centro criptológico nacional

Perfil de Cumplimiento Específico
CCN-STIC 883A

Perfil de Cumplimiento Específico Ayuntamientos <5.000 hab.
(Ayuntamientos pequeños y con limitados recursos)

Mayo 2020

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

NIPO: 083-19-183-2

Fecha de Edición: mayo de 2020

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 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.

Mayo de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

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

Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 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.

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.

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 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.

A tal fin, tras realizar un estudio de las necesidades de seguridad, de los recursos y tras un análisis de riesgos contemplando las vulnerabilidades y amenazas a las que se ven expuestas las Entidades Locales y en particular los Ayuntamientos 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 Entidades Locales que permita la implantación del ENS en las mismas, con necesidades de seguridad de categoría BÁSICA.

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

Este Perfil de Cumplimiento Específico podrá ser de aplicación a todos aquellos Ayuntamientos pequeños de menos de 5.000 habitantes, con limitados recursos y de características similares, incluidos los que se encuentren adheridos al Marco de Certificación de Conformidad con el ENS para el conjunto de Entidades Locales, de acuerdo a lo establecido en el **Abstract- "Marco de Certificación ENS para Entidades Locales".**

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 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. El "*" indica que disponen de criterios específicos de aplicación, los cuales se detallan en el apartado "4. CRITERIOS DE APLICACIÓN DE MEDIDAS".

Dimensiones					
Afectadas	CAT B	CAT M	CAT A		
				Control	Aplicación
categoría	aplica	=	=	[org.1]	BAJO*
categoría	aplica	=	=	[org.2]	BAJO*
categoría	aplica	=	=	[org.3]	BAJO*
categoría	aplica	=	=	[org.4]	BAJO
categoría	aplica	+	++	[op.pl.1]	BAJO*
categoría	aplica	+	++	[op.pl.2]	BAJO
categoría	aplica	=	=	[op.pl.3]	BAJO
D	n.a	aplica	=	[op.pl.4]	n/a[1]
Todas	n.a.	aplica	aplica	[op.pl.5]	n/a
A T	aplica	=	=	[op.acc.1]	BAJO
I C A T	aplica	=	=	[op.acc.2]	BAJO
I C A T	n.a.	aplica	=	[op.acc.3]	n/a
I C A T	aplica	=	=	[op.acc.4]	BAJO
I C A T	aplica	+	++	[op.acc.5]	BAJO
I C A T	aplica	+	++	[op.acc.6]	BAJO
I C A T	aplica	+	=	[op.acc.7]	MEDIO
Todas	aplica	=	=	[op.exp.1]	BAJO*
Todas	aplica	=	=	[op.exp.2]	BAJO*
Todas	n.a	aplica	=	[op.exp.3]	n/a
Todas	aplica	=	=	[op.exp.4]	BAJO
Todas	n.a.	aplica	=	[op.exp.5]	n/a
Todas	aplica	=	=	[op.exp.6]	BAJO
Todas	n.a.	aplica	=	[op.exp.7]	MEDIO*

[1] n/a- No aplica

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación
T	aplica	+	++	[op.exp.8]	BAJO*
Todas	n.a.	aplica	=	[op.exp.9]	MEDIO*
T	n.a.	n.a.	aplica	[op.exp.10]	n/a
Todas	aplica	+	=	[op.exp.11]	BAJO
Todas	n.a.	aplica	=	[op.ext.1]	MEDIO*
Todas	n.a.	aplica	=	[op.ext.2]	MEDIO*
D	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
Todas	aplica	aplica	=	[op.mon.1]	n/a
Todas	aplica	+	++	[op.mon.2]	MEDIO*
Todas	aplica	=	=	[mp.if.1]	BAJO
Todas	aplica	=	=	[mp.if.2]	BAJO
Todas	aplica	=	=	[mp.if.3]	BAJO
D	aplica	+	=	[mp.if.4]	BAJO
D	aplica	=	=	[mp.if.5]	BAJO
D	n.a	aplica	=	[mp.if.6]	n/a
Todas	aplica	=	=	[mp.if.7]	BAJO
D	n.a	n.a	aplica	[mp.if.9]	n/a
Todas	n.a.	aplica	=	[mp.per.1]	n/a
Todas	aplica	=	=	[mp.per.2]	BAJO
Todas	aplica	=	=	[mp.per.3]	BAJO
Todas	aplica	=	=	[mp.per.4]	BAJO
Todas	n.a.	n.a.	aplica	[mp.per.9]	n/a
Todas	aplica	+	=	[mp.eq.1]	BAJO
A	n.a.	aplica	+	[mp.eq.2]	n/a
Todas	aplica	=	+	[mp.eq.3]	BAJO
D	n.a.	n.a.	aplica	[mp.eq.9]	n/a
Todas	aplica	=	+	[mp.com.1]	BAJO
C	n.a	aplica	+	[mp.com.2]	MEDIO*
I A	aplica	+	++	[mp.com.3]	MEDIO*
Todas	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]	BAJO*
I C	n.a.	aplica	=	[mp.si.2]	n/a*
categoría	aplica	=	=	[mp.si.3]	BAJO*

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

3.1 MEDIDAS DE APLICACIÓN

De las 75 medidas de seguridad definidas en el Anexo II del RD 3/2010, **aplican un total de 48*[2] 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 (20):

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.acc] Control de acceso

[op.acc.1] Identificación

[2] Número aproximado de medidas que aplican

[op.acc.2] Requisitos de acceso

[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.4] Mantenimiento

[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.mon] Monitorización del sistema

[op.mon.2] Sistema de métricas

Medidas de Protección (24):

[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.7] Registro de entrada y salida de equipamiento

