# Guía de seguridad TIC
# CCN-STIC 888B

# Guía de configuración segura para GCP


Septiembre 2021

MINISTERIO DE DEFENSA

**Catálogo de Publicaciones de la Administración General del Estado**
**https://cpage.mpr.gob.es**

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-21-166-X

Fecha de Edición: septiembre de 2021
Davinci Tecnologías de la Información, S.L ha participado en la realización y modificación del presente documento y sus anexos, que ha sido financiado por Google.

# PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Septiembre de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

# ÍNDICE

# 1. GUÍA DE CONFIGURACIÓN SEGURA PARA GCP

## 1.1. Descripción del uso de esta guía

El contenido de esta guía muestra el despliegue y configuración para cargas de trabajo en la nube pública de Google Cloud Platform (GCP) siguiendo las exigencias del Esquema Nacional de Seguridad.

Siguiendo los pasos de configuración descritos en esta guía se pueden validar los siguientes principios de seguridad:

- Implementación de una base de identidades fuerte.
- Trazabilidad.
- Seguridad en todas las capas.
- Automatización de las buenas prácticas de seguridad.
- Protección de los datos en tránsito y en reposo.
- Automatización en el procesamiento de datos.
- Gestión de eventos de seguridad.

Una de las principales utilidades de esta guía es explicar y referir a los servicios ofrecidos por GCP para cumplir con las diferentes medidas del Esquema Nacional de Seguridad (ENS). Algunos de estos servicios y su nomenclatura pueden ser nuevos para el lector, por lo que se ha incluido un glosario de términos como anexo al documento, así como referencias a la documentación oficial del fabricante de modo que se facilite la lectura y comprensión por parte del usuario de esta guía.

Muchas de las recomendaciones incluidas en este documento tienen la posibilidad técnica de ser validadas de manera automática durante su planificación en el tiempo (programática). Para todas estas medidas se incluye una referencia a un identificador que corresponde a un chequeo dentro del Security Command Center.

## 1.2. Definición del servicio

Google Cloud Platform (GCP) es un servicio de infraestructura y plataforma de nube completa que puede alojar aplicaciones, simplificar el desarrollo de nuevas soluciones e incluso mejorar los sistemas locales. Google Cloud Platform ofrece un amplio conjunto de productos globales basados en la nube, incluidos recursos para cómputo, almacenamiento, bases de datos, análisis, redes, dispositivos móviles, herramientas para desarrolladores, herramientas de administración, IoT, seguridad y aplicaciones empresariales. Estos servicios ayudan a las empresas a avanzar con mayor rapidez, reducir los costos de TI y escalar. GCP cuenta con la confianza de las mayores compañías y las empresas emergentes más innovadoras para respaldar una amplia variedad de cargas de trabajo, como las aplicaciones web y móviles, el desarrollo de juegos, el almacenamiento y procesamiento de datos, el almacenamiento en general o el archivado, entre muchas otras.

En esta guía se tratan las configuraciones necesarias para el cumplimiento de las medidas de protección definidas a través del Esquema Nacional de Seguridad.

## 1.3. Modelo de seguridad compartida

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre GCP y el cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que GCP opera, administra y controla los componentes del sistema operativo host y la capa de virtualización hasta la seguridad física de las instalaciones en las que funcionan los servicios. El cliente asume la responsabilidad y la administración del sistema operativo que utiliza cada instancia (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociado y de la configuración del firewall del grupo de seguridad que ofrece GCP.

Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de estos en su entorno de TI y de la legislación y los reglamentos correspondientes.

La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y el control por parte del cliente que permite concretar la implementación. Como se muestra a continuación, la diferenciación de responsabilidades se conoce normalmente como seguridad "de" la nube y seguridad "en" la nube.

**Responsabilidad de GCP en relación con la "seguridad de la nube"**: GCP es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube de GCP. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de GCP.

**Responsabilidad del cliente en relación con la "seguridad en la nube"**: la responsabilidad del cliente estará determinada por los servicios de la nube de GCP que el cliente seleccione. Esto determina el alcance del trabajo de configuración a cargo del cliente como parte de sus responsabilidades de seguridad.

Por ejemplo, un servicio como Google Compute Engine (GCE) se clasifica como servicios de infraestructura y, como tal, requiere que el cliente realice todas las tareas de administración y configuración de seguridad necesarias.

GCE es una solución de virtualización similar a los servicios que ofrecen las herramientas de tipo Hypervisor (al menos en lo que a nivel operacional se refiere) en la que un servidor actúa de huésped alojando máquinas virtuales (en este caso, denominadas instancias) e interconectándolas. Los sistemas y servicios instalados en dichas máquinas virtuales y las comunicaciones y permisos entre ellas, así como la protección de datos contenidos y seguridad en dichas comunicaciones, no son gestionados por GCP sino por el cliente.

Los clientes que implementan una instancia de GCE, por tanto, son responsables de la administración del sistema operativo que usen en la misma (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el cliente haya instalado en las instancias y de la configuración del firewall provisto por GCP en cada instancia.

En el caso de los servicios gestionados por GCP, como Cloud Storage (servicios de almacenamiento gestionados) y Google Cloud SQL (servicios de base de datos gestionados), GCP maneja la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de enlace para recuperar y almacenar los datos. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar las herramientas de Identity and Access Management (IAM) para solicitar los permisos correspondientes.


*Fig 1. Representación del modelo de responsabilidad compartida en GCP*

El modelo de responsabilidad compartida entre GCP y sus clientes, abarca también los controles de TI. Del mismo modo que comparten la responsabilidad del entorno, también comparten la administración, el funcionamiento y la verificación de los controles de TI. En este sentido, la presente guía es un recurso para el cliente de GCP

referente al ámbito de la responsabilidad del cliente en cuanto a la seguridad de infraestructura y datos según el tipo de servicios utilizados.

Así mismo, los clientes pueden hacer uso de la documentación de conformidad y control disponible en GCP, así como sus procedimientos de verificación y evaluación de los controles.

A continuación, se enumeran varios ejemplos de controles y se especifica a qué entidad corresponde la responsabilidad según el tipo de control:

- **Controles heredados:** Los controles heredados son aquellos que un cliente hereda de GCP en su totalidad. Son aquellos controles sobre los que el cliente no tiene ningún tipo de acceso, como los controles físicos y de entorno.
- **Controles compartidos:** Aplican tanto a la capa de infraestructura como a las capas de clientes. En un control compartido, el encargado de suministrar los requisitos para la infraestructura recae en GCP y la responsabilidad de la configuración de aplicaciones, bases de datos y sistemas operativos de las instancias (de los huéspedes). Por ejemplo, la administración de parches, la corrección de imperfecciones o la administración de las configuraciones, serían responsabilidad de GCP en lo que se refiere a los elementos internos de la infraestructura (hosts y servicios gestionados). Sin embargo, el cliente será responsable de configurar sus aplicaciones, bases de datos y sistemas operativos huésped.
- **Controles específicos del cliente**: Aquellos elementos que son de absoluta responsabilidad del cliente incluirían la seguridad de zonas, protección de comunicaciones y servicios. El direccionamiento y aislamiento para la protección de la información deberá ser definido por el cliente.

Para tener más detalles de la conformidad de GCP en cuanto a sus responsabilidades de seguridad para ENS de este modelo compartido puede consultar el siguiente documento del fabricante:
https://cloud.google.com/security/compliance/ens/?hl=es-419

## 1.4. Funcionalidades del servicio de GCP

La plataforma GCP ofrece diferentes servicios de infraestructura y de plataforma definidos como herramientas estandarizadas y automatizadas. Se puede diferenciar en esta oferta de servicios entre:

- **Infraestructura**, que incluye recursos de infraestructura como computación, redes y almacenamiento. Ejemplos de estos servicios son:
  - Google VPC (Virtual Private Cloud): Red privada virtual en la nube (redes virtuales gestionadas por el cliente).
  - GCE (Compute Engine): Servicio de instancias gestionadas por el cliente (instancias de Linux y Windows Server).

  - GCE persistent disks: Volúmenes de almacenamiento persistente (almacenamiento virtual gestionado por el cliente).
- **Plataforma**, que ofrece aplicaciones, bases de datos y funciones, todas ellas como servicios gestionados por GCP. La diferencia radica en que el cliente configura parámetros del servicio, pero no el propio servicio. Por ejemplo, el cliente añade instancias y alimenta una base de datos, pero no gestiona el servidor que contiene dicha base de datos. Ejemplos de estos servicios son:
  - Google Cloud SQL. GCP Gestiona servicios de bases de datos relacionales (soporta diferentes tipos de bases de datos) encargándose del mantenimiento, la seguridad y la disponibilidad.
  - Google Cloud Storage (GCS). GCP gestiona servicios de almacenamiento encargándose del mantenimiento, la seguridad y la disponibilidad.
  - Google Cloud Functions (GCF). Funciones como servicio (FaaS) de pago por uso y escalables para ejecutar tu código sin necesidad de gestionar servidores.
- **Software**, que se ofrece bajo demanda de forma totalmente gestionada. Ejemplos de estos servicios son:
  - Google Workspace (GW). Google Workspace es un servicio de Google que proporciona varios productos de Google con un nombre de dominio personalizado por el cliente. Está a disposición la guía ***CCN 888A Guía de Configuración Segura Google Workspace***.
  - Google Docs Editors. Google Docs Editors es una suite de oficina de productividad basada en la web que ofrece Google dentro de su servicio Google Drive.

Todos estos recursos son escalables y elásticos en el tiempo y son medibles por uso. El servicio GCP incluye interfaces de autoservicio que están directamente disponibles para el usuario en forma de interfaces web (UI) y APIs para consumo de manera programática.

La plataforma de nube GCP cumple con las medidas de seguridad exigidas que permiten conseguir la certificación de conformidad del Esquema Nacional de Seguridad en su categoría ALTA. Para obtener más detalles de la conformidad de GCP en cuanto a sus responsabilidades de seguridad para el ENS, es posible consultar el siguiente documento del fabricante, también puede comprobar los productos y servicios que son aprobados para su uso dentro del ENS:
https://cloud.google.com/security/compliance/ens/?hl=es-419

## 2. DESPLIEGUE SEGURO PARA GCP

Al crear una nueva cuenta en el servicio de GCP será preciso tener en cuenta una serie de aspectos que garanticen la continuidad y la confidencialidad de los servicios consumidos. Se detallan a continuación los aspectos necesarios para una correcta configuración de una nueva cuenta:

## 2.1. Información precisa de cuenta

El correo electrónico principal que será proporcionado al dar de alta los servicios en GCP, y al cual quedará asociado el correo electrónico del usuario root de la cuenta deberá ser siempre un correo con el dominio de la empresa de modo que su recuperación sea independiente de la permanencia de determinados empleados en la empresa. Ya que, en caso de necesidad, debe ser posible la recuperación de dicha cuenta de correo o su asignación a otro usuario. En este sentido se recomienda el uso de una lista de distribución cuyo acceso esté correctamente protegido. Esta cuenta root deberá configurarse siguiendo las recomendaciones del apartado 3.1.1 Control de acceso y evitar su uso para tareas habituales.

La información relacionada con contactos alternativos deberá ser correctamente cumplimentada con alias de correo que no dependan de la misma persona. GCP usa esta información para contactar con el usuario en caso de problemas de facturación o seguridad. Deberá comprobarse regularmente que estas cuentas funcionan correctamente y mantener listas de correo para asegurar la recepción de avisos por personal disponible en cada momento.

## 2.2. Proyectos

Todos los recursos de Google Cloud que se asignen y usen deben pertenecer a un proyecto. El proyecto puede considerarse la entidad organizadora de lo que se está compilando. Los proyectos están compuestos por la configuración, los permisos y otros metadatos para describir las aplicaciones. Los recursos de un mismo proyecto pueden trabajar en conjunto con facilidad. Por ejemplo, pueden comunicarse mediante una red interna, sujetos a las reglas de las regiones y las zonas. Un proyecto no puede acceder a los recursos de otro proyecto, a menos que uses una VPC compartida o el intercambio de tráfico entre redes de VPC.

## 2.3. Métodos de pago

El método de pago tiene impacto en cuanto a que la disponibilidad del servicio estará sujeta a la disponibilidad del método de pago. Se recomienda en este aspecto el uso de pago por cuenta bancaria a través de GCP en lugar de tarjeta de crédito, que siempre podrá sufrir problemas de limitaciones o incluso caducidad no controladas.

Si se habilita la facturación, cada proyecto se asociará con una cuenta de facturación. Una sola cuenta puede facturar el uso de recursos de varios proyectos.

Puede consultar más detalles sobre el proceso pagos en el siguiente documento:
https://support.google.com/a/answer/1230192?hl=es

# 3. CONFIGURACIÓN SEGURA PARA GCP

En las secciones siguientes se presentan las medidas de aplicación comprendidas en los ámbitos Marco Operacional y Medidas de Protección del Esquema Nacional de Seguridad.

## 3.1. Marco Operacional

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

### 3.1.1. Control de Acceso

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción. El control de acceso que se implante en un sistema real será un punto de equilibrio entre la usabilidad y la protección de la información.

