centro criptológico nacional

Perfil de Cumplimiento Específico
CCN-STIC 887

Perfil de Cumplimiento Especifico para AWS
Servicio de Cloud Corporativo

Septiembre 2023

MINISTERIO DE DEFENSA

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

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN 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
2024.01.09 16:23:56 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023
NIPO: 083-23-278-X

Fecha de Edición: septiembre de 2023

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.

ÍNDICE

1. INTRODUCCIÓN 4
1.1. MODELO DE RESPONSABILIDAD COMPARTIDA 4
2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO 7
3. DECLARACIÓN DE APLICABILIDAD 8
3.1 MEDIDAS DE APLICACIÓN 10
4. CRITERIOS DE APLICACIÓN DE MEDIDAS 13
4.1 [OP.PL.2] Arquitectura de Seguridad 13
4.2 [OP.ACC] Control de acceso 13
4.3 [OP.EXP.2] Configuración de Seguridad y [OP.EXP.3] Gestión de la configuración de seguridad 13
4.4 [OP.EXP.7] Gestión de incidentes 14
4.5 [OP.EXP.9] Registro de la gestión de incidentes 14
4.6 [OP.EXP.8] Registro de la actividad 14
4.7 [OP.EXT.3] Protección de la cadena de suministro 15
4.8 [OP.EXT.4] Interconexión de sistemas 15
4.9 [OP.NUB.1] Protección de los servicios en la nube 15
4.10 [OP.CONT] Continuidad del servicio 15
4.11 [OP.MON] Monitorización del sistema 16
4.12 [MP.IF] Medidas de protección de instalaciones e infraestructuras 16
4.13 [MP.EQ.2] Bloqueo de puesto de trabajo 16
4.14 [MP.SW.1] Desarrollo de aplicaciones 17
4.15 [MP.SW.2] Aceptación y puesta en servicio 17
4.16 [MP.INFO.2] Calificación de la información 17
4.17 [MP.INFO.3] Firma electrónica 17
4.18 [MP.INFO.5] Limpieza de documentos 18
4.19 [MP.INFO.6] Copias de seguridad 18
4.20 [MP.S.1] Protección del correo electrónico 18
5. CONFIGURACIÓN DE SEGURIDAD 18

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. ANEXO I – 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 Especifico para garantizar la seguridad en los servicios contratados en el Cloud de AWS en las modalidades PaaS, IaaS y SaaS.**

1.1. MODELO DE RESPONSABILIDAD COMPARTIDA

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización hasta la seguridad física de las

instalaciones en las que funcionan los servicios. El cliente asume la responsabilidad y la administración del sistema operativo que utiliza cada instancia (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociado y de la configuración del firewall del grupo de seguridad que ofrece AWS.

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

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

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

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

Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como servicios de Infraestructura y, como tal, requiere que el cliente realice todas las tareas de administración y configuración de seguridad necesarias.

EC2 es una solución de virtualización similar a los servicios que ofrecen las herramientas de tipo Hypervisor (al menos en lo que a nivel operacional se refiere) en la que un servidor actúa de huésped alojando máquinas virtuales (en este caso, denominadas instancias) e interconectándolas. Los sistemas y servicios instalados en dichas máquinas virtuales y las comunicaciones y permisos entre ellas, así como la protección de datos contenidos y seguridad en dichas comunicaciones, no son gestionados por AWS sino por el cliente.

Los clientes que implementan una instancia de Amazon EC2, por tanto, son responsables de la administración del sistema operativo que usen en la misma (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el cliente haya instalado en las instancias y de la configuración del firewall provisto por AWS (llamado grupo de seguridad) en cada instancia.

En el caso de los servicios gestionados por AWS, como Amazon S3 (servicios de almacenamiento gestionados) y Amazon DynamoDB (servicios de base de datos gestionados), AWS maneja la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de enlace para recuperar y almacenar los datos. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar las herramientas de Identity and Access Management (IAM) para solicitar los permisos correspondientes.

