centro criptológico nacional

Perfil de Cumplimiento Específico
CCN-STIC 888

Perfil de Cumplimiento Específico para Google Cloud Servicio de Cloud Corporativo

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

CCN 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: 083-21-169-6

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. INTRODUCCIÓN

1. 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.
2. Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 3/2010, de 8 de enero, 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.
3. 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.
4. 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.
5. 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 3/2010, de 8 de enero, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.
6. 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 PaaS, IaaS y SaaS.**

2. TECNOLOGÍAS IMPLICADAS

7. 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, tanto Google Cloud Platform como Google WorkSpace, 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.

8. 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.
9. 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

10. 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.
11. Se ha determinado que, para los servicios contratados en el Cloud de Google, Google Cloud Platform (GCP) y Google WorkSpace (GW), 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:

Dimensiones						
Afectadas	CAT B	CAT M	CAT A			
				org	Aplicación GCP	Aplicación GW
categoría	aplica	=	=	[org.1]	ALTO	ALTO
categoría	aplica	=	=	[org.2]	ALTO	ALTO
categoría	aplica	=	=	[org.3]	ALTO	ALTO
categoría	aplica	=	=	[org.4]	ALTO	ALTO
categoría	aplica	+	++	[op.pl.1]	ALTO	ALTO
categoría	aplica	+	++	[op.pl.2]	ALTO	ALTO
categoría	aplica	=	=	[op.pl.3]	ALTO	ALTO
D	n.a.	aplica	=	[op.pl.4]	ALTO	ALTO
categoría	n.a.	n.a.	aplica	[op.pl.5]	ALTO	ALTO
A T	aplica	=	=	[op.acc.1]	ALTO	ALTO
I C A T	aplica	=	=	[op.acc.2]	ALTO	ALTO
I C A T	n.a.	aplica	=	[op.acc.3]	ALTO	ALTO
I C A T	aplica	=	=	[op.acc.4]	ALTO	ALTO
I C A T	aplica	+	++	[op.acc.5]	ALTO	ALTO
I C A T	aplica	+	++	[op.acc.6]	ALTO	ALTO
I C A T	aplica	+	=	[op.acc.7]	ALTO	ALTO

categoría	aplica	=	=	[op.exp.1]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.2]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.3]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.4]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.5]	ALTO	ALTO
categoría	aplica	=	=	[op.exp.6]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.7]	ALTO	ALTO
T	aplica	+	++	[op.exp.8]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.exp.9]	ALTO	ALTO
T	n.a.	n.a.	aplica	[op.exp.10]	ALTO	ALTO
categoría	aplica	+	=	[op.exp.11]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.ext.1]	ALTO	ALTO
categoría	n.a.	aplica	=	[op.ext.2]	ALTO	ALTO
D	n.a.	n.a.	aplica	[op.ext.9]	ALTO	ALTO
D	n.a.	aplica	=	[op.cont.1]	n/a	n/a
D	n.a.	n.a.	aplica	[op.cont.2]	ALTO	ALTO
D	n.a.	n.a.	aplica	[op.cont.3]	n/a	n/a
categoría	n.a.	aplica	=	[op.mon.1]	ALTO	ALTO
categoría	aplica	+	++	[op.mon.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.if.1]	n/a	n/a
categoría	aplica	=	=	[mp.if.2]	n/a	n/a
categoría	aplica	=	=	[mp.if.3]	n/a	n/a
D	aplica	+	=	[mp.if.4]	n/a	n/a
D	aplica	=	=	[mp.if.5]	n/a	n/a
D	n.a.	aplica	=	[mp.if.6]	n/a	n/a
categoría	aplica	=	=	[mp.if.7]	n/a	n/a
D	n.a.	n.a.	aplica	[mp.if.9]	n/a	n/a
categoría	n.a.	aplica	=	[mp.per.1]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.3]	ALTO	ALTO
categoría	aplica	=	=	[mp.per.4]	ALTO	ALTO
D	n.a.	n.a.	aplica	[mp.per.9]	n/a	n/a
categoría	aplica	+	=	[mp.eq.1]	ALTO	ALTO
A	n.a.	aplica	+	[mp.eq.2]	ALTO	ALTO
categoría	aplica	=	+	[mp.eq.3]	ALTO	ALTO
D	n.a.	aplica	=	[mp.eq.9]	ALTO	ALTO
categoría	aplica	=	+	[mp.com.1]	ALTO	ALTO
C	n.a.	aplica	+	[mp.com.2]	ALTO	ALTO
I A	aplica	+	++	[mp.com.3]	ALTO	ALTO
categoría	n.a.	n.a.	aplica	[mp.com.4]	ALTO	ALTO
D	n.a.	n.a.	aplica	[mp.com.9]	n/a	n/a

C	aplica	=	=	[mp.si.1]	ALTO	ALTO
I C	n.a.	aplica	+	[mp.si.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.si.3]	ALTO	ALTO
categoría	aplica	=	=	[mp.si.4]	ALTO	ALTO
C	aplica	+	=	[mp.si.5]	ALTO	ALTO
categoría	n.a.	aplica	=	[mp.sw.1]	ALTO	ALTO
categoría	aplica	+	++	[mp.sw.2]	ALTO	ALTO
categoría	aplica	=	=	[mp.info.1]	ALTO	ALTO
C	aplica	+	=	[mp.info.2]	ALTO	ALTO
C	n.a.	n.a.	aplica	[mp.info.3]	ALTO	ALTO
I A	aplica	+	++	[mp.info.4]	n/a	n/a
T	n.a.	n.a.	aplica	[mp.info.5]	n/a	n/a
C	aplica	=	=	[mp.info.6]	ALTO	ALTO
D	aplica	=	=	[mp.info.9]	ALTO	ALTO
categoría	aplica	=	=	[mp.s.1]	n/a	ALTO
categoría	aplica	=	+	[mp.s.2]	ALTO	ALTO
D	n.a.	aplica	+	[mp.s.8]	ALTO	ALTO
D	n.a.	n.a.	aplica	[mp.s.9]	n/a	n/a

Detalles del criterio de aplicación de la medida en apartado 4.

3.1. MEDIDAS DE APLICACIÓN GOOGLE CLOUD PLATFORM

12. De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, aplican un total de **60* medidas** para Google Cloud Platform. Son las siguientes:

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (29):

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento / Gestión de capacidades

[op.pl.5] Componentes certificados

[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.5] Mecanismo de autenticación
[op.acc.6] Acceso local (local logon)
[op.acc.7] Acceso remoto (remote login)
[op.exp] Explotación
[op.exp.1] Inventario de activos
[op.exp.2] Configuración de seguridad
[op.exp.3] Gestión de la configuración
[op.exp.4] Mantenimiento
[op.exp.5] Gestión de cambios
[op.exp.6] Protección frente a código dañino
[op.exp.7] Gestión de incidentes
[op.exp.8] Registro de la actividad de los usuarios
[op.exp.9] Registro de la gestión de incidentes
[op.exp.10] Protección de los registros de actividad
[op.exp.11] Protección de claves criptográficas
[op.ext] Servicios externos
[op.ext.1] Contratación y acuerdos de nivel de servicio
[op.ext.2] Gestión diaria
[op.ext.9] Medios alternativos
[op.cont] Continuidad del servicio
[op.cont.2] Plan de continuidad
[op.mon] Monitorización del sistema
[op.mon.1] Detección de intrusión
[op.mon.2] Sistema de métricas

Medidas de Protección (27):

[mp.per] Gestión del personal
[mp.per.1] Caracterización del puesto de trabajo
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación

[mp.eq] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de equipos portátiles
[mp.eq.9] Medios alternativos
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.com.3] Protección de la autenticidad y de la integridad
[mp.com.4] Segregación de redes
[mp.si] Protección de los soportes de información
[mp.si.1] Etiquetado
[mp.si.2] Criptografía
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.sw] Protección de las aplicaciones informáticas
[mp.sw.1] Desarrollo
[mp.sw.2] Aceptación y puesta en servicio
[mp.info] Protección de la información
[mp.info.1] Datos de carácter personal
[mp.info.2] Calificación de la información
[mp.info.3] Cifrado
[mp.info.6] Limpieza de documentos
[mp.info.9] Copias de seguridad (backup)
[mp.s] Protección de los servicios
[mp.s.2] Protección de servicios y aplicaciones web
[mp.s.8] Protección frente a la denegación de servicios

3.2. MEDIDAS DE APLICACIÓN GOOGLE WORKSPACE

13. De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, aplican un total de **61* medidas** para Google Workspace. Son las siguientes:

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (29):

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento / Gestión de capacidades

[op.pl.5] Componentes certificados

[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.5] Mecanismo de autenticación

[op.acc.6] Acceso local (local logon)

[op.acc.7] Acceso remoto (remote login)

[op.exp] Explotación

[op.exp.1] Inventario de activos

[op.exp.2] Configuración de seguridad

[op.exp.3] Gestión de la configuración

[op.exp.4] Mantenimiento

[op.exp.5] Gestión de cambios

[op.exp.6] Protección frente a código dañino

[op.exp.7] Gestión de incidentes

[op.exp.8] Registro de la actividad de los usuarios

[op.exp.9] Registro de la gestión de incidentes

[op.exp.10] Protección de los registros de actividad

[op.exp.11] Protección de claves criptográficas

[op.ext] Servicios externos

[op.ext.1] Contratación y acuerdos de nivel de servicio

[op.ext.2] Gestión diaria

[op.ext.9] Medios alternativos

[op.cont] Continuidad del servicio

[op.cont.2] Plan de continuidad

[op.mon] Monitorización del sistema

[op.mon.1] Detección de intrusión

[op.mon.2] Sistema de métricas

Medidas de Protección (27):

[mp.per] Gestión del personal

[mp.per.1] Caracterización del puesto de trabajo

[mp.per.2] Deberes y obligaciones

[mp.per.3] Concienciación

[mp.per.4] Formación

[mp.eq] Protección de los equipos

[mp.eq.1] Puesto de trabajo despejado

[mp.eq.2] Bloqueo de puesto de trabajo

[mp.eq.3] Protección de equipos portátiles

[mp.eq.9] Medios alternativos

[mp.com] Protección de las comunicaciones

[mp.com.1] Perímetro seguro

[mp.com.2] Protección de la confidencialidad

[mp.com.3] Protección de la autenticidad y de la integridad

[mp.com.4] Segregación de redes

[mp.si] Protección de los soportes de información

[mp.si.1] Etiquetado

[mp.si.2] Criptografía

[mp.si.3] Custodia

[mp.si.4] Transporte

[mp.si.5] Borrado y destrucción

[mp.sw] Protección de las aplicaciones informáticas

[mp.sw.1] Desarrollo

[mp.sw.2] Aceptación y puesta en servicio

[mp.info] Protección de la información

[mp.info.1] Datos de carácter personal

[mp.info.2] Calificación de la información

[mp.info.3] Cifrado

[mp.info.6] Limpieza de documentos

[mp.info.9] Copias de seguridad (backup)

[mp.s] Protección de los servicios

[mp.s.1] Protección del correo electrónico

[mp.s.2] Protección de servicios y aplicaciones web

[mp.s.8] Protección frente a la denegación de servicios

4. CRITERIOS DE APLICACIÓN DE MEDIDAS GOOGLE CLOUD PLATFORM

4.1. [OP.ACC] Mecanismos de Autenticación

3 El conjunto de medidas "[op.acc] Mecanismos de Autenticación" se aplicarán en categoría y nivel ALTO, con las siguientes particularidades:

- Los mecanismos de autenticación provistos por GC 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 ***Guía de configuración segura de GCP*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.
- Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por GC 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.

4.2. [OP.EXP.2] Configuración de Seguridad

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

- La configuración de seguridad que se aplica a los servicios proporcionados por GC será la reflejada en las ***Guía de configuración segura de GCP*** y sus

servicios relacionados, referenciadas en la sección ***6. Configuración de Seguridad*** de este documento.

