centro criptológico nacional

Perfil de Cumplimiento Específico
CCN-STIC 881A

Perfil de Cumplimiento Específico Universidades

Mayo 2022

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

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.07.08 17:38:54 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-075-2

Fecha de Edición: mayo de 2022
Personal de la CRUE y la empresa CIES han participado en la realización y modificación del presente documento y sus anexos.

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

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y las telecomunicaciones (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 311/2022 por el que se regula el Esquema Nacional de Seguridad, 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 2022

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.

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 311/2022, de 3 de mayo, 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 universidades 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 para Universidades que permita la implantación del ENS en las mismas, con necesidades de seguridad de categoría MEDIA.

2. 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 Específico, 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[1]
Categoría	aplica	aplica	aplica	org.1	MEDIA
Categoría	aplica	aplica	aplica	org.2	MEDIA
Categoría	aplica	aplica	aplica	org.3	MEDIA
Categoría	aplica	aplica	aplica	org.4	MEDIA
Categoría	aplica	+ R1	+ R2	op.pl.1	MEDIA
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	MEDIA
Categoría	aplica	aplica	aplica	op.pl.3	MEDIA
D	aplica	+ R1	+ R1	op.pl.4	MEDIO
Categoría	n.a.	aplica	aplica	op.pl.5	MEDIA
T A	aplica	+ R1	+ R1	op.acc.1	MEDIO
C I T A	aplica	aplica	+ R1	op.acc.2	MEDIO
C I T A	n.a.	aplica	+ R1	op.acc.3	MEDIO
C I T A	aplica	aplica	aplica	op.acc.4	MEDIO
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	MEDIO (+R5) *
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	MEDIO
Categoría	aplica	aplica	aplica	op.exp.1	MEDIA
Categoría	aplica	aplica	aplica	op.exp.2	MEDIA
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	MEDIA
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	MEDIA
Categoría	n.a.	aplica	+ R1	op.exp.5	MEDIA
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	BÁSICA (+ R4)*
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	MEDIA
Categoría	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	MEDIA
Categoría	aplica	aplica	aplica	op.exp.9	MEDIA
Categoría	aplica	+ R1	+ R1	op.exp.10	MEDIA
Categoría	n.a.	aplica	aplica	op.ext.1	MEDIA
Categoría	n.a.	aplica	aplica	op.ext.2	MEDIA
Categoría	n.a.	n.a.	aplica	op.ext.3	N/A[2]
Categoría	n.a.	aplica	+ R1	op.ext.4	MEDIA
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	MEDIA
D	n.a.	aplica	aplica	op.cont.1	MEDIO
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	MEDIA
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	MEDIA
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	BÁSICA (+R1) *

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

[2] N/A- No Aplica

Dimensiones					
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación[1]
Categoría	aplica	aplica	aplica	mp.if.1	MEDIA
Categoría	aplica	aplica	aplica	mp.if.2	MEDIA
Categoría	aplica	aplica	aplica	mp.if.3	MEDIA
D	aplica	+ R1	+ R1	mp.if.4	MEDIO
D	aplica	aplica	aplica	mp.if.5	MEDIO
D	n.a.	aplica	aplica	mp.if.6	MEDIO
Categoría	aplica	aplica	aplica	mp.if.7	MEDIA
Categoría	n.a.	aplica	aplica	mp.per.1	MEDIA
Categoría	aplica	+ R1	+ R1	mp.per.2	BÁSICA*
Categoría	aplica	aplica	aplica	mp.per.3	MEDIA
Categoría	aplica	aplica	aplica	mp.per.4	MEDIA
Categoría	aplica	+ R1	+ R1	mp.eq.1	MEDIA
A	n.a.	aplica	+ R1	mp.eq.2	MEDIO
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	MEDIO
C	aplica	+ R1	+ R1	mp.eq.4	BAJO*
Categoría	aplica	aplica	aplica	mp.com.1	MEDIA
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	MEDIO
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	MEDIO
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	MEDIA
C	aplica	aplica	aplica	mp.si.1	MEDIO
C I	n.a.	aplica	+ R1 + R2	mp.si.2	MEDIO (+R2) *
Categoría	aplica	aplica	aplica	mp.si.3	MEDIA
Categoría	aplica	aplica	aplica	mp.si.4	MEDIA
C	aplica	+ R1	+ R1	mp.si.5	MEDIO
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIA
Categoría	aplica	+ R1	+ R1	mp.sw.2	BÁSICA*
Categoría	aplica	aplica	aplica	mp.info.1	MEDIA
C	n.a.	aplica	aplica	mp.info.2	MEDIO
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	MEDIO
T	n.a.	n.a.	aplica	mp.info.4	ALTO*
C	aplica	aplica	aplica	mp.info.5	MEDIO
D	aplica	+ R1	+ R1 + R2	mp.info.6	MEDIO
Categoría	aplica	aplica	aplica	mp.s.1	MEDIA
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	MEDIA
Categoría	aplica	aplica	+ R1	mp.s.3	MEDIA
D	n.a.	aplica	+ R1	mp.s.4	MEDIO

2.1 MEDIDAS DE APLICACIÓN

De las 73 medidas de seguridad definidas en el Anexo II del RD 3/2010, **aplican un total de 69 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 (29):

[op.pl] Planificación

[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 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.5] Mecanismo de autenticación (usuarios externos)

[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

[op.exp.3] Gestión de la configuración de seguridad

[op.exp.4] Mantenimiento y actualizaciones de seguridad

[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

[op.exp.9] Registro de la gestión de incidentes

[op.exp.10] Protección de claves criptográficas

[op.ext] Servicios externos

[op.ext.1] Contratación y acuerdos de nivel de servicio

[op.ext.2] Gestión diaria

[op.ext.4] Interconexión de sistemas

[op.nub] Servicios en la nube

[op.nub.1] Protección de servicios en la nube

[op.mon] Monitorización del sistema

[op.mon.1] Detección de intrusión

[op.mon.2] Sistema de métricas

[op.mon.3] Vigilancia

Medidas de Protección (36):

[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.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.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.1] Marcado de soportes

[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 de aplicaciones

[mp.sw.2] Aceptación y puesta en servicio

[mp.info] Protección de la información

[mp.info.1] Datos personales

[mp.info.2] Calificación de la información

[mp.info.3] Firma electrónica

[mp.info.4] Sellos de tiempo

[mp.info.5] Limpieza de documentos

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

[mp.s] Protección de los servicios

[mp.s.1] Protección del correo electrónico

[mp.s.2] Protección de servicios y aplicaciones web

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

[mp.s.4] Protección frente a denegación de servicio

3. CRITERIOS DE APLICACIÓN DE MEDIDAS

3.1 [OP.ACC.5] Mecanismos de autenticación (usuarios externos)

Para el acceso a aquellos servicios que manejan información cuya dimensión Confidencialidad [C] se haya valorado a nivel BAJO[3], podrán aplicarse los requisitos de categoría BÁSICA, más el refuerzo R5- Registro.

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

Serán de aplicación los requisitos de categoría BÁSICA, siendo de aplicación también el "Refuerzo R4 – Capacidad de respuesta en caso de incidente":

- [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - Endpoint Detection and Response).

[3] Ver apartado "2. VALORACIÓN DE ACTIVOS ESENCIALES: SERVICIOS E INFORMACIÓN", de la Guía CCN-STIC 881 - Anexo II. Plan_Adecuación Universidades.

3.3 [OP.MON.3] Vigilancia

Serán de aplicación los requisitos de categoría BÁSICA, siendo de aplicación también el "Refuerzo R1 – Correlación de eventos":

- [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

3.4 [MP.PER.2] Deberes y obligaciones

Serán de aplicación los requisitos de categoría BÁSICA.

3.5 [MP.EQ.4] Otros dispositivos conectados a la red

Serán de aplicación los requisitos de nivel BAJO.

3.6 [MP.SI.2] Criptografía

A los requisitos de nivel MEDIO, se le añadirá el "Refuerzo R2 – Copias de seguridad":

- [mp.si.2.r2.1] Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

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

Cuando las aplicaciones no estén destinadas a gestionar servicios corporativos podrían ser de aplicación los requisitos de categoría BÁSICA.

3.8 [MP.INFO.4] Sellos de tiempo

Serán de aplicación los requisitos de nivel ALTO, para aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro. En caso contrario, esta medida no será de aplicación.

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