En GCP el control de accesos está principalmente gobernado por el servicio *GCP Identity and Access Management* (IAM). La correcta configuración de IAM otorga acceso detallado a recursos específicos de Google Cloud y ayuda a evitar el acceso a otros recursos.

IAM te permite adoptar el principio de seguridad de mínimo privilegio, que indica que nadie debe tener más permisos de los que realmente necesita. El principio de mínimo privilegio se detalla en profundidad en el apartado ***3.1.1.3 Segregación de funciones y tareas***.

En IAM, el permiso para acceder a un recurso no se otorga directamente al usuario final. En su lugar, los permisos se agrupan en funciones, y las funciones se otorgan a los miembros autenticados. Una Política de IAM define y aplica qué funciones se otorgan a qué miembros; esta política se vincula a un recurso. Cuando un miembro autenticado intenta acceder a un recurso, IAM verifica la política del recurso para determinar si la acción está permitida.

Para entender el proceso de creación de roles, grupos y cuentas de servicio tanto desde línea de comandos como desde la consola puede consultar el siguiente documento del fabricante:
https://cloud.google.com/iam/docs/overview

En la siguiente imagen, se muestra un diagrama con un ejemplo de jerarquía de recursos de Google Cloud:

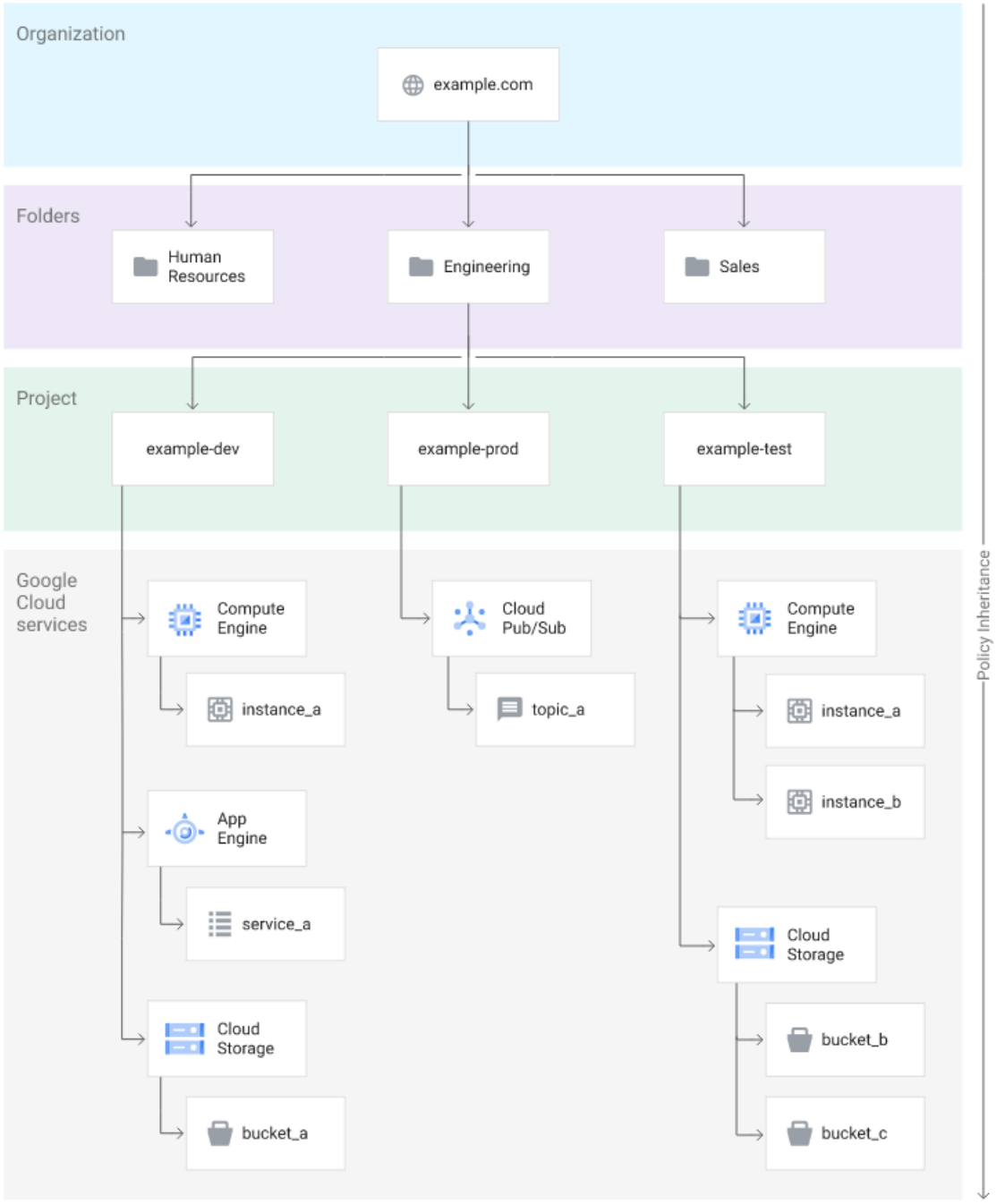


*Fig 2. Jerarquía de recursos de Google Cloud*

#### 3.1.1.1. Identificación

Hay varios tipos de identidades que se deben administrar al abordar cargas de trabajo de GCP seguras y operativas. La identificación de los usuarios del sistema se puede realizarse de las siguientes maneras:

- **Cuenta de Google**: Una cuenta de Google representa a un desarrollador, un administrador o cualquier otra persona que interactúe con Google Cloud.

Cualquier dirección de correo electrónico asociada a una Cuenta de Google puede ser una identidad, incluidos gmail.com y otros dominios.

- **Cuenta de servicio**: Una cuenta de servicio es una cuenta para una aplicación, en lugar de un usuario final individual. Cuando ejecutas el código alojado en Google Cloud, el código se ejecuta como la cuenta que especifiques. Se pueden crear tantas cuentas de servicio como sea necesario para representar los diferentes componentes lógicos de la aplicación.
- **Grupo de Google:** Un Grupo de Google es una colección de Cuentas de Google y cuentas de servicio que posee un nombre. Cada Grupo de Google tiene una dirección de correo electrónico única asociada con el grupo. Los Grupos de Google son una forma conveniente de aplicar una política de acceso a un grupo de usuarios. Se puede otorgar y cambiar los controles de acceso para un grupo completo de una sola vez, en lugar de hacerlo para usuarios individuales o cuentas de servicio uno por uno. También se puede agregar o quitar miembros de un Grupo de Google con facilidad, en lugar de actualizar una política de IAM para agregar o quitar usuarios. Los Grupos de Google no tienen credenciales de acceso y no se pueden usar para establecer la identidad a fin de solicitar acceso a un recurso.
- **Dominio de Google Workspace:** Un dominio de Google Workspace representa un grupo virtual de todas las Cuentas de Google que se crearon en la cuenta de Google Workspace de una organización. Los dominios de Google Workspace representan el nombre del dominio de Internet de la organización (example.com). Al igual que los Grupos de Google, no se pueden usar los dominios de Google Workspace para establecer la identidad, pero permiten la administración conveniente de permisos.
- **Dominio de Cloud Identity:** Un dominio de Cloud Identity es como un dominio de Google Workspace porque representa un grupo virtual de todas las Cuentas de Google en una organización. Sin embargo, los usuarios del dominio de Cloud Identity no tienen acceso a las aplicaciones y las funciones de Google Workspace.
- **Todos los usuarios autenticados:** El valor *"allAuthenticatedUsers"* es un identificador especial que representa a todas las cuentas de servicio y a todos los usuarios de Internet que se autentican con una Cuenta de Google. Este identificador incluye cuentas que no están conectadas a Google Workspace o a un dominio de Cloud Identity, como Cuentas de Gmail personales. Los usuarios que no están autenticados, como los visitantes anónimos, no están incluidos. Algunos tipos de recursos no admiten este tipo de miembro.
- **Todos los usuarios:** El valor *"allUsers"*es un identificador especial que representa a cualquier persona que esté en Internet, incluidos los usuarios autenticados y no autenticados. Algunos tipos de recursos no admiten este tipo de miembro.

Se puede encontrar más información sobre políticas IAM en el siguiente enlace:
https://cloud.google.com/iam/docs/overview

Cuando un miembro autenticado intenta acceder a un recurso, IAM verifica la política de IAM del recurso para determinar si la acción está permitida. A continuación se describen los diferentes conceptos involucrados en la autenticación:

- **Recurso:** Si un usuario necesita acceder a un recurso específico de Google Cloud, se puede otorgar al usuario una función para ese recurso. Algunos servicios permiten que se otorguen permisos de IAM con un nivel de detalle mayor que el nivel de proyecto.
- **Permisos:** Los permisos determinan qué operaciones están permitidas en un recurso. No se otorgan permisos a los usuarios directamente. En su lugar, se identifican las funciones que contienen los permisos adecuados y, luego, se otorgan esas funciones al usuario.
- **Funciones:** Una función es un grupo de permisos. No se pueden otorgar permisos directamente al usuario. En su lugar, se otorga una función. Cuando se otorga una función a un usuario, se otorgan todos los permisos que contiene esa función.
- **Política de IAM:** Se pueden otorgar funciones a los usuarios mediante la creación de una política de IAM, que es una colección de declaraciones que definen quién tiene qué tipo de acceso. Una política se vincula a un recurso y se usa para aplicar el control de acceso cada vez que se accede a ese recurso.
- Para asegurar el correcto uso de identidades en GCP deberá evitarse el uso de múltiples claves de acceso por usuario IAM cuando estas sean necesarias. Mantener más de una clave incrementa el riesgo de accesos no autorizados y el compromiso de credenciales. Por esta misma razón no deben existir claves que no se usen.
- Se deberá utilizar las credenciales de acceso de la organización en lugar de las cuentas personales, como las de Gmail.

Para más detalles puede consultar el siguiente enlace del fabricante: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#manage-identities

#### 3.1.1.2. Requisitos de acceso

El ENS especifica en el control de requisitos de acceso que los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Deberán administrarse permisos para controlar el acceso a las identidades de personas y máquinas que requieren acceso a GCP y sus cargas de trabajo.

**IAM**

Para el control de acceso GCP ofrece Gestión de Identidades y Accesos (IAM), que permite a los administradores decidir quienes tendrán autorización para determinados productos.

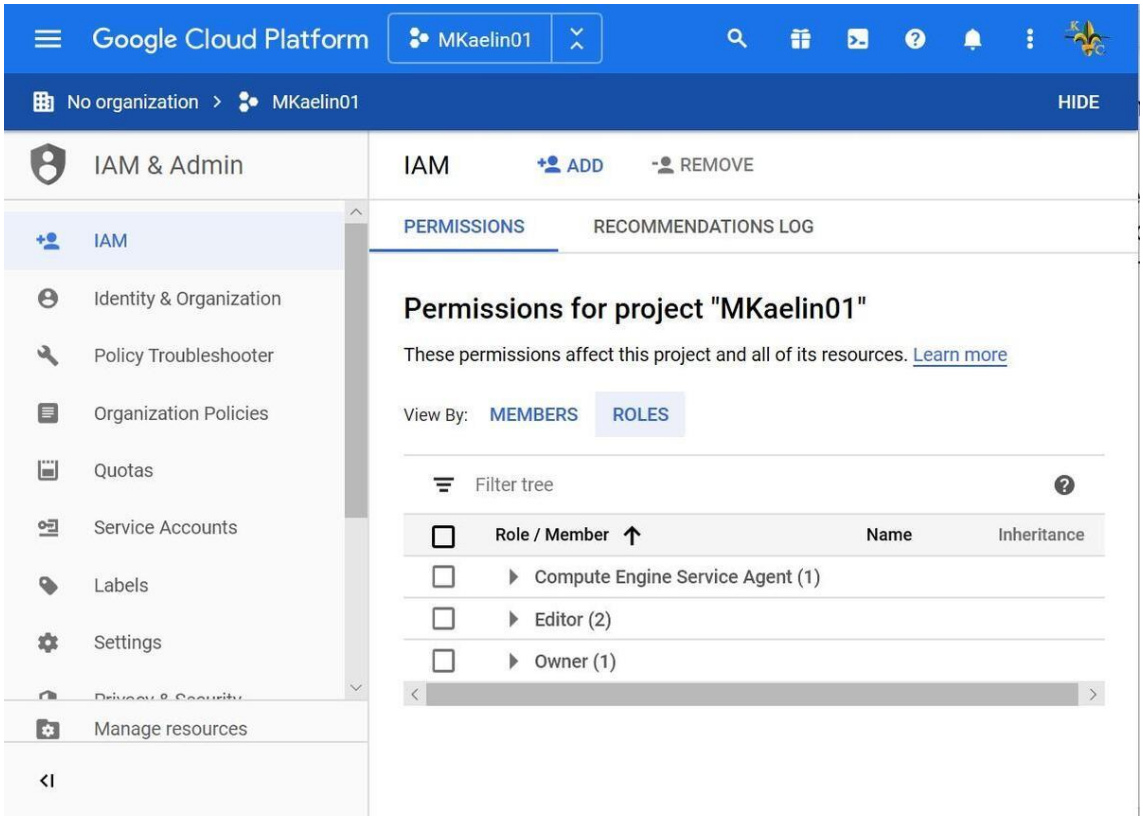


Fig 3. Panel de IAM & Admin de GCP

Los roles IAM se pueden administrar desde diferentes herramientas como Cloud Console, herramienta de línea de comandos de gcloud, la API REST o las bibliotecas cliente.

La mayoría de recursos disponibles en GCP exponen el método ***testIamPermissions()*** que permite comprobar si el emisor autenticado tiene uno o más permisos de IAM específicos del recurso.

Se dispone de diferentes ejemplos para la prueba de permisos en la siguiente guía del fabricante:
https://cloud.google.com/iam/docs/testing-permissions?hl=es#how_to_test_permissions

**Recomendador IAM**
IAM usa el recomendador para comparar las asignaciones de funciones con los permisos que cada miembro usó durante los últimos 90 días. Si se otorga una función a un miembro y este no usa todos los permisos de esa función, es probable que el recomendador de IAM sugiera revocar la función. Si es necesario, el recomendador de IAM también sugerirá funciones menos permisivas como alternativa. Este reemplazo sugerido podría ser una función personalizada nueva o existente, o una o más funciones predefinidas. Excepto en el caso de las recomendaciones para las cuentas de servicio administradas por Google, el recomendador de IAM nunca sugerirá un cambio que aumente el nivel de acceso de un miembro.

Para usar el recomendador de IAM, se recomiendan seguir las siguientes pautas:

- Limpieza inicial de permisos excesivos otorgados: Revisar las recomendaciones de la organización o del proyecto para garantizar que todos los miembros tengan las funciones adecuadas. A continuación se exponen los pasos a seguir a la hora de resolver las recomendaciones dadas por el recomendados de IAM, ordenadas de más importantes a menos:
    - Reducción de permisos en las cuentas de servicio: De forma predeterminada las cuentas de servicio tienen la función de editor. Todos los permisos excesivos aumentan el riesgo de seguridad, por lo que se recomienda priorizar las cuentas de servicio.
    - Prevenir la elevación de privilegios: Las funciones que permiten a los miembros actuar como una cuenta de servicio (***iam.serviceAccounts.actAs***), o bien obtener o establecer la política de IAM de un recurso o miembro permitiendo incluso elevar su propio privilegio. Es recomendable priorizar las recomendaciones relacionadas con estas funciones.
    - Nivel de prioridad alto: Las recomendaciones IAM van asociadas a un nivel de prioridad en función de las funciones que están asociadas a la cuenta. Es recomendable priorizar las recomendaciones con un nivel de prioridad alto.
    - Miembros con privilegios excesivos en un proyecto: Si un miembro tiene una función demasiado permisiva en un proyecto, se deberá revisar las recomendaciones y determinar qué permisos debería tener el usuario o si realmente sí necesita todos los permisos de los que dispone (administrador).
- Después de la limpieza inicial, es recomendable revisar con regularidad las mismas al menos una vez a la semana.

Puedes obtener más información sobre el recomendador de IAM en la siguiente guía del fabricante:
https://cloud.google.com/iam/docs/recommender-best-practices?hl=es

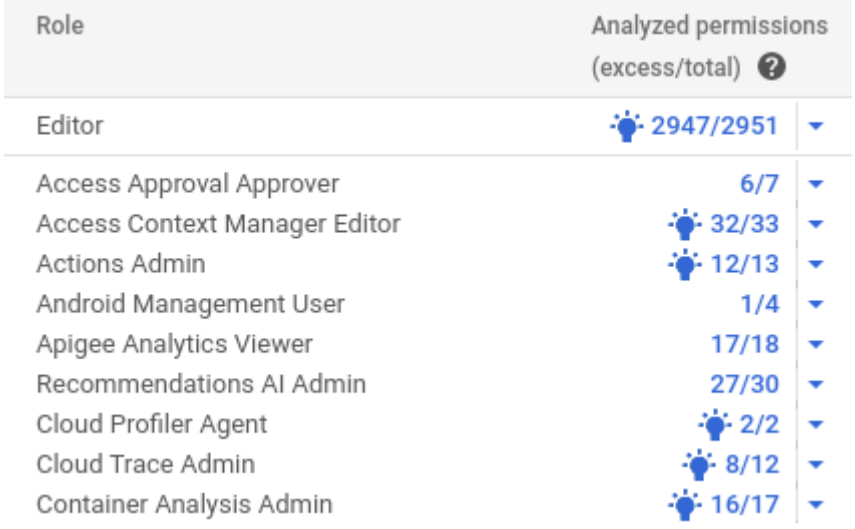

*Fig 4. Ejemplo de recomendaciones*

**Identity-Aware Proxy**

Identity-Aware Proxy (IAP) permite administrar el acceso a aplicaciones que se ejecutan en el entorno estándar y en el entorno flexible de App Engine, Compute Engine y Google Kubernetes Engine (GKE). IAP establece una capa de autorización central para las aplicaciones a las que se accede a través de HTTPS, por lo que se puede adoptar un modelo de control de acceso a nivel de aplicación en lugar de usar firewalls a nivel de red.

Las políticas de IAP se ajustan a la organización. Se pueden definir las políticas de acceso de forma centralizada y aplicarlas a todas tus aplicaciones y recursos. Cuando asignas un equipo dedicado a la creación y aplicación de políticas, proteges al proyecto de que estas se definan o implementen de manera incorrecta en las aplicaciones.

Cuando una aplicación o recurso está protegido por IAP, solo los miembros, también llamados usuarios, que tengan asignada la función correcta de Administración de identidades y accesos (IAM) podrán acceder a ellos a través del proxy. Cuando se otorga a un usuario acceso a una aplicación o un recurso mediante IAP, estará sujeto a los controles de acceso detallados que implementa el producto en uso sin necesidad de una VPN. Cuando un usuario intenta acceder a un recurso protegido por IAP, este realiza comprobaciones de autenticación y autorización.

Puede obtener más información sobre su implementación de IAP en la siguiente guía del fabricante:
https://cloud.google.com/iap/docs/concepts-overview?hl=es

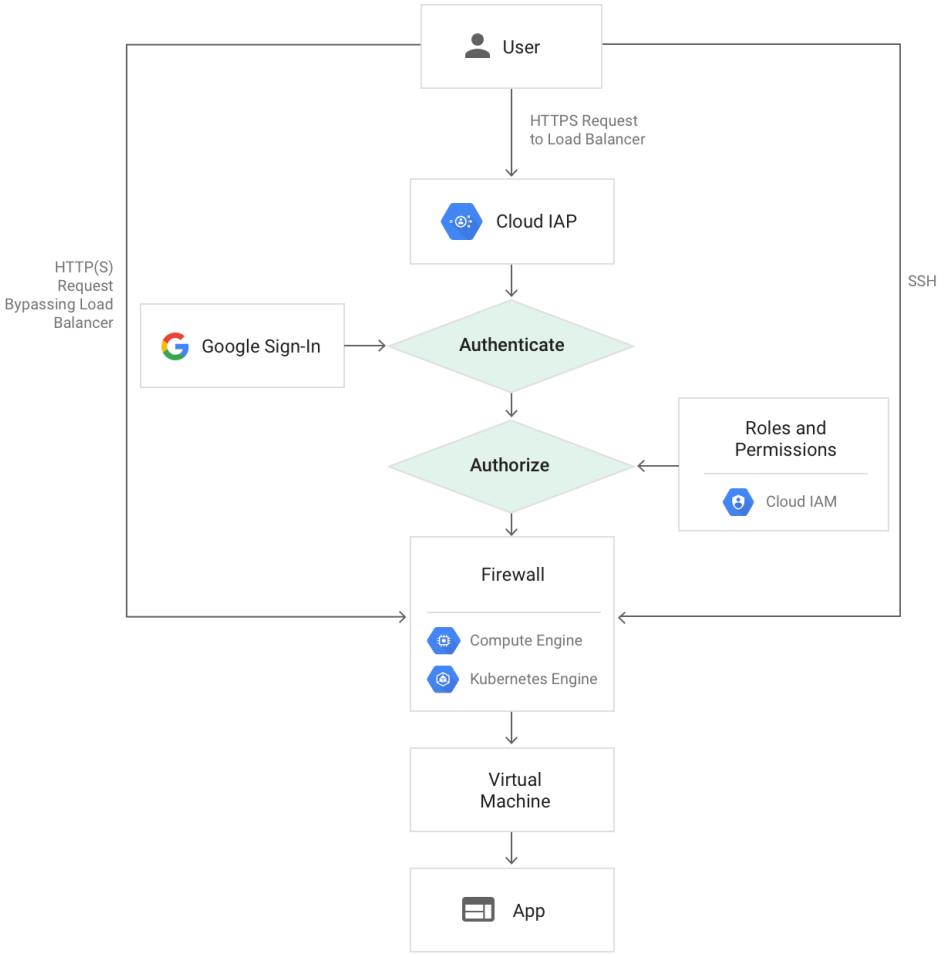


*Fig 5. Funcionamiento de IAP con Compute Engine*

#### 3.1.1.3. Segregación de funciones y tareas

La segregación de funciones y tareas en GCP se lleva a cabo a través de las funciones dentro de IAM. Para administrar el control de acceso con la IAM, se define quién (identidad) tiene qué acceso (función) y a qué recurso. Por ejemplo, las instancias de máquinas virtuales de Compute Engine, los clústeres de Google Kubernetes Engine (GKE) y los depósitos de Cloud Storage son recursos de GCP. Las organizaciones, las carpetas y los proyectos que se usan para organizar los recursos de la organización también son recursos.

Una Política de IAM define y aplica qué funciones se otorgan a qué miembros y esta política se vincula a un recurso. Cuando un miembro autenticado intenta acceder a un recurso, IAM verifica la política del recurso para determinar si la acción está permitida.

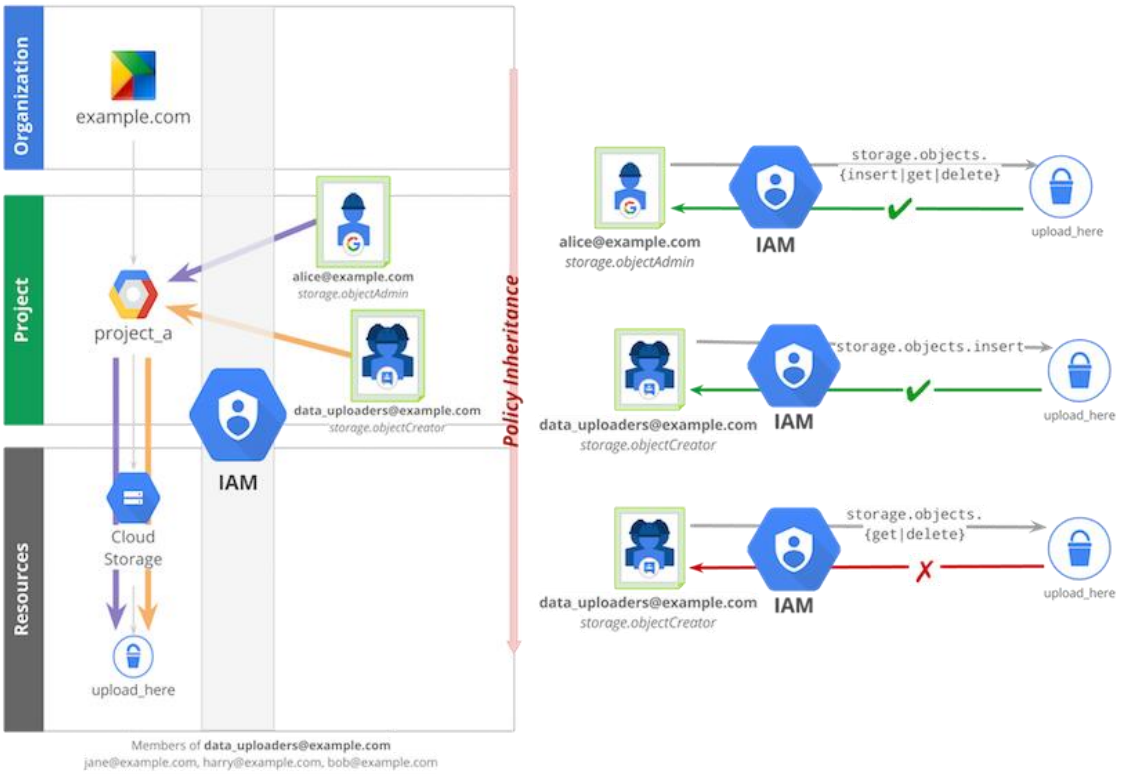


*Fig 6. Ejemplo con diferentes usuarios y funciones dentro de google cloud storage*

- Se deberá aplicar el principio de "separación de obligaciones" al asignar funciones relacionadas con las cuentas de servicio a los usuarios. La separación de obligaciones es el concepto de asegurar que un individuo no tenga todos los permisos necesarios para poder completar una acción maliciosa. En Cloud IAM podría ser una acción como el uso de una cuenta de servicio para acceder a recursos a los que el usuario no debería tener acceso normalmente.