5 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.EXP.10] Protección de los Registros de Actividad de los Usuarios

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

- Se emplearán los mecanismos para la protección de los registros de actividad proporcionados por GC. Sin embargo, será responsabilidad de la entidad usuaria del servicio la correcta configuración de estos mecanismos de protección de registros de actividad. La configuración que debe ser aplicada queda descrita en las ***Guías de configuración segura de GCP*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.
- En aquellos elementos del sistema donde los mecanismos de protección de registro de actividad provistos por GC 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.

4.4. [OP.CONT] Continuidad del servicio

7 Serán de aplicación las medidas de categoría y nivel ALTO. En las guías de ***CCN-STIC 888B Configuración Segura de GCP*** y ***CCN-STIC 888A Configuración Segura de GW (apartado 2.1.3.1)*** 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 GC.

4.5. [MP.IF] Medidas de protección de instalaciones e infraestructuras

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

- Al encontrarse el sistema físico en las instalaciones del proveedor de servicios en la nube, solo será exigible que la empresa proveedora del servicio disponga de conformidad con el ENS para este servicio Cloud.

4.6. [MP.IF.9] Instalaciones alternativas

9 La aplicación de la medida “mp.if.9 Instalaciones Alternativas”, solo será de aplicación cuando se haya valorado la dimensión de disponibilidad como ALTO, y

siempre tomando en consideración las soluciones de redundancia en las instalaciones que ofrece el proveedor de servicio Cloud.

4.7. [MP.SW.1] Desarrollo de Aplicaciones

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

11 En caso contrario, se aplicará esta medida con los requisitos y nivel de seguridad indicados.

5. CRITERIOS DE APLICACIÓN DE MEDIDAS GOOGLE WORKSPACE

5.1. [OP.ACC] Mecanismos de Autenticación

12 El conjunto de medidas "[op.acc] Mecanismos de Autenticación" se aplicarán en categoría y nivel ALTO, con las siguientes particularidades:

- Los mecanismos de autenticación provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.
- Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por GC 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.

5.2. [OP.EXP.6] Protección frente a código dañino

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

- Los mecanismos para la protección frente a código dañino provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.

5.3. [OP.EXP.7] Gestión de incidentes

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

- Los mecanismos para la gestión de incidentes provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.

5.4. [OP.EXP.8] Registro de Actividad de los Usuarios

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

- Los mecanismos para el registro de actividad de los usuarios provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6 Configuración de seguridad*** de este documento.
- En aquellos elementos del sistema donde los mecanismos de registro de actividad provistos por GC 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.

5.5. [OP.MON.1] Detección de intrusión

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

- Los mecanismos para la gestión de incidentes provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.

5.6. [MP.INFO.2] Calificación de la información

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

- Los mecanismos para la gestión de incidentes provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.

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

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

- Los mecanismos para la gestión de incidentes provistos por GC 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 ***Guía de configuración segura de GW*** y sus servicios relacionados, referenciadas en la sección ***6. Configuración de seguridad*** de este documento.

5.8. [MP.IF] Medidas de protección de instalaciones e infraestructuras

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

- Al encontrarse el sistema físico en las instalaciones del proveedor de servicios en la nube, solo será exigible que la empresa proveedora del servicio disponga de conformidad con el ENS para este servicio Cloud.

5.9. [MP.IF.9] Instalaciones alternativas

20 La aplicación de la medida "mp.if.9 Instalaciones Alternativas", solo será de aplicación cuando se haya valorado la dimensión de disponibilidad como ALTO, y siempre tomando en consideración las soluciones de redundancia en las instalaciones que ofrece el proveedor de servicio Cloud.

5.10. [MP.SW.1] Desarrollo de Aplicaciones

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

22 En caso contrario, se aplicará esta medida con los requisitos y nivel de seguridad indicados.

6. CONFIGURACIÓN DE SEGURIDAD

23 Para dar respuesta a los requisitos establecidos en este Perfil de Cumplimiento Específico usando la tecnología GC en cualquiera de sus modalidades, se deberá consultar lo establecido en la guía ***CCN-STIC 888B Configuración Segura de GCP*** y en la guía ***CCN-STIC 888A Configuración Segura GW***, y aplicar las configuraciones indicadas en dicho documento.

24 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