Guía de Seguridad de las TIC
CCN-STIC 1009

Procedimiento de Empleo Seguro
Google Cloud Platform



Noviembre 2026

Edita:





CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 7
5 FASE DE INSTALACIÓN 10
6 FASE DE CONFIGURACIÓN 11
6.1 MODO DE OPERACIÓN SEGURO 11
6.1.1 CERTIFICATE AUTHORITY SERVICE 11
6.1.2 CLOUD ARMOR 11
6.1.3 CLOUD LOGGING 12
6.1.4 GOOGLE KMS WITH EKM SOLUTION 12
6.1.5 IDENTITY AND ACCESS MANAGEMENT (IAM) 12
6.1.6 CLOUD ASSET INVENTORY 12
6.1.7 KEY MANAGEMENT SERVICE 13
6.1.8 GOOGLE SENSITIVE DATA PROTECTION 13
6.1.9 CHROME ENTERPRISE PREMIUM 14
6.1.10 GOOGLE CLOUD IDENTITY 15
6.2 AUTENTICACIÓN 16
6.3 ADMINISTRACIÓN DEL PRODUCTO 17
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 17
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 17
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 18
6.5 GESTIÓN DE CERTIFICADOS 18
6.6 SERVIDORES DE AUTENTICACIÓN 18
6.7 SINCRONIZACIÓN 18
6.8 ACTUALIZACIONES 19
6.9 AUTO-CHEQUEOS 19
6.10 ALTA DISPONIBILIDAD 20
6.11 AUDITORÍA 20
6.11.1 REGISTRO DE EVENTOS 20
6.11.2 ALMACENAMIENTO LOCAL 21
6.11.3 ALMACENAMIENTO REMOTO 21
6.12 BACKUP 21
7 REFERENCIAS 23
8 ABREVIATURAS 25

1 INTRODUCCIÓN

Los servicios de **Google Cloud Platform** ofrecen un conjunto de soluciones avanzadas diseñadas para proteger la infraestructura, los datos y la identidad de los usuarios en entornos cloud de Google. Estos servicios permiten implementar controles de seguridad robustos, garantizando la protección contra amenazas y facilitando el cumplimiento normativo.

Este **Procedimiento de Empleo Seguro (PES)** abarca los siguientes servicios de seguridad de Google Cloud Platform cualificados en el CPSTIC:

- *Chrome Enterprise Premium (formerly known as BeyondCorp Enterprise)*
- *Google Certificate Authority Service*
- *Cloud Armor*
- *Google Cloud Platform Identity*
- *Cloud Logging*
- *Google KMS with EKM solution*
- *Identity & Access Management (IAM)*
- *Cloud Asset Inventory*
- *Key Management Service*
- *Google Sensitive Data Protection (formerly Cloud Data Loss Prevention or DLP)*

La administración de estos servicios se realiza, en su mayoría, a través de la **consola de Google Cloud Platform (*Google Cloud Platform Console*)**, mientras que algunos servicios específicos se gestionan desde la **consola de Administración (*Admin Console*)** de Google. A lo largo de este documento se detallará la configuración segura recomendada para cada uno de ellos, siguiendo las mejores prácticas de seguridad y los estándares establecidos por el **Centro Criptológico Nacional (CCN)**.

Para más información sobre los servicios mencionados en este PES, se puede consultar una descripción [Resumen Servicios] de cada uno de ellos en la documentación de Google.

2 OBJETO Y ALCANCE

Este documento se desarrolla para varios de los servicios de Google Cloud Platform listados en el CPSTIC:

a) El servicio **Cloud Armor** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

b) El servicio **Google Cloud Identity** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

c) El servicio **Google KMS with EKM solution** se incluye en la familia de *Dispositivos de gestión de claves criptográficas*. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

d) El servicio **Identity & Access Management (IAM)** se incluye en la familia de Gestión de Identidades. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

e) El servicio **Key Management Service** se incluye en la familia de *Dispositivos de gestión de claves criptográficas*. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

f) El servicio **Sensitive Data Protection (formerly Cloud Data Loss Prevention or DLP)** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

g) El servicio **Cloud Asset Inventory** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

h) El servicio **Cloud Logging** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

i) El servicio **Google Certificate Authority Service** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

j) El servicio **Chrome Enterprise Premium (formerly known as BeyondCorp Enterprise)** se incluye en la familia de Otras Herramientas. **No aplica una versión evaluada** específica dada la naturaleza en nube del servicio.

El alcance de este documento cubre las recomendaciones y medidas de seguridad necesarias para el despliegue y configuración segura de todos los servicios de Google mencionados.

Los servicios de Google Cloud Platform han sido incluidos en el catálogo CPSTIC, para conocer el listado más reciente y preciso, la categoría o nivel y la familia consulte el sitio web del CPSTIC [CPSTIC].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Los servicios de seguridad de **Google Cloud Platform** descritos en este **Procedimiento de Empleo Seguro (PES)** no requieren un proceso de entrega segura tradicional, ya que se trata de **servicios alojados en la infraestructura en nube de Google**.

El acceso a estos servicios se realiza directamente a través de **la consola de Google Cloud Platform** [GCP Console] o la **consola de Administración** [Admin Console] dependiendo del tipo de servicio, lo que elimina la necesidad de un proceso de instalación o entrega física.

Los siguientes servicios son accesibles a través de la consola de Google Cloud Platform:

- *Google Certificate Authority Service*
- *Cloud Armor*
- *Cloud Logging*
- *Google KMS with EKM solution*
- *Identity & Access Management (IAM)*
- *Cloud Asset Inventory*
- *Key Management Service*
- *Google Sensitive Data Protection (formerly Cloud Data Loss Prevention or DLP)*

Los siguientes servicios son accesibles a través de la consola de Administración:

- *Chrome Enterprise Premium (formerly known as BeyondCorp Enterprise)*
- *Google Cloud Identity*

Para acceder a la consola de Google Cloud Platform, Google ofrece la posibilidad de empezar con una versión de prueba hasta que se active la cuenta pagada de forma completa. La información para comenzar a usar los servicios de Google Cloud Platform viene especificada en la documentación oficial.

Para acceder a la consola de Administración de Google, es preciso crear o disponer de un espacio de trabajo [Google Workspace] y administrarlo a través de esta consola.