**Mínimo privilegio**

Como práctica recomendada, deben concederse los permisos mínimos necesarios para la función de trabajo. Las políticas IAM deben permitir sólo los privilegios necesarios para cada rol.

Para ello se recomienda seguir las buenas prácticas del fabricante:

- El uso de funciones básicas dentro de GCP (viewer, editor, owner) incluyen muchos permisos en todos los servicios de GCP. En entornos de producción, se recomienda no usar estas funciones básicas, a menos que no haya otra alternativa. En su lugar se pueden otorgar funciones predefinidas por GCP más limitadas o funciones personalizadas, creadas por los administradores de IAM.
- Se deberá otorgar funciones con el menor alcance posible. Se recomienda comenzar con el mínimo nivel de permisos e ir añadiendo permisos adicionales según vaya surgiendo la necesidad.
- Las cuentas de servicio no pueden tener privilegios de administrador.

#### 3.1.1.4. Proceso de gestión de derechos de acceso

El ENS exige en esta sección el cumplimiento de los principios de mínimo privilegio, explicado en el apartado ***3.1.1.3 Segregación de funciones y tareas,*** de necesidad de conocer y de capacidad de autorizar.

Existe además la posibilidad de usar políticas RBAC, pero solo en los servicios de GKE. Kubernetes incluye un mecanismo de control de acceso basado en roles (RBAC) que permite configurar conjuntos de permisos precisos y detallados que definen cómo un usuario de Google Cloud o un grupo de usuarios determinado puede interactuar con cualquier objeto de Kubernetes en el clúster o en un espacio de nombres específico del clúster.

Kubernetes RBAC está habilitado de forma predeterminada. Puede acceder a más información sobre permisos RBAC en la guía ***CCN 888C Guía de Configuración Segura de Contenedores en GCP***.

**Acceso a VM**

Google Compute Engine ofrece varios métodos de acceso a las máquinas virtuales (VM) de GCE:

- Acceso a SO: El acceso al SO permite administrar el acceso SSH a las instancias con la IAM sin tener que crear y administrar claves SSH individuales. El acceso al SO mantiene una identidad de usuario de Linux coherente en todas las instancias de VM y es la forma recomendada para administrar muchos usuarios en múltiples instancias o proyectos. El acceso a SO permite aplicar la autenticación multifactor añadiendo más seguridad a la hora de conectar con las VM.
- Administra Llaves SSH en metadatos: Cuando se crean y administran Llaves SSH, se puede permitir que los usuarios accedan a una instancia de Linux a través de herramientas de terceros. Se pueden controlar las Llaves SSH públicas que están disponibles para una instancia de Linux, editando los metadatos de la instancia. También se pueden definir llaves SSH a nivel de proyecto, dando acceso a la gran mayoría de instancias.

Para la implementación del acceso a SO con verificación en dos pasos, puede consultar la guía del fabricante:
https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication?hl=es-419

Para más información sobre la implementación de claves SSH a nivel de proyecto o instancia se adjunta la guía del fabricante:
https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys?hl=es-419

#### 3.1.1.5. Mecanismos de autenticación

Los mecanismos de inicio de sesión por parte de los usuarios han de ser sólidos. Medidas como la educación de los usuarios para evitar contraseñas comunes o reutilizadas así como el uso de contraseñas con una longitud mínima ayudan a mejorar la seguridad de las cuentas.

El Esquema Nacional de Seguridad exige el uso de dos factores de autenticación para los niveles Medio y Alto. Esta autenticación multifactor o MFA está soportada en GCP con mecanismos de software o hardware para proporcionar una capa adicional de verificación.

MFA aporta seguridad adicional, ya que exige a los usuarios que proporcionen una autenticación exclusiva obtenida de un mecanismo de MFA admitido por GCP, además de sus credenciales de inicio de sesión habituales, para obtener acceso a los servicios de GCP:

- Llaves de seguridad: Entre todos los métodos de verificación en dos pasos, las llaves de seguridad ofrecen el mayor nivel de seguridad. Se trata de una llave física que los usuarios introducen en un puerto USB de un ordenador y que deben tocar para generar una firma criptográfica cuando se les solicite.
- Mensaje de Google: En lugar de generar e introducir un código de verificación en dos pasos, los usuarios pueden configurar sus dispositivos móviles Android o Apple para recibir un mensaje de inicio de sesión. De este modo, cuando inicien sesión en su cuenta de Google a través de un ordenador, recibirán el mensaje "¿Estás intentando iniciar sesión?" en su dispositivo móvil. Una vez hecho esto, basta con que toquen su dispositivo móvil para confirmar su identidad.
- Aplicación Google Authenticator: Google Authenticator genera códigos de verificación en dos pasos de un solo uso en dispositivos móviles Android o Apple. Con esta aplicación, los usuarios generan un código de verificación en su dispositivo móvil que pueden introducir cada vez que se les solicite en un ordenador, en un portátil o incluso en el propio dispositivo móvil para iniciar sesión.
- Códigos de seguridad: En los casos en los que el usuario no pueda acceder a su dispositivo móvil o trabaje en un área de alta seguridad donde no se le permita llevarlo, puede usar un código de seguridad para realizar la verificación en dos pasos. También puede generar códigos de verificación de reserva e imprimirlos con antelación.
- Mensaje de texto o llamada telefónica: Google envía un código de verificación en dos pasos a dispositivos móviles a través de un mensaje de texto o una llamada de voz.

- Se deberá activar el doble factor de autenticación para todas las cuentas que no sean cuentas de servicios.
- Para las cuentas que son administradores, se deberá activar el factor de autenticación más fuerte: Llaves de seguridad. Las llaves de seguridad son llaves

físicas reales que se utilizan para acceder a las cuentas de administrador de la organización de Google.

Para la implementación de la verificación en dos pasos, puede consultar la guía del fabricante:
https://support.google.com/cloudidentity/answer/9176657?hl=es#zippy=%2Cactivar-la-implementaci%C3%B3n-obligatoria

La categoría ALTA de ENS exige la suspensión de las credenciales tras un periodo definido de no utilización. Este requerimiento se puede abordar en GCP con Cloud Monitoring. Cloud Monitoring recopila métricas, eventos y metadatos de Google Cloud.

Para buscar la última vez en que se usó una cuenta de servicio de la organización puede seguir la guía del fabricante:
https://cloud.google.com/iam/docs/service-account-monitoring?hl=es#find-single-account

Para buscar la última vez en que se usó una clave de una cuenta de servicio de la organización puede seguir la guía del fabricante:
https://cloud.google.com/iam/docs/service-account-monitoring?hl=es#find-single-key

#### 3.1.1.6. Acceso Local y Remoto

Al ser GCP un servicio cloud accesible por el usuario final a través de internet deberán tenerse en cuenta en todo caso las exigencias del capítulo del ENS relativo a acceso local y remoto.

La categoría Básica de ENS ya exige que el número de intentos de acceso será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.

También se debe asegurar que los accesos exitosos y fallidos estén correctamente registrados. Se puede compartir los datos de registros de auditoría con Google Cloud Platform (GCP). Esos datos se envían a GCP Cloud Logging, donde se puede consultar los registros y controlar cómo se enrutan y almacenan. Cloud Logging permite almacenar, buscar, analizar, supervisar y generar alertas sobre los datos y los eventos de registro de Google Cloud.

En la consola de administración, se puede compartir los datos de la cuenta de Google Workspace o Cloud Identity con los servicios incluidos en la cuenta de Google Cloud Platform (GCP) de la organización.

Para compartir datos entre con los servicios de Google Cloud Platform, puede seguir la guía del fabricante:
https://support.google.com/a/answer/9320190

### 3.1.2. Explotación

#### 3.1.2.1. Inventario de activos

Este apartado del marco operacional del Esquema Nacional de Seguridad exige el mantenimiento de un inventario actualizado de activos, incluyendo detalles de naturaleza y responsable.

**Tags (Etiquetas)**
Una etiqueta es un par clave-valor que te ayuda a organizar los recursos de Google Cloud. Se puede adjuntar una etiqueta a cada recurso y, luego, usarlas para filtrarlos. La información sobre las etiquetas se reenvía al sistema de facturación a fin de que se puedan desglosar los cargos de facturación según las etiquetas. Una práctica común es etiquetar los recursos destinados a producción, etapa de pruebas o desarrollo por separado para buscar con facilidad los recursos que pertenecen a cada etapa de desarrollo cuando sea necesario.

Las etiquetas pueden asociarse a los siguientes recursos:

- Instancias (VM)
- Reglas de reenvío
- Imágenes
- Discos persistentes
- Instantáneas de discos persistentes
- Segmentos de Cloud Storage
- Direcciones IP estáticas
- Túneles VPN

El fabricante recomienda el uso de etiquetas en las siguientes situaciones:

- Etiquetas de equipo o del centro de costes: Agregar etiquetas por equipo o centro de costes para distinguir los recursos que pertenecen a distintos equipos (por ejemplo, team:research y team:analytics). Ayuda a la hora de contabilizar costes por equipos.
- Etiquetas de componentes: Permite etiquetar por tipo de recurso (por ejemplo, component:redis, component:frontend, component:ingest y component:dashboard).
- Etiquetas de entorno o etapa: Permite etiquetar por entorno de pruebas o producción (por ejemplo, environment:production y environment:test).
- Etiquetas de estado: Permite etiquetar un recurso en función del estado en el que se encuentra, obsoleto, activo por eliminar (por ejemplo, state:active, state:readytodelete y state:archive).

Para la creación y administración de las etiquetas dentro de Google Cloud, puede obtener más información en la guía del fabricante:
https://cloud.google.com/resource-manager/docs/creating-managing-labels?hl=es#using_console

**Cloud Asset Inventory**

Cloud Asset Inventory proporciona servicios de inventario basados en una base de datos de series temporales. Esta base de datos conserva un historial de cinco semanas de metadatos de los recursos de GCP. El servicio de exportación de Cloud Asset Inventory permite exportar todos los metadatos de los elementos en una marca de tiempo determinada o exportar el historial de cambios durante un período.

Con Cloud Asset Inventory se pueden realizar las siguientes funciones:

- Buscar recursos: Permite buscar metadatos de activos dentro de un proyecto, organización o carpeta.
- Exporta el historial y los metadatos de los recursos: Permite exportar todos los metadatos de activo en una marca de tiempo determinada a un archivo de Cloud Storage o una tabla de BigQuery. También permite exportar el historial de cambios de varios elementos durante un período determinado. El historial de cambios de eventos muestra todos los eventos de creación, eliminación y actualización de los recursos especificados a lo largo del tiempo.
- Supervisar cambios en los recursos: Permite supervisar los cambios en los recursos y políticas, previamente definidas, mediante notificaciones en tiempo real

Para obtener más información sobre cómo implementar la supervisión en tiempo real de algunos recursos puede seguir la guía del fabricante:
https://cloud.google.com/asset-inventory/docs/monitoring-asset-changes

- Analiza los elementos: Permite analizar políticas de IAM dentro de un proyecto, una carpeta o una organización.

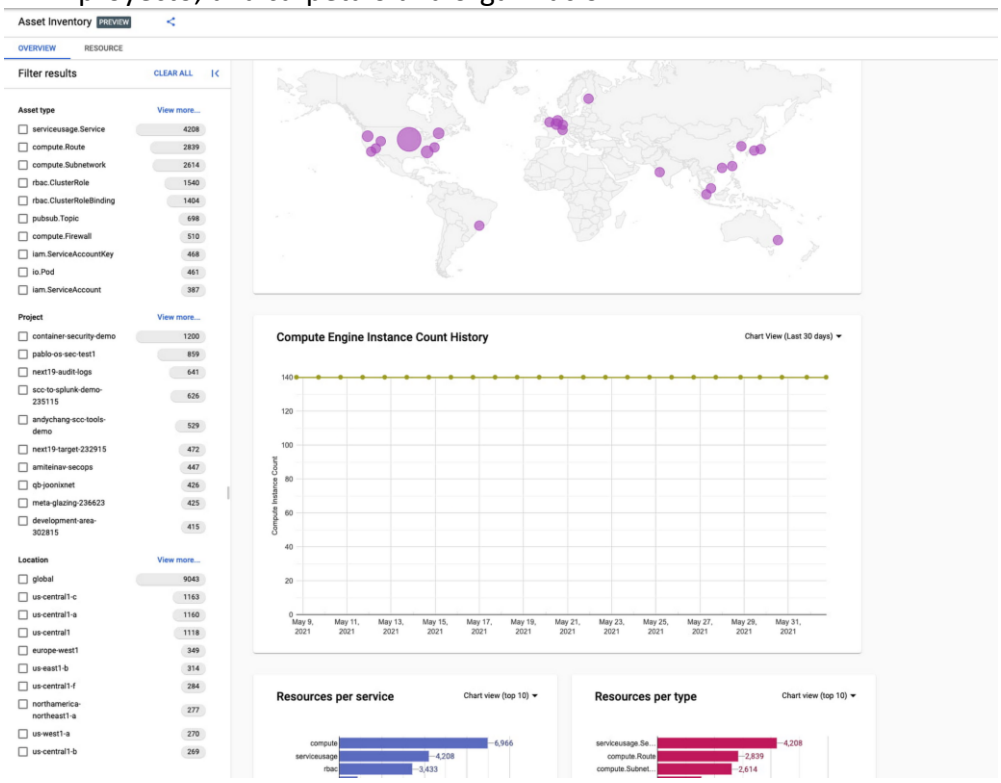


*Fig 7. Pantalla de muestra de Cloud Asset Inventory.*

#### 3.1.2.2. Mantenimiento

El Esquema Nacional de Seguridad requiere en esta medida la correcta gestión de anuncios de seguridad y la correcta procedimentación para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

**Instancias de Cloud SQL**
Las instancias de Cloud SQL necesitan actualizaciones ocasionales para corregir errores, evitar vulnerabilidades de seguridad y actualizar las versiones. Después de aplicar las actualizaciones, Cloud SQL reinicia las instancias, lo que puede causar una interrupción en el servicio.

