centro criptológico nacional

Perfil de Cumplimiento Específico
CCN-STIC 886

Perfil de Cumplimiento Específico para Sistemas Cloud Privados y Comunitarios

Diciembre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.02.10 13:19:43 +01'00'

NIPO: 083-19-265-8

Fecha de Edición: diciembre de 2019
Instituto CIES ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

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 en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director 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 Especifico para garantizar la seguridad en los sistemas que alojan servicios Cloud en modalidad de despliegue privada o comunitaria, con necesidades de seguridad de categoría MEDIA.**

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

7. Este perfil de cumplimiento podrá ser de aplicación a todas aquellas entidades en las que el sistema de información que soporta el Sistema de Cloud Privados o Comunitarios, tras un proceso correcto de valoración haya obtenido una categorización MEDIA.

8. Siempre y cuando se trate de un sistema dedicado exclusivamente a esta solución Cloud en su modalidad de despliegue privada o comunitaria, instalada on-premise y ofreciendo servicios de Software as a Service (SaaS).

9. De acuerdo a lo establecido en la Guía de seguridad de las TIC *CCN-STIC-823 Utilización de servicios en la Nube*, las nubes con modelos de despliegue privados se definen como aquellas que se basan en una infraestructura operada únicamente por una organización y que ofrecen servicios únicamente a esa misma organización.

10. Por otro lado, las nubes con modelos de despliegue comunitarios se definen como aquellas alojadas en infraestructuras compartidas por varias organizaciones, relacionadas entre ellas compartiendo requisitos de servicio, donde uno de los miembros del colectivo controla la infraestructura.

11. Este perfil de cumplimiento podrá ser de aplicación, bajo las premisas previamente dispuestas, en los sistemas alojados en infraestructuras propias de la entidad interesada, o alojados en infraestructuras contratadas a proveedores de servicios de *housing*, siempre y cuando la responsabilidad de administración y configuración segura de la plataforma recaigan sobre la entidad.

3. DECLARACIÓN DE APLICABILIDAD

12. 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.

13. Se ha determinado que, para garantizar la seguridad en los sistemas a los que hace referencia este Perfil de Cumplimiento Especifico, la relación de medidas que son de aplicación y la exigencia en el nivel de seguridad de cada medida aplicada, es la que se indica en la siguiente tabla, donde el carácter "*" indica que disponen de criterios específicos de aplicación, los cuales se detallan en el apartado "*4. CRITERIOS DE APLICACIÓN DE CONTROLES*":

Dimensiones					
Afectadas	CAT B	CAT M	CAT A		
				org	Aplicación
categoría	aplica	=	=	[org.1]	ALTO
categoría	aplica	=	=	[org.2]	ALTO
categoría	aplica	=	=	[org.3]	ALTO
categoría	aplica	=	=	[org.4]	ALTO

categoría	aplica	+	++	[op.pl.1]	MEDIO
categoría	aplica	+	++	[op.pl.2]	MEDIO
categoría	aplica	=	=	[op.pl.3]	ALTO
D	n.a.	aplica	=	[op.pl.4]	MEDIO

Dimensiones Afectadas	CAT B	CAT M	CAT A	org	Aplicación
categoría	n.a.	n.a.	aplica	[op.pl.5]	n/a[1]
A T	aplica	=	=	[op.acc.1]	ALTO
I C A T	aplica	=	=	[op.acc.2]	ALTO
I C A T	n.a.	aplica	=	[op.acc.3]	ALTO
I C A T	aplica	=	=	[op.acc.4]	ALTO
I C A T	aplica	+	++	[op.acc.5]	MEDIO*
I C A T	aplica	+	++	[op.acc.6]	BAJO*
I C A T	aplica	+	=	[op.acc.7]	ALTO
categoría	aplica	=	=	[op.exp.1]	ALTO
categoría	aplica	=	=	[op.exp.2]	ALTO
categoría	n.a.	aplica	=	[op.exp.3]	ALTO
categoría	aplica	=	=	[op.exp.4]	ALTO
categoría	n.a.	aplica	=	[op.exp.5]	ALTO
categoría	aplica	=	=	[op.exp.6]	ALTO*
categoría	n.a.	aplica	=	[op.exp.7]	ALTO
T	aplica	+	++	[op.exp.8]	MEDIO
categoría	n.a.	aplica	=	[op.exp.9]	ALTO
T	n.a.	n.a.	aplica	[op.exp.10]	n/a
categoría	aplica	+	=	[op.exp.11]	ALTO
categoría	n.a.	aplica	=	[op.ext.1]	ALTO
categoría	n.a.	aplica	=	[op.ext.2]	ALTO
D	n.a.	n.a.	aplica	[op.ext.9]	n/a
D	n.a.	aplica	=	[op.cont.1]	ALTO
D	n.a.	n.a.	aplica	[op.cont.2]	n/a
D	n.a.	n.a.	aplica	[op.cont.3]	n/a
categoría	n.a.	aplica	=	[op.mon.1]	ALTO
categoría	aplica	+	++	[op.mon.2]	MEDIO