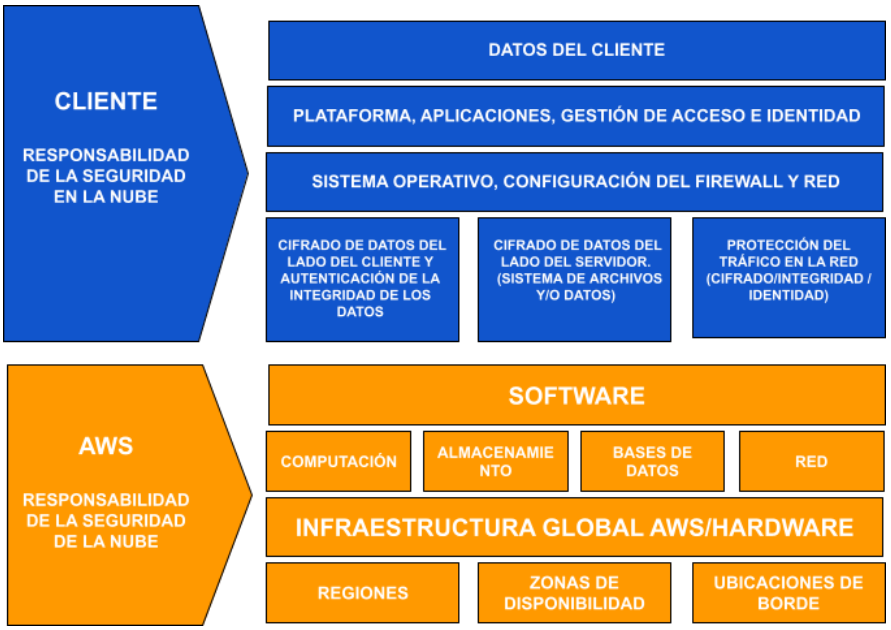

Fig. 1 - Representación del modelo de responsabilidad compartida en AWS

El modelo de responsabilidad compartida entre AWS y sus clientes, abarca también los controles de TI. Del mismo modo que comparten la responsabilidad del entorno, también comparten la administración, el funcionamiento y la verificación de los controles de TI. En este sentido, la presente guía es un recurso para el cliente de AWS referente al ámbito de la responsabilidad del cliente en cuanto a la seguridad de infraestructura y datos según el tipo de servicios utilizados.

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

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

- **Controles heredados:** Los controles heredados son aquellos que un cliente hereda de AWS en su totalidad. Son aquellos controles sobre los que el cliente no tiene ningún tipo de acceso, como los controles físicos y de entorno.

- **Controles compartidos:** Aplican tanto a la capa de infraestructura como a las capas de clientes. En un control compartido, el encargado de suministrar los requisitos para la infraestructura recae en AWS y la responsabilidad de configuración de aplicaciones, bases de datos y sistemas operativos de las instancias (de los huéspedes). Por ejemplo, la administración de parches, la corrección de imperfecciones o la administración de las configuraciones, serían responsabilidad de AWS en lo que se refiere a los elementos internos de la infraestructura (hosts y servicios gestionados). Sin embargo, el cliente será responsable de configurar sus aplicaciones, bases de datos y sistemas operativos huésped.

- **Controles específicos del cliente:** Aquellos elementos que son de absoluta responsabilidad del cliente incluirían la seguridad de zonas, protección de comunicaciones y servicios. El direccionamiento y el aislamiento para la protección de la información deberá ser definido por el cliente.