En ambos casos, también se puede **contactar con el equipo de ventas de Google para soporte acerca del acceso a los servicios de Google** que incluye el presente Procedimiento de Empleo Seguro, dependiendo si es a Google Cloud Platform o Google Workspace.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los servicios de seguridad de **Google Cloud Platform** incluidos en este **Procedimiento de Empleo Seguro (PES)** son soluciones cloud gestionadas íntegramente dentro de la infraestructura de **Google**, sin necesidad de instalación en entornos físicos o Centros de Proceso de Datos (CPD).

4.3 REGISTRO Y LICENCIAS

El acceso y uso de los servicios de seguridad de Google incluidos en este documento requieren un registro y la asignación de licencias adecuadas dentro del entorno cloud de Google.

El registro se realiza a través de:

a) **Consola de Google Cloud Platform (Google Cloud Platform Console)**, donde los administradores pueden habilitar y configurar los servicios según las necesidades de la organización.

b) **Consola de Administración (Admin Console)**, utilizada para la gestión de identidades, dispositivos y políticas de seguridad relacionadas con servicios de Google específicos. Para poder gestionar esta consola es preciso disponer de un espacio de trabajo de Google.

Los diferentes servicios de Google se basan en un modelo de cuotas [CUOTAS] según los consumos de los recursos que precisen los usuarios. Por tanto, **no se precisan licencias** por parte de Google para poder acceder a estos servicios.

Es posible que algunos servicios cuenten con niveles distintos según las características y funcionalidades de seguridad que ofrezcan. Los siguientes niveles han sido tenidos en cuenta para la evaluación:

- *Google Certificate Authority Service* – **N/A**
- *Cloud Armor* – **Nivel Standard / Premium**
- *Cloud Logging* – **N/A**
- *Google KMS with EKM solution*– **Nivel de protección EXTERNAL**
- *Identity & Access Management (IAM)* – **N/A**
- *Cloud Asset Inventory* – **N/A**
- *Key Management Service* – **Nivel de protección SOFTWARE**
- *Sensitive Data Protection (formerly Cloud Data Loss Prevention or DLP)* – **N/A**
- *Chrome Enterprise Premium (formerly known as BeyondCorp Enterprise)* – **N/A**
- *Google Cloud Identity* – **Nivel Free**

4.4 CONSIDERACIONES PREVIAS

Todos los servicios contemplados en este Procedimiento de Empleo Seguro (PES) se sirven a través de la nube pública de Google Cloud Platform.

Para operar con los servicios de Google incluidos en este Procedimiento de Empleo Seguro (PES), es necesario disponer previamente de un Workspace de Google.

Se debe configurar un Workspace asociado a la organización que desplegará los servicios de seguridad.

Durante la configuración, es obligatorio registrar un **dominio válido**, el cual debe corresponder a la organización corporativa que hará uso de estos servicios.

Una vez el dominio ha sido validado y el Workspace está operativo, se habilita el acceso a la **consola de Administración de Google**. En esta consola, a través del servicio Cloud Identity, se gestionan las identidades que podrán hacer uso de los servicios de Google dentro de la organización definida.

Al acceder a la **Consola de Google Cloud Platform**, se podrá visualizar la organización previamente creada en Workspace, permitiendo la gestión de los servicios en la nube de manera centralizada.

Solo los **administradores y usuarios con permisos adecuados** podrán operar dentro de la Google Cloud Platform Console, gestionar configuraciones de seguridad y administrar los servicios incluidos en este PES.

Se recomienda establecer políticas de control de acceso basadas en roles (IAM) para restringir y gestionar los permisos dentro del entorno corporativo.

Por último, es necesario **restringir las comunicaciones TLS para securizar los canales de comunicación con las consolas de Google en la nube**, ya sea con la consola de Google Cloud Platform o la consola de Administración. Para ello, seguir las siguientes consideraciones:

a) El administrador de Google Workspace, una vez completadas las directrices de configuración de seguridad de los servicios proporcionados por la consola de Administración, debe ponerse en contacto con Google para limitar las comunicaciones TLS habilitadas en su organización. De este modo, todas las conexiones se ajustarán a los parámetros criptográficos aceptados para la categoría ALTA de ENS, tal y como se indica en las directrices CCN.

b) Para restringir el uso de comunicaciones de versiones TLS inferiores a v1.2 al intercambiar recursos los servicios de Google dentro de GCP es necesario configurar la restricción TLS [Configuración TLS].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El correcto funcionamiento y la seguridad de los servicios Google dependen de una serie de componentes dentro del entorno de operación. Estos componentes permiten la gestión de identidades, el control de accesos, el almacenamiento de registros y la protección de la infraestructura cloud, asegurando un despliegue seguro y conforme a las mejores prácticas de seguridad.

Dado que cada uno de estos servicios cubre una funcionalidad específica dentro del ecosistema de **Google Cloud Platform**, pueden actuar como **componentes del entorno operacional de otros servicios**. Es decir, los servicios de seguridad de GCP no solo operan de manera independiente, sino que también interactúan entre sí para proporcionar un entorno seguro y cohesionado.

El entorno de operación debe estar diseñado para garantizar la disponibilidad, integridad y confidencialidad de los servicios, aplicando mecanismos de autenticación robustos, gestión segura de claves y protección contra amenazas.

A continuación, se describen los principales servicios y componentes que deben estar presentes en el entorno de operación para la correcta implementación y uso de los servicios de seguridad de Google:

- **Infraestructura de Google Cloud Platform (GCI)**. Se trata del conjunto subyacente de servicios y recursos proporcionados por Google para ofrecer un

entorno de nube sólido, escalable y seguro. GCI apoya el despliegue, la gestión y el funcionamiento de soluciones basadas en la nube, habilitando funcionalidades como servicios de computación, almacenamiento, redes, identidad y seguridad para sus usuarios.

