliente y HSM habilitado. Implemente los contenedores en este clúster. Elimine el clúster GKE anterior. Use Cloud HSM para generar bytes aleatorios y brindar una capa adicional de seguridad.
- C. Cree un nuevo conjunto de claves mediante Cloud Key Management Service. Extraiga esta clave a un certificado. Utilice el comando `kubectf` para actualizar la configuración de Kubernetes. Valide utilizando firmas digitales MAC y utilice un script de inicio para generar bytes aleatorios.
- D. Cree un nuevo llavero con el servicio de administración de claves en la nube. Extraiga esta clave en un Certificado. Utilice la consola de Google Cloud para actualizar la configuración de Kubernetes. Valide utilizando firmas digitales MAC y utilice un script de inicio para generar bytes aleatorios.



## 3.2 | Pregunta de diagnóstico 7 Discusión



Cymbal Bank necesita migrar las aplicaciones de procesamiento de préstamos existentes a Google Cloud. Estas aplicaciones transforman la información financiera confidencial. Todos los datos deben estar cifrados en todas las etapas, incluido el uso compartido entre sockets y RAM. También se debe realizar una prueba de integridad cada vez que se inicien estas instancias. Debe utilizar las claves de cifrado de Cymbal Bank para configurar las instancias de Compute Engine.

¿Qué debes hacer?

- A. Cree una instancia de máquina virtual confidencial con claves de cifrado proporcionadas por el cliente. En Cloud Logging, recopile todos los registros de `sevLaunchAttestationReportEvent`.
- B. Cree una instancia de VM protegida con claves de cifrado proporcionadas por el cliente. Registro en la nube, recopila todos los registros para `earlyBootReportEvent`.
- C. Cree una instancia de VM confidencial con claves de cifrado administradas por el cliente. Registro en la nube, recopila todos los registros para `earlyBootReportEvent`.
- D. Cree una instancia de máquina virtual protegida con claves de cifrado administradas por el cliente. En Cloud Logging, recopile todos los registros de `sevLaunchAttestationReportEvent`.

# 3.2      Gestión del cifrado en reposo, en tránsito y en uso

## Cursos



### [Seguridad en Google Cloud](#)

- M4 Configuración de la nube privada virtual para Aislamiento y seguridad •
- M5 Protección de Compute Engine: Técnicas y mejores prácticas • M6 Protección de datos en la nube: técnicas y mejores prácticas
- M8 Protege el motor Google Kubernetes



### [Gestión de la seguridad en Google Cloud](#)

- M4 Configuración de la nube privada virtual para Aislamiento y seguridad

### [Prácticas recomendadas de seguridad en Google Cloud](#)

- M1 Protección de Compute Engine • M2 Protección de datos en la nube • M4 Protección de Google Kubernetes Engine

## Insignias de habilidad



## Documentación

- [Clases de almacenamiento | Google Cloud](#)
- [Gestión del ciclo de vida de los objetos | Almacenamiento en la nube \(CMEK\) | Documentación del motor Kubernetes |](#)
- [Nube de Google](#)
- [Configuración de un disco de arranque personalizado | Kubernetes Documentación del motor | Google Cloud](#)
- [Uso de Cloud KMS con otros productos](#)
- [Claves rotativas | Documentación de Cloud KMS](#)
- [VM confidencial y Compute Engine | Google Nube](#)

## 3.3 | Pregunta de diagnóstico 08 Discusión



Estás creando un modelo de IA en Google Cloud para analizar datos de clientes y predecir el comportamiento de compra. Este modelo tendrá acceso a información confidencial, como el historial de compras y los datos demográficos.

Para proteger estos datos y evitar el uso indebido del modelo, ¿cuáles son los TRES controles de seguridad más importantes a implementar?

- A. Habilite Google Cloud Armor en su modelo implementado para bloquear solicitudes maliciosas.
- B. Almacene todos los datos de entrenamiento del modelo en BigQuery con acceso público para mayor transparencia.
- C. Configure los roles de IAM para otorgar acceso completo al modelo a todos los usuarios de Google Cloud.
- D. Implementar el modelo en una región con los más altos estándares de seguridad de datos.
- E. Supervise el rendimiento del modelo para detectar anomalías y sesgos y luego intervenga manualmente si es necesario.

### 3.3 Pregunta de diagnóstico 09 Discusión



Estás creando un modelo de aprendizaje automático en Google Cloud y tienes que elegir entre dos opciones: gestionar la infraestructura tú mismo (IaaS) o utilizar los servicios gestionados de Google (PaaS).

- A. Inspección del tráfico de red y detección de intrusiones
- B. Cumplimiento de las políticas de seguridad interna
- C. Ubicación de los datos y restricciones de residencia
- D. Controles de acceso y permisos granulares
- E. Refuerzo físico del servidor y parches de seguridad

Para garantizar la mejor postura de seguridad tanto para el modelo como para sus datos, ¿cuáles DOS factores debería priorizar al definir los requisitos de seguridad para cada opción de alojamiento?

## 3.3 Pregunta de diagnóstico 10 Discusión



Tiene la tarea de desarrollar un sistema de IA en Google Cloud para una empresa de telecomunicaciones. Este sistema de IA realizará un análisis de sentimientos sobre las conversaciones que los agentes tienen con los clientes y brindará recomendaciones conversacionales para mejorar la satisfacción del cliente en el futuro.

¿Qué controles de seguridad específicos de IA/ML necesita planificar al desarrollar este sistema?

- A. Seleccione los servicios de inteligencia artificial de Google Cloud que aprovechen un modelo PaaS. Son los únicos que pueden garantizar una base segura desde el diseño.
- B. Implemente su solución de IA mediante grupos de instancias administradas (MIG). Estos tienen controles de seguridad integrados específicos para ejecutar cargas de trabajo de IA.
- C. Aproveche un escáner de detección de amenazas específico para el modelo de IA. Las amenazas entre los sistemas de IA y los sistemas que no son de IA tienen muy poco en común.
- D. Los sistemas de IA están más interconectados que los sistemas que no son de IA. Prepárese para nuevos vectores de ataque, ya que los atacantes pueden aprovechar las vulnerabilidades de un sistema para atacar a otro.

### 3.3      Protección de las cargas de trabajo de IA

#### Cursos



Seguridad en Google Cloud

- M2 Asegura el acceso a Google Nube
- M6 Protección de datos en la nube:  
Técnicas y mejores prácticas •  
Contenido relacionado con M10  
Vulnerabilidades: Técnicas y  
Mejores prácticas
- Monitoreo, registro, auditoría y escaneo de M11



Gestión de la seguridad en Google Cloud

- M2 asegura el acceso a Google Cloud



Mejores prácticas de seguridad en Nube de Google

- M2 Protección de datos en la nube:  
Técnicas y mejores prácticas



Mitigación de vulnerabilidades de seguridad en Nube de Google

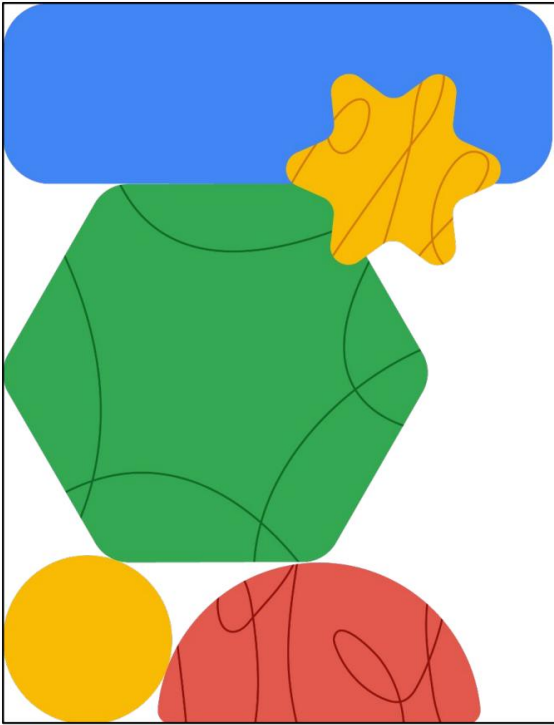
- Contenido relacionado con M2  
Vulnerabilidades: Técnicas y  
Mejores prácticas
- Monitoreo, registro, auditoría y escaneo de M3

#### Documentación

Cómo la protección de datos sensibles puede ayudar a proteger

Cargas de trabajo de inteligencia artificial generativa electrónica

PaaS vs. IaaS vs. SaaS



## Sección 4:

## Gestión de operaciones

## 4.1 | Pregunta de diagnóstico 01 Discusión



Cymbal Bank ha recibido archivos fuente de Docker de sus desarrolladores externos en un repositorio de Artifact Registry. Estos archivos de Docker formarán parte de un proceso de CI/CD para actualizar la oferta de préstamos personales de Cymbal Bank. El banco quiere evitar la posibilidad de que los usuarios remotos utilicen arbitrariamente los archivos de Docker para ejecutar cualquier código. Se le ha encomendado la tarea de utilizar el escaneo a pedido de Container Analysis para escanear las imágenes para una actualización única.

¿Qué debes hacer?

- A. Prepare un archivo `cloudbuild.yaml`. En este archivo, agregue cuatro pasos en orden (compilación, escaneo, verificación de gravedad e inserción) y especifique la ubicación del repositorio de Artifact Registry. Especifique el nivel de gravedad como **CRÍTICO**. Inicie la compilación con el comando `gcloud builds submission`.
- B. Prepare un archivo `cloudbuild.yaml`. En este archivo, agregue cuatro pasos en orden (escaneo, compilación, verificación de gravedad e inserción) y especifique la ubicación del repositorio de Artifact Registry. Especifique el nivel de gravedad como **ALTO**. Inicie la compilación con el comando `gcloud builds submission`.
- C. Prepare un archivo `cloudbuild.yaml`. En este archivo, agregue cuatro pasos en orden (escaneo, verificación de gravedad, compilación y envío) y especifique la ubicación del repositorio de Artifact Registry. Especifique el nivel de gravedad como **ALTO**. Inicie la compilación con el comando `gcloud builds submission`.
- D. Prepare un archivo `cloudbuild.yaml`. En este archivo, agregue cuatro pasos en orden (compilación, verificación de gravedad, escaneo e inserción) y especifique la ubicación del repositorio de Artifact Registry. Especifique el nivel de gravedad como **CRÍTICO**. Inicie la compilación con el comando `gcloud builds submission`.



## 4.1 | Pregunta de diagnóstico 02 Discusión



La gerencia de Cymbal Bank está preocupada por el riesgo de que las máquinas virtuales puedan verse comprometidas por actores maliciosos. Más específicamente, quieren recibir alertas inmediatas si ha habido cambios en la secuencia de arranque de cualquiera de sus instancias de Compute Engine.


¿Qué debes hacer?

- A. Establezca una política a nivel de organización que requiera que todas las máquinas virtuales de Compute Engine se configuren como máquinas virtuales protegidas. Utilice el arranque seguro habilitado con la interfaz de firmware extensible unificada (UEFI). Valide eventos de integridad en Cloud Monitoring y coloque alertas en eventos de certificación de lanzamiento.
- B. Establezca políticas de medición de Cloud Logging en las máquinas virtuales. Utilice Cloud Logging para colocar alertas siempre que las medidas reales y las medidas políticas no coincidan.
- C. Establezca una política a nivel de organización que requiera que todas las máquinas virtuales de Compute Engine se configuren como Máquinas virtuales protegidas. Utilice el arranque medido habilitado con el módulo de plataforma de confianza virtual (vTPM). Valide los eventos de integridad en Cloud Monitoring y coloque alertas en los eventos de validación de arranque tardío.
- D. Establecer políticas a nivel de proyecto que requieran que todas las máquinas virtuales de Compute Engine se configuren como máquinas virtuales protegidas. Utilice el arranque medido habilitado con el módulo de plataforma de confianza virtual (vTPM). Valide los eventos de integridad en Cloud Monitoring y coloque alertas en los eventos de validación de arranque tardío.

## 4.1 | Pregunta de diagnóstico 03 Discusión

Cymbal Bank ejecuta una aplicación Node.js en una instancia de Compute Engine. Cymbal Bank necesita compartir esta imagen base con un grupo de Google de "desarrollo". Esta imagen base debe admitir el arranque seguro para las instancias de Compute Engine implementadas a partir de esta imagen. ¿Cómo automatizarías la creación de la imagen?


¿Cómo automatizarías la creación de imágenes?

- 
- A. Prepare un script de shell. Agregue el comando `gcloud computing`  
Las instancias terminan con el nombre de la instancia de Node.js. Configurar  
Certificados para arranque seguro. Agregue imágenes de `gcloud computing`  
Cree y especifique el disco y la zona persistentes de la instancia de Compute Engine y los archivos de certificado. Agregue `gcloud computing images add-iam-policy-binding` y especifique el grupo "development".
  - B. Inicie la instancia de Compute Engine. Configure los certificados para el arranque seguro. Prepare un archivo de configuración `cloudbuild.yaml`. Especifique la ubicación del disco persistente de Compute Engine y el grupo "development". Utilice el comando `gcloud builds submission --tag` y especifique la ruta del archivo de configuración y los certificados.
  - C. Prepare un script de shell. Agregue el comando `gcloud computing instances start` al script para iniciar la instancia de Compute Engine de Node.js. Configure el arranque medido para un arranque seguro. Agregue `gcloud computing images create` y especifique el disco persistente y la zona de la instancia de Compute Engine.
  - D. Detenga la instancia de Compute Engine. Configure el arranque medido para un arranque seguro. Prepare un  
Archivo de configuración `cloudbuild.yaml`. Especifique la ubicación del disco persistente de la instancia de Compute Engine y el grupo "desarrollo". Utilice el comando `gcloud builds submission --tag` y especifique la ruta del archivo de configuración.

## 4.1 | Pregunta de diagnóstico 04 Discusión

Cymbal Bank utiliza contenedores Docker para interactuar con las API de su aplicación de banca personal. Estas API cumplen con la normativa PCI-DSS. El entorno de Kubernetes que ejecuta los contenedores no tendrá acceso a Internet para descargar los paquetes necesarios.

¿Cómo automatizarías el proceso que construye estos contenedores?

- 
- A. Cree una imagen de base. Defina un trabajo en Jenkins para Docker. imagen. Cargue la configuración de implementación y el contenedor Definición de plantilla de Packer para un repositorio Git. En la plantilla, incluye un atributo de preprocesador para etiquetar la imagen con el repositorio Git y Container Registry. Utilice Jenkins para crear el contenedor e implementarlo en Google Kubernetes Engine. Utilice Container Registry para distribuir la imagen.
  - B. Cree una imagen inmutable. Defina un trabajo en Jenkins para la imagen de Docker. Cargue la implementación Configuración y definición de contenedor Plantilla de Packer en un repositorio Git. En la plantilla, incluya un atributo de postprocesador para etiquetar la imagen con el repositorio Git y Container Registry. Use Jenkins para crear el contenedor e implementarlo en Google Kubernetes Engine. Use Container Registry para distribuir la imagen.
  - C. Cree una imagen de base. Almacene todos los artefactos y una plantilla de definición de Packer en un repositorio de Git. Use Container Registry para crear los artefactos y la definición de Packer. Use Cloud Build para extraer el contenedor creado e implementarlo en un clúster de Google Kubernetes Engine (GKE). Agregue los usuarios y grupos necesarios al proyecto de GKE.
  - D. Cree una imagen inmutable. Almacene todos los artefactos y una plantilla de definición de Packer en un repositorio de Git. Utilice Container Registry para crear los artefactos y la definición de Packer. Utilice Cloud Build para extraer el contenedor creado e implementarlo en un clúster de Google Kubernetes Engine (GKE). Agregue los usuarios y grupos necesarios al proyecto de GKE.

# 4.1 Automatización de la seguridad de la infraestructura y las aplicaciones

## Cursos



### Seguridad en Google Cloud

- M5 Protección de Compute Engine: Técnicas y mejores prácticas
- M8 Asegurando Google Kubernetes Engine: técnicas y mejores prácticas



### Prácticas recomendadas de seguridad en Google Nube

- M1 Protección del motor de cómputo: Técnicas y mejores prácticas
- M4 Protege Google Kubernetes Motor: Técnicas y Mejores Prácticas

## Insignias de habilidad



## Documentación

- [Uso del escaneo a pedido en su compilación en la nube](#)
- [Documentación de análisis de contenedores | Tubería](#)
- [Nube de Google](#)
- [Escaneo de contenedores | Análisis de contenedores](#)
- [Documentación | Google Cloud](#)
- [Creación de imágenes protegidas personalizadas | Máquina virtual protegida | Nube de Google](#)
- [Creación, eliminación y desuso de elementos personalizados](#)
- [Imágenes | Documentación de Compute Engine | Google Nube](#)
- [Administrar el acceso a imágenes personalizadas | Computación](#)
- [Documentación del motor | Google Cloud](#)
- [Mejores prácticas de gestión de imágenes | Computación](#)
- [Documentación del motor | Google Cloud](#)
- [Implementación en GKE | Documentación de Cloud Build](#)
- [Inicio rápido: crear y enviar una imagen de Docker con](#)
- [Construcción en la nube](#)
- [Construcciones de imágenes automatizadas con Jenkins, Packer y Kubernetes | Centro de arquitectura de la nube | Google Nube](#)

## 4.2 | Pregunta de diagnóstico 05 Discusión



Cymbal Bank tiene aplicaciones Docker implementadas en Google Kubernetes Engine. El banco no tiene contenedores sin conexión. Este clúster de GKE está expuesto a Internet público y recientemente se recuperó de un ataque. Cymbal Bank sospecha que alguien en la organización cambió las reglas del firewall y le ha encomendado que analice y encuentre todos los detalles relacionados con el firewall para el clúster. Quiere la información más completa Solución rentable para esta tarea.


¿Qué debes hacer?

- A. Vea los registros de GKE en Cloud Logging. Utilice el herramienta de alcance de registro para filtrar el registro de reglas de firewall. Cree un tema de Pub/Sub. Exporte los registros a un Pub/Sub Tema que utiliza el comando `gcloud logging sinks create`. Use Dataflow para leer desde Pub/Sub y consultar la transmisión.
- B. Vea los registros de GKE en el clúster de GKE local. Use la herramienta kubect! Sysdig Capture para filtrar el registro de reglas de firewall. Cree un tema de Pub/Sub. Exporte estos registros a un tema de Pub/Sub mediante el clúster de GKE. Use Dataflow para leer desde Pub/Sub y consultar la transmisión.
- C. Visualice los registros de GKE en el clúster de GKE local. Utilice Docker-explorer para explorar el sistema de archivos de Docker. Filtre y exporte los registros de Firewall a Cloud Logging. Cree un conjunto de datos en BigQuery para aceptar los registros. Utilice el comando `gcloud logging sinks create` para exportar los registros a un conjunto de datos de BigQuery. Realice una consulta en este conjunto de datos.
- D. Vea los registros de GKE en Cloud Logging. Use la herramienta de determinación del alcance de registros para filtrar el registro de reglas de firewall. Cree un conjunto de datos en BigQuery para aceptar los registros. Exporte los registros a BigQuery con el comando `gcloud logging sinks create`. Consulte este conjunto de datos.

## 4.2 | Pregunta de diagnóstico 06 Discusión

Cymbal Bank experimentó recientemente un problema de seguridad. Un empleado deshonesto con permisos de administrador para Compute Engine asignó a los usuarios existentes de Compute Engine algunos permisos arbitrarios. Usted tiene la tarea de encontrar todos estos permisos arbitrarios.

¿Qué debe hacer para encontrar estos permisos de manera más eficiente?

- 
- A. Utilice la detección de amenazas de eventos y configure las exportaciones continuas para filtrar y escribir únicamente registros de Firewall en el Centro de Comando de Seguridad. En el Centro de comando de seguridad, seleccione Detección de amenazas de eventos Como fuente, filtrar por evasión: iam, y ordenar para encontrar el tiempo de ataque. ventana. Haga clic en Persistencia: concesión anómala de IAM para mostrar los detalles del hallazgo. Ver la fuente propiedad de la sección Detalles del hallazgo.
- B. Utilice la detección de amenazas de eventos y configure las exportaciones continuas para filtrar y escribir solo registros de firewall en el Centro de comando de seguridad. En el Centro de comando de seguridad, seleccione Detección de amenazas de eventos como origen, filtre por categoría: anomalías y ordene para encontrar la ventana de tiempo de ataque. Haga clic en Evasión: concesión anómala de IAM para mostrar los detalles del hallazgo. Vea la **propiedad** Origen de la sección Detalles del hallazgo.
- C. Utilice la detección de amenazas de eventos y active el detector de concesiones anómalas de IAM. Publique los resultados en Centro de comando de seguridad. En el Centro de comando de seguridad, seleccione Detección de amenazas de eventos como origen, filtre por categoría: iam y ordene para encontrar la ventana de tiempo del ataque. Haga clic en Persistencia: concesión anómala de IAM para mostrar los detalles del hallazgo. Vea la **propiedad** Origen de la sección Detalles del hallazgo.
- D. Utilice la detección de amenazas de eventos y active el detector de concesión anómala de IAM. Publique los resultados en Cloud Logging. En el Centro de comando de seguridad, seleccione Cloud Logging como origen, filtre por categoría: anomalías y ordene para encontrar la ventana de tiempo del ataque. Haga clic en Persistencia: concesión anómala de IAM para mostrar los detalles del hallazgo. Vea la **propiedad** Origen de la sección Detalles del hallazgo.

## 4.2 | Pregunta de diagnóstico 07 Discusión



Cymbal Bank quiere utilizar Cloud Storage y BigQuery para almacenar datos de uso de depósitos seguros.

Cymbal Bank necesita un enfoque rentable para auditar únicamente las actividades de acceso a datos de Cloud Storage y BigQuery.

¿Cómo utilizarías los registros de auditoría en la nube para habilitar este análisis?

- A. Habilite los registros de acceso a datos para ADMIN\_READ, DATA\_READ y DATA\_WRITE en nivel de servicio para BigQuery y Cloud Storage.
- B. Habilite los registros de acceso a datos para ADMIN\_READ, DATA\_READ y DATA\_WRITE en el nivel de la organización.
- C. Habilite los registros de acceso a datos para ADMIN\_READ, DATA\_READ y DATA\_WRITE para Cloud Storage. Todos los registros de acceso a datos están habilitados para BigQuery de forma predeterminada.
- D. Habilite los registros de acceso a datos para ADMIN\_READ, DATA\_READ y DATA\_WRITE para BigQuery. Todos los registros de acceso a datos están habilitados para Cloud Storage de forma predeterminada.

## 4.2 | Pregunta de diagnóstico 08 Discusión



Cymbal Bank ha sufrido un ataque remoto de botnet en instancias de Compute Engine en un proyecto aislado. El proyecto afectado ahora requiere una investigación por parte de una agencia externa.

Una agencia externa solicita que proporcione todos los eventos de administración y del sistema para analizarlos en su herramienta forense local. Desea utilizar la solución más rentable para permitir el análisis externo.

¿Qué debes hacer?

- A. Utilice la detección de amenazas de eventos. Active el detector de concesión anómala de IAM para detectar todos los administradores y usuarios con permisos de administrador o del sistema. Exporte estos registros al Centro de comando de seguridad. Otorgue a la agencia externa acceso al Centro de comando de seguridad.
- B. Utilice los registros de auditoría de la nube. Filtre los registros de auditoría de la actividad de administración solo para el proyecto afectado. Utilice un Tema de Pub/Sub para transmitir los registros de Cloud Audit Logs a la herramienta forense de la agencia externa.
- C. Utilice el Centro de comando de seguridad. Seleccione Cloud Logging como fuente y filtre por Categoría: Actividad de administración y categoría: Actividad del sistema. Vea la propiedad Origen de la sección Detalles del hallazgo. Use los temas de Pub/Sub para exportar los hallazgos a la herramienta forense de la agencia externa.
- D. Utilice Cloud Monitoring y Cloud Logging. Filtre Cloud Monitoring para ver solo el sistema y Registros de administración. Expandir los registros de administración y del sistema en Cloud Logging. Use Pub/Sub para exportar los hallazgos de Cloud Logging a la herramienta forense o al almacenamiento de la agencia externa.



## 4.2 | Pregunta de diagnóstico 09 Discusión



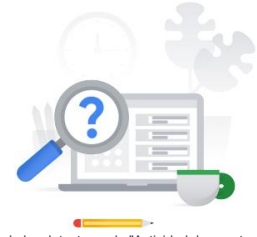
La solicitud de préstamo del departamento de préstamos de Cymbal Bank recopila informes de crédito que contienen información de pago de crédito de los clientes.

Según la política del banco, los informes en formato PDF se almacenan durante seis meses en Cloud Storage y los registros de acceso a los informes se almacenan durante tres años. Debe configurar una solución de almacenamiento rentable para los registros de acceso.

¿Qué debes hacer?

- A. Configure un conjunto de datos de exportación de registros en BigQuery para recopilar datos de Cloud Logging y Cloud Monitoring. Cree reglas de vencimiento de tablas para eliminar registros después de tres años.
- B. Configure un conjunto de datos de exportación de registros en BigQuery para recopilar datos de Cloud Logging y Security Command Center. Cree reglas de vencimiento de tabla para eliminar registros después de tres años.
- C. Configure un depósito de exportación de registros en Cloud Storage para recopilar datos de Seguridad Centro de comando. Configure reglas de administración del ciclo de vida de los objetos para eliminar registros después de tres años.
- D. Configure un depósito de exportación de registros en Cloud Storage para recopilar datos de Cloud Audit Registros. Configure reglas de administración del ciclo de vida de los objetos para eliminar los registros después de tres años.

## 4.2 | Pregunta de diagnóstico n.º 10: Discusión



Cymbal Bank utiliza instancias de Compute Engine para sus API y recientemente descubrió actividades de minería de bitcoin en algunas instancias. El banco quiere detectar todos los intentos futuros de minería y notificar al equipo de seguridad. El equipo de seguridad puede ver el Centro de Comando de Seguridad y los registros de auditoría de la nube.

¿Cómo se debe configurar la detección y notificación?

- A. Utilice los detectores de amenazas de Event Threat Detection. Exporte los hallazgos de los detectores de "Actividad de cuenta sospechosa" y "Comportamiento de IAM anómalo" y publíquelos en un tema de Pub/Sub. Cree una función de Cloud Run para enviar notificaciones de actividades sospechosas. Utilice las notificaciones de Pub/Sub para invocar la función de Cloud Run.
- B. Habilite el conjunto de herramientas de VM Manager en Security Command Center. Realice un análisis de las instancias de Compute Engine. Publique los resultados en Cloud Audit Logging. Cree una alerta en Cloud Monitoring para enviar notificaciones de actividades sospechosas.
- C. Habilite la detección de anomalías en el Centro de comando de seguridad. Cree y configure un Pub/Sub Tema y un servicio de correo electrónico. Cree una función de Cloud Run para enviar notificaciones por correo electrónico sobre actividades sospechosas. Exporte los hallazgos a un tema de Pub/Sub y utilícelos para invocar la función de Cloud Run.
- D. Habilite el escáner de seguridad web en el Centro de comando de seguridad. Realice un análisis de las instancias de Compute Engine. Publique los resultados en Cloud Audit Logging. Cree una alerta en Cloud Monitoring para enviar notificaciones sobre actividades sospechosas.

# 4.2 Configuración del registro, la supervisión y la detección

## Cursos



### Seguridad en Google Cloud

Monitoreo y registro de M11  
Auditoría y escaneo

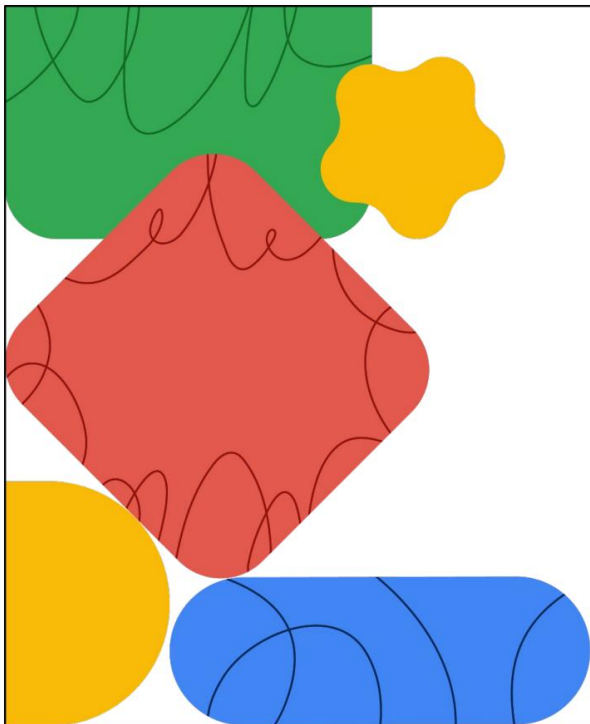


### Mitigación de la seguridad Vulnerabilidades en Google Cloud

Monitoreo, registro, auditoría y escaneo de M3

## Documentación

- [Controles de seguridad y análisis forense para aplicaciones de GKE | Cloud Architecture Center](#)
- [Escenarios para exportar datos de registro: seguridad y análisis de acceso | Arquitectura en la nube](#)
- [Centro | Google Cloud](#)
- [Controles de seguridad y análisis forense para aplicaciones de GKE | Cloud Architecture Center](#)
- [Descripción general de los registros de auditoría de la nube](#)
- [Registros de auditoría de la nube con almacenamiento en la nube | Google Nube](#)
- [Configurar registros de auditoría de acceso a datos](#)
- [Escenarios para exportar Cloud Logging](#)
- [Requisitos de cumplimiento | Arquitectura en la nube](#)
- [Centro | Google Cloud](#)
- [Fuentes de seguridad para vulnerabilidades y amenazas |](#)
- [Centro de comando de seguridad | Google Cloud](#)
- [Configuración del Centro de Comando de Seguridad](#)
- [Habilitar notificaciones de chat y correo electrónico en tiempo real](#)



## Sección 5: Apoyando los requisitos de cumplimiento

## 5.1 Pregunta de diagnóstico 01



El departamento de préstamos de Cymbal Bank almacena información confidencial, como el historial crediticio, la dirección y el número de teléfono de sus clientes, en archivos de Parquet. Debe cargar esta información de identificación personal (PII) en Cloud Storage para que esté segura y cumpla con la norma ISO 27018.

¿Cómo debe proteger esta información confidencial utilizando las claves de cifrado de Cymbal Bank y utilizando la menor cantidad de recursos computacionales?

- A. Genere una clave AES-256 como una cadena de bytes de 32 bytes. Descodificarla como una cadena base 64. Subir el blob al depósito usando esta clave.
- B. Genere una clave RSA como una cadena de bytes de 32 bytes. Descodificarla como una cadena base 64. Subir el blob al depósito usando esta clave.
- C. Genere una clave de cifrado administrada por el cliente (CMEK) mediante cifrado RSA o AES256. Descodificarla como una cadena de base 64. Subir el blob al depósito utilizando esta clave.
- D. Genere una clave de cifrado administrada por el cliente (CMEK) mediante Cloud KMS. Descodificarla como una cadena de base 64. Subir el blob al depósito utilizando esta clave.

## 5.1 Pregunta de diagnóstico 02



Está diseñando una aplicación web para Cymbal Bank para que los clientes que tengan problemas con las tarjetas de crédito puedan comunicarse con agentes de soporte especializados. Los clientes pueden ingresar su número de tarjeta de crédito completo cuando chatean o envían un correo electrónico a los agentes de soporte. Desea garantizar el cumplimiento de PCI-DSS y evitar que los agentes de soporte vean esta información de la manera más rentable.

¿Qué debes hacer?

- A. Utilice claves de cifrado proporcionadas por el cliente (CSEK) y el Servicio de administración de claves en la nube (KMS) para detectar y cifrar información confidencial.
- B. Detectar información confidencial con Cloud Natural Language
- C. Utilice claves de cifrado administradas por el cliente (CMEK) y el Servicio de administración de claves en la nube (KMS) para detectar y cifrar información confidencial.
- D. Implementar la protección de datos confidenciales utilizando su API REST.

## 5.1 Pregunta de diagnóstico 03



Usted es ingeniero de la nube en Cymbal Bank. Debe compartir con su director de tecnología los estándares de auditoría y cumplimiento que cubren los controles sobre informes financieros y los controles públicos y privados sobre seguridad, disponibilidad y confidencialidad.

A. FIP 140-2

B. RGPD

C. PCI-DSS

D. Medias Rojas

¿Qué norma de cumplimiento cubre esto?

## 5.1 Pregunta de diagnóstico 04



El analista de seguros de Cymbal Bank necesita recopilar y almacenar información médica protegida y anónima de pacientes de varios hospitales. La información se almacena actualmente en Cloud Storage, donde cada hospital tiene una carpeta que contiene su propio contenedor. Se le ha encomendado la tarea de recopilar y almacenar los datos de atención médica de estos contenedores en el contenedor Cloud Storage de Cymbal Bank, manteniendo al mismo tiempo el cumplimiento de la HIPAA.

¿Qué debes hacer?

- A. Crea una nueva carpeta. Crea un nuevo almacenamiento en la nube  
En esta carpeta, dale al analista de seguros la información  
Rol de "Editor" en la nueva carpeta. Recopila todos los datos del hospital  
En este depósito. Utilice los datos de atención médica de Google Cloud  
Kit de herramientas de protección para monitorear este depósito.
- B. Cree un nuevo proyecto. Cree un nuevo depósito de almacenamiento en la nube en este proyecto con  
Claves de cifrado proporcionadas por el cliente (CSEK). Otorgue al analista de seguros el rol de "lector" en el proyecto  
que contiene el depósito de almacenamiento en la nube. Utilice la API de DLP para buscar y enmascarar datos de  
información de identificación personal (PII) para cumplir con la HIPAA.
- C. Cree un nuevo proyecto. Utilice el kit de herramientas de protección de datos de Google Cloud Healthcare para configurar  
un depósito de recopilación, alertas de supervisión, receptores de registros de auditoría y recursos de supervisión de  
Forseti. Utilice Dataflow para leer los datos de los depósitos de origen y escribir en los nuevos depósitos de recopilación.  
Otorgue al analista de seguros el rol de "Editor" en la carpeta de cobro.
- D. Utilice la API de Cloud Healthcare para leer los datos de los depósitos del hospital y utilizarlos  
Desidentificación para redactar la información confidencial. Utilice Dataflow para ingerir la fuente de API de Cloud  
Healthcare y escribir datos en un nuevo proyecto que contenga el depósito de Cloud Storage. Otorgue al analista  
de seguros el rol de "Editor" en este proyecto.



## 5.1 Pregunta de diagnóstico 05

Cymbal Bank planea lanzar un nuevo sitio web público donde los clientes puedan pagar sus cuotas mensuales equivalentes (EMI) con tarjetas de crédito. Necesita crear una solución de procesamiento de pagos segura con

Google Cloud que cumpla con los requisitos de aislamiento de PCI-DSS. ¿Cómo diseñaría un entorno de procesamiento de pagos seguro con los servicios de Google Cloud para cumplir con PCI-DSS?

Seleccione las dos opciones correctas

- A. Cree un nuevo proyecto de Google Cloud con acceso restringido (separado del entorno de producción) para la solución de procesamiento de pagos. Cree una nueva instancia de Compute Engine y configure reglas de firewall, un túnel VPN y un balanceador de carga interno.
- B. Cree un nuevo proyecto de Google Cloud con acceso restringido (separado del proyecto de producción) entorno) para la solución de procesamiento de pagos. Configure reglas de firewall, un túnel VPN y un balanceador de carga de proxy SSL para un nuevo entorno flexible de App Engine.
- C. Cree un nuevo proyecto de Google Cloud con acceso restringido (separado del proyecto de producción) entorno) para la solución de procesamiento de pagos. Configure reglas de firewall, un túnel VPN y un balanceador de carga HTTP(S) para una nueva instancia de Compute Engine.
- D. Implemente una instancia de Ubuntu Compute Engine. Instale las bibliotecas necesarias para las soluciones de pago y el cifrado/descifrado. Implemente con Terraform.
- E. Implemente una imagen base de Linux a partir de imágenes de sistemas operativos preconfiguradas. Instale solo las bibliotecas que necesite. Realice la implementación con Terraform.




51.

Determinación de los requisitos regulatorios para la nube


Documentación

<a href="#">Subir un objeto mediante CSEK   Almacenamiento en la nube</a>	<a href="#">Bibliotecas de clientes de protección de datos confidenciales   Pérdida de datos</a>
<a href="#">Claves de cifrado gestionadas por el cliente (CMEK)  </a>	<a href="#">Documentación de prevención</a>
<a href="#">Documentación de Cloud KMS</a>	<a href="#">Demostración de prevención de pérdida de datos</a>
<a href="#">Claves de cifrado proporcionadas por el cliente   Nube</a>	<a href="#">Descripción general de los controles de servicio de VPC   Google Cloud</a>
<a href="#">Almacenamiento</a>	<a href="#">Conozca la API de Google Cloud Healthcare: Parte 1</a>
<a href="#">Opciones de cifrado de datos   Almacenamiento en la nube</a>	<a href="#">Compartir y colaborar   Almacenamiento en la nube</a>
<a href="#">Certificado de conformidad con la norma ISO/IEC 27018   Google Cloud</a>	<a href="#">Guía general de HIPAA de Google Cloud Platform</a>
<a href="#">Automatizar la clasificación de datos cargados en</a>	<a href="#">Configuración de un proyecto alineado con HIPAA   Arquitectura en la nube</a>
<a href="#">Almacenamiento en la nube   Centro de arquitectura de la nube  </a>	<a href="#">Centro</a>
<a href="#">Nube de Google</a>	<a href="#">Cumplimiento del estándar de seguridad de datos PCI   Nube</a>
<a href="#">Descripción general de la protección de datos confidenciales</a>	<a href="#">Centro de arquitectura</a>



Planificar el tiempo

Para preparar



¿Cuándo harás el examen?

---

¿Cuántas semanas tienes para prepararte?

---

¿Cuántas horas dedicarás cada semana a preparar el examen?

---

¿Cuántas horas en total prepararás?

---

Google Cloud

Ejemplo de plan de estudio

Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6
<div></div> <div>Nube de Google Fundamentos: Centro Infraestructura</div>	<div></div> <div>Establecimiento de redes en Nube de Google: 1. Fundamentos 2. Enrutamiento y direccionamiento 3. Arquitectura de red</div>	<div></div> <div>Redes en Google Cloud: 4. Seguridad de la red 5. Equilibrio de carga 6. Nube híbrida y multicloud</div>	<div></div> <div>Construir y proteger redes en Nube de Google Insignia de habilidad</div>	<div></div> <div>Gestión de la seguridad en Google Cloud</div>	<div></div> <div>La mejor seguridad Prácticas en Nube de Google</div>
Semana 7	Semana 8	Semana 9	Semana 10	Semana 11	Semana 12
<div></div> <div>Mitigación de la seguridad Vulnerabilidades en Nube de Google</div>	<div></div> <div>Implementar la nube Seguridad Fundamentos sobre Habilidad de Google Cloud Insignia</div>	<div></div> <div>Google Motor Kubernetes Mejores prácticas: Habilidad de seguridad Insignia</div>	<div></div> <div>Revisar documentación</div>	<div></div> <div>Preguntas de muestra</div>	<div></div> <div>Tomar el examen de certificación</div>

## Plan de estudio semanal

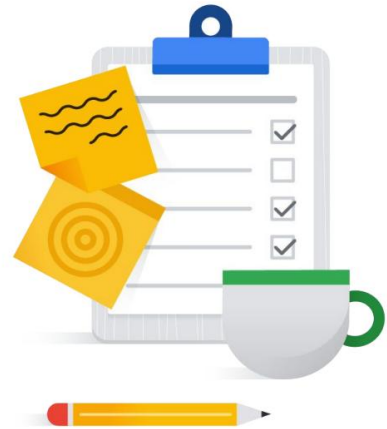
Ahora, piensa en lo que has aprendido sobre tus conocimientos y habilidades a través de las preguntas de diagnóstico de este curso. Deberías tener una mejor comprensión de las áreas en las que debes concentrarte y de los recursos disponibles.

Utilice la siguiente plantilla para planificar sus objetivos de estudio para cada semana. Considere

lo siguiente: • ¿En qué sección(es) de la guía de examen o área(s) temática(s) se centrará? • ¿Qué cursos (o módulos específicos) lo ayudarán a aprender más? • ¿En qué insignias de habilidades o laboratorios trabajará para la práctica? • ¿Qué enlaces de documentación revisará? • ¿Qué recursos adicionales utilizará, como preguntas de muestra?

Puedes realizar algunas o todas estas actividades de estudio cada semana.

Duplique la plantilla semanal según la cantidad de semanas que durará su viaje de preparación individual.



# Plantilla de estudio semanal (ejemplo)

Área(s) de enfoque:

Administrar cuentas de servicio

Cursos/módulos a realizar:

[Gestión de la seguridad en Google Cloud M3 Identity and Access Management](#)  
[Prácticas recomendadas de seguridad en Google Cloud M1 Protección de Compute Engine, M4 Protección de Google Motor Kubernetes](#)

Insignias de habilidad/  
laboratorios para completar:

[Implemente los principios básicos de seguridad en la nube en Google Cloud](#)

Documentación a  
revisar:

[Cuentas de servicio | Documentación de IAM | Google Cloud](#)  
[Creación de credenciales de cuenta de servicio de corta duración | Documentación de IAM | Google Cloud](#)  
[Cómo restringir el uso de cuentas de servicio | Documentación de Resource Manager | Google Cloud](#)

Estudio adicional:

Preguntas de muestra 1-3

# Plantilla de estudio semanal

Área(s) de enfoque:

Cursos/módulos a realizar:

Insignias de habilidad/  
laboratorios para completar:

Documentación a revisar:

Estudio adicional: