centro criptológico nacional

Perfil de Cumplimiento Especifico
CCN-STIC 884

Perfil de Cumplimiento Especifico para Azure
Servicio de Cloud Corporativo

Diciembre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO 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
2020.02.10 13:13:50 +01'00'

NIPO: 083-19-264-2

Fecha de Edición: diciembre de 2019

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

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 servicios contratados en el Cloud de Microsoft Azure 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 Microsoft Azure, en su modalidad de despliegue como nube pública y ofreciendo servicios de Software

as a Service (SaaS), Platform as a Service (PaaS) e Infraestructure as a Service (IaaS), según corresponda en cada servicio contratado.

8. De acuerdo a 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 Especifico, la solución Cloud de Microsoft Azure 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 Microsoft Azure, 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
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]	ALTO
categoría	aplica	+	++	[op.pl.2]	ALTO
categoría	aplica	=	=	[op.pl.3]	ALTO
D	n.a.	aplica	=	[op.pl.4]	ALTO
categoría	n.a.	n.a.	aplica	[op.pl.5]	ALTO
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]	ALTO*
I C A T	aplica	+	++	[op.acc.6]	ALTO*
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]	ALTO*
categoría	n.a.	aplica	=	[op.exp.9]	ALTO
T	n.a.	n.a.	aplica	[op.exp.10]	ALTO*
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]	n/a
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]	ALTO

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

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

3.1 MEDIDAS DE APLICACIÓN

12. De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, **aplican un total de 56* medidas**. 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 (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.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.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.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.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 MEDIDAS

4.1 [OP.ACC] Mecanismos de Autenticación

13. El conjunto de medidas “op.acc Mecanismos de Autenticación” serán de aplicación en categoría y nivel ALTO, con las siguientes particularidades:

    - Los mecanismos de autenticación provistos por Azure 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 Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.

- Para el acceso a aquellos elementos del sistema donde los mecanismos de autenticación provistos por Azure 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

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

    - La configuración de seguridad que es de aplicación a los servicios proporcionados por Azure será la reflejada en las Guías de configuración segura de Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.

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

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

16. 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 Azure 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 Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.
    - En aquellos elementos del sistema donde los mecanismos de registro de actividad provistos por Azure 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.EXP.10] Protección de los Registros de Actividad de los Usuarios

17. 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 Azure. 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 Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.

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

4.5 [OP.EXT.9] Medios Alternativos

18. Será de aplicación la medida "op.ext.9 Medios Alternativos" únicamente cuando, tras la correcta categorización del sistema, se establezca un nivel de seguridad ALTO en la dimensión de Trazabilidad del sistema.

19. En este caso, la medida será de aplicación con la siguiente particularidad:

    - Se utilizarán los mecanismos de replicación de medios provistos por Azure.
    - La correcta configuración de estos mecanismos queda descrita en las Guías de configuración segura de Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.

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

20. 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.

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, 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

22. 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.

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

4.8 [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.

26. Sin embargo, será recomendable aplicar las configuraciones de seguridad para la calificación de información descritos en las Guías de configuración segura de Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.

4.9 [MP.INFO.4] Firma Electrónica

27. 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.

4.10 [MP.INFO.6] Limpieza de documentos

28. 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.

4.11 [MP.INFO.9] Copias de Seguridad

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

    - Se emplearán los mecanismos para la creación de copias de seguridad proporcionados por Azure. 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 Azure y sus servicios relacionados, referenciadas en el apartado 5 de esta Guía relativo a la Configuración de seguridad.

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

31. 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

32. Para dar respuesta a los requisitos establecidos en este Perfil de Cumplimiento Especifico usando la tecnología Azure en cualquiera de sus modalidades, se deberá consultar lo establecido en las guías “CCN-STIC 884A Configuración Segura de Azure”, “CCN-STIC 884B Configuración Segura de Azure Kubernetes”, “CCN-STIC 884C Configuración Segura de Azure SQL Server” y “CCN-STIC 884D Configuración Segura de Azure Cognitive Services” y aplicar las configuraciones indicadas en dichas guías.

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