[mp.per] Gestión del personal

[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.3] Protección de equipos portátiles

[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.1] Etiquetado

[mp.si.2] Criptografía

[mp.si.3] Custodia

[mp.si.4] Transporte

[mp.si.5] Borrado y destrucción

[mp.info] Protección de la información

[mp.info.1] Datos de carácter personal

[mp.info.2] Calificación de la información

[mp.info.4] Firma electrónica

[mp.info.5] Sellos de tiempo

[mp.info.6] Limpieza de documentos

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

[mp.s] Protección de los servicios

[mp.si.1] Protección del correo electrónico

4. CRITERIOS DE APLICACIÓN DE MEDIDAS

4.1 [ORG.1] Política de seguridad, [ORG.2] Normativa de seguridad, [ORG.3] Procedimientos de seguridad, [OP.PL.1] Análisis de riesgos

Para este conjunto de medidas, serán de aplicación los requisitos de categoría BÁSICA que, en el caso de los Ayuntamientos adheridos al Marco de Certificación de EELL, y de acuerdo con lo establecido en el Abstract- "Marco de Certificación ENS para Entidades Locales", se abordarán de manera conjunta para todos los Ayuntamientos adheridos al mismo de la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente.

4.2 [OP.EXP.7] Gestión de incidentes y [OP.EXP.9] Registro de la gestión de incidentes

Serán de aplicación los requisitos de categoría MEDIA, según los procedimientos establecidos por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente y en coordinación con ésta, relativos a la obligatoriedad de comunicación de incidentes.

4.2.1 [OP.EXP.8] Registro de actividad de los usuarios

Serán de aplicación los requisitos de nivel BAJO, en el sistema de información del Ayuntamiento, mientras que los relacionados con los servicios correrán por cuenta de la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente.

4.3 [OP.EXT.1] Contratación y acuerdos de nivel de servicio y [OP.EXP.2] Gestión de diaria

Serán de aplicación los requisitos de categoría MEDIA, según los procedimientos establecidos por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente.

4.4 [OP.MON.2] Sistema de métricas

Serán de aplicación los requisitos de categoría MEDIA, al ser necesarios la recopilación de los datos relativos sobre incidentes de seguridad para dar respuesta a la Encuesta INÉS (Informe Nacional sobre el Estado de la Seguridad).

4.5 [OP.COM.2] Protección de la confidencialidad

Serán de aplicación los requisitos de nivel MEDIO, con las siguientes particularidades:

- Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
- Será recomendable que se empleen algoritmos acreditados por el Centro Criptológico Nacional.

4.6 [OP.COM.3] Protección de la autenticidad y la integridad

Serán de aplicación los requisitos de nivel MEDIO, con las siguientes particularidades:

- Aplicarán los requisitos de nivel BAJO íntegramente.
- Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
- Será recomendable que se empleen algoritmos acreditados por el Centro Criptológico Nacional.

4.7 [MP.SI] Protección de los soportes de información

Para el conjunto de medidas de "[mp.si] Protección de los soportes de información", como norma general, serán de aplicación los requisitos en nivel BAJO y categoría BÁSICA, según sea de aplicación, con las siguientes particularidades:

- La medida "[mp.si.1] Etiquetado" aplicará a los dispositivos removibles (CD, DVD, discos extraíbles, pendrives, memorias USB, u otros de naturaleza análoga) cuando estos contengan información relacionada con los servicios dentro del alcance del ENS y a los documentos (formato electrónico y soporte papel) que forman parte del Sistema de Gestión de la Seguridad de la Información (SGSI).
- La medida "[mp.si.2] Criptografía", será de aplicación con los requisitos de nivel MEDIO, en el caso de que estos vayan a ser utilizados fuera de las instalaciones.
- La medida "[mp.si.5] Borrado y destrucción", también será de aplicación para los discos duros del equipamiento.

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

Esta medida no será de aplicación al ser de aplicación al sistema de información donde residen los servicios (Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente), siendo responsabilidad de éste su aplicación.

4.9 [MP.INFO.4] Firma Electrónica

Serán de aplicación los requisitos en diferentes niveles para esta medida, con las siguientes particularidades:

- MEDIO: cuando se utilice firma electrónica para la actividad administrativa y esta sea necesaria para garantizar la verificación y validación de la firma electrónica.
- BAJO: cuando se utilice firma electrónica para funcionalidades distintas de la actividad administrativa.

- N.A. (no aplica): cuando no se utilice la firma electrónica en relación con los servicios que se encuentran dentro del alcance.

4.10 [MP.INFO.5] Sellos de tiempo

Serán de aplicación los requisitos de nivel ALTO, para aquella información que sea susceptible de ser utilizada como evidencia electrónica, siempre y cuando el servicio de sello de tiempo no sea provisto por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente, en cuyo caso la aplicación de estos requisitos será responsabilidad de esta.

4.11[MP.INFO.9] Copias de seguridad (*backup*)

Serán de aplicación los requisitos de nivel BAJO, siempre y cuando el servicio de copias de seguridad no sea provisto por la Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente y no se aloje información relacionada con los servicios ENS en el sistema de información del Ayuntamiento, siendo en este caso responsabilidad del Ayuntamiento su aplicación.

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

Serán de aplicación los requisitos de categoría BÁSICA, siempre y cuando el correo electrónico intervenga en la prestación de los servicios dentro del alcance del ENS.

4.13 [MP.S.2] Protección de los servicios y aplicaciones *web*

Esta medida no será de aplicación al ser de aplicación al sistema de información donde residen los servicios (Diputación Provincial, Cabildo, Consejo Insular u órgano equivalente), siendo responsabilidad de éste su aplicación.