categoría	aplica	=	=	[mp.if.1]	ALTO*
categoría	aplica	=	=	[mp.if.2]	ALTO*
categoría	aplica	=	=	[mp.if.3]	ALTO*
D	aplica	+	=	[mp.if.4]	ALTO*
D	aplica	=	=	[mp.if.5]	ALTO*
D	n.a.	aplica	=	[mp.if.6]	ALTO*
categoría	aplica	=	=	[mp.if.7]	ALTO*
D	n.a.	n.a.	aplica	[mp.if.9]	n/a*
categoría	n.a.	aplica	=	[mp.per.1]	ALTO

[1] n/a- No aplica

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	org	Aplicación
categoría	aplica	=	=	[mp.per.2]	ALTO
categoría	aplica	=	=	[mp.per.3]	ALTO
categoría	aplica	=	=	[mp.per.4]	ALTO
D	n.a.	n.a.	aplica	[mp.per.9]	n/a
categoría	aplica	+	=	[mp.eq.1]	ALTO
A	n.a.	aplica	+	[mp.eq.2]	MEDIO
categoría	aplica	=	+	[mp.eq.3]	MEDIO
D	n.a.	aplica	=	[mp.eq.9]	ALTO
categoría	aplica	=	+	[mp.com.1]	MEDIO
C	n.a.	aplica	+	[mp.com.2]	MEDIO
I A	aplica	+	++	[mp.com.3]	MEDIO
categoría	n.a.	n.a.	aplica	[mp.com.4]	n/a
D	n.a.	n.a.	aplica	[mp.com.9]	n/a
C	aplica	=	=	[mp.si.1]	n/a*
I C	n.a.	aplica	+	[mp.si.2]	n/a*
categoría	aplica	=	=	[mp.si.3]	n/a*
categoría	aplica	=	=	[mp.si.4]	n/a*
C	aplica	+	=	[mp.si.5]	ALTO*
categoría	n.a.	aplica	=	[mp.sw.1]	n/a
categoría	aplica	+	++	[mp.sw.2]	MEDIO
categoría	aplica	=	=	[mp.info.1]	ALTO
C	aplica	+	=	[mp.info.2]	ALTO*
C	n.a.	n.a.	aplica	[mp.info.3]	n/a
I A	aplica	+	++	[mp.info.4]	n/a*
T	n.a.	n.a.	aplica	[mp.info.5]	n/a
C	aplica	=	=	[mp.info.6]	ALTO*
D	aplica	=	=	[mp.info.9]	ALTO
categoría	aplica	=	=	[mp.s.1]	*
categoría	aplica	=	+	[mp.s.2]	MEDIO
D	n.a.	aplica	+	[mp.s.8]	MEDIO
D	n.a.	n.a.	aplica	[mp.s.9]	n/a

3.1 MEDIDAS DE APLICACIÓN

14. De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, **aplican un total de 56*[2] medidas**. Son las siguientes:

[2] Como mínimo aplicarían 56 medidas

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 (26):

[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.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.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.cont] Continuidad del servicio

[op.cont.1] Análisis de impacto

[op.mon] Monitorización del sistema

[op.mon.1] Detección de intrusión

[op.mon.2] Sistema de métricas

Medidas de Protección (26):

[mp.if] Protección de las instalaciones e infraestructuras

[mp.if.1] Áreas separadas y con control de acceso

[mp.if.2] Identificación de las personas

[mp.if.3] Acondicionamiento de los locales

[mp.if.4] Energía eléctrica

[mp.if.5] Protección frente a incendios

[mp.if.6] Protección frente a inundaciones

[mp.if.7] Registro de entrada y salida de equipamiento

[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.si] Protección de los soportes de información