- **Plataforma de Google Cloud Platform (GCP)**. Plataforma que ofrece un conjunto de servicios de computación en nube proporcionados por Google.
- **Consola de Google Cloud Platform**. Esta consola es una interfaz de gestión basada en web para GCP. Sirve de eje centralizado para que los administradores y desarrolladores interactúen con los recursos de GCP, gestionen los servicios, configuren los ajustes, supervisen el rendimiento y accedan a las funciones de seguridad.
- **Consola de Administración**. Consola utilizada por los administradores del Workspace para gestionar identidades y dispositivos.
- **Google Cloud Identity**. Este servicio ofrece un conjunto de funciones administrativas dentro de la consola de administración para la gestión de cuentas alojadas en Google, dispositivos y aplicaciones dentro del dominio del cliente.
- **Identity & Access Management (IAM)**. IAM proporciona a los administradores la capacidad de gestionar los recursos de la nube de forma centralizada controlando quién puede realizar qué acción en recursos específicos.
- **Cloud Logging**. Este servicio ingiere datos de registro de aplicaciones y sistemas, así como datos de registro personalizados de miles de máquinas virtuales y contenedores. Cloud Logging permite analizar y exportar en tiempo real los registros seleccionados al almacenamiento a largo plazo.
- **Key Management Service**. Cloud KMS es un servicio de gestión de claves alojado en la nube que le permite gestionar claves criptográficas para los servicios en la nube del mismo modo que lo hace en las instalaciones. Puede generar, utilizar, rotar y destruir claves criptográficas.
- **Cloud Load Balancing**: Actúa como front-end para distribuir el tráfico entrante a través de múltiples servicios back-end. Proporciona escalabilidad, disponibilidad y equilibrio de carga para la aplicación. Corresponde a un Balanceador de carga HTTP(S) regional desplegado en la Unión Europea.
- **Cloud Storage**. Es un servicio RESTful para almacenar y acceder a los datos de los clientes en la infraestructura de Google. El servicio combina el rendimiento y la escalabilidad de la nube de Google con funciones avanzadas de seguridad y uso compartido.
- **Resource Manager API**. Este servicio permite gestionar el acceso a los recursos de Google Cloud Platform mediante políticas de organización.
- **BigQuery**. Se trata de un servicio de análisis de datos totalmente gestionado que permite a las empresas analizar Big Data.
- **Pub/Sub**. Pub/Sub está diseñado para proporcionar mensajería asíncrona fiable, de muchos a muchos, entre aplicaciones. Las aplicaciones editoras pueden enviar mensajes a un “tema” y otras aplicaciones pueden suscribirse a ese tópico para recibir los mensajes. Al desacoplar emisores y receptores,

Pub/Sub permite a los desarrolladores comunicarse entre aplicaciones escritas de forma independiente.

- **Keystore**: Se trata del servicio interno de gestión de claves de Google. Almacena la clave maestra del proceso de cifrado en reposo [CIFRADO] de datos de clientes en Google.
- **Compute Engine**. Compute Engine ofrece capacidades de virtualización escalable de máquinas en la nube, con opciones para utilizar determinadas CPU, GPU o TPU. Su principal funcionalidad es resolver problemas analíticos y de procesamiento a gran escala en la infraestructura de computación, almacenamiento y redes de Google.
- **Google Kubernetes Engine**. Google Kubernetes Engine, basado en el orquestador de contenedores de código abierto Kubernetes, permite ejecutar contenedores en GCP. Este servicio se encarga del aprovisionamiento y el mantenimiento del clúster de máquinas virtuales subyacente, del escalado de la aplicación y de la logística operativa, como el registro, la supervisión y la gestión del estado del clúster.
- **Security Command Center**: Este servicio es el servicio centralizado de informes sobre vulnerabilidades y amenazas de Google Cloud Platform. También proporciona inventario y descubrimiento de activos y permite identificar configuraciones erróneas, vulnerabilidades y amenazas.
- **Usuarios autorizados**. Son los usuarios con privilegios de administración sobre una u otras las funcionalidades de seguridad de los servicios de Google incluidos en este PES. Según el tipo de usuario autorizado, puede gestionar los servicios a través de la consola de administración o la consola de Google Cloud Platform.
- **EKM partner**. Es el sistema de administración de claves externas integrado con el servicio Cloud External Key Manager. La evaluación de este servicio contempla la integración con Thales.

5 FASE DE INSTALACIÓN

Dado que los servicios de seguridad incluidos en este **Procedimiento de Empleo Seguro (PES)** son **soluciones SaaS** gestionadas dentro de la infraestructura de **Google Cloud Platform**, no requieren un proceso de instalación tradicional en servidores o equipos locales.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

A continuación, se describe paso a paso cómo **activar la configuración específica de cada uno de los servicios de Google** que contempla el presente Procedimiento de Empleo Seguro para que estos operen en el modo de cumplimiento requerido.

En primer lugar, para hacer uso de cualquiera de los servicios de Google, es preciso habilitar las APIs [APIs] en caso de que vengan deshabilitadas por defecto para el proyecto de Google Cloud Platform de una organización.

De forma común a todos los servicios que aplique, se deben tener en cuenta las siguientes consideraciones:

a) Los recursos gestionados por el servicio estarán desplegados en regiones controladas, como es el caso de regiones dentro de la **Unión Europea**. Este criterio se ha seguido a lo largo de la evaluación de los diferentes servicios para el correcto cumplimiento con los estándares del ENS para categoría ALTA.

b) Por defecto, para algunos servicios los logs de datos de acceso están desactivados, por lo que es preciso activarlos explícitamente como se define en la documentación oficial [LOGS].

c) **Todos los mecanismos criptográficos** de los que haga uso el servicio o configure el usuario final **seguirán los estándares de seguridad definidos por las guías de CCN para la categoría ALTA del ENS**.

d) Los servicios se han desplegado a nivel de **proyecto** dentro de una **organización** en el entorno de GCP.

6.1.1 CERTIFICATE AUTHORITY SERVICE

La funcionalidad principal de este servicio consiste en gestionar autoridades de certificación, por lo que es preciso crear, al menos, un grupo de AC (CA pool), una AC raíz (root CA) y emitir certificados [Certificate Authority].

Cuando se crean por primera vez las CAs, estas utilizan claves gestionadas por Google mediante el servicio Cloud KMS. El usuario administrador que gestione el servicio Certificate Authority puede elegir el algoritmo utilizado.

Para una correcta operación del servicio, se deben crear plantillas de certificado y políticas de emisión de certificados.

6.1.2 CLOUD ARMOR

Las políticas de seguridad que gestiona este servicio son las políticas de seguridad con alcance regional [Cloud Armor].

