centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 888

Perfil de Cumplimiento Específico para Google Cloud Servicio de Cloud Corporativo

Mayo 2025

MINISTERIO
DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO 083-25-180-9 (edición en línea)

centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2025.07.29 11:05:19 +02'00'

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

ÍNDICE

1. INTRODUCCIÓN

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.

Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 311/2022, de 3 de mayo, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Las Guías CCN-STIC, del Centro Criptológico Nacional, podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.

Los criterios de aplicación de las medidas de seguridad se definirán en función de la responsabilidad de la organización frente a la del proveedor de servicios en la nube, tal y como se expone en la sección ***1.1. Modelo de responsabilidad compartida*** de este mismo documento.

El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

Las auditorías se realizarán en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en el Anexo I y Anexo III del Real Decreto 311/2022, de 3 de mayo, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de Seguridad de los Sistemas de Información.

A tal fin, tras realizar un análisis de riesgos contemplando las vulnerabilidades y amenazas a las que hace frente el uso de esta tecnología en las entidades del Sector Público, y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando **el siguiente Perfil de Cumplimiento Específico para garantizar la seguridad en los servicios contratados en el Cloud de Google en las modalidades IaaS, PaaS, SaaS y FaaS.**

Es posible obtener información actualizada sobre el cumplimiento del ENS para Google Cloud en el siguiente enlace:

https://cloud.google.com/security/compliance/ens

1.1 MODELO DE RESPONSABILIDAD COMPARTIDA

El modelo de responsabilidad compartida de GCP define las responsabilidades entre Google y sus clientes. En este modelo, Google es responsable de la infraestructura subyacente, mientras

que los clientes son responsables de la seguridad de sus aplicaciones, datos y acceso de usuarios dentro del entorno de la nube dependiendo del modelo de servicio elegido Los modelos de servicio en la nube son operados y controlados según sea la responsabilidad para los modos concretos ya sea IaaS, PaaS, SaaS o FaaS.

Los servicios de IaaS (Infraestructura como Servicio) ofrecen servicios de procesamiento, almacenamiento y redes en un modelo de pago por uso. Dentro de los servicios se incluyen, entre otros, los siguientes: Compute Engine, Cloud Storage y servicios de herramientas de redes, como Cloud VPN, Cloud Load Balancing y Cloud DNS. En IaaS, 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 de las reglas de firewall que ofrece el servicio, mientras que la responsabilidad de Google se enfoca en la infraestructura subyacente y la seguridad física.

El modelo PaaS (Plataforma como Servicio) proporciona el entorno de ejecución en el que se puede desarrollar y ejecutar las aplicaciones, se incluyen los servicios como App Engine, Google Kubernetes Engine (GKE) y BigQuery. En este modelo GCP se responsabiliza más de los controles, compartiendo la responsabilidad con el cliente a nivel de aplicación y administración de IAM, siendo el cliente responsable de la seguridad de los datos y medidas de protección.

En el modelo SaaS (Software como Servicio), se pueden usar cuando la organización no cuenta con la experiencia interna o el requisito empresarial de compilar la aplicación, pero requiere la capacidad de procesar cargas de trabajo, incluyendo aplicaciones como Google Workspace, Chronicle y SaaS de terceros disponibles en Google Cloud Marketplace. GCP es responsable en mayor parte de la seguridad, mientras que el cliente es responsable de los accesos y del almacenamiento de los datos en la aplicación.

FaaS (Función como Servicio) proporciona la plataforma para que los desarrolladores puedan ejecutarun código pequeño de un solo propósito que se ejecutan en respuesta a eventos particulares llamados funciones. La responsabilidad compartida es similar a la de SaaS como Cloud Functions.

El cliente, como responsable, debe ser el experto en conocer los requisitos normativos y de seguridad de la la protección de los datos y recursos confidenciales como de los servicios que implementará en base al cumplimiento de las reglamentaciones vigentes, los estándares de seguridad, los planes de administración de riesgos y los requisitos de seguridad.

Las responsabilidades se definen según el tipo de carga de trabajo que se debe ejecutar y los servicios de la nube que se necesitan como de la protección y seguridad de los propios activos de la nube. Esta diferenciación de responsabilidades en la que el cliente o Google son responsables son llamados con los siguientes términos, seguridad “de” la nube y seguridad “en” la nube.

En general el término **“seguridad en la nube”** es utilizado para referirse a los principios y prácticas generales que se aplican a la seguridad de cualquier entorno o servicio de la nube, como la gestión de identidades, accesos, protección de datos, seguridad de la red de GCP.

Por otro lado, el término **“seguridad de la nube”** se utiliza para referirse a la implementación específica de la seguridad que ofrece GCP en la que es responsable de la infraestructura subyacente, conformada por hardware, software, redes y acceso a las instalaciones.

Por ejemplo, GCE es un producto de infraestructura como servicio (IaaS) que permite crear y ejecutar máquinas virtuales en la infraestructura de Google, que ofrece el escalamiento, el rendimiento y el valor que permite iniciar con facilidad clusters de procesamiento grandes en la infraestructura de Google. Los sistemas y servicios instalados en dichas máquinas virtuales, las comunicaciones y permisos entre ellas, así como la protección de datos contenidos y seguridad en dichas comunicaciones, no son gestionados por Google sino por el cliente.

Al ser el cliente el responsable de los servicios, por ejemplo, en la implementación de una máquina virtual con GCE, es el encargado de la configuración y gestión del sistema operativo instalado, así como la protección del software, ejecución de las actualizaciones y parches publicados por cada proveedor del sistema operativo. También es responsable de la seguridad de la información a través de la configuración de las reglas de firewall y del diseño de la arquitectura de la red a través de las VPC.

Como parte de la protección del acceso a los datos, el cliente es responsable de definir las configuraciones de identidad a través de GCP IAM, permitiendo administrar el acceso a la cuenta y recursos de la nube, proporcionando una visión centralizada.

Fig. 1 – Representación del modelo de responsabilidad compartida en Google

Como se muestra en la figura, Google siempre es responsable de la infraestructura y la red subyacente, y el cliente siempre es responsable de los datos y políticas de acceso.

Varias industrias tienen estándares regulatorios que definen controles de seguridad que se deben implementar, por lo que es necesario comprender la responsabilidad de los controles de seguridad disponibles, como en el caso de esta guía, seguir los lineamientos y regulaciones determinadas por el Esquema Nacional de Seguridad.

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.

Google ha desarrollado un destino compartido para abordar los desafíos que quedan fuera del modelo de responsabilidad compartida, considerando la relación entre GCP y el cliente como una asociación contínua para mejorar la seguridad. Este consiste en asumir la responsabilidad de que GCP sea más seguro incluyendo el uso de una zona de destino segura, clara y transparente sobre los controles de seguridad. Este incluye la cuantificación del riesgo con el seguro cibernético mediante el programa de protección contra riesgos, para evolucionar desde el marco estándar de responsabilidad compartida hasta un modelo que ayude a proteger la organización y generar confianza en GCP.

Dentro de los recursos se incluyen los siguientes:

- **Bases de seguridad,** para analizar las principales inquietudes de seguridad y las principales recomendaciones.
- **Planos seguros (blueprints),** que permiten implementar y **mantener** soluciones seguras, las que tienen recomendaciones de seguridad de GCP habilitadas de forma predeterminada.
- **Prácticas recomendadas,** dadas por el marco de arquitectura que abordan las recomendaciones de seguridad principales para incorporar en los diseños, y permite conectarse con expertos.
- **Guías de navegación de la zona destino,** que guían a través de **decisiones** principales para crear una base segura en las cargas de trabajo como la integración de identidades, seguridad y administración de claves y la estructura de red.

Para conocer más detalles sobre las responsabilidades compartidas y destino compartido en Google Cloud, se puede seguir el siguiente enlace:

https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

Este perfil de cumplimiento podrá ser de aplicación en todas aquellas entidades cuyo sistema de información, tras un correcto proceso de categorización, obtenga unas necesidades de seguridad de nivel ALTO o inferior, y los servicios de los que se componga dicho sistema de información se correspondan únicamente con los ofrecidos por la solución Cloud de Google, en su modalidad de despliegue como nube pública y ofreciendo servicios de software como servicio, plataforma como servicio e infraestructura como servicio, según corresponda en cada servicio contratado.

De acuerdo con lo establecido en la Guía de seguridad de las TIC CCN-STIC-823 Utilización de servicios en la Nube, se definen las nubes con modelos de despliegue públicos como aquellas cuya infraestructura es ofrecida al público general o a un gran grupo de industria, y dicha

infraestructura es controlada por un proveedor de servicios en la nube.

Para la aplicación de este Perfil de Cumplimiento Específico, la solución Cloud de Google ofrece servicios en cualquiera de las categorías cuyos sistemas son poseedores de la certificación ENS en categoría ALTA.

3. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad es el conjunto de medidas que son de aplicación para el cumplimiento del ENS. El conjunto de medidas dependerá de los niveles asociados a las dimensiones de seguridad.

Se ha determinado que, para los servicios contratados en el Cloud de Google, las medidas que son de aplicación o no y, en caso de aplicar, la exigencia en nivel de madurez de la medida es el siguiente (el "*" indica que la medida en cuestión requiere de unos criterios específicos de aplicación, que se detallan en el apartado "4. CRITERIOS DE APLICACIÓN DE MEDIDAS"):

Medidas de Seguridad		Categoría o dimensiones	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 +R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3

Medidas de Seguridad		Categoría o dimensiones	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	**Medidas de protección**				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				

Medidas de Seguridad		Categoría o dimensiones	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1 + R2
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica

Medidas de Seguridad		Categoría o dimensiones	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

3.1 MEDIDAS DE APLICACIÓN

El conjunto completo de medidas puede encontrarse en este enlace: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

De las 73 medidas de seguridad definidas en el Anexo II del RD 311/2022, se aplican un total de **27 medidas**. Son las siguientes:

Marco Organizativo (0)

Marco Operacional (15):

[op.acc]	**Control de Acceso**
[op.acc.1]	Identificación
[op.acc.2]	Requisitos de acceso
[op.acc.3]	Segregación de funciones y tareas
[op.acc.4]	Proceso de gestión de derechos de acceso
[op.acc.6]	Mecanismo de autenticación (usuarios de la organización)
[op.exp]	**Explotación**
[op.exp.1]	Inventario de activos
[op.exp.4]	Mantenimiento y actualizaciones de seguridad
[op.exp.6]	Protección frente a código dañino
[op.exp.7]	Gestión de incidentes
[op.exp.8]	Registro de la actividad
[op.exp.10]	Protección de claves criptográficas
[op.ext]	**Recursos externos**
[op.ext.3]	Protección de la cadena de suministro
[op.ext.4]	Interconexión de sistemas
[op.cont]	**Continuidad del servicio**

[op.cont.2]	Plan de continuidad
[op.mon]	**Monitorización del sistema**
[op.mon.1]	Detección de intrusión
[op.mon.3]	Vigilancia

Medidas de Protección (11):

[mp.com]	**Protección de las comunicaciones**
[mp.com.1]	Perímetro seguro
[mp.com.2]	Protección de la confidencialidad
[mp.com.3]	Protección de la integridad y de la autenticidad
[mp.com.4]	Separación de flujos de información en la red
[mp.si]	**Protección de los soportes de información**
[mp.si.2]	Criptografía
[mp.info]	**Protección de la información**
[mp.info.3]	Firma electrónica
[mp.info.5]	Limpieza de documentos
[mp.info.6]	Copias de seguridad
[mp.s]	**Protección de los servicios**
[mp.s.1]	Protección del correo electrónico
[mp.s.2]	Protección de servicios y aplicaciones web
[mp.s.4]	Protección frente a denegación de servicio

4. CRITERIOS DE APLICACIÓN DE MEDIDAS

4.1 [OP.ACC] Control de acceso

El conjunto de medidas “op.acc Control de Acceso” serán de aplicación con las siguientes particularidades:

- La entidad u organización que hace uso de los servicios de la plataforma Google Cloud, deberá cumplir con las exigencias indicadas en el Esquema Nacional de seguridad para la autenticación.

- La configuración de la autenticación y los servicios relacionados se encuentran descritas en la Guía de configuración segura de GCP.

- Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por GCP no puedan ser aplicados, como en el caso de los equipos de administración del sistema, serán de aplicación estas medidas en la categoría y nivel ALTO.

- La medida de seguridad del ENS Mecanismo de autenticación (usuarios externos) [op.acc.5] referente al acceso de usuarios que no son usuarios de la organización (en particular, los ciudadanos administrados) no es de aplicación en el ámbito de GCP, dado que no es previsible que usuarios ajenos a la organización accedan a GCP (sin perjuicio de los accesos que puedan realizar a las aplicaciones o sistemas soportados por la infraestructura de GCP, en cuyo ámbito sí que serán de aplicación las exigencias de la citada medida de seguridad [op.acc.5]).

4.2 [OP.EXP] Explotación

Serán de aplicación [OP.EXP.2] Configuración de Seguridad y [OP.EXP.3] Gestión de la configuración de seguridad, estas medidas de categoría y nivel ALTO , con las siguientes particularidades:

- La configuración de seguridad que se aplique a los servicios proporcionados por GCP será la reflejada en las Guías de configuración segura de GCP y sus servicios relacionados, referenciadas en la sección 5. Configuración de Seguridad de este documento.

- La retirada de las cuentas y contraseñas estándar antes de la entrada en operación de los equipos [op.exp.2.1], la configuración atendiendo a las reglas de mínima funcionalidad [op.exp.2.2] y seguridad por defecto [op.exp.2.3] y la gestión de las máquinas virtuales de un modo seguro [op.exp.2.4] deberá implementarse en el diseño de las aplicaciones y en el nivel de software soportado por los servicios de GCP teniendo en cuenta, en su caso, las diferentes guías CCN-STIC sobre la configuración segura de tecnologías específicas.

- Será de aplicación [OP.EXP.8] Registro de la actividad, únicamente cuando tras la correcta categorización del sistema, se establezca un nivel de seguridad ALTO en la dimensión Trazabilidad, teniendo en cuenta las siguientes particularidades:

- Los mecanismos para el registro de las actividades en el sistema provistos por GCP se ajustan a los requisitos exigibles en el Esquema Nacional de Seguridad siempre y cuando sean configurados a tal efecto por la entidad usuaria del servicio.

- Esta configuración que debe ser aplicada, queda descrita en las Guías de configuración segura de GCP y sus servicios relacionados.

- En aquellos elementos del sistema donde los mecanismos de registro de actividad provistos por GCP no puedan ser aplicados, como en el caso de los equipos de administración del sistema, serán de aplicación estas medidas en la categoría y nivel ALTO.

En el resto de los componentes del sistema deberán tener una configuración de seguridad asociada siguiendo los requisitos exigidos en el Anexo II del ENS.

4.3 [OP.EXT.3] Protección de la cadena de suministro

Será de aplicación la medida de categoría y nivel ALTO, con las siguientes particularidades:

- La entidad usuaria deberá tener en cuenta los servicios prestados por GCP en los análisis de impacto de los incidentes sobre el sistema.

- La entidad usuaria deberá estimar el riesgo de dichos incidentes en función de la criticidad de los servicios de GCP utilizados, de los sistemas desplegados en la nube y del grado de dependencia de este proveedor.

- Será responsabilidad de la entidad prestadora del servicio, ajustarse a los requisitos exigibles en el ENS para la protección de su propia cadena de suministro.

4.4 [OP.EXT.4] Interconexión de sistemas

Será de aplicación la medida de categoría y nivel ALTO siempre y cuando la entidad usuaria del servicio establezca enlaces de información para el intercambio de información y servicios entre sus sistemas locales con los sistemas desplegados en la nube de GCP, entre varios sistemas desplegados en la nube de GCP o entre los sistemas desplegados en la nube de GCP y otros sistemas externos.

En las Guías de configuración segura de GCP se describen las diferentes configuraciones de seguridad para entornos híbridos que aprovechan los servicios de GCP para el correcto cumplimiento de los requisitos exigibles en el ENS.

4.5 [OP.NUB] Servicios en la nube

Será de aplicación la medida de categoría y nivel ALTO. Las diferentes configuraciones de seguridad que deben ser aplicadas en los sistemas que proporcionan servicios en la nube quedarán descritas en las ***Guías de configuración segura de GCP.***

4.6 [OP.CONT] Continuidad del servicio

Serán de aplicación las medidas de categoría y nivel ALTO. En las ***Guías de configuración segura de GCP*** se describen a los diferentes servicios y capacidades disponibles en la plataforma para cumplir con este requerimiento de la mejor manera posible, pero será responsabilidad de la entidad usuaria la correcta implementación de estos servicios en función de las necesidades y casuística de uso de GCP.

Será de aplicación la medida "op.cont.2 Plan de continuidad" únicamente cuando, tras la correcta categorización del sistema, se establezca un nivel de seguridad ALTO en la dimensión Disponibilidad del sistema.

En este caso, la medida será de aplicación con las siguientes particularidades:

- En el ámbito del sistema Cloud, únicamente será de aplicación el control respecto al equipamiento informático alternativo y los medios de comunicación alternativos.
- Se utilizarán los mecanismos de replicación de medios provistos por GCP.
- La correcta configuración de estos mecanismos queda descrita en las Guías de configuración segura de GCP y sus servicios relacionados.
- En el desarrollo de los análisis de impacto, la entidad usuaria deberá tener en cuenta la posible criticidad de los elementos del sistema sostenidos por GCP para la continuidad de sus servicios, así como determinar los requisitos de disponibilidad de sus servicios y los elementos considerados críticos.