[mp.si.5] Borrado y destrucción

[mp.sw] Protección de las aplicaciones informáticas

[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.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 servicio

4. CRITERIOS DE APLICACIÓN DE CONTROLES

4.1 [OP.ACC.5] Mecanismos de Autenticación

15. Serán exigibles los requisitos de nivel MEDIO para esta medida, con las siguientes particularidades:

- En el caso de utilizarse como factor "algo que se sabe", no será requerido que:
  - Las credenciales se activen una vez estén bajo el control efectivo del usuario.
  - Las credenciales estarán bajo el control exclusivo del usuario.
- El cambio de las credenciales en el primer acceso será responsabilidad de los usuarios finales de la plataforma, por lo que deberá incluirse en las normas de uso de la misma, haciendo mención expresa a que se deberá cambiar la contraseña en el primer acceso.
- No será requerido el uso de doble factor de autenticación para los usuarios finales de la plataforma.
- El uso de doble factor de autenticación sí será requerido para:
  - Los usuarios finales con privilegios de administrador, así como otros usuarios finales de la plataforma a criterio del Responsable de Seguridad.
  - Los usuarios que realicen tareas de configuración y mantenimiento de la plataforma.

4.2 [OP.ACC.6] Acceso Local (Local logon)

16. Serán exigibles los requisitos de nivel BAJO para esta medida, con las siguientes particularidades en el acceso a los servicios Cloud:

- Solo será necesario el registro de los accesos fallidos, siempre y cuando la tecnología no permita registrar los accesos con éxito.

- En caso de que la tecnología no permita que el sistema informe a los usuarios, de sus obligaciones inmediatamente después de obtener el acceso, mediante un mensaje emergente, en el portal de acceso deberá referenciarse a la política de privacidad y a la normativa de uso de la plataforma.

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

17. Serán de aplicación los requisitos de categoría ALTA para esta medida, con la siguiente particularidad:

    - En caso de que no sea posible implementar esta medida en el sistema que soporta el servicio Cloud, será necesario implementar una medida compensatoria mediante la configuración de inspección del tráfico cifrado (Deep Packet Inspection) en la solución de protección perimetral utilizada (cortafuegos).

18. Esta particularidad en la Protección Frente a Código Dañino únicamente será de aplicación en el sistema donde se alojan los servicios Cloud.

19. En cuanto a los equipos empleados para realizar tareas de configuración y mantenimiento del servicio y la plataforma, deben aplicar los requisitos de esta medida de protección para categoría ALTA.

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

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

    - Si el sistema Cloud se encuentra externalizado en la modalidad de PaaS (servicio de *housing*), solo será exigible que la empresa proveedora del servicio disponga de conformidad con el ENS para este servicio PaaS (servicio de *housing*).

    - En caso contrario la aplicación de estas medidas será exigible en los niveles de seguridad indicados.

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

4.5 [MP.SI] Protección de soportes de información

22. El conjunto de medidas “mp.si Protección de los soportes de información”, no será de aplicación siempre y cuando se prohíba expresamente el uso de dispositivos extraíbles y/u otros soportes de información (incluido para la creación de copias de seguridad) en la normativa del sistema, a excepción de la medida “mp.si.5 Borrado y destrucción”, que sí será de aplicación para los discos duros y demás medios de almacenamiento.

4.6 [MP.SW.1] Desarrollo de Aplicaciones

23. Esta medida no será de aplicación siempre y cuando se prohíba expresamente 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.

4.7 [MP.INFO.2] Calificación de la Información

24. 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.

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

4.8 [MP.INFO.4] Firma Electrónica

26. 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.

4.9 [MP.INFO.6] Limpieza de documentos

27. 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.

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

4.10 [MP.S.1] Protección del Correo Electrónico

29. Esta medida no será de aplicación, siempre y cuando no se contemple el uso del correo electrónico para tareas directamente relacionadas con la configuración y/o mantenimiento del sistema y así sea considerado por el Responsable de Seguridad.

5. CONFIGURACIÓN DE SEGURIDAD

30. Para dar respuesta a los requisitos establecidos en este Perfil de Cumplimiento Especifico usando la tecnología NextCloud en su modalidad on-premise, se deberá consultar lo establecido en la “Guía CCN-STIC 826 Configuración Segura de NextCloud en el ENS” y aplicar las configuraciones indicadas para ENS categoría ALTA de dicha guía.

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