Cuando se configure el recurso objetivo donde se aplicarán las políticas de seguridad regionales, y sus reglas asociadas, será un **servicio Backend de un balanceador de carga**, el cual será también **regional.**

La configuración de las políticas de seguridad y reglas WAF preconfiguradas de Cloud Armor se realiza conforme a la documentación oficial. Respecto a las reglas WAF, la configuración evaluada ha contemplado la compatibilidad con **ModSecurity Core Rule Set (CRS) 3.3.**

6.1.3 CLOUD LOGGING

Los buckets que contienen los logs registrados por el servicio de Cloud Logging están cifrados por defecto con criptografía simétrica. Para que esta protección se realice haciendo uso de **claves gestionadas por el cliente (CMEKs)**, es preciso habilitarlas para la organización [Cloud Logging].

Los buckets de log pueden configurarse con un tiempo personalizado de retención para la auditoría almacenada. Por defecto, si no se configura, son 30 días de retención.

Cloud Logging permite crear receptores de logs en el proyecto de la organización en Google Cloud Platform. De entre las posibilidades, la evaluación contempló enviar la auditoría a buckets de Cloud Storage.

Se debe configurar la localización por defecto del almacenamiento de los logs.

6.1.4 GOOGLE KMS WITH EKM SOLUTION

La conexión entre este servicio y el partner EKM se puede realizar mediante dos vías: mediante conexión por Internet o mediante una VPC. La primera opción, **vía Internet**, es la configuración evaluada [EKM].

Para poder operar con el servicio, es preciso crear keyrings y sus claves.

6.1.5 IDENTITY AND ACCESS MANAGEMENT (IAM)

Es preciso crear los activos del servicio de IAM necesarios para ejercer su funcionalidad de seguridad. Estos se refieren a las cuentas de servicio y sus pares de claves RSA público/privadas [IAM].

La **clave privada que se genere para cada cuenta de servicio debe ser protegida de forma segura** por el usuario administrador y que no sea accesible en texto claro por ningún usuario fuera de los autorizados a gestionar el servicio de IAM.

El servicio permite federar las identidades para los usuarios (Workforce Identity federation) o para las cargas de trabajo (Workload Identity federation). Para ambas federaciones, la configuración evaluada contempla el soporte con los protocolos OIDC o SAML 2.0.

El acceso que permite el servicio de IAM se realiza de forma condicional, basado en el tiempo o basado en el recurso accedido. La evaluación contempla **Google Cloud Platform Storage como recurso** donde se aplicarán las políticas y condiciones establecidas por IAM.

Para la configuración evaluada, las cuentas principales que se utilizarán para asignar permisos y probar las funcionalidades de seguridad de este servicio son las **cuentas de servicio de Google**.

6.1.6 CLOUD ASSET INVENTORY

Cloud Asset Inventory utiliza el servicio de IAM para el control de acceso. **Cada método de API de Cloud Asset Inventory requiere que el llamador tenga los** permisos necesarios [Asset Inventory].

Este servicio permite exportar los metadatos de los activos del entorno de Google Cloud Platform. Se ofrecen varios destinos de exportación, como son BigQuery o Cloud Storage, pero la evaluación contempló los buckets de este último como destino de envío de metadatos.

Para recibir notificaciones en tiempo real sobre los cambios en los recursos y las políticas, es preciso crear un feed y suscribirse a él. Cuando se crea el feed, se pueden supervisar los cambios en los tipos de recursos admitidos.

6.1.7 KEY MANAGEMENT SERVICE

Google recomienda limitar el conjunto de permisos de acuerdo con el principio de mínimos privilegios. En la configuración evaluada, se tuvo en cuenta un único rol que administraba las funcionalidades de seguridad, denominado cloudkms.admin [KMS].

El **llavero de claves** o *keyring* es el recurso principal gestionado por Cloud KMS para gestionar las claves y sus versiones asociadas, las cuales pueden tener diversos estados. La documentación oficial explica cómo crearlos, cómo crear una llave simétrica y cómo realizar la importación de claves, mediante envoltura de claves, en caso de haberlas generado de forma externa.

El uso de CMEK de Cloud KMS otorga a los usuarios autorizados del servicio la propiedad y el control de las claves que protegen sus datos en reposo en Google Cloud Platform.

De forma predeterminada, las versiones de claves en Cloud KMS pasan 30 días en el estado programado para su destrucción (**DESTROY_SCHEDULED**) antes de que se destruyan. A veces, el estado programado para destrucción se denomina *estado borrado de forma no definitiva*. La duración durante la cual las versiones de claves permanecen en este estado se puede configurar.

Cloud KMS permite también realizar la verificación de firmas MAC.

Dependiendo del uso que se le vaya a dar a una clave gestionada por Cloud KMS, este servicio define propósitos de clave, donde cada algoritmo permite llevar a cabo una operación criptográfica distinta.

6.1.8 GOOGLE SENSITIVE DATA PROTECTION

El recurso donde las políticas de protección de datos y demás funcionalidades de seguridad que ofrece el servicio SDP fueron evaluadas sobre buckets de Cloud Storage [SDP]. Otras posibilidades, no contempladas durante la evaluación, pueden ser datos de *Datastore* o una tabla de *BigQuery*.

La documentación oficial de Google ofrece información sobre los tipos de archivos y modos de análisis admitidos.

Sensitive Data Protection puede detectar y clasificar datos sensibles almacenados en una ubicación. Para ello, genera acciones después de que una operación se complete con éxito. Este servicio ofrece múltiples acciones, donde las evaluadas son las siguientes:

- Guardar los resultados del trabajo de protección de datos sensibles en una tabla de BigQuery.
- Publicar una notificación que contenga el nombre del trabajo de Protección de datos sensibles como un atributo en un canal de Pub/Sub.
- Publicar un resumen de los resultados del trabajo en Security Command Center.

- Anonimizar/Ofuscar los resultados de los datos inspeccionados y escribir el contenido desidentificado en un archivo nuevo.
- Enviar un correo electrónico cuando se complete la tarea a los propietarios (*owners*) del proyecto.

Cuando Sensitive Data Protection realiza un análisis de inspección para identificar datos sensibles, cada análisis se ejecuta como un *trabajo*. SDP crea y ejecuta un recurso de trabajo cada vez que se indica que inspeccione un repositorio de Google Cloud Platform, incluidos los buckets de Cloud Storage. Cuando un nuevo trabajo de inspección se crea, es necesario especificar las acciones que llevará a cabo cuando se complete dicho trabajo.

Existen tres opciones para las claves criptográficas que pueden utilizarse con los métodos de desanonimización criptográfica en la protección de datos sensibles. La configuración evaluada contempló el uso de **HMAC-SHA-256** para **hashing criptográfico**.

6.1.9 CHROME ENTERPRISE PREMIUM

Se debe tener en cuenta que el servicio se activa en la consola de Google Cloud Platform. Para ello, crear en la consola un proyecto debajo de la organización. En el proyecto creado, se habilitará la suscripción a **Chrome Enterprise Premium** siguiendo estos pasos:

- La suscripción se activa en la **Admin Console** > "*Billing*" > "*Subscriptions*" > "*Add or upgrade a subscription*". Se selecciona la sección "*Devices & Browser*" y se hace clic en "*GET STARTED*". Después de ello, completar el resto de los pasos para activar correctamente la suscripción.

La primera configuración que se debe realizar para este servicio es accediendo a las guías de configuración que contiene la consola de Administración ("*Admin Console*" > "*Chrome browser*" > "*Setup guide*" > "*Chrome browser*").

A continuación, se listan algunas consideraciones de configuración que permite al servicio Chrome Enterprise Premium operar de igual forma que la configuración evaluada:

- Permitir los **informes de navegador**, como pueden ser eventos de reutilización de contraseñas, descargas de malware, instalación de extensiones, entre otros. Para ello, en la consola de Administración, buscar "*Browser reporting*" > "*Event reporting*" y hacer clic para configurar los siguientes campos:
  - Seleccionar "*Enable event reporting*".
  - En el campo "*Additional Settings window*", seleccionar "*Default event types*" > "*All types*" y "*Optional event types*" y hacer clic en el cuadro "*Login*".
- Garantizar el **análisis de contenido para subida, bajada o transferencia de ficheros** a través de conectores de Chrome Enterprise. Para ello, realizar la siguiente configuración:
  - Seleccionar "*Chrome Enterprise Premium*" como API de servicio que Chrome necesitará para este propósito.
  - **Retrasar la subida** hasta que finalice el análisis.
  - Para **revisar si hay datos sensibles y buscar software malicioso**, activar ambos modos.

- Para que el **contenido de ficheros no se mande para análisis**, seleccionar "*Block the upload*" para ficheros protegidos por contraseña con un tamaño superior, según la configuración evaluada, a 50 MB.

- Garantizar el **análisis masivo de contexto del texto** a través de conectores de Chrome Enterprise, realizar la siguiente configuración:
  - Seleccionar "*Chrome Enterprise Premium*" como API de servicio que Chrome necesitará para este propósito.
  - Habilitar el modo de **revisión si no hay ningún dato sensible**.
  - Seleccionar el valor 100, de acuerdo con la configuración evaluada, como el valor **mínimo de número de caracteres**.
- Garantizar la **verificación de URL en tiempo real**, seleccionando "*Chrome Enterprise Premium*" como API de servicio que Chrome necesitará para este propósito

Los niveles de acceso contextuales combinan condiciones y valores que definen el contexto de un usuario o dispositivo. Estos niveles de acceso definen el contexto en el que los usuarios pueden acceder a las aplicaciones.

La evaluación consideró restringir el acceso basado en la política de dispositivo. Esta configuración se puede lograr accediendo en la consola de Administración a "*Security*" > "*Access and data control*" > "*Context-Aware Access*".

- Activar la opción "***TURN ON***" para activar el acceso por nivel.
- Crear un nivel de acceso basado en las condiciones definidas que contengan atributos. La configuración evaluada contempló configurar este nivel de acceso de acuerdo con "**Basic mode**".
- Asignar un nivel de acceso a las aplicaciones. Para la configuración evaluada, **Google Drive** es la aplicación considerada para este fin.

Para poder **detectar la exfiltración de datos** con Chrome, se requiere utilizar reglas que prevenga la fuga de información sensible. Esta configuración se encuentra en "*Security*" > "*Access and data control*" > "*Data protection*". La configuración evaluada contempla el uso de la regla "***Blocking file downloads from drive.google.com***".

Respecto a la auditoría, para proporcionar un método seguro de almacenamiento de logs, el usuario administrador deberá habilitar el uso compartido de datos de eventos de registro con Google Cloud Platform. Para ello, vaya a "*Menu*" > "*Account*" > "*Account Settings*" > "*Legal and compliance*" y haga clic en "*Enabled*" en la opción "*Sharing Options*".

Los administradores responsables de la configuración del servicio deberán asegurarse de que los recursos protegidos por **Chrome Enterprise Premium** sólo sean accesibles desde navegadores **Chrome** registrados en el propio servicio. Del mismo modo, todas las reglas y políticas deberán crearse y aplicarse **previamente** sobre la unidad organizativa (OU) correspondiente **antes** de incorporar los usuarios a dicha OU.

6.1.10 GOOGLE CLOUD IDENTITY

El despliegue del servicio Cloud Identity se realiza siguiendo la configuración que indica la documentación oficial [Cloud Identity].

La política de contraseñas debe configurarse para todas las identidades gestionadas por Cloud Identity. Esta política se puede configurar en la consola de administración como sigue:

- "*Menu*" > "*Security*" > "*Authentication*" > "*Password management*" y activar las Casillas "***Enforce strong password***" y "***Enforce strong password at the next login***".
- "*Menu*" > "*Security*" > "*Authentication*" > "*Password management*" y en el campo "*Length*" establecer un mínimo de **longitud de contraseña de 15 caracteres** para los usuarios.

Para cada nuevo usuario creado, el administrador de Cloud Identity debe **establecer manualmente una contraseña de acceso por primera vez** que cumpla los estándares de seguridad de CCN. Adicionalmente, debe forzar que el usuario cambie su contraseña en el primer login activando la casilla "**Ask the user to change his password when they log in**" antes de crear el usuario.

La **duración de la sesión también debe configurarse para las aplicaciones de Google**. Para ello, acceder al apartado "*Menu*" > "*Security*" > "*Access and data control*" > "*Google Cloud Platform session control*", seleccionar la unidad organizativa y, debajo de "*Reauthentication policy*", seleccionar "*Require reauthentication*" de la lista desplegable. La configuración evaluada contempla este valor establecido a **12 horas.**

Para proporcionar un **método seguro de almacenamiento de auditoría**, el administrador de la consola de administración debe establecer la compartición de eventos con Google Cloud Platform. Esto se puede lograr accediendo a "*Menu*" > "*Account*" > "*Account settings*" > "*Legal and compliance*" y haciendo clic en "*Sharing Options*" > "***Enabled***".

Para proteger frente a ataques de fuerza bruta, el administrador debe **forzar los** dos pasos de verificación **en todos los usuarios**.

El módulo de servicios de la consola de Administración permite al administrador configurar las aplicaciones de Google disponibles para los usuarios finales de la organización. Para la configuración evaluada se contempla activar la opción de "***Drive and Docs***". Para ello, en la consola de Administración, acceder a "*Apps*" > "*Google Workspace*" > "*Drive and Docs*" > "*Configured Organizational Unit*" > "*Service status - ON*".

6.2 AUTENTICACIÓN

Google define la autenticación como el proceso mediante el cual se confirma tu identidad mediante el uso de algún tipo de credencial. La autenticación consiste en demostrar que un usuario es quien dice ser.

Google proporciona muchas APIs y servicios, que requieren autenticación para acceder. Google también proporciona una serie de servicios que alojan aplicaciones escritas por nuestros clientes. Estas aplicaciones también deben determinar la identidad de sus usuarios.

Los servicios de Google Cloud Platform usan el servicio Identity & Access Management (IAM) para la autenticación. IAM ofrece control detallado, por principal y por recurso. En el proceso de autenticación sobre los servicios de Google Cloud Platform, por lo general, se usa un permiso que incluye todos los servicios de Google Cloud Platform.

Google ofrece una guía para elegir el método de autenticación que mejor se corresponda a cada caso de uso de sus servicios de Google Cloud Platform [Autenticación].

Las API de Google implementan y extienden el framework de OAuth 2.0. Los permisos de OAuth 2.0 pueden proporcionar una segunda capa de protección, que es útil si tu código se ejecuta en un entorno en el que la seguridad del token es crucial. En esta situación, puedes usar permisos más detallados para reducir el riesgo en caso de que exista un token vulnerado. Puedes encontrar la lista de permisos que acepta un método de API en sus páginas de referencia de la API en la documentación del producto.

Además de autenticar usuarios, es posible que debas permitir que otros servicios interactúen con tu API. Si bien las aplicaciones cliente pueden proporcionar a los usuarios un mensaje de acceso web a fin de que envíen sus credenciales, necesitas otro enfoque para una comunicación segura entre los servicios.

Cloud Identity permite administrar las identidades que usan los empleados de una organización para acceder a los servicios de Google Cloud Platform, proporcionando autenticación.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

Los servicios de seguridad de Google incluidos en este Procedimiento de Empleo Seguro (PES) se administran de forma remota a través de la **consola de Google Cloud Platform** o la **consola de Administración**, dependiendo del servicio. Al tratarse de soluciones basadas en la nube, no existe un acceso local tradicional a nivel de hardware o software instalado en la infraestructura del cliente.

La administración remota de estos servicios debe realizarse utilizando conexiones seguras, asegurando que el acceso se proteja mediante:

- **Autenticación multifactor (MFA)** para usuarios administradores [MFA].
- **Protocolos seguros como HTTPS y TLS 1.2 o superior.**
- **Control de accesos basado en roles (RBAC) mediante IAM**, garantizando que cada usuario tenga únicamente los permisos necesarios.

Además, algunos servicios pueden permitir administración mediante **APIs REST** o herramientas de línea de comandos como **gcloud CLI**, para automatizar configuraciones y facilitar la integración con otros sistemas de seguridad.

Se recomienda evitar el acceso a los recursos de Google Cloud Platform negando las solicitudes realizadas con la seguridad de la capa de transporte TLS inferior a v1.2. Para ello, es necesario seguir las consideraciones de restricción de versiones TLS [Configuración TLS].

Es obligatorio que las **configuraciones criptográficas** declaradas para los servicios que aplique deben cumplir con las especificaciones de la guía **[CCN-STIC-807]**.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

La gestión de administradores en estos servicios se realiza a través de Identity & Access Management (IAM) y, en algunos casos, mediante Cloud Identity en la consola de Administración, permitiendo definir roles específicos para cada usuario o grupo dentro de la organización.

Para garantizar una administración segura, se deben considerar las siguientes prácticas:

a) La información sobre los roles de administración que proporciona Cloud Identity puede verse en la documentación oficial [ROLES].

b) La descripción de los roles y permisos que gestiona Identity & Access Management (IAM) puede encontrarse en la documentación oficial [PERMISOS].

c) La configuración de la **política de contraseñas y sesiones** vienen definidas en las consideraciones definidas en la sección 6.1.10 GOOGLE CLOUD IDENTITY.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Los servicios incluidos en este Procedimiento de Empleo Seguro (PES) son soluciones gestionadas en la infraestructura cloud de Google y no requieren configuración de interfaces, puertos o servicios por parte del usuario final.

Al tratarse de servicios cloud administrados directamente por Google, la gestión de la conectividad y los protocolos de comunicación se realiza de manera centralizada, sin que el usuario deba intervenir en la configuración de puertos o servicios específicos.

6.5 GESTIÓN DE CERTIFICADOS

En la infraestructura de Google, se utiliza la Seguridad de transporte de la capa de la aplicación (ALTS) en la capa de la aplicación (7) para la autenticación, integridad y encriptación de las llamadas RPC de Google desde el frontend de Google (GFE) a un servicio y entre servicios.

ALTS utiliza cuentas de servicio para la autenticación con cada servicio que se ejecuta en la infraestructura de Google funcionando como una identidad de servicio con credenciales criptográficas asociadas.

Para más información, consultar la documentación oficial [ALTS].

En términos de servicio evaluado, la sección 6.1.1 CERTIFICATE AUTHORITY SERVICE incluye las **consideraciones necesarias para la gestión de certificados y autoridades de certificación** que proporciona Certificate Authority Service.

Aunque la gestión de certificados es realizada por Google, el cliente es responsable de **utilizar un navegador compatible con certificados ECDSA-256**. Para garantizar una conexión segura, el cliente debe asegurarse de que el navegador utilizado para acceder a los servicios de Google Cloud Platform sea compatible con este tipo de certificados.

6.6 SERVIDORES DE AUTENTICACIÓN

Los servicios incluidos en este Procedimiento de Empleo Seguro (PES) no requieren el uso de servidores de autenticación externos para su funcionamiento.

La gestión de identidades y accesos se realiza de manera centralizada a través de los sistemas de autenticación propios de Google, como **Cloud Identity** e **Identity & Access Management (IAM)**, sin necesidad de integración con servidores LDAP, RADIUS, SAML o Kerberos externos.

6.7 SINCRONIZACIÓN

Los servicios incluidos en este **Procedimiento de Empleo Seguro (PES)** son soluciones **SaaS** gestionadas íntegramente por **Google**, por lo que la configuración de la sincronización de tiempo no es posible por parte del usuario final.

Google proporciona su propia infraestructura de sincronización basada en **Network Time Protocol (NTP)** dentro de su entorno operacional, asegurando que todos los procesos internos mantengan una referencia temporal precisa y consistente. Esto garantiza la integridad de los registros de auditoría, la correcta validación de certificados y la sincronización de eventos dentro de los servicios de seguridad.

Dado que la funcionalidad de **NTP** es gestionada de forma centralizada por Google, los usuarios no requieren configurar servidores de tiempo externos ni realizar ajustes adicionales en los servicios cubiertos en este PES.

6.8 ACTUALIZACIONES

Los servicios incluidos en este Procedimiento de Empleo Seguro (PES) son soluciones SaaS, por lo que su mantenimiento, disponibilidad y actualización son gestionados directamente por **Google**. Esto significa que el usuario final no tiene control sobre la aplicación de actualizaciones, ya que es el propio fabricante quien se encarga de corregir vulnerabilidades, mejorar el rendimiento y garantizar la seguridad de los servicios.

Dado que todas las actualizaciones de los servicios SaaS son gestionadas por **Google**, el usuario final no requiere realizar acciones adicionales para mantener actualizado dichos servicios. Sin embargo, se recomienda revisar periódicamente la configuración de los servicios utilizados para mantener la seguridad y disponibilidad de los servicios cubiertos en este PES.

6.9 AUTO-CHEQUEOS

Los servicios incluidos en este Procedimiento de Empleo Seguro (PES) son soluciones SaaS gestionadas directamente por Google, por lo que las funciones de **auto chequeo** y monitorización del estado de los servicios son responsabilidad exclusiva del fabricante.

Google realiza auto chequeos internos y continuos en su infraestructura para garantizar la disponibilidad, integridad y rendimiento de los servicios. Sin embargo, estas operaciones son completamente transparentes para el usuario final.

Aunque los servicios de Google Cloud Platform no ofrecen auto-chequeos directos al usuario final, **Security Command Center (SCC)** proporciona funcionalidades avanzadas para la identificación y análisis de vulnerabilidades y amenazas en el entorno cloud. SCC cuenta con varios componentes clave:

- **Security Health Analytics**: Identifica vulnerabilidades y desconfiguraciones en el entorno cloud mediante módulos específicos que evalúan el estado de seguridad de los servicios de Google.
- **Web Security Scanner**: Detecta vulnerabilidades de seguridad en aplicaciones web desplegadas en el entorno de GCP.
- **Container Threat Detection**: Evalúa cambios y accesos remotos sobre contenedores de **Google Kubernetes Engine (GKE)**, alertando en caso de actividad maliciosa.
- **Virtual Machine Threat Detection**: Escanea máquinas virtuales a nivel de hipervisor para detectar aplicaciones potencialmente maliciosas o comportamientos sospechosos.

Por lo tanto, aunque los auto-chequeos sobre la infraestructura de Google son gestionados internamente, el uso de **Security Command Center (SCC)** permite a los administradores obtener visibilidad sobre el estado de seguridad de los servicios desplegados en Google Cloud Platform, facilitando la detección y respuesta ante amenazas.

6.10 ALTA DISPONIBILIDAD

Google ha diseñado su infraestructura cloud para garantizar un alto nivel de disponibilidad mediante:

- **Redundancia geográfica**: Los servicios están distribuidos en múltiples centros de datos ubicados en distintas regiones, lo que permite la recuperación automática ante fallos de infraestructura o interrupciones localizadas.
- **Balanceo de carga global**: Google utiliza balanceadores de carga distribuidos globalmente para gestionar el tráfico y asegurar que los servicios permanezcan accesibles incluso en condiciones de alta demanda o fallos parciales.
- **Recuperación ante desastres**: La infraestructura de Google incluye mecanismos de recuperación rápida para minimizar el impacto de fallos críticos en el entorno cloud.
- **Aplicación de parches y actualizaciones sin interrupciones**: Las actualizaciones de seguridad y las mejoras en el servicio se implementan de manera transparente, sin afectar la disponibilidad para los usuarios finales.

La gestión de la disponibilidad es completamente transparente para el usuario final, quien no necesita realizar ninguna configuración o intervención para garantizar el funcionamiento continuo de los servicios cubiertos por este PES.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

Los servicios de Google Cloud Platform escriben registros de auditoría que registran actividades y accesos administrativos dentro de tus recursos de Google Cloud Platform. Los registros de auditoría ayudan a responder "*¿quién hizo qué, dónde y cuándo?*" dentro de tus recursos de Google Cloud Platform con el mismo nivel de transparencia que en los entornos locales. Habilitar registros de auditoría ayuda a las entidades de seguridad, auditoría y cumplimiento a supervisar los datos y sistemas de Google Cloud Platform en busca de posibles vulnerabilidades o el uso inadecuado de datos externos.

Para obtener una lista de los Google Cloud Platform servicios que proporcionan registros de auditoría, consulta Google Cloud Platform servicios con registros de auditoría [AUDITORÍA GCP]. Con el tiempo, todos los servicios de Google Cloud Platform proporcionarán registros de auditoría.

Para obtener una descripción general de los registros de auditoría de Google Workspace, consulta Registros de auditoría de Google Workspace [AUDITORÍA WORKSPACE].

6.11.2 ALMACENAMIENTO LOCAL

Los servicios incluidos en este **Procedimiento de Empleo Seguro (PES)** son soluciones **SaaS (Software as a Service),** por lo que **no existe almacenamiento local** de registros o datos en los dispositivos o infraestructura del usuario final.

Toda la información generada por los servicios es almacenada y gestionada directamente en la infraestructura cloud de **Google**, eliminando la necesidad de almacenamiento local o intervención por parte del usuario para la retención o gestión de datos.