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 AWS, 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 AWS 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 AWS, 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"):

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación[1]
MARCO ORGANIZATIVO					
Categoría	aplica	aplica	aplica	org.1	N/A
Categoría	aplica	aplica	aplica	org.2	N/A
Categoría	aplica	aplica	aplica	org.3	N/A
Categoría	aplica	aplica	aplica	org.4	N/A
MARCO OPERACIONAL					
Planificación					
Categoría	aplica	+ R1	+ R2	op.pl.1	N/A
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	N/A *
Categoría	aplica	aplica	aplica	op.pl.3	N/A
D	aplica	+ R1	+ R1	op.pl.4	ALTO
Categoría	n.a.	aplica	aplica	op.pl.5	N/A
Control de acceso					
T A	aplica	+ R1	+ R1	op.acc.1	ALTO*
C I T A	aplica	aplica	+ R1	op.acc.2	MEDIO*
C I T A	n.a.	aplica	+ R1	op.acc.3	ALTO*
C I T A	aplica	aplica	aplica	op.acc.4	ALTO*
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.5	N/A*
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.acc.6	ALTO*
Explotación					
Categoría	aplica	aplica	aplica	op.exp.1	ALTA
Categoría	aplica	aplica	aplica	op.exp.2	N/A*
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	N/A*

[1] En la columna "Aplicación", se reflejará la categoría (BÁSICA, MEDIA, ALTA) que corresponda en caso de que en esa medida se vean afectadas las cinco (5) dimensiones de seguridad (Confidencialidad- C, Integridad-I, Autenticidad-A, Trazabilidad-T, Disponibilidad-D). En caso, de que no se vean afectadas las cinco (5) dimensiones, se reflejará el nivel a aplicar (BAJO, MEDIO, ALTO).

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación[1]
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	BÁSICA
Categoría	n.a.	aplica	+ R1	op.exp.5	N/A
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	BÁSICA
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	BÁSICA*
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	MEDIO*
Categoría	aplica	aplica	aplica	op.exp.9	BÁSICA
Categoría	aplica	+ R1	+ R1	op.exp.10	ALTA
Servicios externos					
Categoría	n.a.	aplica	aplica	op.ext.1	ALTA
Categoría	n.a.	aplica	aplica	op.ext.2	ALTA
Categoría	n.a.	n.a.	aplica	op.ext.3	N/A*
Categoría	n.a.	aplica	+ R1	op.ext.4	N/A*
Servicios en la nube					
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	N/A*
Continuidad del servicio					
D	n.a.	aplica	aplica	op.cont.1	N/A*
D	n.a.	n.a.	aplica	op.cont.2	ALTO*
D	n.a.	n.a.	aplica	op.cont.3	N/A*
D	n.a.	n.a.	aplica	op.cont.4	N/A*
Monitorización del sistema					
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	BÁSICA*
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	N/A*
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	ALTA (-R4) *
MEDIDAS DE PROTECCIÓN					
Protección de las instalaciones e infraestructuras					
Categoría	aplica	aplica	aplica	mp.if.1	N/A*
Categoría	aplica	aplica	aplica	mp.if.2	N/A*
Categoría	aplica	aplica	aplica	mp.if.3	N/A*
D	aplica	+ R1	+ R1	mp.if.4	N/A*
D	aplica	aplica	aplica	mp.if.5	N/A*
D	n.a.	aplica	aplica	mp.if.6	N/A*
Categoría	aplica	aplica	aplica	mp.if.7	N/A*
Gestión del personal					
Categoría	n.a.	aplica	aplica	mp.per.1	N/A
Categoría	aplica	+ R1	+ R1	mp.per.2	N/A
Categoría	aplica	aplica	aplica	mp.per.3	N/A
Categoría	aplica	aplica	aplica	mp.per.4	N/A

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación[1]
Protección de los equipos					
Categoría	aplica	+ R1	+ R1	mp.eq.1	N/A
A	n.a.	aplica	+ R1	mp.eq.2	N/A*
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	N/A
C	aplica	+ R1	+ R1	mp.eq.4	N/A
Protección de las comunicaciones					
Categoría	aplica	aplica	aplica	mp.com.1	ALTA
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	ALTO
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	BAJO
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	MEDIA
Protección de los soportes de información					
C	n.a.	aplica	aplica	mp.si.1	N/A
C I	n.a.	aplica	+ R1 + R2	mp.si.2	ALTO
Categoría	aplica	aplica	aplica	mp.si.3	N/A
Categoría	aplica	aplica	aplica	mp.si.4	N/A
C	aplica	+ R1	+ R1	mp.si.5	N/A
Protección de las aplicaciones informáticas					
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	N/A*
Categoría	aplica	+ R1	+ R1	mp.sw.2	MEDIA (-req. base) *
Protección de la información					
Categoría	aplica	aplica	aplica	mp.info.1	N/A
C	n.a.	aplica	aplica	mp.info.2	N/A*
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	N/A*
T	n.a.	n.a.	aplica	mp.info.4	N/A*
C	aplica	aplica	aplica	mp.info.5	N/A*
D	aplica	+ R1	+ R1 + R2	mp.info.6	N/A*
Protección de los servicios					
Categoría	aplica	aplica	aplica	mp.s.1	ALTA*
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	BÁSICA
Categoría	aplica	aplica	+ R1	mp.s.3	N/A
D	n.a.	aplica	+ R1	mp.s.4	ALTO

3.1 MEDIDAS DE APLICACIÓN

De las 73 medidas de seguridad definidas en el Anexo II del RD 311/2022, aplican un total de **25 medidas**. Son las siguientes:

Marco Organizativo (0)

Marco Operacional (17):

[op.pl]	**Planificación**
[op.pl.4]	Dimensionamiento/gestión de la capacidad
[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.1]	Contratación y acuerdos de nivel de servicio
[op.ext.2]	Gestión diaria
[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 (8):

[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.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.PL.2] Arquitectura de Seguridad

La medida de seguridad [op.pl.2] no requiere una configuración específica o la utilización de herramientas concretas en el ámbito de seguridad. No obstante, en el apartado Arquitectura de Seguridad [op.pl.2] de la ***CCN-STIC 887A Guía de Configuración Segura para AWS*** se referencian tecnologías nativas en las que la entidad usuaria puede apoyarse para el diseño seguro de la arquitectura de las cargas de trabajo.

4.2 [OP.ACC] Control de acceso

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

- Los mecanismos de autenticación provistos por AWS 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 AWS*** y sus servicios relacionados, referenciadas en la sección ***5. Configuración de seguridad*** de este documento.

- Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por AWS 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 AWS, dado que no es previsible que usuarios ajenos a la organización accedan a AWS (sin perjuicio de los accesos que puedan realizar a las aplicaciones o sistemas soportados por la infraestructura de AWS, en cuyo ámbito sí que serán de aplicación las exigencias de la citada medida de seguridad [op.acc.5]).

4.3 [OP.EXP.2] Configuración de Seguridad y [OP.EXP.3] Gestión de la configuración de seguridad

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

- La configuración de seguridad que se aplique a los servicios proporcionados por AWS será la reflejada en las ***Guías de configuración segura de AWS*** 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 AWS teniendo en cuenta, en su caso, las diferentes guías CCN-STIC sobre la configuración segura de tecnologías específicas.

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.

4.4 [OP.EXP.7] Gestión de incidentes

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

- En la guía ***CCN-STIC 887F Guía de respuesta a incidentes de seguridad en AWS*** se describen las diferentes configuraciones y servicios para el adecuado tratamiento de los incidentes de seguridad en entornos de nube pública de AWS.

4.5 [OP.EXP.9] Registro de la gestión de incidentes

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

- En las guías ***CCN-STIC 887A Guía de Configuración Segura para AWS*** y ***CCN-STIC 887F Guía de respuesta a incidentes de seguridad en AWS*** se describen las tecnologías, herramientas y recomendaciones para el adecuado registro de las actuaciones relacionadas con la gestión de incidentes ocurridos en los sistemas desplegados en AWS.

4.6 [OP.EXP.8] Registro de la actividad

Será de aplicación esta medida 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 AWS 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 AWS*** y sus servicios relacionados, referenciadas en la sección ***5. Configuración de seguridad*** de este documento.