Durante un evento de mantenimiento, una instancia de Cloud SQL pierde conectividad durante menos de 60 segundos en promedio. El tiempo de inactividad puede ser mayor para las instancias que tienen una carga alta antes de que comience el mantenimiento o que tengan discos muy grandes.

Dentro de la configuración de estas instancias, se permite modificar los períodos de mantenimiento. Los períodos de mantenimiento son bloques de tiempo en los que Cloud SQL programa esta tarea de mantenimiento. Si no especificas un período de preferencia, las actualizaciones disruptivas pueden ocurrir en cualquier momento.

Para instancias de Cloud SQL con alta disponibilidad, es decir, con réplicas de lectura y conmutación por error, las réplicas de lectura se inhabilitarán para llevar a cabo las actualizaciones de mantenimiento. No hay garantías sobre cuándo ocurrirán, además, es posible que estas puedan superponerse o que sucedan en un momento muy cercano a la actualización de la instancia principal. Las instancias de conmutación por error se inhabilitan para llevar a cabo las actualizaciones de mantenimiento. Reciben las actualizaciones de mantenimiento **justo antes** que la instancia principal. No se puede establecer un período de mantenimiento directamente en una instancia de conmutación por error, ya que estas instancias comparten el período de mantenimiento de la instancia principal.

Para configurar un período de mantenimiento en una instancia, puedes consultar la guía del fabricante:
https://cloud.google.com/sql/docs/mysql/set-maintenance-window?hl=es#set-maintenance

#### 3.1.2.3. Registro de la actividad de los usuarios

Tal y como se desarrolla en el apartado 3.1.1.6 Acceso Local y Remoto la solución de GCP Cloud Logging ha de ser aprovechada para el registro tanto de intentos de acceso exitoso y los intentos fallidos.

Los registros de auditoría de Cloud brindan los siguientes registros de auditoría para cada proyecto, carpeta y organización de Cloud:

- Registros de auditoría de actividad del administrador: Contienen entradas de registro para las llamadas a la API y otras acciones que modifican la configuración o los metadatos de los recursos. Por ejemplo, registran en qué momento los usuarios crean instancias de VM o cambian los permisos de administración de identidades y accesos. Los registros de auditoría de actividad del administrador se escriben siempre; no se permite configurarlos ni inhabilitarlos.
- Registros de auditoría de acceso a los datos: Contienen llamadas a la API que leen la configuración o los metadatos de los recursos, así como llamadas a la API controladas por el usuario que crean, modifican o leen datos de los recursos que proporciona el usuario. Los registros de auditoría de acceso a los datos no registran las operaciones de acceso a los datos realizadas en recursos que se comparten de manera pública (disponibles para todos los usuarios o todos los usuarios autenticados) o a los que se puede acceder sin iniciar sesión. Los registros de auditoría de acceso a datos, excepto los registros de auditoría de acceso a datos de BigQuery, están inhabilitados de forma predeterminada.

Para configurar los registros de auditoría de acceso a los datos, puede consultar la guía del fabricante:
https://cloud.google.com/logging/docs/audit/configure-data-access?hl=es

- Registros de auditoría de política denegada: Cloud Logging registra los registros de auditoría de políticas denegados cuando un servicio de Google Cloud rechaza el acceso a un usuario o a una cuenta de servicio debido a un incumplimiento de política de seguridad. Los registros de auditoría denegados por políticas se generan de forma predeterminada

#### 3.1.2.4. Protección de los registros de actividad

El nivel de seguridad ALTO para esta medida exige no sólo el registro de actividades de usuarios del sistema sino su centralización y la automatización de la recolección y correlación de eventos.

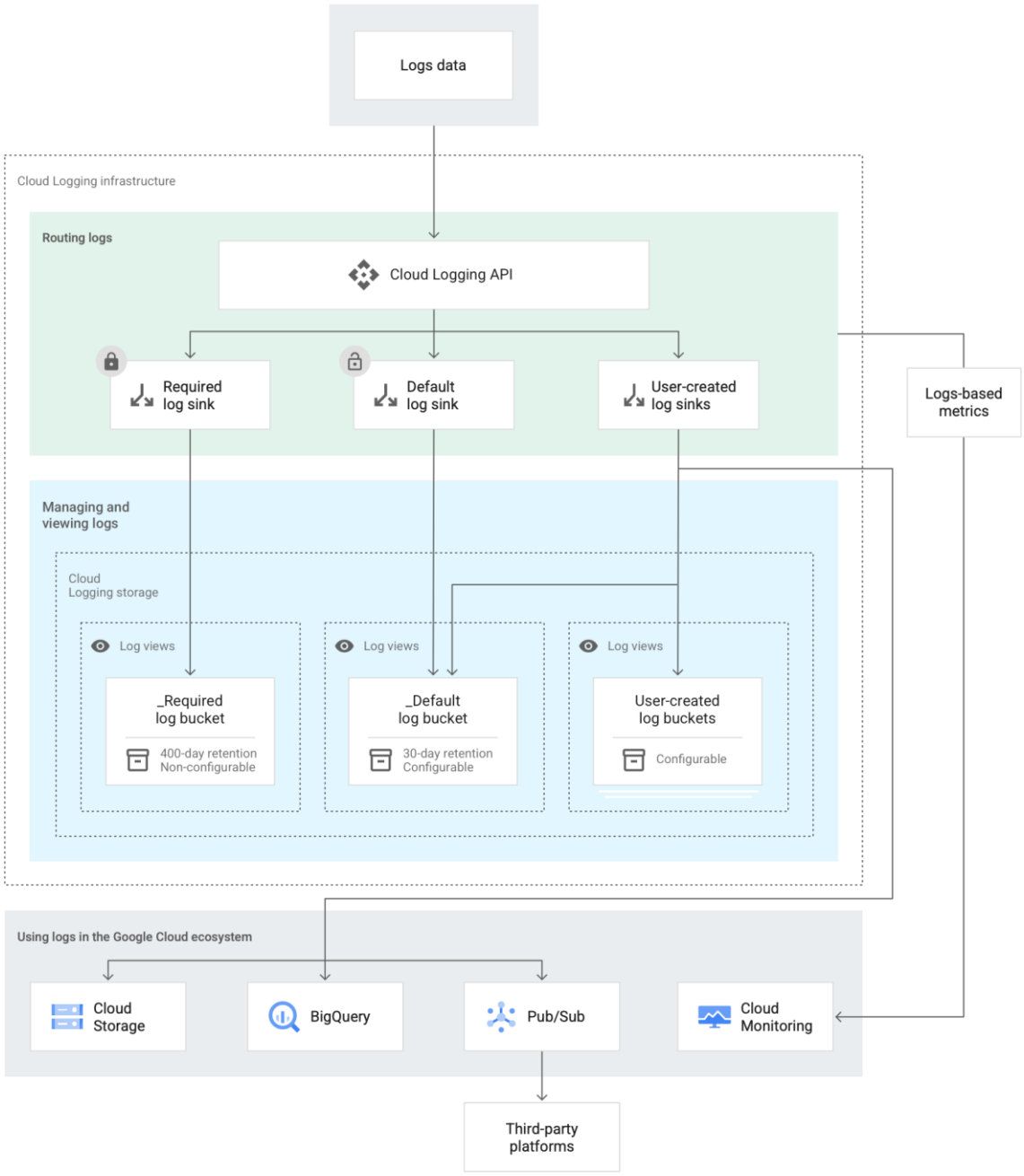


*Fig 8. Almacenamiento de las entradas de registro de Cloud Logging.*

Cloud Logging recibe entradas de registro a través de la API de Cloud Logging donde pasan a través del enrutador de registros. Los receptores del enrutador de registros verifican cada entrada de registro con los filtros de inclusión y exclusión existentes que determinan si la entrada de registro se debe enviar a destinos de almacenamiento, incluidos en los depósitos de Cloud Logging, o si se excluye por completo.

Los receptores enrutan las entradas de registro a los destinos de almacenamiento. Cloud Logging proporciona dos receptores de registros predefinidos para cada proyecto de Google Cloud: **_Required** y **_Default**. Todos los registros que se generan en un proyecto de Google Cloud se procesan de forma automática a través de estos dos receptores de

registro y, luego, se almacenan en los depósitos de registro de nombres **_Required** y **_Default** correspondientes.

Independientemente de cómo los receptores de registros predefinidos procesan las entradas de registro, Cloud logging permite crear receptores de registro para enrutar algunos o todos los registros a varios destinos. Para la implementación de estos receptores, puede consultar la guía del fabricante:
https://cloud.google.com/logging/docs/export/configure_export_v2?hl=es#creating_managing_sinks

Cloud Logging usa depósitos de registro como contenedores en los proyectos de Google Cloud para almacenar y organizar los datos de registros. Los registros que se almacenan en Cloud Logging se indexan, optimizan y entregan para que se puedan analizar los registros en tiempo real. Todos los registros generados en el proyecto se almacenan en los depósitos de registro _Required y _Default.

Cloud Logging también da la opción de crear depósitos de registro personalizados. Para ello puede consultar la guía del fabricante:
https://cloud.google.com/logging/docs/buckets?hl=es

La encriptación en reposo ya se proporciona en Google Cloud, incluido el enrutador de registros de Cloud Logging. Además, para mayor protección de estos registros se permite el uso de claves de encriptación. En lugar de que Google administre las claves de encriptación que protegen los datos, se permite crearlas, controlarlas y administrarlas en Cloud Key Management Service.

Las CMEK permiten controlar las claves que se usan para encriptar los datos en reposo. Se pueden usar para cumplir con los siguientes requisitos dentro de la organización de Google Cloud:

- Cumplimiento y control interno: Las CMEK se pueden usar para controlar datos sensibles o regulados que se almacenan en productos de Google Cloud (Cloud Storage).
- Requisitos reglamentarios: Para materiales confidenciales.
- Encriptación avanzada.

Para la implementación de las CMEK, puede consultar la guía del fabricante:
https://cloud.google.com/logging/docs/routing/managed-encryption?hl=es#getting-started

#### 3.1.2.5. Protección de claves criptográficas

Para la correcta protección de las claves criptográficas durante todo su ciclo de vida tal y como exige el Esquema Nacional de Seguridad GCP cuenta con su servicio Cloud Key Management.

**Creación de claves simétricas**

El cifrado simétrico se basa en una sola clave, tanto para hacer el cifrado como para el descifrado de los datos. A la hora de crear una clave simétrica, esta debe ser agregada a un llavero de claves dentro de Google Cloud. Es importante tener en cuenta que durante la creación de esta llave, se puede definir el período de rotación de claves, explicado en el siguiente punto. Para la creación de un llavero y de una clave, puede consultar la guía del fabricante:
https://cloud.google.com/kms/docs/creating-keys#create_a_key_ring
https://cloud.google.com/kms/docs/creating-keys#create_a_key

**Período de rotación de claves simétricas**
Se puede crear una clave con un período de rotación específico, que es el tiempo que transcurre entre la generación automática de versiones de claves nuevas. También se puede crear una clave con un período de rotación siguiente específico. En caso de no especificar un período, Cloud KMS determina estos ajustes de forma automática.

En el caso de la encriptación simétrica, se recomienda usar el servicio de rotación de claves de manera periódica y automática como medida de seguridad.

Para implementar y configurar la rotación automática, puedes consultar la guía del fabricante:
https://cloud.google.com/kms/docs/rotating-keys

**Creación de claves asimétricas**
A la hora de crear una clave asimétrica, esta debe ser agregada a un llavero de claves dentro de Google Cloud. Para la creación de un llavero y de una clave, puede consultar la guía del fabricante:
https://cloud.google.com/kms/docs/creating-asymmetric-keys#create_a_key_ring

Para la creación de una clave de desencriptación asimétrica puede consultar la guía del fabricante:
https://cloud.google.com/kms/docs/creating-asymmetric-keys#create_a_key

Para la creación de una clave de firma asimétrica, puede consultar la guía del fabricante:
https://cloud.google.com/kms/docs/creating-asymmetric-keys#create_an_asymmetric_signing_key

**Acceso a las claves asimétricas**
Para un usuario o servicio que realizará una firma, se otorga el permiso ***cloudkms.cryptoKeyVersions.useToSign*** sobre la clave asimétrica.
Para un usuario o servicio que recuperará la clave pública, se otorga el permiso ***cloudkms.cryptoKeyVersions.viewPublicKey*** sobre la clave asimétrica. Para la validación de la firma se necesita la clave pública.