6.11.3 ALMACENAMIENTO REMOTO

El almacenamiento de registros y datos generados por los servicios cubiertos en este Procedimiento de Empleo Seguro (PES) se realiza de manera centralizada en la infraestructura cloud de Google, utilizando mecanismos de transmisión y almacenamiento seguros para garantizar la confidencialidad e integridad de la información:

- **Transmisión segura**: Los datos se transmiten mediante protocolos seguros como **TLS 1.2 o superior**. Para las comunicaciones internas entre servicios dentro de la infraestructura de **Google Cloud Platform**, se emplea el protocolo propietario **ALTS (Application Layer Transport Security)**, que proporciona cifrado de extremo a extremo y autenticación mutua entre los servicios.
- **Retención de registros**: Los registros son almacenados conforme a las políticas de retención definidas por Google, permitiendo su disponibilidad para auditorías y análisis forenses.
- **Acceso restringido**: El acceso a los registros almacenados remotamente está controlado mediante **Identity & Access Management (IAM)**, asegurando que solo los administradores y usuarios autorizados puedan consultar o modificar los registros.
- **Integración con servicios de análisis**: Los registros almacenados pueden ser procesados y analizados mediante servicios como **Cloud Logging** y **Security Command Center**, facilitando la detección de amenazas y la respuesta ante incidentes.

La gestión del almacenamiento remoto es responsabilidad de Google, por lo que el usuario final no requiere realizar configuraciones adicionales para garantizar la seguridad y disponibilidad de los datos.

6.12 BACKUP

Los servicios incluidos en este **Procedimiento de Empleo Seguro (PES)** son soluciones **SaaS (Software as a Service)** gestionadas directamente por **Google**, por lo que la realización de copias de seguridad de la infraestructura y los datos almacenados en los servicios es responsabilidad exclusiva de **Google**.

Google aplica mecanismos de respaldo automáticos para garantizar la disponibilidad y protección de los datos almacenados en su infraestructura cloud. Sin embargo, estos procesos son gestionados internamente por Google, sin intervención directa del usuario final.

Aunque las copias de seguridad de los servicios son gestionadas por Google, el usuario final puede:

- **Exportar configuraciones y registros** mediante la consola de administración, las APIs oficiales o las herramientas proporcionadas por Google, pudiendo obtener la información en formatos soportados por el servicio (por ejemplo, CSV o JSON) para mantener una copia bajo su control.
- **Proteger las copias exportadas**: La seguridad y protección de estos archivos exportados es responsabilidad del usuario, quien debe aplicar controles adecuados de acceso, almacenamiento y cifrado para garantizar la confidencialidad e integridad de los datos.

El usuario final debe evaluar los requisitos específicos de su organización y establecer las políticas de seguridad adecuadas para las copias de datos exportadas desde los servicios de **Google Cloud Platform.**

7 REFERENCIAS

Resumen Servicios	https://cloud.google.com
CPSTIC	https://cpstic.ccn.cni.es
GCP Console	https://console.cloud.google.com
Admin Console	https://admin.google.com
Google Workspace	https://workspace.google.com
Cuotas	https://cloud.google.com/pricing/list
Configuración TLS	https://docs.cloud.google.com/docs/security/compliance/restrict-tls-versions#restrict
Cifrado	https://docs.cloud.google.com/docs/security/encryption/default-encryption
APIs	https://docs.cloud.google.com/endpoints/docs/openapi/enable-api
Logs	https://docs.cloud.google.com/logging/docs/audit/configure-data-access
Certificate Authority	https://docs.cloud.google.com/certificate-authority-service/docs/ca-service-overview
Cloud Armor	https://docs.cloud.google.com/armor/docs/cloud-armor-overview
Cloud Logging	https://docs.cloud.google.com/logging/docs/overview
EKM	https://docs.cloud.google.com/kms/docs/key-management-service
IAM	https://docs.cloud.google.com/iam/docs/overview
Asset Inventory	https://docs.cloud.google.com/asset-inventory/docs/asset-inventory-overview
KMS	https://docs.cloud.google.com/kms/docs/key-management-service
SDP	https://docs.cloud.google.com/sensitive-data-protection/docs/sensitive-data-protection-overview
Cloud Identity	https://docs.cloud.google.com/identity/docs/how-to/set-up-cloud-identity-admin
Autenticación	https://docs.cloud.google.com/docs/authentication#auth-decision-tree
CCN-STIC-807	https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html
Permisos	https://docs.cloud.google.com/iam/docs/roles-overview
Roles	https://docs.cloud.google.com/identity/docs/how-to/create-cloud-identity-user-accounts
ALTS	https://docs.cloud.google.com/docs/security/encryption-in-transit?hl=es-419#service_integrity_encryption
Auditoría GCP	https://docs.cloud.google.com/logging/docs/audit/services

Auditoría Workspace	https://docs.cloud.google.com/logging/docs/audit/gsuite-audit-logging
MFA	https://docs.cloud.google.com/docs/authentication/mfa-requirement

8 ABREVIATURAS

ALTS	Application Layer Transport Security
API	Application Programming Interface
CCN	Centro Criptológico Nacional
CEP	Chrome Enterprise Premium
CLI	Command Line Interface
CMEK	Customer-Managed Encryption Keys
CPD	Centro de Proceso de Datos
CPU	Central Processing Unit
CRS	Core Rule Set
CSV	Comma-Separated Values
DLP	Data Loss Prevention
ECDSA	Elliptic Curve Digital Signature Algorithm
EKM	External Key Manager
ENS	Esquema Nacional de Seguridad
GCI	Google Cloud Platform Infrastructure
GCP	Google Cloud Platform
GFE	Google Front End
GKE	Google Kubernetes Engine
GPU	Graphics Processing Unit
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
IAM	Identity and Access Management
JSON	JavaScript Object Notation
KMS	Key Management Service
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MFA	Multi-Factor Authentication
NTP	Network Time Protocol
OIDC	OpenID Connect
PES	Procedimiento de Empleo Seguro
RBAC	Role-Based Access Control
REST	Representational State Transfer
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
SAML	Security Assertion Markup Language
SCC	Security Command Center
SDP	Sensitive Data Protection
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
TIC	Tecnologías de la Información y la Comunicación
TPU	Tensor Processing Unit
URL	Uniform Resource Locator
VPC	Virtual Private Cloud