- En aquellos elementos del sistema donde los mecanismos de registro de actividad provistos por AWS 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.

4.7 [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 AWS 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 AWS 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.

4.8 [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 AWS, entre varios sistemas desplegados en la nube de AWS o entre los sistemas desplegados en la nube de AWS y otros sistemas externos.

En la guía ***CCN-STIC 887C Guía de Configuración Segura de Conectividad Híbrida en AWS*** se describen las diferentes configuraciones de seguridad para entornos híbridos que aprovechan los servicios de AWS para el correcto cumplimiento de los requisitos exigibles en el ENS.

4.9 [OP.NUB.1] Protección de los 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 AWS*** referenciadas en la sección ***5. Configuración de seguridad*** de este documento**.**

4.10 [OP.CONT] Continuidad del servicio

Serán de aplicación las medidas de categoría y nivel ALTO. En la guía ***CCN-STIC 887A Configuración Segura de AWS*** 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 AWS.

Será de aplicación la medida “op.cont.4 Medios Alternativos” 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 AWS.
- La correcta configuración de estos mecanismos queda descrita en las Guías de configuración segura de AWS y sus servicios relacionados, referenciados en la sección 5. Configuración de seguridad de este documento.
- 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 AWS para la continuidad de sus servicios, así como determinar los requisitos de disponibilidad de sus servicios y los elementos considerados críticos.

4.11 [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 AWS y sus servicios relacionados, referenciadas en la sección ***5. Configuración de seguridad*** de este documento.

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

Serán de aplicación las medidas 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.
- En caso de que el sistema de la entidad usuaria se enlace mediante una arquitectura híbrida con el proveedor de servicios en la nube, será responsabilidad de la organización usuaria ajustarse a los requisitos exigibles del ENS para la protección de las instalaciones e infraestructuras locales conectadas a dichos servicios Cloud.

4.13 [MP.EQ.2] Bloqueo de puesto de trabajo

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

- Entendiendo como puesto de trabajo los escritorios remotos provistos por la solución de virtualización de escritorios de AWS (Amazon Workspaces), será responsabilidad de la entidad usuaria la correcta configuración de seguridad.

- La aplicación de esta configuración de seguridad asociada al bloqueo de puesto de trabajo queda descrita en la ***Guía 887 CCN-STIC 887E Guía de configuración segura para Amazon WorkSpaces*** referenciada en el punto ***5. Configuración de seguridad*** de este documento.

4.14 [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.

4.15 [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.

4.16 [MP.INFO.2] Calificación 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.

- AWS 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 la guía ***CCN-STIC 887A Guía de configuración segura para AWS***, referenciada en el punto ***5. Configuración de seguridad*** de este documento.

4.17 [MP.INFO.3] Firma electrónica

Esta medida 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.

4.18 [MP.INFO.5] Limpieza de documentos

Esta medida será de aplicación 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.

4.19 [MP.INFO.6] Copias de seguridad

Será aplicable esta medida 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 AWS. 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 AWS*** y sus servicios relacionados, referenciadas en la sección ***5. Configuración de seguridad*** de este documento.

En aquellos elementos del sistema donde los mecanismos de copia de seguridad provistos por AWS 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.

4.20 [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 AWS.

5. CONFIGURACIÓN DE SEGURIDAD

Para dar respuesta a los requisitos establecidos en este Perfil de Cumplimiento Especifico usando la tecnología AWS en cualquiera de sus modalidades, se deberá consultar lo establecido en las guías "***CCN-STIC 887A Guía de Configuración Segura para AWS***", "***CCN-STIC 887C Guía de Configuración Segura de Conectividad Híbrida en AWS***", "***CCN-STIC 887D Guía de Configuración Segura para entornos multi-cuenta en AWS***", "***CCN-STIC-887E Guía de Configuración Segura para Amazon WorkSpaces***", ***"CCN-STIC 887F Guía de respuesta a incidentes de seguridad en AWS"***

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