Guía de Seguridad de las TIC
CCN-STIC 890B

Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (Sector Público)

Marzo 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.03.22 09:56:03 +01'00'

Pº de la Castellana 109, 28046 Madrid

Nipo: 083-23-092-4

Fecha de Edición: marzo 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

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 Esquema Nacional de Seguridad 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.

De conformidad con lo dispuesto en el ENS (RD311/2022), los instrumentos normativos previstos (instrucciones técnicas de seguridad y/o guías de seguridad) 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, ha validado el presente perfil de cumplimiento específico, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, garantizando que las medidas de seguridad implementadas son las necesarias y proporcionadas en relación con el nivel de madurez, riesgo residual asumible y recursos disponibles.

A tal fin, tras un análisis de riesgos contemplando las vulnerabilidades, los riesgos y las amenazas a las que se ven expuestas las entidades, organismos u organizaciones; y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando el siguiente Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad que permita la implantación del ENS en las mismas.

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

El objetivo que se persigue con este Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad para el Sector Público, es posibilitar el cumplimiento del Esquema Nacional de Seguridad (ENS) para categoría BÁSICA de los sistemas de información que soportan la tramitación de servicios prestados en entidades, organismos u organizaciones con dificultades para abordar el proceso de adecuación al ENS, con el propósito de facilitar la obtención de la Certificación de Conformidad mediante el cumplimiento de unos requisitos esenciales de seguridad.

Siendo los citados servicios los siguientes:

- S 13 REGISTRO GENERAL
- S 14 ARCHIVO

- S 15 CONTRATACIÓN
- S 18 TESORERÍA
- S 19 GESTIÓN DE PERSONAL
- S 32 PREVENCIÓN Y SALUD
- S 40 TRANSPARENCIA
- S 41 SERVICIOS PRESUPUESTARIOS
- S 42 SECRETARÍA (SERVICIOS JURÍDICOS)
- S 43 ÓRGANOS DE GOBIERNO
- S 100 SERVICIO FINALISTA[1] QUE ENGLOBA LAS FUNCIONES DE LA ORGANIZACIÓN[2]

3. DECLARACIÓN DE APLICABILIDAD

Teniendo en cuenta la casuística del modelo propuesto se ha determinado que, para garantizar la seguridad de los sistemas concernidos, la relación de medidas del Anexo II del ENS que resultan de aplicación y exigencia en el nivel de seguridad, son las recogidas en la siguiente tabla. 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[3]
Categoría	aplica	aplica	aplica	org.1	BÁSICA
Categoría	aplica	aplica	aplica	org.2	BÁSICA
Categoría	aplica	aplica	aplica	org.3	BÁSICA
Categoría	aplica	aplica	aplica	org.4	BÁSICA
Categoría	aplica	+ R1	+ R2	op.pl.1	BÁSICA
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	N/A
Categoría	aplica	aplica	aplica	op.pl.3	BÁSICA
D	aplica	+ R1	+ R1	op.pl.4	N/A
Categoría	n.a.	aplica	aplica	op.pl.5	N/A
T A	aplica	+ R1	+ R1	op.acc.1	BAJO
C I T A	aplica	aplica	+ R1	op.acc.2	BAJO
C I T A	n.a.	aplica	+ R1	op.acc.3	N/A
C I T A	aplica	aplica	aplica	op.acc.4	BAJO
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	+ [R1 o R2 o R3 o R4]	op.acc.6	BAJO (+R1) *

[1] SF: Servicio Finalista, prestado a terceros y descritos en las funciones del organismo.

[2] Ver tabla de alcance del Anexo III CCN-STIC 890 Categorización del Sistema.