4.7 [OP.MON] Monitorización del sistema

Será de aplicación las medidas de categoría y nivel ALTO, con las siguientes particularidades:

- La configuración que debe ser aplicada, en cuanto a la monitorización del sistema, queda descrita en las **Guías de configuración segura de GCP** y sus servicios relacionados.

4.8 [MP.SW.1] Desarrollo de aplicaciones

Esta medida no será de aplicación siempre y cuando se prohíban expresamente en la normativa del sistema las tareas de desarrollo en el sistema que soporta la plataforma Cloud y así lo considere el Responsable de Seguridad.

En caso contrario, se aplicará esta medida con los requisitos y nivel de seguridad indicados atendiendo al principio del mínimo privilegio.

4.9 [MP.SW.2] Aceptación y puesta en servicio

Será de aplicación la medida de categoría MEDIA, con las siguientes particularidades:

- Será responsabilidad de la entidad usuaria la correcta configuración de seguridad de los requisitos base de la medida de seguridad, relacionados con el correcto funcionamiento de una aplicación previa entrada a producción.

4.10 [MP.INFO] Protección de la información

Será aplicable esta medida únicamente cuando tras la correcta categorización del sistema, se establezca un nivel de seguridad ALTO en la dimensión de Confidencialidad, teniendo en cuenta las siguientes particularidades:

- Esta medida será aplicable en todos aquellos documentos que formen parte del sistema de gestión de la seguridad de la información relacionados con la plataforma (procedimientos, políticas, etc.) y en los relativos al funcionamiento y normas de uso de los servicios Cloud, que se pongan a disposición de los usuarios.

- No será exigible la aplicación de esta medida en los documentos compartidos por los usuarios haciendo uso de los servicios Cloud.

- GCP dispone de varios servicios para la protección de la información y de los datos en las bases de datos, con los que aplicar medidas de protección de acceso a datos confidenciales, y serán descritas en las ***Guías de configuración segura para GCP***.

La medida [MP.INFO.3] Firma electrónica no será de aplicación siempre y cuando no se contemple el uso de la firma electrónica para funcionalidades relacionadas con el uso y/o administración, configuración o mantenimiento de la plataforma, y así sea considerado por el Responsable de Seguridad.

La medida [MP.INFO.5] Limpieza de documentos, se aplicará en todos aquellos documentos que formen parte del sistema de gestión de la seguridad de la información relacionados con la plataforma (procedimientos, políticas, etc.) y en los relativos al funcionamiento y normas de uso de los servicios Cloud, que se pongan a disposición de los usuarios, y será responsabilidad de la entidad usuaria disponer de los procedimientos a tal efecto.

4.11 [MP.INFO.6] Copias de seguridad

Será aplicable la medida [MP.INFO.6] Copias de seguridad, únicamente cuando tras la correcta categorización del sistema, se establezca un nivel de seguridad ALTO en la dimensión Disponibilidad, teniendo en cuenta las siguientes particularidades:

- Se emplearán los mecanismos para la creación de copias de seguridad proporcionados por GCP. Sin embargo, será responsabilidad de la entidad usuaria del servicio la correcta configuración de estos mecanismos de copias de seguridad.

- La configuración que debe ser aplicada queda descrita en las ***Guías de*** configuración ***segura de GCP*** y sus servicios relacionados.

- En aquellos elementos del sistema donde los mecanismos de copia de seguridad provistos por GCP no puedan ser aplicados, como en el caso de los equipos de administración del sistema, será de aplicación esta medida en la categoría y nivel ALTO.

4.12 [MP.S.1] Protección del correo electrónico

Esta medida no será de aplicación, siempre y cuando no se contemple el uso de las herramientas

de correo electrónico provistas por GCP.

5. CONFIGURACIÓN DE SEGURIDAD

Para dar respuesta a los requisitos establecidos en este Perfil de Cumplimiento Específico usando la tecnología GCP en cualquiera de sus modalidades, se deberá consultar lo establecido en las guías "***CCN-STIC 888A Guía de Configuración Segura para Google Workspace***", "***CCN-STIC 888B Guía de Configuración Segura para GCP***", "***CCN-STIC 888C Guía de Configuración Segura para Contenedores GCP***" y aplicar las configuraciones indicadas en dichos documentos.

Si opta por el uso de otras tecnologías para la aplicación de este Perfil de Cumplimiento Específico para Sistemas Cloud Corporativos, será necesario que la configuración de seguridad haya sido previamente validada por el CCN.

PUBLICACIONES DE DEFENSA

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