Puedes encontrar más información sobre los permisos y funciones de Cloud KMS en el siguiente documento del fabricante:

https://cloud.google.com/kms/docs/reference/permissions-and-roles

**Rotación de claves asimétricas**
Cloud KMS no admite la rotación automática de claves asimétricas, ya que se requieren pasos adicionales para poder usar la nueva versión de las claves asimétricas.

Para rotar una clave de manera manual, puede consultar la guía del fabricante:
https://cloud.google.com/kms/docs/rotating-keys#manual

### 3.1.3. Continuidad del servicio

Los desastres vinculados con las tecnologías de la información, como los errores en los centros de datos, los daños en los servidores o los ataques cibernéticos no sólo pueden interrumpir las operaciones comerciales, sino también provocar pérdida de datos, afectar los ingresos y dañar su reputación.

**Regiones y zonas**
Una región es una ubicación geográfica específica donde se pueden alojar recursos. Las regiones tienen tres o más zonas.

Los recursos que se ubican en una zona, como las instancias de máquina virtual o los discos persistentes zonales, se denominan recursos zonales. Otros recursos, como las direcciones IP externas estáticas, son regionales. Cualquier recurso de esa región puede usar los recursos regionales, sin importar la zona, mientras que, en el caso de los recursos zonales, solo los pueden usar otros recursos en la misma zona.

Ubicar recursos en diferentes zonas de una región reduce el riesgo de interrupciones en la infraestructura que afectan a todos los recursos de forma simultánea. Ubicar recursos en diferentes regiones proporciona un grado aún mayor de independencia de fallas. Esto te permite diseñar sistemas sólidos con recursos distribuidos en diferentes dominios con fallas.

Deberá implementarse la correcta distribución de servicios según zonas de disponibilidad para limitar al máximo los riesgos asociados a una única ubicación.

### 3.1.4. Monitorización del sistema

**Cloud Monitoring**
Cloud Monitoring recopila medidas de los servicio y recursos de Google Cloud que se utilizan.

Con Cloud Monitoring se ofrece la posibilidad de crear políticas de alertas y verificaciones de las actividades de los recursos. Por ejemplo, cuando un servicio no cumple con los requisitos que se definan (por ejemplo, el 90% de las peticiones con respuesta 200 HTTP superan los 100ms).

Se puede configurar Cloud Monitoring para que haga sondeos de un servicio de forma periódica de una manera que imita cómo los usuarios acceden al servicio. Cuando se configura una verificación de tiempo de actividad, los servidores en al menos tres ubicaciones diferentes probarán el servicio de forma periódica y, luego, registran el éxito y la latencia del sondeo.

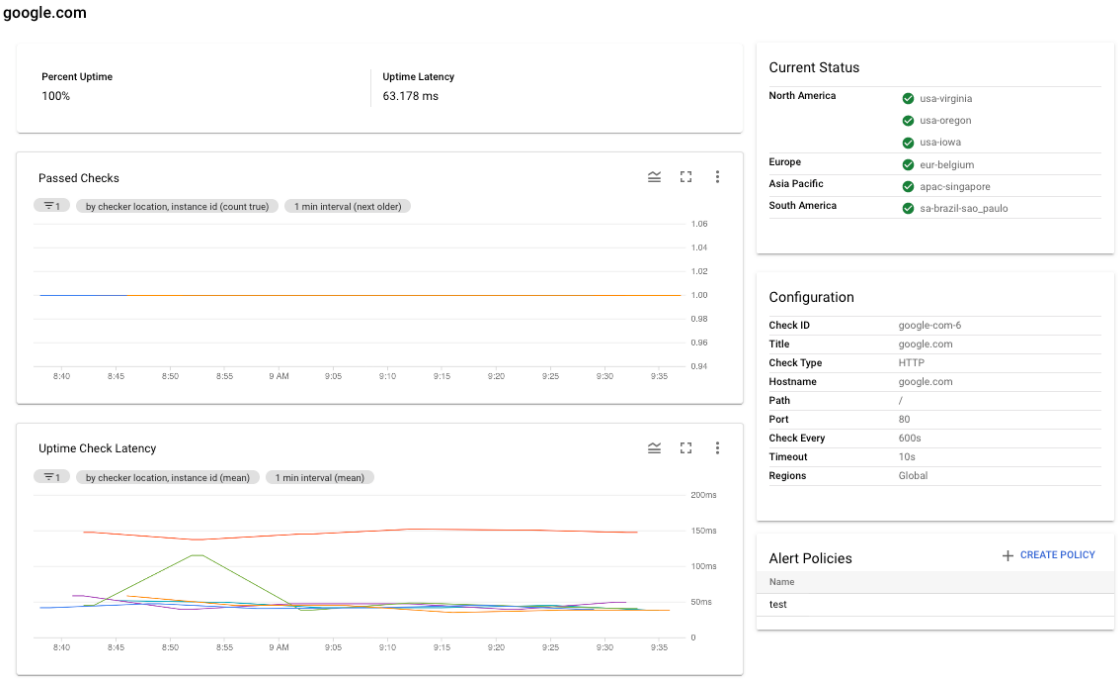


*Fig 11. Página de Verificaciones de tiempo de actividad.*

En caso de que la verificación de tiempo de actividad falle, se pueden configurar una política de alertas que envíen una notificación por diferentes canales, como el correo electrónico. Una política de alertas describe el conjunto de condiciones que se desea supervisar.

Para la creación de políticas de alertas, puede consultar la guía del fabricante: https://cloud.google.com/monitoring/alerts/using-alerting-ui?hl=es-419

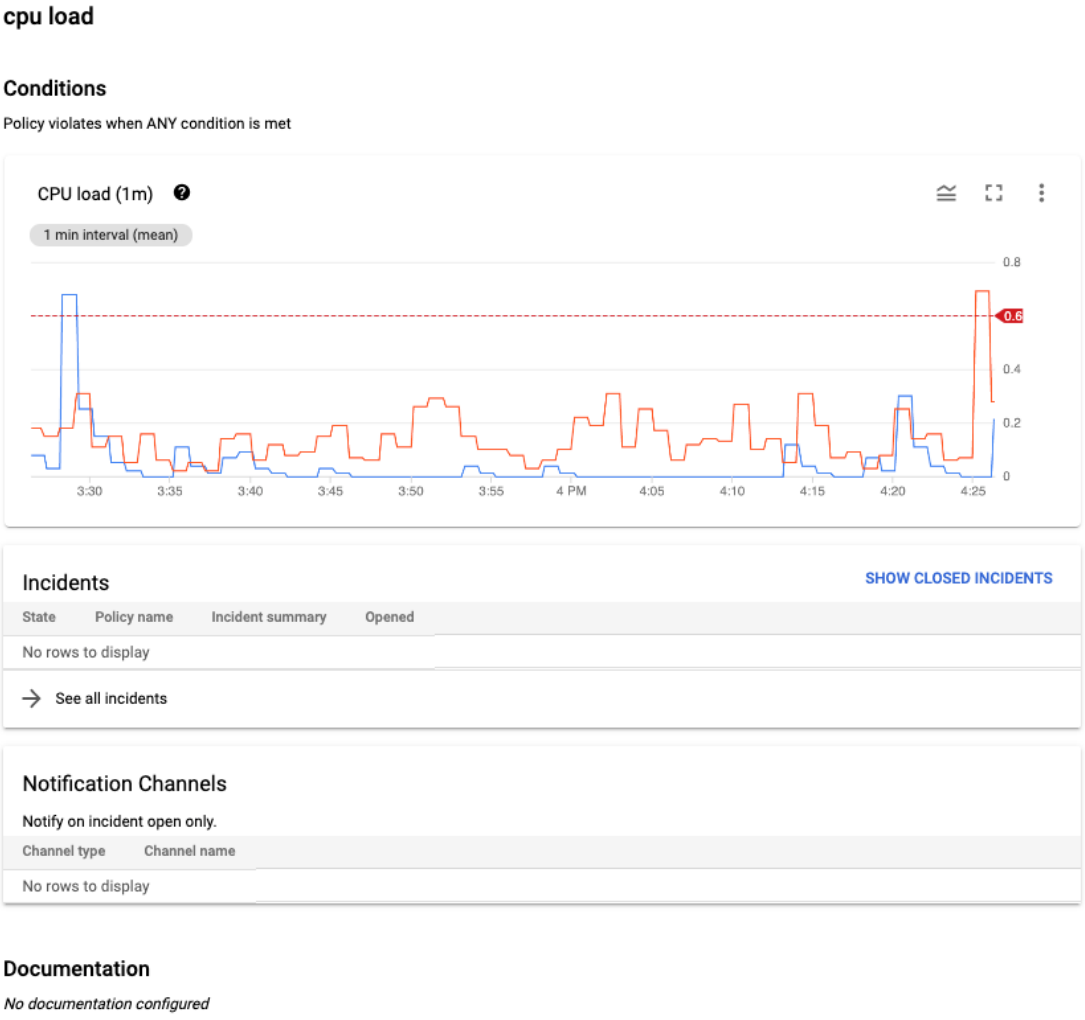


*Fig 10. Panel de monitorización de una VM con una política de alerta cuando se supera el 60% de uso de la CPU.*

Cloud Monitoring también permite la creación de gráficos personalizados para supervisar cualquier dato o métrica que se recopile en el proyecto. Entre ellos:

- Métricas del sistema generadas por los servicios de Google Cloud: Estas métricas proporcionan información sobre cómo funciona el servicio. Por ejemplo, Compute Engine.

Se pueden consultar todas las métricas de las que dispone Cloud monitoring de los servicios de Google Cloud en el siguiente documento del fabricante: https://cloud.google.com/monitoring/api/metrics_gcp?hl=es-419

- Métricas del sistema y de aplicaciones que recopila el agente de Cloud Monitoring: Estas métricas proporcionan información adicional sobre los recursos del sistema y las aplicaciones que se ejecutan en instancias de Compute Engine. De manera opcional, se puede configurar el agente para recopilar métricas de complementos de terceros.

Para la implementación del agente en servicios de terceros, puede consultar la guía del fabricante:
https://cloud.google.com/monitoring/agent/plugins?hl=es-419

- Métricas personalizadas que recibe la API de Cloud Monitoring configuradas por aplicaciones de la organización.
- Métricas basadas en registros: Recopilan información numérica sobre los registros escritos en Cloud Logging. Las métricas basadas en registros definidas por Google incluyen el recuento de errores que detectan los servicios y la cantidad total de entradas de registro que recibió el proyecto de Google Cloud.

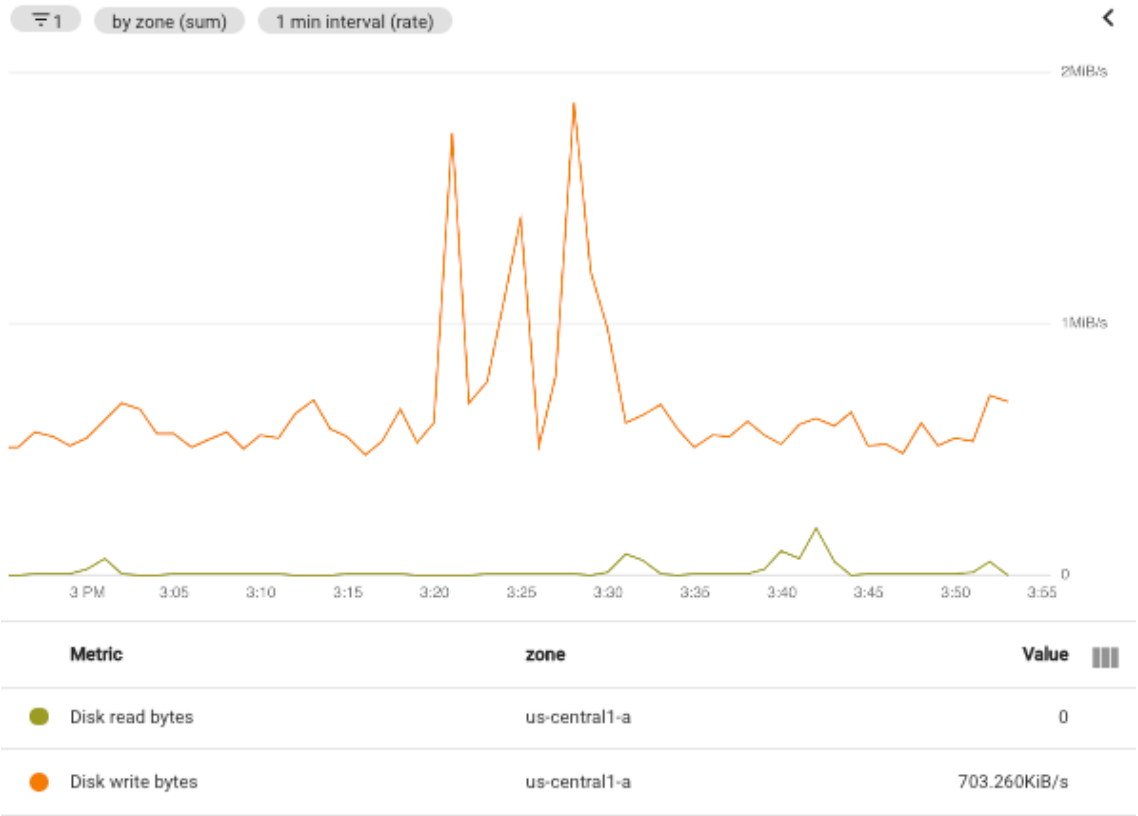


*Fig 11. Gráfico personalizado de un disco persistente.*

#### 3.1.4.1. Detección de intrusión

Para estas tareas se recomienda el uso del Security Command Center, el cual es un servicio de detección de amenazas que monitoriza continuamente para identificar actividades maliciosas y comportamientos no autorizados con el fin de proteger datos, cargas de trabajo y cuentas de GCP.

Security Command Center permite filtrar y ver vulnerabilidades y resultados de amenazas de muchas maneras diferentes, como filtrar en un tipo de resultado

específico, un tipo de recurso o un recurso específico. Las funciones de Security Command Center se otorgan a nivel de organización, carpeta o proyecto.

**Detección de anomalías**

La detección de anomalías es un servicio integrado que usa señales de comportamiento desde fuera del sistema. Muestra información detallada sobre las anomalías de seguridad detectadas para las instancias de máquina virtual (VM), como potenciales filtraciones de credenciales y minería de criptomonedas.

Categorías de detección de amenzas:

| ID | Descripción |
|---|---|
| account_has_leaked_credentials | Las credenciales para una cuenta de servicio de Google Cloud se filtran accidentalmente en línea o se ven comprometidas. |
| resource_compromised_alert | Posible compromiso de un recurso en la organización. |
| resource_involved_in_coin_mining | Las señales de comportamiento en torno a una VM de la organización indican que puede haber sido comprometida y podría estar en uso para la criptominería. |
| outgoing_intrusion_attempt | Intentos de intrusión y análisis de puertos: uno de los recursos o servicios de Google Cloud de la organización se ha usado para actividades de intrusión, como un intento de vulnerar o comprometer un sistema objetivo. Estos incluyen ataques de fuerza bruta de SSH, análisis de puertos y ataques de fuerza bruta de FTP. |
| resource_used_for_phishing | Uno de los recursos o servicios de Google Cloud de la organización se ha usado para la suplantación de identidad (phishing). |

**Detección de amenazas a contenedores**

Container Threat Detection detecta los ataques más comunes en el entorno de ejecución del contenedor y muestra las alertas dentro del Security Command Center.

La instrumentación de detección de Container Threat Detection puede detectar los siguientes eventos:

- Ejecución de un binario dañino
- Carga de bibliotecas externas
- Shells inversas

Puede obtener más información sobre la detección de amenazas a contenedores dentro de la guía ***CCN 888C Guía de Configuración Segura de Contenedores en GCP***.

### 3.1.5. Event Threat Detection

Event Threat Detection usa datos de registro dentro de los sistemas. Consume los registros de Cloud logging a medida que están disponibles. Cuando se detecta una amenaza, Event Threat Detection lo muestra en el Security Command Center.

Algunos resultados de Event Threat Detection son los siguientes:

| ID | Descripción |
|---|---|
| Ataques de fuerza bruta a SSH | Event Threat Detection detecta la fuerza bruta de SSH mediante la autenticación de contraseñas analizando los registros de syslog en busca de errores repetidos, seguidos de un éxito. |
| Abuso de IAM | Event Threat Detection detecta la adición de otorgamientos de IAM que podrían considerarse anómalos, como los siguientes:<br>• Agregar a un usuario fuera de la organización una política con la función de editor de proyectos.<br>• Invitar a un usuario externo a la organización como propietario del proyecto.<br>• Una cuenta de servicio que otorga permisos sensibles<br>• Se agregó la cuenta de servicio desde fuera de la organización. |
| Software Malicioso | Event Threat Detection detecta software malicioso examinando los registros de flujo de VPC y los registros de Cloud DNS para establecer conexiones con las IP y los dominios de control y comandos conocidos. |
| Suplantación de identidad | Event Threat Detection detecta la suplantación de identidad (phishing) mediante la evaluación de los registros de flujo de VPC y de los registros de Cloud DNS para conexiones a IP y dominios de suplantación de identidad (phishing) conocidos. |

Para obtener más información sobre Event Threat Detection puede consultar la siguiente guía del fabricante:
https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview?hl=es-419

## 3.2. Medidas de protección

### 3.2.1. Protección de las comunicaciones

#### 3.2.1.1. Protección de la confidencialidad

Esta medida del Esquema Nacional de Seguridad exige el uso del cifrado adecuado para la información en tránsito.

Google Cloud usa certificados SSL para proporcionar privacidad y seguridad desde un cliente hacia un balanceador de cargas. Para lograrlo, el balanceador de cargas debe tener un certificado SSL y la clave privada que le corresponde al certificado. La comunicación entre el cliente y el balanceador de cargas es privada, por lo que es ilegible para cualquier tercero que no tenga esta clave privada.

GCP ofrece tres tipos de balanceadores de carga que requieren certificados SSL:

| Tipo de balanceador de cargas | Protocolo del cliente al balanceador de cargas |
|---|---|
| Balanceadores de cargas HTTPS internos | HTTPS o HTTP/2 |
| Balanceadores de cargas HTTPS externos | HTTPS o HTTP/2 |
| Balanceadores de cargas de proxy SSL | SSL (TLS) |

Se pueden obtener certificados autoadministrados o se pueden usar certificados administrados por Google, que Google obtiene y administra.

- Los certificados SSL autoadministrados son certificados que se obtienen, aprovisionan y renuevan ajenos a Google.

Para la implementación de un certificado autoadministrados, se puede utilizar la siguiente guía del fabricante:
https://cloud.google.com/load-balancing/docs/ssl-certificates/self-managed-certs?hl=es#create-key-and-cert

- Los certificados SSL administrados por Google son certificados que Google Cloud obtiene y administra para los dominios de la organización, y los renueva de manera automática. Los certificados administrados por Google son certificados de validación de dominio (DV). No demuestran la identidad de una organización o de un individuo asociados con el certificado, y no admiten nombres comunes (comodín).

Para la implementación de un certificado administrado por Google, se puede utilizar la siguiente guía del fabricante:

https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs?hl=es

De forma predeterminada, el balanceo de cargas de HTTP(S) y el balanceo de cargas de proxy SSL usan un conjunto de características de SSL que proporciona una seguridad sólida y una compatibilidad amplia. Se pueden definir las políticas de SSL para controlar las características de SSL que el balanceador de cargas negocia con los clientes. Además, se puede usar una política de SSL para configurar la versión mínima de TLS y las características de SSL habilitadas en el balanceador de carga.

Cuando se crea una política de SSL se ofrecen tres perfiles administrados por Google, además de la posibilidad de crear un perfil personalizado:

- COMPATIBLE: Permite que el conjunto más amplio de clientes, incluidos aquellos que solo admiten características de **SSL desactualizadas**, negocien SSL con el balanceador de cargas.
- MODERNO: Admite un amplio conjunto de características de SSL, lo que permite que los clientes modernos negocien SSL.
- RESTRINGIDO: admite un conjunto reducido de características de SSL con la intención de cumplir con requisitos de cumplimiento más estrictos.
- Personalizado: Permite seleccionar características de SSL de forma individual.

| Característica | Compatible | Moderno | Restringido |
|---|---|---|---|
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 | X | X | X |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | X | X | X |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | X | X | X |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | X | X | X |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | X | X | X |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | X | X | X |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | X | X | |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | X | X | |

| Característica | Compatible | Moderno | Restringido |
|---|---|---|---|
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | X | X | |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | X | X | |
| TLS_RSA_WITH_AES_128_GCM_SHA256 | X | | |
| TLS_RSA_WITH_AES_256_GCM_SHA384 | X | | |
| TLS_RSA_WITH_AES_128_CBC_SHA | X | | |
| TLS_RSA_WITH_AES_256_CBC_SHA | X | | |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | X | | |

- Se deberá asegurar que los balanceadores de carga HTTPS o SSL no permiten políticas poco seguras. TLS1.0 y TLS1.1 son protocolos que ya no tienen soporte oficial, por tanto, su seguridad es baja.

Para la implementación de una política de SSL, se puede consultar la siguiente guía del fabricante:
https://cloud.google.com/load-balancing/docs/use-ssl-policies?hl=ES

#### 3.2.1.2. Segregación de redes

Virtual Private Cloud (GCP VPC) permite lanzar recursos de GCP en una red virtual que haya definido. Dicha red virtual equivale a las redes tradicionales que se utilizan en centros de datos habituales, con los beneficios que supone utilizar la infraestructura escalable de GCP.

Por defecto cuando se inicia un proyecto en GCP, se crea una red predeterminada. Esta red predeterminada tiene como nombre ***default***, y es una red en modo automático. Las redes en modo automático crean subredes y rutas de subredes en cada región de Google Cloud. También estas redes crean reglas de firewall predefinidas.

- Se deberá eliminar la red por defecto del proyecto (default).

Aunque las redes en modo automático puedan ser útiles al comienzo del proyecto, las redes VPC en modo personalizado son más adecuadas para entornos de producción. Los principales motivos son:

- Este tipo de redes se integran mejor en los esquemas de administración de direcciones IP ya existentes, pues las redes en modo automático usan el mismo rango de IP internas, pudiendo superponerse cuando se conectan con entornos locales.

- No puedes conectar dos redes VPC en modo automático porque las subredes usan rangos primarios idénticos.
- Permite la personalización de los nombres de las redes y subredes haciéndolos más descriptivos.

**Subredes**

A la hora de crear subredes el fabricante recomienda el uso de rangos de direccionamiento amplios. De manera convencional las redes suelen estar separadas en muchos rangos de direcciones pequeñas, ya sea para identificar o aislar alguna aplicación, sin embargo, para facilitar la administración de las subredes se recomiendan rangos de dirección más grandes. Google Cloud usa un enfoque de red definida por software (SDN) para proporcionar una malla completa de accesibilidad entre todas las VM de la red de VPC global. La cantidad de subredes no afecta el comportamiento del enrutamiento. Se pueden usar cuentas de servicio o etiquetas de red para aplicar políticas de enrutamiento o reglas de firewall específicas. La identidad en Google Cloud no se basa solo en la dirección IP de la subred.

**Conexión entre redes VPC**

Las redes de VPC son espacios de usuario aislado y se pueden comunicar entre sí de varias formas:

- Intercambio de tráfico entre redes de VPC: El intercambio de tráfico entre redes de VPC permite que dos redes de VPC se conecten de forma interna a través de la SDN de Google, sin importar si pertenecen al mismo proyecto o la misma organización. Cuando las redes de VPC intercambian tráfico, se puede acceder a todas las subredes, los rangos de alias de IP y las reglas de reenvío interno, y cada red de VPC mantiene su propio firewall distribuido.
- Enrutamiento externo (IP pública o puerta de enlace de NAT): Si no se necesita comunicación mediante direcciones IP privadas, se puede usar enrutamiento externo con direcciones IP externas o una puerta de enlace de NAT. Las VM con dirección externa se comunican entre sí de forma privada a través de la red troncal de Google, sin importar la región en la que se ubiquen ni el nivel de servicio de red que tengan.
- Cloud VPN: Cloud VPN proporciona un servicio administrado para conectar redes de VPC mediante la creación de un túnel IPSec entre dos extremos con enrutamiento estático o dinámico.

Se pueden consultar las ventajas y desventajas de uso de cada método en el siguiente documento del fabricante:
https://cloud.google.com/architecture/best-practices-vpc-design?hl=es-419#choose-method

### 3.2.2. Protección de la información

#### 3.2.2.1. Cifrado de la información

El Esquema Nacional de Seguridad exige para la categoría ALTA un correcto cifrado de la información tanto su almacenamiento como durante su transmisión. El correcto uso de la criptografía necesaria para las comunicaciones está descrito en la sección ***3.2.1.1 Protección de la confidencialidad*** en la presente guía.

**Compute Engine**
De forma predeterminada, Compute Engine encripta el contenido en reposo del cliente. Compute Engine controla y administra esta encriptación sin que se deba realizar ninguna acción adicional. Sin embargo, si se desea controlar y administrar esta encriptación, se pueden usar las claves de encriptación. Las claves de encriptación no encriptan los datos de forma directa, sino que se usan para encriptar las claves de encriptación de datos que encriptan los datos.