[3] 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[3]
		R4] + R5 + R8 + R9	+ R5 + R6 + R7 + R8 + R9		
Categoría	aplica	aplica	aplica	op.exp.1	BÁSICA
Categoría	aplica	aplica	aplica	op.exp.2	BÁSICA
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	N/A
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	BAJO *
Categoría	aplica	aplica	aplica	op.exp.9	N/A
Categoría	aplica	+ R1	+ R1	op.exp.10	BÁSICA
Categoría	n.a.	aplica	aplica	op.ext.1	N/A
Categoría	n.a.	aplica	aplica	op.ext.2	N/A
Categoría	n.a.	n.a.	aplica	op.ext.3	N/A
Categoría	n.a.	aplica	+ R1	op.ext.4	N/A
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	N/A
D	n.a.	aplica	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
D	n.a.	n.a.	aplica	op.cont.4	N/A
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	N/A
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	BÁSICA
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	N/A
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
Categoría	n.a.	aplica	aplica	mp.per.1	N/A
Categoría	aplica	+ R1	+ R1	mp.per.2	BÁSICA
Categoría	aplica	aplica	aplica	mp.per.3	BÁSICA
Categoría	aplica	aplica	aplica	mp.per.4	BÁSICA
Categoría	aplica	+ R1	+ R1	mp.eq.1	BÁSICA
A	n.a.	aplica	+ R1	mp.eq.2	N/A
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	BAJO
C	aplica	+ R1	+ R1	mp.eq.4	BAJO
Categoría	aplica	aplica	aplica	mp.com.1	BÁSICA *
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	BAJO
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	N/A
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	N/A
C	n.a.	aplica	aplica	mp.si.1	N/A
C I	n.a.	aplica	+ R1 + R2	mp.si.2	N/A
Categoría	aplica	aplica	aplica	mp.si.3	BÁSICA
Categoría	aplica	aplica	aplica	mp.si.4	BÁSICA

Dimensiones Afectadas	CAT B	CAT M	CAT A	Control	Aplicación[3]
C	aplica	+ R1	+ R1	mp.si.5	BAJO
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	N/A
Categoría	aplica	+ R1	+ R1	mp.sw.2	N/A
Categoría	aplica	aplica	aplica	mp.info.1	BÁSICA
C	n.a.	aplica	aplica	mp.info.2	N/A
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	BÁSICA
T	n.a.	n.a.	aplica	mp.info.4	N/A
C	aplica	aplica	aplica	mp.info.5	BAJO
D	aplica	+ R1	+ R1 + R2	mp.info.6	BAJO
Categoría	aplica	aplica	aplica	mp.s.1	BÁSICA
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	N/A
Categoría	aplica	aplica	+ R1	mp.s.3	BÁSICA
D	n.a.	aplica	+ R1	mp.s.4	N/A

3.1 MEDIDAS DE APLICACIÓN

De las 73 medidas de seguridad definidas en el Anexo II del ENS, **aplican un total de 35*[4] 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 (14):

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.3] Adquisición de nuevos componentes

[op.acc] Control de acceso

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[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.2] Configuración de seguridad

[4] Número aproximado de medidas que aplican

[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.mon] Monitorización del sistema

[op.mon.2] Sistema de métricas

Medidas de Protección (17):

[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 dispositivos portátiles

[mp.eq.4] Otros dispositivos conectados a la red.

[mp.com] Protección de las comunicaciones

[mp.com.1]Perímetro seguro

[mp.com.2]Protección de la confidencialidad

[mp.si] Protección de los soportes de información

[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.3] Firma electrónica

[mp.info.5] Limpieza de documentos

[mp.info.6] Copias de seguridad (backup)

[mp.s] Protección de los servicios

[mp.si.1] Protección del correo electrónico

[mp.s.3] Protección de la navegación web

4. CRITERIOS DE APLICACIÓN DE MEDIDAS

4.1 [OP.PL.1] Análisis de riesgos

Automatizado en Gobernanza. Para su desarrollo se han analizado las necesidades de seguridad, los recursos que se disponen y contemplando las vulnerabilidades y amenazas a las que se ven expuestos los sistemas.

4.2 [OP.ACC.6] Mecanismo de autenticación (usuarios de la organización)

Para el acceso local al sistema de información de la entidad serán de aplicación los requisitos de categoría BÁSICA, en caso de aplicación del Refuerzo R1-Contraseñas, este mecanismo de autenticación será válido en todos los casos.

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

Los eventos y actividades de los usuarios requeridos serán la de los usuarios en los servidores.

4.4 [MP.COM.1] Perímetro Seguro

En caso de que no exista red, los equipos tendrán configurado el firewall del sistema operativo.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL