



---

## Seguridad

Stephanie Wong  
Developer Advocate, Google Cloud

En este módulo, abordamos el tema de la seguridad.

Google opera de forma segura en la nube desde hace 20 años. Existe una fuerte creencia de que la seguridad potencia la innovación. El principal enfoque del arquitecto de nube debe ser la seguridad. Todo lo demás viene después.

# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

En este módulo, aprenderá a diseñar sistemas seguros con las prácticas recomendadas de la industria. Por ejemplo, cuando diseñe un sistema seguro, aprenderá a aplicar el principio de privilegio mínimo y la separación de inquietudes. Realizar auditorías habituales también son una parte clave de la ejecución de un sistema seguro.

Aproveche Security Command Center de Google para identificar las vulnerabilidades como parte de su proceso. Además, cuando protege los sistemas, debe considerar la administración como un elemento importante. Aprenderá cómo las carpetas y políticas de la organización pueden simplificar la administración.

Evitar el acceso de visitantes no deseados es siempre un desafío. La autenticación y autorización son enfoques que se pueden implementar de diferentes formas. Conocerá la mejor manera de utilizar Identity Platform, Identity-Aware Proxy y los roles de IAM.

Además, aprenderá a administrar el acceso a los recursos y su autorización mediante máquinas y procesos con cuentas de servicio. En un nivel inferior del control de acceso, aprenderá a proteger el acceso a las redes mediante IP privadas, firewalls y el acceso privado a Google Cloud.

Finalmente, aprenderá a aprovechar Cloud DNS y Google Cloud Armor para mitigar ataques de DSD. Como puede ver, abordaremos muchos temas relacionados con la seguridad. Comencemos.

# Objetivos de aprendizaje

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

En este módulo, aprenderá a diseñar sistemas seguros con las prácticas recomendadas de la industria. Por ejemplo, cuando diseñe un sistema seguro, aprenderá a aplicar el principio de privilegio mínimo y la separación de inquietudes. Realizar auditorías habituales también son una parte clave de la ejecución de un sistema seguro.

# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

Aproveche Security Command Center de Google para identificar las vulnerabilidades como parte de su proceso.

# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

Además, cuando protege los sistemas, debe considerar la administración como un elemento importante. Aprenderá cómo las carpetas y políticas de la organización pueden simplificar la administración.

# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

Evitar el acceso de visitantes no deseados es siempre un desafío. La autenticación y autorización son enfoques que se pueden implementar de diferentes formas. Conocerá la mejor manera de utilizar Identity Platform, Identity-Aware Proxy y los roles de IAM.

# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

Además, aprenderá a administrar el acceso a los recursos y su autorización mediante máquinas y procesos con cuentas de servicio.

# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

En un nivel inferior del control de acceso, aprenderá a proteger el acceso a las redes mediante IP privadas, firewalls y el acceso privado a Google Cloud.



# Objetivos de aprendizaje

---

- Diseñar sistemas seguros siguiendo prácticas recomendadas como la separación de inquietudes, el principio de privilegio mínimo y las auditorías periódicas
- Aprovechar Security Command Center de Google para ayudar a identificar vulnerabilidades
- Simplificar la administración de la nube con carpetas y políticas de la organización
- Autenticar y autorizar usuarios mediante Identity Platform, Identity-Aware Proxy y roles de IAM
- Administrar el acceso y la autorización de los recursos por parte de máquinas y procesos mediante cuentas de servicio
- Proteger redes con IP privadas, firewalls y acceso privado a Google Cloud
- Mitigar ataques de DSD mediante Cloud DNS y Google Cloud Armor

Finalmente, aprenderá a aprovechar Cloud DNS y Google Cloud Armor para mitigar ataques de DSD.

Como puede ver, abordaremos muchos temas relacionados con la seguridad. Comencemos.

# Temario

---

## Conceptos de seguridad

Protección de las personas

Protección del acceso a las máquinas

Seguridad de red

Encriptación



Primero, hablemos sobre algunos conceptos relacionados con la seguridad y algunas de las prácticas recomendadas para su diseño.

# La seguridad de Google Cloud es una responsabilidad compartida entre usted y Google

## Transparencia

- El cliente es responsable de ciertas acciones, y Google de otras.
- Google Cloud proporciona las herramientas y el acceso necesarios para supervisar su servicio.
- Google Cloud proporciona los controles y atributos necesarios para aprovechar la seguridad de la plataforma.

## Separación de obligaciones

- ¿Qué proporciona la plataforma?
- ¿De qué debe encargarse usted?

Cuando migra una aplicación a Google Cloud, Google se encarga de muchas de las capas inferiores de la pila de seguridad general. Dada su gran escala, Google puede brindar un nivel de seguridad mayor en estas capas, comparado con lo que podrían costear por sí mismos la mayoría de los clientes. Esto no significa que Google es el responsable de todos los aspectos de seguridad.

La seguridad de Google Cloud es una responsabilidad compartida entre usted y Google, por lo que es importante establecer una división clara de las obligaciones para que no exista ambigüedad entre sus responsabilidades y los servicios que proporciona la plataforma. Para ello, debe haber transparencia. Como cliente, usted es responsable de algunas acciones, mientras que Google es responsable de otras. Google Cloud proporciona las funciones y los controles necesarios para aprovechar la plataforma junto con las herramientas que le permitirán supervisar sus servicios.

## La seguridad se implementa en capas

- Google Cloud proporciona herramientas que, cuando se configuran adecuadamente, habilitan un entorno seguro.
- Usted también puede integrar herramientas de terceros para mejorar la seguridad.
- Existen herramientas para supervisar y auditar sus redes y recursos.



Google implementa la seguridad en capas. La base consiste en hardware y servidores personalizados que se cargan mediante un sistema de carga de inicio verificado.

La seguridad es primordial en toda la pila. Cuando implementa medidas de seguridad, como establecer reglas de firewall o configurar IAM, se asegura de tener un entorno seguro (siempre y cuando las haya configurado de forma correcta). Algunas de las herramientas que proporciona Google Cloud se pueden usar para supervisar y auditar sus redes (hablaremos de ellas en breve), o bien puede instalar sus propias herramientas.

## Principio de privilegio mínimo

- Los usuarios deberían poder ejecutar únicamente las tareas necesarias para realizar sus trabajos.
  - Este principio también se aplica a las instancias de máquinas y a los procesos de entorno de ejecución.
- Use IAM para aplicar este principio.
  - Identifique a los usuarios con sus datos de acceso.
  - Identifique las máquinas y los códigos mediante las cuentas de servicio.
  - Asigne roles IAM a los usuarios y las cuentas de servicio para restringir las tareas que pueden realizar.

Hablemos de algunas prácticas recomendadas cuando se implementa la seguridad.

El principio de privilegio mínimo es una práctica en la que se otorga al usuario únicamente el conjunto de permisos mínimo que necesita para realizar una tarea. Se debería aplicar a los procesos y las instancias de máquinas, así como a los usuarios. Google Cloud proporciona IAM para ayudar a aplicar este principio. Puede usarla para identificar a los usuarios a través de sus datos de acceso o a las máquinas mediante cuentas de servicio. Debe asignar roles a los usuarios y las cuentas de servicio para restringir lo que pueden hacer de acuerdo con el principio de privilegio mínimo.

## Separación de obligaciones

La separación de obligaciones significa lo siguiente:

- Ninguna persona puede cambiar ni borrar datos sin ser detectada.
- Ninguna persona puede robar datos sensibles.
- No puede haber una misma persona a cargo de diseñar e implementar sistemas sensibles, así como tampoco de elaborar informes sobre ellos.

Por ejemplo, las personas que escriben el código no deberían implementarlo, y las que lo implementan, no deberían poder cambiarlo.

- Use proyectos diferentes para las distintas obligaciones.
- Es posible otorgar derechos distintos a diferentes personas en diversos proyectos.
- Use carpetas para ayudar a organizar los proyectos.

La separación de obligaciones es otra práctica recomendada, que tiene dos objetivos principales:

1. Prevenir el conflicto de intereses
2. Detectar fallas de control, como una violación de la seguridad o robo de información

Desde un punto de vista práctico, esto significa que una misma persona no puede cambiar o borrar datos sin ser detectada. La misma persona no puede robar datos sensibles ni estar a cargo de diseñar o implementar sistemas sensibles, así como tampoco de elaborar informes sobre tales sistemas.

Por ejemplo, el desarrollador que escribe el código no debería ser el responsable de implementarlo, y la persona que lo implementa no debería poder cambiarlo. Un enfoque que se emplea para lograr esta separación de obligaciones en Google Cloud consiste en utilizar múltiples proyectos. Es posible otorgar a diferentes personas los derechos correspondientes a los diversos proyectos mediante permisos que siguen el principio de separación de obligaciones. Las carpetas son especialmente útiles para organizar múltiples proyectos.

## Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



También es fundamental auditar los registros de Google Cloud para descubrir ataques y violaciones potenciales de la seguridad. Todos los servicios de Google Cloud generan registros de auditoría, por lo que se dispone de una amplia fuente de información. Algunos de estos registros son de administrador, de acceso a los datos, de flujo de VPC, de firewall y del sistema, por lo que se proporciona una vista detallada de las actividades para su auditoría.

## Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



También es fundamental auditar los registros de Google Cloud para descubrir ataques y violaciones potenciales de la seguridad. Todos los servicios de Google Cloud generan registros de auditoría, por lo que se dispone de una amplia fuente de información. Estos registros incluyen los siguientes:



# Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



De administrador.

# Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



De acceso a los datos.

## Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



De flujo de VPC.

## Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



De firewall.

## Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



Y de sistemas.

## Audite los registros de Google Cloud de forma habitual para descubrir ataques

Todos los servicios de Google Cloud generan registros de auditoría:

- Registros de administrador
- Registros de acceso a los datos
- Registros de flujo de VPC
- Registros de firewall
- Registros del sistema



Debido a esto, se proporciona una vista detallada de las actividades para su auditoría.

## Google Cloud satisface numerosos estándares de cumplimiento de todo el mundo, tanto gubernamentales como de terceros

- Aunque Google Cloud se certificó como un servicio seguro, esto no significa que su aplicación está certificada.
- No se preocupe por la certificación de las herramientas y los servicios de Google Cloud. En su lugar, enfóquese en las compilaciones que realiza en la plataforma.



ISO/IEC 27001



HIPAA



FedRAMP



SOC 1

A menudo, la migración a la nube requiere que mantenga el cumplimiento de los lineamientos o requisitos reglamentarios. Google Cloud satisface numerosos estándares de cumplimiento de todo el mundo, tanto gubernamentales como de terceros, y cuenta con certificaciones de ISO/IEC 27001, HIPAA y SOC 1 como un servicio seguro; sin embargo, esto no significa que las aplicaciones que se ejecutan en esta plataforma están certificadas. Su preocupación siempre debe enfocarse en las compilaciones que realiza.

## Security Command Center proporciona acceso a la configuración de seguridad de la organización y del proyecto

The screenshot displays the Google Cloud Security Command Center interface. On the left is a sidebar with navigation links for various security services. The main content area is titled 'Security Command Center' and includes a '+ AGREGAR FUENTES DE SEGURIDAD' button and a 'CONFIGURACIÓN' link. Below the title bar are tabs for 'PANEL', 'ELEMENTOS', 'RESULTADOS', and 'VULNERABILIDADES'. The 'PANEL' tab is active, showing a 'Recursos' section with a '1 day' filter and a 'Resumen de recursos' table. The table lists various resources and their counts. To the right of the table is a 'Resultados' section with four cards: 'Security Health Analytics', 'Event Threat Detection', 'Resumen de hallazgos', and 'Detección de anomalías', each showing 'No current findings'.

Recurso	New	Borrado	Total
Application	0	1	19
Service	0	1	15
Version	0	2	39
bigquery.Dataset	0	1	51
ManagedZone	0	0	4
CryptoKey	0	2	8
CryptoKeyVersion	0	1	27
KeyRing	0	2	9
Organización	0	0	1

Google Cloud también ofrece la plataforma Security Command Center, que proporciona acceso a la configuración de seguridad de la organización y los proyectos. Como puede ver en esta captura de pantalla, Security Command Center incluye un panel con un análisis del estado de la seguridad, detecciones de amenazas, detecciones de anomalías y un informe de resumen. Cuando se detecta una amenaza, se proporciona un conjunto de recomendaciones prácticas.



# Temario

---

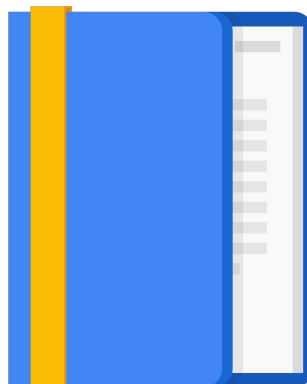
Conceptos de seguridad

Protección de las personas

Protección del acceso a las  
máquinas

Seguridad de red

Encriptación



Ahora, hablemos sobre la protección de las personas.

## Para otorgar a otras personas acceso a sus proyectos, debe agregarlas como miembros y asignarles uno o más roles

- Los miembros se identifican con sus datos de acceso.
- Agregue miembros a grupos para facilitar la administración.
- Los roles son simplemente una lista de permisos.
- Use Console para descubrir fácilmente los permisos que se asignan a los roles.

The screenshot displays the Google Cloud Console interface for the 'bigquery\_user' role. On the left, a table lists various roles and their status. On the right, a detailed view of the 'bigquery\_user' role is shown, including its description and a list of 15 assigned permissions.

Tipo	Título	Se usa en	Estado
<input type="checkbox"/>	Administrador de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Administrador de conexión de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Usuario de conexión de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Editor de datos de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Propietario de datos de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Lector de datos de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Usuario de trabajo de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Visualizador de metadatos de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Usuario de sesión de lectura de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Usuario de BigQuery	BigQuery	Habilitado
<input type="checkbox"/>	Propietario de recursos de Cloud	Recursos de nube	Habilitado

**Usuario de BigQuery** + EDITAR ROL | CREAR A PARTIR DEL ROL

ID: roles/bigquery-user  
Escala de lanzamiento de la función: Despliegue general

**Descripción**  
Access to run queries and create datasets

**15 permisos asignados**  
bigquery.config.get  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.datasets.getiamPolicy  
bigquery.jobs.create  
bigquery.jobs.list  
bigquery.models.list  
bigquery.models.create  
bigquery.routines.list  
bigquery.savedqueries.get  
bigquery.savedqueries.list  
bigquery.tables.list  
bigquery.transfers.get  
resourceManager.projects.get  
resourceManager.projects.list

Cuando otorga permisos a otras personas para que accedan a sus proyectos, debe agregarlos como miembros y asignarles uno o más roles. Los roles son simplemente una lista de permisos. Use Cloud Console para ver los permisos que se otorgan a los roles, como se muestra a la derecha. Aquí, puede ver el rol `bigquery_user` y los 15 permisos asociados que se le asignaron. Puede asignar estos roles predefinidos a los miembros o personalizar sus propios roles.

Tenga en cuenta que cualquier miembro que agregue a su proyecto se identificará mediante sus datos de acceso. Recomendamos que cree grupos para simplificar la administración de los miembros y sus permisos. De esta forma, solo bastará con agregar a los miembros nuevos a un grupo para que estos reciban automáticamente los permisos de ese grupo. Esto también se aplica si quita miembros del grupo, ya que se les quitarán los permisos de ese grupo automáticamente.

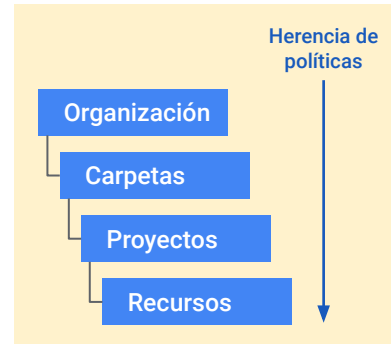
# Use las políticas de Identity and Access Management para proteger los entornos y administrar los recursos

## Otorgue roles a Grupos de Google en lugar de a usuarios individuales

- Los grupos pueden ser más detallados que los roles de trabajo.
- Use múltiples grupos para obtener un mejor control (como *solo lectura*).

## Roles

- Prefiera los roles predefinidos en lugar de los personalizados.
- Otorgue roles con el permiso más restringido posible (privilegio mínimo).
- Limite el uso de los roles “propietario” y “editor”.
- Considere la herencia de jerarquía cuando asigne los roles.



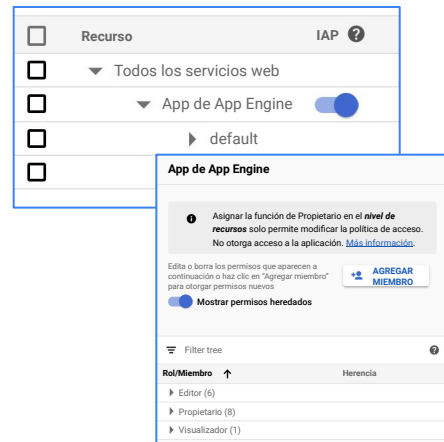
También recomendamos utilizar políticas de la organización y carpetas para simplificar la protección de sus entornos y administrar sus recursos. Las políticas de la organización se aplican a todos los recursos que están bajo una organización, y las políticas de IAM también se heredan de manera descendente, como se muestra a la derecha. Las carpetas heredan las políticas de la organización, los proyectos heredan las políticas de las carpetas, y así sucesivamente.

Ya mencioné que los roles se deben otorgar a los grupos, y no a los usuarios individuales, ya que esto simplifica la administración. Asegúrese de definir los grupos cuidadosamente y de especificarlos con mayor detalle que los roles de trabajo. Lo ideal es usar múltiples grupos para tener un mejor control.

En cuanto a los roles, prefiera usar predefinidos en lugar de personalizados. Google definió roles por una razón, y es poco probable que un rol no se adapte a su caso de uso. Cuando otorgue roles, recuerde el principio de privilegio mínimo: siempre otorgue el permiso más restringido posible. Limite los roles de propietario y editor, ya que la mayoría de los usuarios no los necesitan, o no deberían necesitarlos.

# Identity-Aware Proxy simplifica la autorización para las aplicaciones y las VM de Google Cloud

- Funciona con las aplicaciones que se implementan detrás del balanceador de cargas HTTP(S) en Compute Engine, GKE o App Engine.
- Cuando se configura, obliga a los usuarios a acceder con sus datos.
- Los administradores controlan quién puede acceder a una app.
- Permite que los empleados accedan de forma segura a las aplicaciones basadas en la Web sin necesidad de usar una VPN.



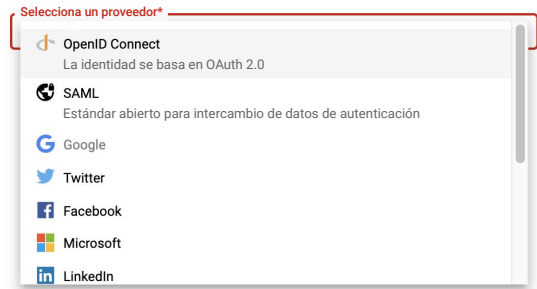
También recomendamos que aproveche el uso de Cloud Identity-Aware Proxy o Cloud IAP. Cloud IAP proporciona acceso administrado a las aplicaciones que se ejecutan en el entorno estándar y en el entorno estándar y flexible de App Engine, Compute Engine y GKE. Permite que los empleados accedan de forma segura a las aplicaciones basadas en la Web que se implementan en Google Cloud sin necesidad de utilizar una VPN. Los administradores controlan quién puede acceder, y los usuarios deben ingresar sus credenciales para entrar a las aplicaciones. En las capturas de pantalla que aparecen a la derecha, se muestra cómo se habilita Cloud IAP en una aplicación de App Engine, así como el diálogo para agregar miembros o permisos nuevos.

## Identity Platform proporciona autenticación como un servicio

- Brinda un acceso federado que se integra en muchos proveedores comunes.
- Se usa para proporcionar opciones de acceso y registro para las aplicaciones de usuarios finales.

### Método de acceso

Selecciona y configura un proveedor de identidad.



Google Cloud también ofrece Identity Platform como una plataforma de administración de identidades y accesos de clientes (CIAM) para agregar la administración de identidades y accesos a las aplicaciones. En otras palabras, Identity Platform proporciona opciones de acceso y registro para las aplicaciones de los usuarios finales.

Debe seleccionar un proveedor de servicios para usar Identity Platform. Hay disponible una amplia variedad de protocolos compatibles, como SAML, OpenID, Correo electrónico y contraseña, Teléfono, Redes sociales y Apple. En esta imagen, se muestra parte de la configuración con una lista de proveedores potenciales.

# Temario

---

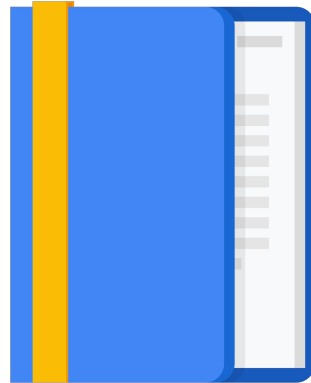
Conceptos de seguridad

Protección de las personas

Protección del acceso a las máquinas

Seguridad de red

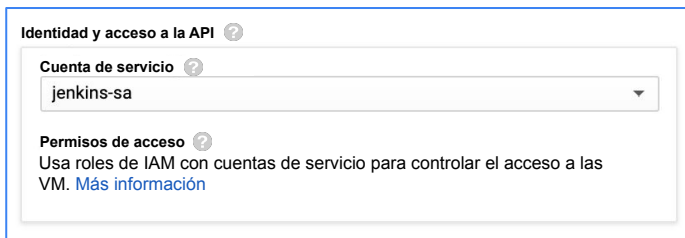
Encriptación



Acabamos de hablar sobre la asignación de roles a miembros. Nos enfocamos en los usuarios y Grupos de Google, pero existe otro tipo de miembros que ayudan a proteger el acceso a las máquinas.

## Las cuentas de servicio se pueden usar para las identidades de máquinas o aplicaciones

- Cree una cuenta de servicio y otórguele uno o más roles.
- Puede asignar esa cuenta de servicio a grupos de nodos de GKE o VM.
- Esas máquinas se ejecutan únicamente mediante los derechos que otorgan los roles.



Una cuenta de servicio es un tipo especial de cuenta que usa una aplicación, una instancia de máquina virtual o un grupo de nodos de GKE. Las aplicaciones o los servicios usan cuentas de servicio para realizar llamadas a la API autorizadas. La cuenta de servicio es la identidad del servicio y define los permisos que controlan los recursos a los que puede acceder el servicio.

Una cuenta de servicio es una identidad y un recurso. Se usa como entidad para su aplicación o servicio con el fin de autenticarlo, por ejemplo, una VM de Compute Engine que se ejecuta como una cuenta de servicio. Para brindar a las VM el acceso a los recursos necesarios, debe otorgar los roles de IAM relevantes a la cuenta de servicio. Al mismo tiempo, debe controlar quién puede crear VM con la cuenta de servicio para que las VM aleatorias no supongan la identidad. Aquí, la cuenta de servicio es el recurso al que se le otorga el permiso. Debe asignar el rol ServiceAccountUser a los usuarios en los que confía para que utilicen la cuenta de servicio.

## Las cuentas de servicio se pueden usar para las identidades de máquinas o aplicaciones

- Genere y descargue una clave cuando cree una cuenta de servicio.
- Puede usar esta clave para la autenticación.
- La clave se descarga como un archivo JSON.
- Las claves administradas por el usuario son credenciales extremadamente potentes.
- Almacene la clave de manera segura.

### Crear una clave (opcional)

Descarga un archivo que contenga la clave privada. Almacena el archivo de forma segura, ya que, si se pierde, no se puede recuperar esta clave. Sin embargo, si no estás seguro de por qué necesitas una clave, omite este paso por ahora.

+ CREAR CLAVE

```
{
  "type": "service_account",
  "project_id": "project-id",
  "private_key_id": "48e95bf20887235536f772dcf25d47b89f8cf49",
  "private_key": "-----BEGIN PRIVATE KEY-----\nmIIIEvAIBADANE",
  "client_email": "my-service-account@project-id.iam.gserviceaccount.com",
  "client_id": "113723034034071973858",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/my-service-account@project-id.iam.gserviceaccount.com"
}
```

Cada cuenta de servicio se asocia con pares de claves RSA públicas o privadas que se usan para autenticarse en Google. Estas claves las puede administrar Google o el usuario.

Google almacena las claves que administra, sean públicas o privadas. Estas claves se rotan con frecuencia, con un período de uso máximo de dos semanas. En el caso de las claves que administra el usuario, el desarrollador es el propietario de las públicas y las privadas. Se pueden utilizar desde fuera de Google Cloud. Las claves administradas por el usuario se pueden administrar con la API de IAM, la herramienta de línea de comandos de gcloud o la página de cuentas de servicio en Cloud Console. Es posible crear hasta 10 pares de claves por cuenta de servicio para admitir la rotación de claves.

Las claves administradas por el usuario son credenciales muy potentes y pueden representar un riesgo de seguridad si no se administran de forma adecuada. Para limitar su uso, aplique la Restricción de políticas de la organización `constraints/iam.disableServiceAccountKeyCreation` a proyectos, carpetas o, incluso, a toda su organización. Después de aplicar esta restricción, puede habilitar las claves administradas por el usuario en ubicaciones bien controladas para minimizar el riesgo potencial causado por claves no administradas. Considere usar Cloud Key Management Service (Cloud KMS) para administrar sus claves de forma segura.

En la diapositiva, se muestra la generación de una clave mediante Cloud Console. La



clave privada se muestra en la captura de pantalla. Es su responsabilidad almacenarla de forma segura.

## Puede usar claves de cuentas de servicio para configurar la CLI

- Le permite otorgar acceso controlado a Google Cloud a los desarrolladores sin necesidad de otorgarles acceso a Cloud Console.
- También es útil para la automatización cuando configura VM a fin de ejecutar canalizaciones de CI/CD.
- Use `gcloud auth activate-service-account --key-file=[PATH TO KEY FILE]`.

Para que los desarrolladores obtengan acceso controlado a los recursos sin adquirir el acceso a Cloud Console, se puede configurar la utilidad de línea de comandos de `gcloud` a fin de usar credenciales de cuentas de servicio para hacer solicitudes. El comando que aparece en esta diapositiva, `gcloud auth activate-service-account`, tiene el mismo propósito que el acceso de autenticación de `gcloud`, pero usa la cuenta de servicio en lugar de las credenciales del usuario.

Tal como mencioné antes, el archivo de claves contiene la clave privada en formato JSON.

# Temario

---

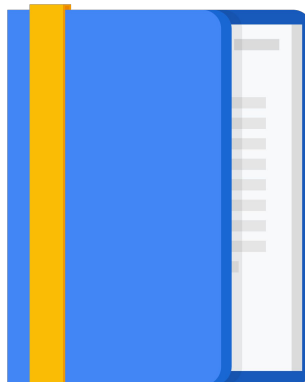
Conceptos de seguridad

Protección de las personas

Protección del acceso a las  
máquinas

Seguridad de red

Encriptación

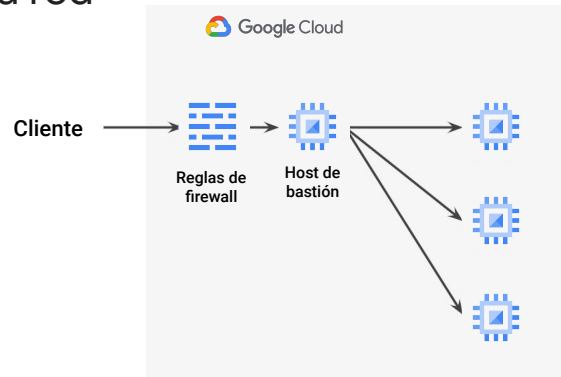


En un módulo anterior, hablamos sobre las redes, pero no vimos muchos conceptos sobre la seguridad de las redes. Hagámoslo ahora.

## Quite IP externas para evitar el acceso a las máquinas desde fuera de la red

- Use un host de bastión para proporcionar acceso a las máquinas privadas.
- También puede establecer conexiones SSH con las máquinas internas mediante Identity-Aware Proxy desde la consola y la CLI.
- Use Cloud NAT para proporcionar una salida a Internet desde las máquinas internas.

*Todo el tráfico de Internet debe finalizar en un balanceador de cargas, un firewall externo (proxy o WAF), API Gateway o IAP. De esa forma, los servicios internos no se pueden iniciar ni pueden obtener direcciones IP públicas.*



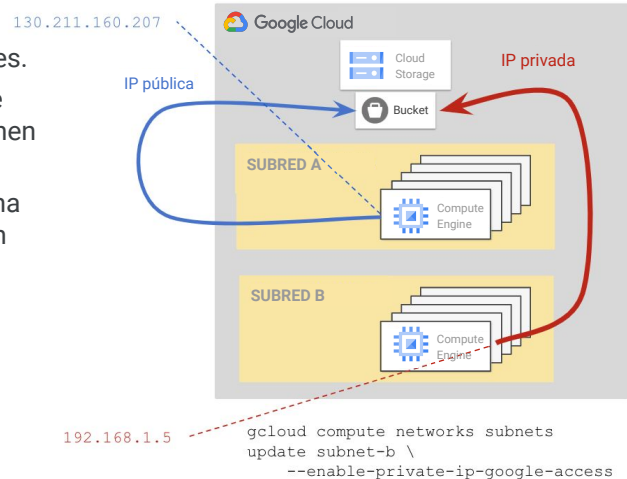
En primer lugar, recomendamos quitar las IP externas para evitar el acceso a las máquinas desde fuera de la red cuando sea posible.

Existen varias opciones disponibles para comunicarse de forma segura con las VM sin direcciones IP públicas. Estos servicios no tienen direcciones IP públicas porque se implementan para que otras instancias del proyecto las consuman o para que se consuman mediante otras opciones de interconexión dedicada. No obstante, en el caso de las instancias sin una dirección IP externa, esto puede ser un requisito a fin de obtener acceso externo, por ejemplo, para que se apliquen actualizaciones o parches. Entre las opciones para acceder a las VM, se incluyen un host de bastión (a fin de habilitar el acceso externo a las máquinas privadas), Identity-Aware Proxy (a fin de habilitar el acceso mediante SSH) o Cloud NAT (a fin de brindar una opción de salida a Internet para las máquinas internas). Las instancias de VM que solo tienen direcciones IP internas también pueden usar el Acceso privado a Google.

En el diagrama que se encuentra a la derecha, se muestra un cliente externo que accede a los recursos de Compute Engine mediante un host de bastión. El host está detrás de un firewall en el que se puede filtrar el acceso. Independientemente del método que elija, todo el tráfico de Internet debe terminar en un balanceador de cargas, un firewall externo, API Gateway o IAP. De esa forma, los servicios internos no se pueden iniciar ni pueden obtener direcciones IP públicas.

## El acceso privado permite el acceso a los servicios de Google Cloud mediante una dirección interna

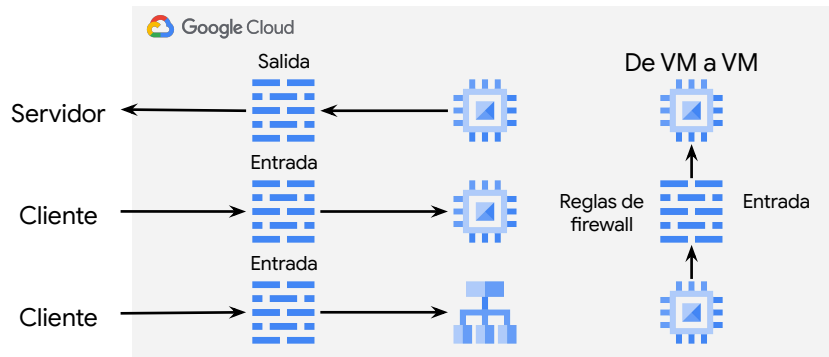
- Se habilita cuando se crean subredes.
- Permite el acceso a los servicios de Google Cloud desde las VM que tienen solo IP internas.
  - Por ejemplo, una máquina con una sola IP interna podría alcanzar un bucket de Cloud Storage.



Las instancias de VM que solo tienen direcciones IP internas también pueden usar el Acceso privado a Google para acceder a los servicios de Google que tienen direcciones IP externas. En el diagrama de la derecha, se muestra una instancia de Compute Engine que accede a un bucket de Cloud Storage mediante su dirección IP interna. El Acceso privado a Google se debe habilitar cuando se crea la subred. Puede lograr esto con el comando de gcloud que aparece aquí o mediante Cloud Console.

## Configure reglas de firewall para permitir el acceso a las VM

- De forma predeterminada, se deniega la entrada a todos los puertos.
- Agregue reglas de firewall para controlar qué clientes pueden acceder a las VM y en qué puertos.
- La seguridad a nivel de la aplicación es responsabilidad del cliente.



Independientemente de si sus instancias de VM tienen direcciones IP públicas, siempre debe configurar reglas de firewall para controlar el acceso.

De forma predeterminada, se deniega la entrada a todos los puertos y se permite la salida. Su responsabilidad consiste en definir reglas independientes a fin de permitir o denegar el acceso a instancias específicas para puertos, protocolos y rangos de IP determinados.

En este gráfico, se ilustran algunas situaciones en las que se pueden configurar reglas de firewall. La primera situación consiste en la salida desde Compute Engine hacia servicios externos. Para la entrada, se deben configurar reglas de firewall si se proporciona acceso directo a una instancia o si se realiza mediante un balanceador de cargas. En el gráfico de la derecha, se ilustra la situación de comunicación de instancia a instancia de VM. Aquí, también se deben considerar reglas de firewall para controlar el acceso. Recuerde que usted sigue siendo el responsable de la seguridad a nivel de la aplicación.

## Controle el acceso a las API mediante Cloud Endpoints

- Proteja y supervise sus API públicas.
- Controle quién tiene acceso a su API.
- Valide cada llamada mediante tokens web de JSON y las claves de la API de Google.
- Se integra en Identity Platform.



Si necesita administrar API, puede usar Cloud Endpoints. Endpoints es una puerta de enlace de administración de API que le permite desarrollar, implementar y administrar API en cualquier backend de Google Cloud. Brinda funciones para proteger y supervisar sus API públicas, controlar a quién se otorga acceso (por ejemplo, mediante Auth0) y validar cada llamada mediante la versión firmada de un token web de JSON con una clave privada de cuenta de servicio. Cloud Endpoints también se integra en Identity Platform para la autenticación.

## Restrinja el acceso a sus servicios únicamente a TLS

- Todos los extremos de servicios de Google Cloud usan HTTPS.
- La configuración de sus extremos de servicio depende de usted.
- En la configuración del balanceador de cargas, cree únicamente un frontend seguro.



The screenshot shows the 'IP y puerto de frontend nuevos' (New Frontend IP and Port) configuration window. It includes the following fields and options:

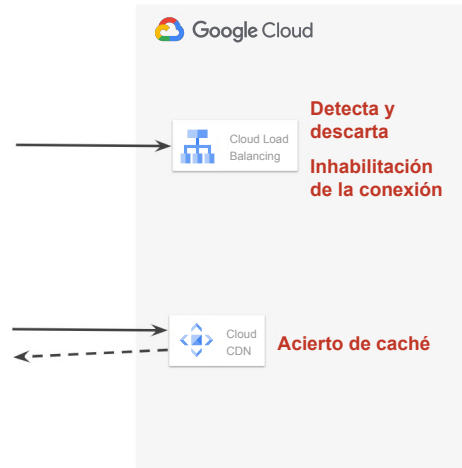
- Nombre (opcional)**: A text input field with a placeholder 'minúsculas, sin espacios' and a note 'El nombre es permanente'.
- Agregar una descripción**: A link to add a description.
- Protocolo**: A dropdown menu set to 'HTTPS (incluye HTTP/2)'.
- Nivel de servicio de red**: Two radio buttons, 'Premium (nivel de proyecto actual, cambiar)' (selected) and 'Estándar'.
- Versión de IP**: A dropdown menu set to 'IPv4'.
- Dirección IP**: A dropdown menu set to 'Efímera'.
- Puerto**: A dropdown menu set to '443'.
- Certificado**: A dropdown menu set to 'my-cert (Managed)'.

Todos los extremos de servicios de Google Cloud usan HTTPS. Recomendamos que utilice TLS en los extremos de su servicio. Además, es su responsabilidad configurar estos extremos para TLS. Cuando configura balanceadores de cargas, asegúrese de crear frontends seguros. En este diálogo, se muestra la configuración de un frontend. El protocolo seleccionado es HTTPS. También se muestra la selección del certificado.



## Aproveche los servicios de red de Google Cloud para obtener protección contra DSD

- Los balanceadores de cargas globales detectan ataques y, luego, los descartan.
- Si habilita la CDN, se protegerán los recursos del backend.



Google proporciona asistencia contra ataques de DSD en la infraestructura mediante balanceadores de cargas globales en los tráficos de nivel 3 y 4. Si habilita la CDN, también se protegerán los recursos de backend porque un DSD origina un acierto de caché en lugar de alcanzar los recursos, como se muestra en la imagen de la derecha.

## Use Google Cloud Armor para crear políticas de seguridad de red

- Puede permitir o denegar el acceso a sus recursos de Google Cloud mediante rangos o direcciones IP.
- Cree listas de organizaciones permitidas para admitir el acceso de las direcciones conocidas.
- Cree listas de organizaciones denegadas para bloquear atacantes conocidos.

Seguridad de red

Cloud Armor

Políticas de SSL

### Crear política de seguridad

Una política de seguridad contiene una o más reglas. Las reglas le indican a la política de seguridad qué hacer (la acción) y cuándo (la condición). Los objetivos son los elementos a los que se aplica la regla. [Más información](#)

- 1 Configura la política
- 2 Agregar más reglas (opcional)
- 3 Aplica políticas a los objetivos (opcional)

**Nombre** ⓘ  
El nombre es permanente.

**Descripción** (opcional)

**Acción de la regla predeterminada** ⓘ  
☐ Permitir  
☒ Denegar

**Código de denegación** ⓘ

[Próximo paso](#)

[Crear política](#) [Cancelar](#)

REST o línea de comandos equivalente

En el módulo Herramientas de redes, mencionamos a Google Cloud Armor.

Puede usar Google Cloud Armor para crear políticas de seguridad de redes y obtener funciones adicionales cuando integre la protección contra DSD. Por ejemplo, puede crear listas de organizaciones permitidas a fin de admitir las direcciones conocidas o requeridas, y listas de organizaciones denegadas para bloquear a los atacantes conocidos.

En este cuadro de diálogo, se muestra una configuración típica de la política de seguridad, en la que se comienza seleccionándola como parte de la lista de organizaciones permitidas o denegadas mediante la opción de Permitir o Denegar la regla. Si se elige la opción Denegar, la acción apropiada en este ejemplo debería ser un error 403.

## Google Cloud Armor admite reglas de firewall de aplicación web (WAF) de capa 7

- Predefine reglas para evitar ataques comunes, como inyección de SQL y secuencia de comandos entre sitios.
- Con el lenguaje de reglas flexible puede permitir o denegar el tráfico mediante encabezados de solicitud, ubicación geográfica, direcciones IP, cookies, etcétera.
- Ejemplos:

```
inIpRange(origin.ip, '9.9.9.0/24')
request.headers['cookie'].contains('80=BLAH')
origin.region_code == 'AU'
inIpRange(origin.ip, '1.2.3.4/32') &&
request.headers['user-agent'].contains('WordPress')
evaluatePreconfiguredExpr('xss-canary')
```

Además de la seguridad en las capas 3 y 4, Google Cloud Armor admite reglas de aplicación de capa 7. Por ejemplo, se proporcionan reglas predefinidas para la secuencia de comandos entre sitios (XSS) y los ataques de inyección de SQL. Google Cloud Armor proporciona un lenguaje de reglas para filtrar el tráfico de solicitudes. Como ejemplo, considere la primera expresión en esta diapositiva: `inIpRange(origin.ip, '9.9.9.0/24')`. En este caso, la expresión es verdadera si la IP de origen en una solicitud se encuentra dentro del rango 9.9.9.0/24.

La segunda línea, `request.headers['cookie'].contains('80=BLAH')`, es verdadera si la cookie 80 con el valor BLAH existe en el encabezado de la solicitud, y la tercera línea es verdadera si el código de la región de origen es AU. Las expresiones se pueden combinar de forma lógica con los operadores lógicos AND y OR.

Todas las expresiones se asignan a una regla de permiso o denegación que, luego, se aplica al tráfico entrante.

# Temario

---

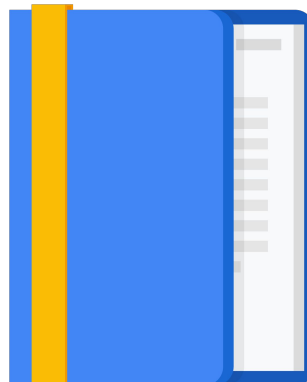
Conceptos de seguridad

Protección de las personas

Protección del acceso a las  
máquinas

Seguridad de red

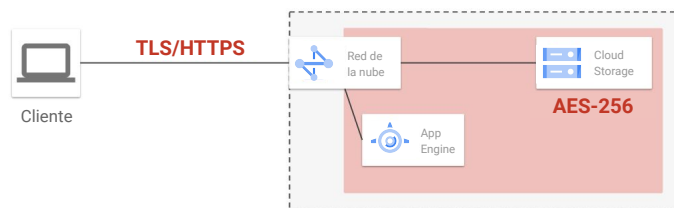
Encriptación



Finalmente, hablemos de la encriptación.

## Google Cloud proporciona encriptación de datos en reposo por parte del servidor de forma predeterminada

- La clave de encriptación de datos (DEK) utiliza la clave simétrica AES-256.
- Las claves se encriptan mediante claves de encriptación de claves (KEK).
- Google controla las claves raíz en Cloud KMS.
- Las claves se rotan automáticamente de forma periódica.
- Cuenta con desencriptación sobre la marcha mediante el acceso de usuarios autorizados, y no genera un impacto visible en el rendimiento.

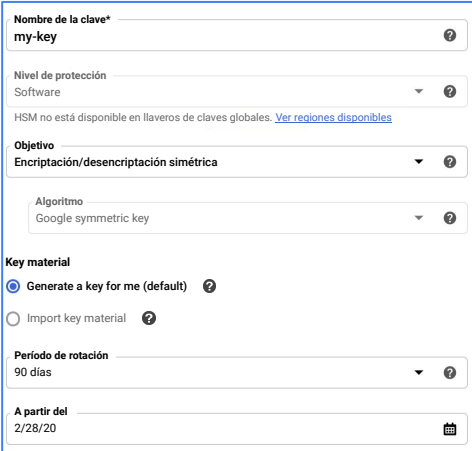


Google Cloud encripta los datos del cliente almacenados en reposo de forma predeterminada, sin que los usuarios deban realizar ninguna acción obligatoria adicional. Se usa una clave de encriptación de datos (o DEK) que utiliza la clave simétrica AES-256. Google encripta esta clave mediante una clave de encriptación de claves (KEK). De esta forma, la DEK se puede almacenar de forma local en los datos encriptados a fin de realizar una desencriptación rápida sin que el usuario vea un impacto visible en el rendimiento. Para proteger las KEK, se almacenan en Cloud KMS. Las claves se rotan automáticamente de forma periódica para una mayor seguridad.

En este diagrama, se muestra una aplicación sencilla de App Engine que utiliza Cloud Storage. Los datos se encriptan con AES-256 mediante una DEK, y se desencriptan de forma transparente en la aplicación cuando se leen los datos.

## Por motivos de cumplimiento, es posible que deba administrar sus propias claves

- Las claves de encriptación administradas por el cliente se crean en la nube mediante Cloud Key Management Service (KMS).
- Usted crea las claves y especifica la frecuencia de rotación.
- Puede seleccionar sus claves cuando cree recursos de almacenamiento, como buckets y discos.



Nombre de la clave\*  
my-key

Nivel de protección  
Software

HSM no está disponible en llaveros de claves globales. [Ver regiones disponibles](#)

Objetivo  
Encriptación/descripción simétrica

Algoritmo  
Google symmetric key

Key material  
☒ Generate a key for me (default) ☐ Import key material

Período de rotación  
90 días

A partir del  
2/28/20

Por motivos de cumplimiento, es posible que deba administrar sus propias claves de encriptación en lugar de generar claves automáticamente, como lo acabamos de mencionar.

En ese caso, puede usar Cloud Key Management Service (o Cloud KMS) para generar lo que se conoce como claves de encriptación administradas por el cliente (CMEK). Estas claves se almacenan en Cloud KMS para que los servicios de Cloud las usen directamente. Puede crear la clave manualmente mediante un diálogo similar al que aparece aquí, y especificar la frecuencia de rotación, que es de 90 días de forma predeterminada. Las claves que genere se podrán usar después cuando cree recursos de almacenamiento, como discos o buckets.

## Las claves de encriptación proporcionadas por el cliente se crean en su entorno y se proporcionan a Google Cloud

- Use sus propias claves con los servicios de Google Cloud.
- La aplicación que realiza las llamadas proporciona las CSEK por llamada a la API.
- Solo Google las almacena en caché en una RAM.
- Desencriptan una única carga útil (o columna) o un único bloque de datos obtenidos.
- Son compatibles con Compute Engine (discos persistentes) y Cloud Storage.

Cuando debe generar su propia clave de encriptación o administrarla de manera local, Google Cloud admite claves de encriptación proporcionadas por el cliente (CSEK). Estas claves se mantienen de forma local y no en Google Cloud. Las claves se proporcionan como parte de las llamadas de servicio a la API, y Google solo las mantiene en la memoria y las utiliza para desencriptar una única carga útil o un único bloque de datos obtenidos. Actualmente, las claves de encriptación proporcionadas por el cliente se pueden utilizar con Cloud Storage y Compute Engine.

## Se puede usar la API de Data Loss Prevention para buscar y ocultar datos sensibles a fin de protegerlos.

- Analiza datos en Cloud Storage, BigQuery o Firestore.
- También puede analizar imágenes.
- Detecta muchos tipos diferentes de datos sensibles, incluidos los siguientes:
  - Correos electrónicos
  - Tarjetas de crédito
  - Números de identificación fiscal
- Usted puede agregar sus propios tipos de información.
- Puede borrar o enmascarar datos sensibles, o bien asignar tokens a ellos o identificar su ubicación.

CREDIT\_CARD\_NUMBER ✕ EMAIL\_ADDRESS ✕  
GCP\_CREDENTIALS ✕ IMEI\_HARDWARE\_ID ✕  
IP\_PASSPORT ✕ MAC\_ADDRESS ✕ PASSPORT ✕  
MAC\_ADDRESS\_LOCAL ✕ PHONE\_NUMBER ✕  
US\_BANK\_ROUTING\_MICR ✕  
US\_EMPLOYER\_IDENTIFICATION\_NUMBER ✕  
US\_INDIVIDUAL\_TAXPAYER\_IDENTIFICATION\_NUMBER ✕  
US\_SOCIAL\_SECURITY\_NUMBER ✕

También puede usar la API de Data Loss Prevention para buscar y ocultar datos sensibles a fin de protegerlos. Cloud DLP permite clasificar y ocultar de forma rápida y escalable elementos de datos sensibles, como números de tarjetas de crédito, nombres, números de seguridad social, números de identificación internacionales determinados y de EE.UU., números de teléfono y credenciales de Google Cloud. Cloud DLP usa más de 90 detectores predefinidos para clasificar estos datos y, así, identificar patrones, formatos y sumas de comprobación; incluso comprende pistas contextuales. Algunos de estos datos se indican en el lado derecho. También tiene la opción de ocultar los datos con técnicas como el enmascaramiento, el hash seguro, la asignación de tokens, el agrupamiento y la encriptación para preservar el formato.



## Actividad 12: Modele servicios seguros de Google Cloud

Consulte el Cuaderno de ejercicios de Design and Process.

- Dibuje un diagrama en el que se ilustren los requisitos de seguridad de su caso de éxito.



En esta actividad de diseño, dibuje un diagrama en el que se muestren los requisitos de seguridad de su caso de éxito. Le mostraré un ejemplo de lo que debe dibujar.

## Actividad 12: Modele servicios seguros de Google Cloud

Consulte el Cuaderno de ejercicios de Design and Process.

- Dibuje un diagrama en el que se ilustren los requisitos de seguridad de su caso de éxito.



En esta actividad de diseño,

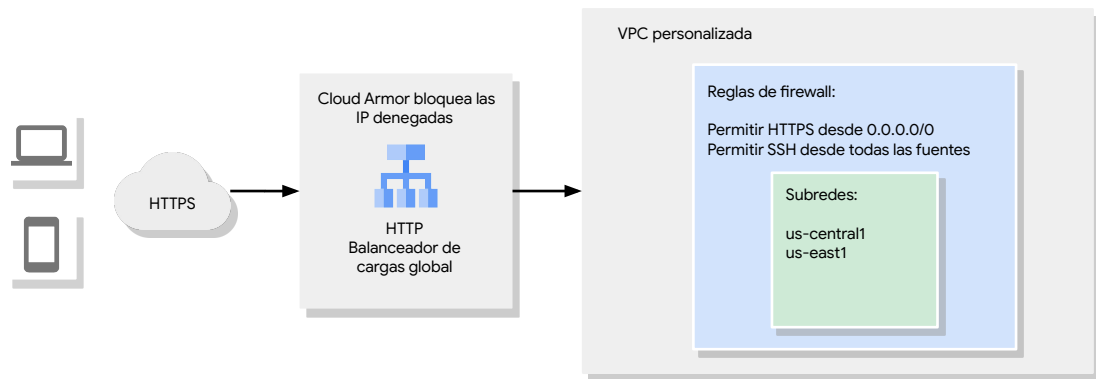
## Actividad 12: Modele servicios seguros de Google Cloud

Consulte el Cuaderno de ejercicios de Design and Process.

- Dibuje un diagrama en el que se ilustren los requisitos de seguridad de su caso de éxito.



dibuje un diagrama en el que se muestren los requisitos de seguridad de su caso de éxito. Le mostraré un ejemplo de lo que debe dibujar.



En este diagrama, se ilustra una red de VPC personalizada con dos subredes en EE.UU. Tal vez us-central1 es nuestra región principal y us-east1 es la región de respaldo. Las reglas de firewall permiten la entrada de HTTPS desde la fuente interna, y de SSH desde fuentes conocidas. De lo contrario, la regla de firewall de entrada implícita llamada "Rechazar todo" inhabilita todo el tráfico entrante de cada red de VPC.

Debido a que admitimos HTTPS desde cualquier lugar, es útil configurar Google Cloud Armor en un balanceador de cargas HTTP global para bloquear las direcciones IP denegadas en el perímetro de la red de Google Cloud. Este es un diseño sencillo, pero un gran punto de partida porque nos permite aumentar los backends sin cambiar el diseño de seguridad.

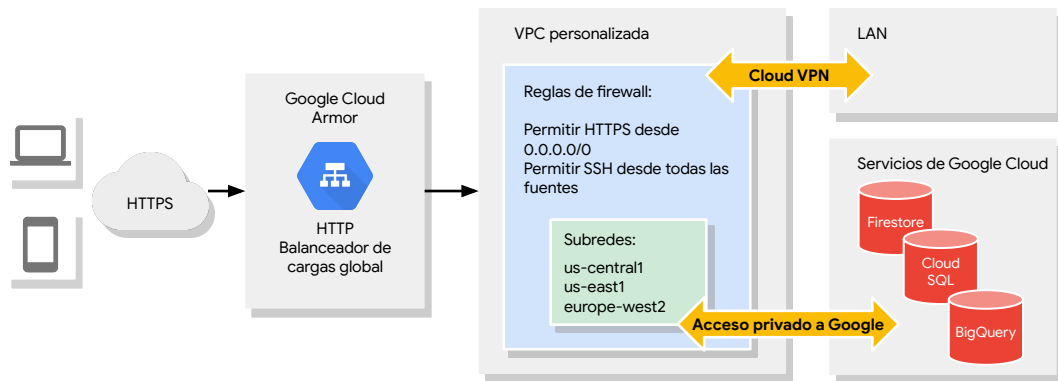
Consulte la actividad 12 del cuaderno de ejercicios a fin de crear un diagrama similar para su caso de éxito.

## Revisión de la actividad 12: Modele servicios seguros de Google Cloud

- Dibuje un diagrama en el que se ilustren los requisitos de seguridad de su caso de éxito.



En esta actividad, se le solicitó dibujar un diagrama en el que se indicaran los requisitos de seguridad para su caso de éxito.



Este es el diagrama que dibujé para nuestro portal de viajes en línea, ClickTravel.

Tiene un diseño similar al que le mostré anteriormente. Primero, configuré Google Cloud Armor en un balanceador de cargas HTTP global para bloquear las direcciones IP denegadas. Mi red de VPC personalizada tiene subredes en us-central1 para los clientes estadounidenses y una subred de respaldo en us-east1. Además, tiene una subred en europe-west2 para los clientes europeos.

Las reglas de mi firewall solo permiten SSH desde fuentes conocidas, y aunque admito HTTPS desde cualquier lugar, puedo denegar direcciones IP con Google Cloud Armor en el perímetro de la red de Google Cloud. También configuré túneles de Cloud VPN a fin de comunicarme de forma segura con mis redes locales para el servicio de informes.

Si bien mi balanceador de cargas necesita una dirección IP pública, puedo crear mis servicios de backend sin direcciones IP externas a fin de protegerlos. Para que esas instancias se comuniquen con los servicios de la base de datos de Google Cloud, habilité el Acceso privado a Google. De esta forma, se permite que el tráfico de los servicios de inventario, pedidos y estadísticas sean siempre privados, a la vez que se reducen los costos de redes.

# Repaso

---

## Seguridad

En este módulo, hablamos de la forma de proteger nuestros recursos de Google Cloud. Esto incluye los datos almacenados y la red. También aprendimos a proteger a las personas mediante IAM, Identity-Aware Proxy y Cloud Identity, y a proteger nuestras aplicaciones y máquinas mediante cuentas de servicio.

Recuerde que la prioridad debe ser la seguridad. Todo lo demás viene después.

# Cuestionario

---

¿Qué servicio de Google Cloud puede utilizar para aplicar el principio de privilegio mínimo cuando usa Google Cloud?

- A. Miembros y roles de IAM
- B. Reglas de firewall
- C. Claves de encriptación
- D. Certificados SSL

¿Qué servicio de Google Cloud puede utilizar para aplicar el principio de privilegio mínimo cuando usa Google Cloud?

- A. Miembros y roles de IAM
- B. Reglas de firewall
- C. Claves de encriptación
- D. Certificados SSL



# Cuestionario

---

¿Qué servicio de Google Cloud puede utilizar para aplicar el principio de privilegio mínimo cuando usa Google Cloud?

A. Miembros y roles de IAM

B. Reglas de firewall

C. Claves de encriptación

D. Certificados SSL

- A. Esta es la respuesta correcta. El principio de privilegio mínimo requiere solo la utilización de los permisos del usuario precisos para las tareas que se necesitan realizar. IAM proporciona este nivel de control.
- B. Incorrecto. Las reglas de firewall admiten o deniegan el tráfico, no los usuarios.
- C. Incorrecto. Las claves de encriptación se usan para la integridad, no el acceso.
- D. Incorrecto. Los certificados SSL se usan para la autenticación y encriptación, no para los permisos.

A es la respuesta correcta. El principio de privilegio mínimo requiere solo la utilización de los permisos del usuario precisos para las tareas que se necesitan realizar. IAM proporciona este nivel de control.

La respuesta B no es correcta. Las reglas de firewall admiten o deniegan el tráfico, no los usuarios.

La respuesta C no es correcta. Las claves de encriptación se usan para la integridad, no el acceso.

La respuesta D no es correcta. Los certificados SSL se usan para la autenticación y encriptación, no para los permisos.

# Cuestionario

---

Usted no quiere que los programadores tengan acceso a los recursos de producción. ¿Cuál es la forma más sencilla de hacerlo en Google Cloud?

- A. Crear una regla de firewall que bloquee el acceso de los desarrolladores a las bases de datos y los servidores de producción
- B. Crear proyectos de producción y desarrollo, y no otorgar acceso a los desarrolladores a los recursos de producción
- C. Usar diferentes cuentas de servicio para los recursos de producción y desarrollo en su proyecto
- D. Configurar el acceso privado junto con Identity-Aware Proxy

Usted no quiere que los programadores tengan acceso a los recursos de producción. ¿Cuál es la forma más sencilla de hacerlo en Google Cloud?

- A. Crear una regla de firewall que bloquee el acceso de los desarrolladores a las bases de datos y los servidores de producción
- B. Crear proyectos de producción y desarrollo, y no otorgar acceso a los desarrolladores a los recursos de producción
- C. Usar diferentes cuentas de servicio para los recursos de producción y desarrollo en su proyecto
- D. Configurar el acceso privado junto con Identity-Aware Proxy

# Cuestionario

---

Usted no quiere que los programadores tengan acceso a los recursos de producción. ¿Cuál es la forma más sencilla de hacerlo en Google Cloud?

- A. Crear una regla de firewall que bloquee el acceso de los desarrolladores a las bases de datos y los servidores de producción
- B. Crear proyectos de producción y desarrollo, y no otorgar acceso a los desarrolladores a los recursos de producción
- C. Usar diferentes cuentas de servicio para los recursos de producción y desarrollo en su proyecto
- D. Configurar el acceso privado junto con Identity-Aware Proxy

- A. Incorrecto. Los firewalls admiten o deniegan tráfico, no usuarios ni roles, por lo que no sería posible restringir el acceso de los desarrolladores, o al menos no de una forma sencilla que se pueda mantener.
- B. Esta es la respuesta correcta. La forma más sencilla es tener proyectos independientes y no otorgar a los desarrolladores el acceso al proyecto de producción.
- C. Incorrecto. Existirían muchos desafíos si se opta por esta solución (al igual que la respuesta A) porque, si bien se puede realizar, no es una opción sencilla ni confidencial.
- D. Incorrecto. IAP se usa principalmente a fin de habilitar el acceso a Google Cloud desde redes no confiables para las aplicaciones y SSH/RDP, pero no para toda la infraestructura.

B es la respuesta correcta. La forma más sencilla es tener proyectos independientes y no otorgar a los desarrolladores el acceso al proyecto de producción.

La respuesta A no es correcta. Los firewalls admiten o deniegan tráfico, no usuarios ni roles, por lo que no sería posible restringir el acceso de los desarrolladores, o al menos no de una forma sencilla que se pueda mantener.

La respuesta C no es correcta. Existirían muchos desafíos si se opta por esta solución (al igual que A) porque, si bien se puede realizar, no es una opción sencilla ni confidencial.

La respuesta D no es correcta. IAP se usa principalmente a fin de habilitar el acceso a Google Cloud desde redes no confiables para las aplicaciones y SSH/RDP, pero no para toda la infraestructura.

# Cuestionario

---

¿Cuáles atributos de Google Cloud podrían ayudar a evitar los ataques de DSD?

- A. El balanceador de cargas global de HTTP
- B. CDN
- C. Google Cloud Armor
- D. Todas las opciones anteriores

¿Cuáles atributos de Google Cloud podrían ayudar a evitar los ataques de DSD?

- A. El balanceador de cargas global de HTTP
- B. CDN
- C. Google Cloud Armor
- D. Todas las opciones anteriores

# Cuestionario

---

¿Cuáles atributos de Google Cloud podrían ayudar a evitar los ataques de DSD?

- A. El balanceador de cargas global de HTTP
- B. CDN
- C. Google Cloud Armor
- D. Todas las opciones anteriores

La respuesta correcta es D. El balanceo de cargas HTTPS mitiga y absorbe muchos ataques de capa 4 y otros inferiores, como desbordes SYN, desbordes de fragmentación de IP y el agotamiento de puertos. CDN almacena en caché el contenido que puede almacenarse de esa forma en puntos de presencia cercanos a los usuarios.

Si ocurriera un ataque de DSD en el contenido que se puede almacenar en caché, las solicitudes se envían a los puntos de presencia, no a sus servidores o su infraestructura. De esta forma, aumenta la probabilidad de que el ataque se absorba. Google Cloud Armor está diseñado para la mitigación de DSD, y trabaja junto con Cloud Load Balancing a fin de detectar ataques de DSD.

La respuesta correcta es D. El balanceo de cargas HTTPS mitiga y absorbe muchos ataques de capa 4 y otros inferiores, como desbordes SYN, desbordes de fragmentación de IP y el agotamiento de puertos. CDN almacena en caché el contenido que puede almacenarse de esa forma en puntos de presencia cercanos a los usuarios.

Si ocurriera un ataque de DSD en el contenido que se puede almacenar en caché, las solicitudes se envían a los puntos de presencia, no a sus servidores o su infraestructura. De esta forma, aumenta la probabilidad de que el ataque se absorba. Google Cloud Armor está diseñado para la mitigación de DSD, y trabaja junto con

Cloud Load Balancing a fin de detectar ataques de DSD.



# Cuestionario

---

¿Qué debe hacer para habilitar la encriptación cuando usa Cloud Storage?

- A. Simplemente habilitar la encriptación cuando configure un bucket
- B. Habilitar la encriptación y subir una clave
- C. Crear una clave de encriptación mediante Cloud Key Management Service y seleccionarla cuando cree un bucket de Cloud Storage
- D. Nada, la encriptación se habilita de forma predeterminada

¿Qué debe hacer para habilitar la encriptación cuando usa Cloud Storage?

- A. Simplemente habilitar la encriptación cuando configure un bucket
- B. Habilitar la encriptación y subir una clave
- C. Crear una clave de encriptación mediante Cloud Key Management Service y seleccionarla cuando cree un bucket de Cloud Storage
- D. Nada, la encriptación se habilita de forma predeterminada

# Cuestionario

---

¿Qué debe hacer para habilitar la encriptación cuando usa Cloud Storage?

- A. Simplemente habilitar la encriptación cuando configure un bucket
- B. Habilitar la encriptación y subir una clave
- C. Crear una clave de encriptación mediante Cloud Key Management Service y seleccionarla cuando cree un bucket de Cloud Storage
- D. Nada, la encriptación se habilita de forma predeterminada

La respuesta correcta es D. Cloud Storage siempre encripta los datos del servidor antes de escribirlos en el disco. Para la encriptación del servidor, existen opciones de claves de encriptación administradas o proporcionadas por el cliente, pero estas se usan generalmente por motivos de cumplimiento y no son necesarias.

La respuesta correcta es D. Cloud Storage siempre encripta los datos del servidor antes de escribirlos en el disco. Para la encriptación del servidor, existen opciones de claves de encriptación administradas o proporcionadas por el cliente, pero estas se usan generalmente por motivos de cumplimiento y no son necesarias.

## Más recursos

Productos de seguridad de Google Cloud

<https://cloud.google.com/security/products/>

Encriptación en reposo

<https://cloud.google.com/security/encryption-at-rest/default-encryption/>

Encriptación en tránsito

<https://cloud.google.com/security/encryption-in-transit/>

Puede consultar estos recursos útiles cuando considere proteger sus aplicaciones y datos.