Se tienen las siguientes dos opciones para las claves de encriptación de claves en Compute Engine:

- Usar Cloud Key Management Service para crear y administrar claves de encriptación de claves. Para la implementación de esta opción, se puede consultar la siguiente guía del fabricante:
  https://cloud.google.com/compute/docs/disks/customer-managed-encryption?hl=es-419
- Crea y administra tus propias claves de encriptación de claves. Para la implementación de esta opción, se puede consultar la siguiente guía del fabricante:
  https://cloud.google.com/compute/docs/disks/customer-supplied-encryption?hl=es-419

**Cloud SQL**
Dentro del servicio Cloud SQL se permite la encriptación gestionada por el cliente. Esta encriptación es a nivel de columnas. En caso de tener una tabla con nombres y números de tarjeta, Cloud SQL ofrece la posibilidad de encriptar esas columnas de la tabla. Esta encriptación se hace a través de una clave de encriptación almacenada en Cloud Key Management Service (Cloud KMS).

Puedes encontrar más información sobre este servicio en la sección ***3.1.2.5 Protección de claves criptográficas*** de esta misma guía.

### 3.2.3. Protección de los servicios

#### 3.2.3.1. Protección de servicios y aplicaciones web

Los sistemas dedicados a la publicación de información no deberán ser publicados sin estar antes protegidos frente a las amenazas propias de los servicios web.

**Google Cloud Armor**

Google Cloud Armor ofrece unas características principales, que permite proteger las aplicaciones de ataques externos.

***Control de acceso basado en IP y en geolocalización***

Filtra el tráfico entrante en función de las direcciones IPv4 e IPv6 o del enrutamiento entre dominios sin clase (CIDR). Aplica controles de acceso basados en la ubicación para permitir o rechazar el tráfico según la información geográfica mediante la asignación de GeoIP de Google.

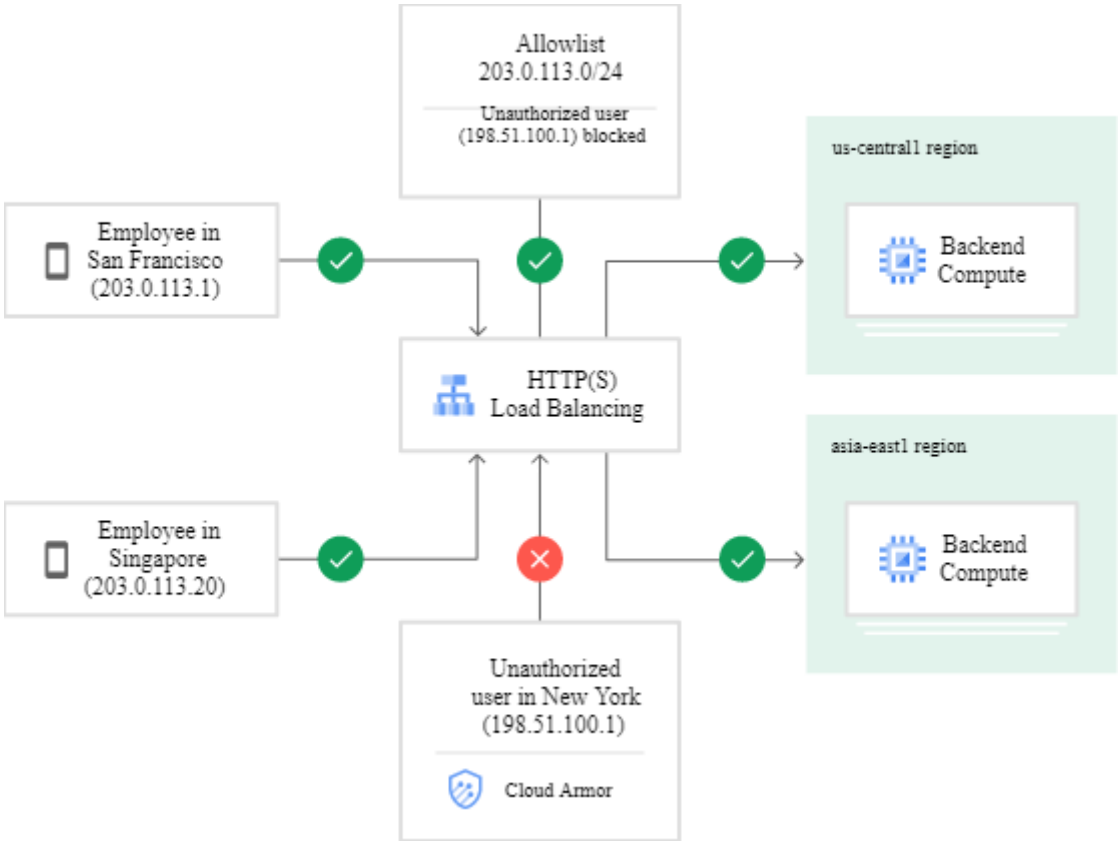


*Fig 12. Restricción del acceso al balanceador de cargas con una lista de admisión.*

Para la implementación de una lista de admisión, se puede consultar la guía del fabricante:
https://cloud.google.com/armor/docs/common-use-cases?hl=es#limit-access-to-https

***Protección frente a riesgos OWASP***

Las reglas de WAF preconfiguradas de Google Cloud Armor se pueden agregar a una política de seguridad para detectar y denegar solicitudes de capa 7 no deseadas que contengan intentos de inyección de SQL o XSS. Google Cloud Armor detecta las solicitudes maliciosas y las coloca en el perímetro de la infraestructura de Google. Las solicitudes no se envían mediante proxy al servicio de backend, sin importar dónde se implemente el servicio de backend.

Para la implementación de esta característica, se puede consultar la guía del fabricante:

https://cloud.google.com/armor/docs/common-use-cases?hl=es#owasp-top-10

***Visibilidad y monitorización***

Cloud Armor permite monitorizar todas las métricas asociadas a las políticas de seguridad desde el panel de Cloud Monitoring. Permite observar los patrones sospechosos del tráfico de aplicaciones directamente desde Cloud Armor, dentro del panel de control de Security Command Center.

***Reglas de WAF preconfiguradas***

Las reglas preconfiguradas de Google Cloud Armor son reglas complejas de firewall de aplicación web (WAF) con decenas de firmas que se compilan a partir de estándares de la industria de código abierto. Las reglas permiten que Google Cloud Armor evalúe decenas de firmas de tráfico distintas, ya que consulta las reglas con nombres prácticos en lugar de requerir que se defina cada firma de forma manual.
La lista completa de reglas de WAF se encuentra en el siguiente documento del fabricante:
https://cloud.google.com/armor/docs/rule-tuning?hl=es

#### 3.2.3.2. Protección frente a la denegación de servicio

**Google Cloud Armor**

Google Cloud Armor ayuda a proteger la infraestructura y aplicaciones de los ataques de denegación de servicio distribuidos (DSD) de capa 3 o capa 4, los ataques de capa 7 del volumen y otros ataques de aplicación dirigidos. Aprovecha la red global de Google y la infraestructura distribuida para detectar y absorber ataques y filtrar el tráfico a través de políticas de seguridad configurables por el usuario en el perímetro de la red de Google

**Firewall Insights**

Las Estadísticas de firewall proporcionan informes que contienen información sobre el uso del firewall y el impacto de varias reglas de firewall en la red VPC.

Los informes de métricas y las estadísticas de firewall permiten mejorar la configuración de las reglas de una red VPC. Con los informes de métricas, se pueden realizar las siguientes tareas:

- Verificar que las reglas de firewall se usen de la manera prevista.
- Durante los períodos específicos, verificar que las reglas de firewall permitan o bloqueen las conexiones previstas.
- Realizar una depuración en tiempo real de las conexiones que se interrumpen de forma involuntaria debido a las reglas de firewall.
- Usar Cloud Monitoring para detectar intentos maliciosos de acceder a tu red, incluida la recepción de alertas cuando hay cambios significativos en los recuentos de aciertos de las reglas de firewall. Para la implementación de esta característica, puede usar la guía del fabricante:
  https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/working-with-common-use-cases#detect-increase-hit-count

Para generar los informes de métricas y estadísticas de firewall, puede seguir la siguiente guía del fabricante:
https://cloud.google.com/recommender/docs/insights/using-insights

## 4. GLOSARIO DE TÉRMINOS

A continuación, se describen los términos, acrónimos y abreviaturas relacionados con la tecnología objeto de esta guía con el objeto de facilitar la comprensión de la misma

| Término | Definición |
|---|---|
| Cloud KMS | Cloud Key Management Service |
| DSD | Denegación de servicio distribuidos |
| ENS | Esquema Nacional de Seguridad |
| FaaS | Funciones como servicio |
| GCE | Google Compute Engine |
| GCF | Google Cloud Functions |
| GCP | Google Cloud Platform |
| GCS | Google Cloud Storage |
| GKE | Google Kubernetes Engine |
| GW | Google Workspace |
| IAM | Identity and Access Management |
| IAP | Identity-Aware Proxy |
| MFA | Autenticación de múltiples factores |
| RBAC | Acceso basado en roles |
| SDN | Redes definidas por software |
| SSL | Secure Sockets Layer |
| TLS | Seguridad de la capa de transporte |
| VM | Virtual Machine (máquina virtual) |
| VPC | Virtual Private Cloud |
| WAF | Web application firewal |

## 5. GLOSARIO DE SERVICIOS GCP

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guía incluyendo enlaces a la documentación concreta de cada uno de ellos.

| Servicio | URL de documentación del servicio |
|---|---|
| Cloud Asset Inventory | https://cloud.google.com/asset-inventory |
| Cloud Logging | https://cloud.google.com/logging |
| Cloud Monitoring | https://cloud.google.com/monitoring |
| Container Threat Detection | https://cloud.google.com/security-command-center/docs/concepts-container-threat-detection-overview?hl=es-419 |
| Event Threat Detection | https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview?hl=es-419 |
| Firewall Insights | https://cloud.google.com/network-intelligence-center/docs/firewall-insights |
| Google Cloud Armor | https://cloud.google.com/armor?hl=es |
| Google Cloud Functions | https://cloud.google.com/functions?hl=es |
| Google Cloud SQL | https://cloud.google.com/sql?hl=es |
| Google Cloud Storage | https://cloud.google.com/storage |
| Google Compute Engine | https://cloud.google.com/compute?hl=es |
| Google Compute Engine Persistent Disks | https://cloud.google.com/persistent-disk?hl=es |
| Google Docs Editors | https://www.google.es/intl/es/docs/about/ |
| Google Kubernetes Engine | https://cloud.google.com/kubernetes-engine?hl=es-419 |
| Google VPC | https://cloud.google.com/vpc?hl=es-419 |
| Google Workspace | https://workspace.google.com/intl/es-419_ar/ |
| Identity-Aware Proxy | https://cloud.google.com/iap |
| Security Command Center | https://cloud.google.com/security-command-center?hl=es |

## 6. CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio. Estas medidas sirven para valorar el nivel de cumplimiento de la organización.

| Control ENS | Descripción medida | Identificador control guías ENS GCP | Descripción control | Chequeo automatizado |
|---|---|---|---|---|
| [op.acc.1] | Identificación | [op.acc.1.gcp.iam.1] | Se deberá utilizar las credenciales de acceso de la organización en lugar de las cuentas personales, como las de Gmail. | CIS 1.1 Ensure that corporate login credentials are used |
| [op.acc.3] | Segregación de funciones y tareas | [op.acc.3.gcp.org.1] | Se deberá aplicar el principio de "separación de obligaciones" al asignar funciones relacionadas con las cuentas de servicio a los usuarios. La separación de obligaciones es el concepto de asegurar que un individuo no tenga todos los permisos necesarios para poder completar una acción maliciosa. En Cloud IAM podría ser una acción como el uso de una cuenta de servicio para acceder a recursos a los que el usuario no debería tener acceso normalmente. | CIS 1.8 Ensure that Separation of duties is enforced while assigning service account related roles to users |
| | | [op.acc.3.gcp.iam.2] | Las cuentas de servicio no pueden tener privilegios de administrador. | CIS 1.5 Ensure that Service Account has no Admin privileges |
| [op.acc.5] | Mecanismo de autenticación | [op.acc.5.gcp.iam.3] | Se deberá activar el doble factor de autenticación para todas las cuentas que no sean cuentas de servicios. | CIS 1.2 Ensure that multi-factor authentication is enabled for all non-service accounts |
| | | [op.acc.5.gcp.iam.4] | Para las cuentas que son administradores, se deberá activar el factor de autenticación más fuerte: Llaves de seguridad. Las llaves de | CIS 1.3 Ensure that Security Key Enforcement is enabled for all admin accounts |

| Control ENS | Descripción medida | Identificador control guías ENS GCP | Descripción control | Chequeo automatizado |
|---|---|---|---|---|
| | | | seguridad son llaves físicas reales que se utilizan para acceder a las cuentas de administrador de la organización de Google. | |
| [mp.com.2] | Protección de la confidencialidad | [mp.com.2.gcp.lb.1] | Se deberá asegurar que los balanceadores de carga HTTPS o SSL no permiten políticas poco seguras. | CIS 3.9 Ensure no HTTPS or SSL proxy load balancers permit SSL policies with weak cipher suites |
| [mp.com.4] | Segregación de redes | [mp.com.4.gcp.vpc.1] | Se deberá eliminar la red por defecto del proyecto (default). | CIS 3.1 Ensure that the default network does not exist in a project |

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL