

CCN-STIC 890A

Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (Entidades Locales)



Noviembre 2025

Edita:



© Centro Criptológico Nacional, 2025

Fecha de Edición: noviembre de 2025

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	4
2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO	4
2.1 SERVICIOS PRESTADOS POR LOS AYUNTAMIENTOS DE HASTA 2.000 HABITANTES 5	
2.2 SERVICIOS PRESTADOS POR LOS AYUNTAMIENTOS MAYORES DE 2.000 HABITANTES Y HASTA 5.000 HABITANTES.....	7
2.3 SERVICIOS PRESTADOS POR LAS ENTIDADES LOCALES MENORES	7
2.4 SERVICIOS PRESTADOS POR AYUNTAMIENTOS (O AGRUPACIONES) DE HASTA 5.000 HABITANTES CON VALORACIÓN MÁS ELEVADA EN ALGUNA DE SUS DIMENSIONES	8
2.4.1 SERVICIOS DE COMPETENCIA MUNICIPAL	8
2.4.2 SERVICIOS DE COMPETENCIA MUNICIPAL INCLUIDOS CON LOS ANEXOS I Y II DE LA DIRECTIVA NIS2.....	9
3. DECLARACIÓN DE APLICABILIDAD	10
3.1 MEDIDAS DE APLICACIÓN	12
4. CRITERIOS DE APLICACIÓN DE MEDIDAS.....	14
4.1 [OP.PL.1] ANÁLISIS DE RIESGOS	14
4.2 [OP.ACC.6] MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN) 14	
4.3 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD	14
4.4 [OP.CONT.2] PLAN DE CONTINUIDAD.....	14
4.5 [MP.IF.1] ÁREAS SEPARADAS Y CONTROL DE ACCESO	15
4.6 [MP.COM.1] PERÍMETRO SEGURO.....	15
4.7 [MP.INFO.6] COPIAS DE SEGURIDAD	15

1. INTRODUCCIÓN

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) en 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 determina una postura de seguridad conforme a 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 (RD 311/2022), 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 proporcionales en relación con el contexto de la amenaza, nivel de madurez, riesgo residual asumible y recursos disponibles.

A tal fin, tras un análisis de riesgos contemplando las dificultades, brechas de seguridad, riesgos asociados y las potenciales 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 Fundamentales de Seguridad (PCE-RFS) que permita la implantación del ENS en las mismas.

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

El objetivo que se persigue con el Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (PCE-RFS) es posibilitar el cumplimiento del Esquema Nacional de Seguridad (ENS) para categoría BÁSICA de los sistemas de información que dan soporte a la tramitación de servicios e información cuando su valoración, realizada conforme al anexo I del RD ENS 311/2022, es de nivel bajo en todas las dimensiones de seguridad (C- Confidencialidad, I- Integridad, T- Trazabilidad, A- Autenticidad, D- Disponibilidad). Este perfil se destina a 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 requisitos fundamentales de seguridad empleando la metodología eficiente de certificación en el ENS automatizada en la Plataforma de Gobernanza (μ CeENS).

Los certificados expedidos con anterioridad a la fecha de publicación de la actualización de este PCE se mantendrán vigentes hasta su fecha de expiración.

En todo caso, este PCE tiene un carácter transitorio, las entidades dentro del alcance deberán continuar mejorando la seguridad de la información hasta alcanzar el nivel correspondiente a la categorización de sus servicios e información, por lo que, pasado este primer hito en las siguientes certificaciones podrán acogerse al PCE que les corresponda o al modelo estándar de adecuación del ENS.

En caso de que alguna de las entidades dentro del alcance de este PCE preste servicios y/o información cuya valoración, realizada conforme al anexo I del RD ENS 311/2022, sea de nivel medio/alto en alguna de las dimensiones de seguridad (C- Confidencialidad, I- Integridad, T- Trazabilidad, A- Autenticidad, D- Disponibilidad) y quiera aplicar las medidas de este PCE, debe comprometerse a mejorar la seguridad de su sistema de información de forma progresiva hasta alcanzar el nivel de seguridad que le corresponde. En el Anexo III. Compromiso de mejora del sistema de información, se ofrece un modelo para manifestarlo.

Como ejemplo se consideran servicios valorados en algunas de sus dimensiones de nivel medio/alto los siguientes:

- Padrón de habitantes.
- Sociosanitarios (servicios sociales, aplicación ley dependencia, discapacidad...);
- Gestión tributaria.

La exclusión de estos servicios se debe a las especiales características que la distinta legislación atribuye, bien al propio servicio o a la información, p.e., por requerir mayor confidencialidad de la información (servicios sociales o sociosanitarios o la información tributaria).

El alcance será el sistema de información, que da soporte a la tramitación de los servicios y la información, de las siguientes entidades:

- Ayuntamientos de menos 5.000 hab. y agrupaciones de estos municipios (p.e. mancomunidades que presten servicios culturales o deportivos) siempre que presten todos o alguno de los servicios incluidos en el PCE.
- Entidades locales menores (artículo 24 y ss. de la Ley 5/1985, de 2 de abril, reguladora de las Bases de Régimen Local como caseríos, parroquias, aldeas, barrios, anteiglesias, pedanías...) que presten todos o alguno de los servicios incluidos en el PCE.

2.1 Servicios prestados por los Ayuntamientos de hasta 2.000 habitantes

A continuación, se describen los servicios e información para los **Ayuntamientos de hasta 2.000 habitantes**, basado en el análisis de los artículos 25, 26 y 27 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, considerando que se

trata de entidades locales de pequeño tamaño que por sus características carecen de recursos para prestar servicios adicionales.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
Servicios finalistas				
S01	Urbanismo	Gestión del planeamiento, licencias y autorizaciones, expropiaciones	Planeamiento	Planeamiento
			Licencias y autorizaciones	Expedientes de tramitación: Licencias Urbanismo Expropiaciones
S02	Promoción económica municipal	Diversas actuaciones de promoción del municipio incluyendo las culturales, deportivas, promoción del turismo, económica local	Mercados y abastos	Gestión de actividades comerciales (abastos y mercado)
			Otras acciones de promoción económica (turismo, ferias...)	Gestión de actividades de promoción económica en turismo, ferias, venta ambulante
S03	Actividades culturales y deportivas	Servicios vinculados a la promoción cultural y deportiva en la entidad	Cultura	Gestión de actividades culturales
			Deportes	Gestión de instalaciones deportivas
S04	Servicios funerarios	Servicios de cementerio público		Expedientes adquisición tumbas y personas fallecidas
S05	Medioambiente	Gestión del medioambiente urbano	Control de animales domésticos	Expedientes de registro y control de animales
S06	Personal	Gestión de los RRHH municipales		Expedientes de personal
S07	Servicios Generales (Secretaría _Intervención)	Gestión de los expedientes municipales de diversa índole	Secretaría (informes, control de actas, declaraciones de bienes e intereses, libro decretos)	Informes, actas, declaraciones de bienes, grabaciones de plenos, libro decretos
			Intervención (gestión presupuestaria, cuenta general)	Gestión presupuestaria
			Tesorería (ingresos/pagos)	Ingresos y pagos
			Sistema de cumplimiento: Protección de datos, Transparencia (web, derecho de acceso), participación ciudadana.	Gestión de las obligaciones de la normativa
			Contratación/compras	Expedientes de contratación: propuestas, memoria, ofertas

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
			Archivo	Archivo de expedientes municipales

2.2 Servicios prestados por los Ayuntamientos mayores de 2.000 habitantes y hasta 5.000 habitantes

A continuación, se describen **otros servicios adicionales a los indicados en el apartado anterior que pueden prestar los Ayuntamientos de más de 2.001 hab.** En este caso se toma como referencia también la sentencia del Tribunal Supremo Sala de lo Contencioso-Administrativo, (Sección Quinta) núm. 1.642/2024, de 16 de octubre (ECLI:ES:TS:2024:5003, donde se indica que el alcantarillado es obligatorio para los Ayuntamientos que cuenten con núcleos de población superiores a los 2.000 habitantes):

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S08	Infraestructuras	Gestión de obras en diversas infraestructuras municipales	Obras menores en el municipio	Gestión de solicitudes, realización obras menores
			Alcantarillado	Gestión de solicitudes de alcantarillado y reparaciones

2.3 Servicios prestados por las Entidades Locales Menores

A continuación, se describen los **servicios que pueden prestar las Entidades Locales Menores** (caseríos, parroquias, aldeas, barrios, anteiglesias, juntas vecinales o concejos, pedanías, lugares, anejos o parroquias rurales, etc.). Si bien existe una casuística variada de este tipo de entidades y de los servicios, se toma como referencia el contenido del artículo 38 del Real Decreto Legislativo 781/1986, de 18 de abril, por el que se aprueba el texto refundido de las disposiciones legales vigentes en materia de Régimen Local.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
-----	-------------------------	--------------------------	---	--------------------------

S01	Reparación de infraestructuras	La construcción, conservación y reparación de fuentes, lavaderos y abrevaderos	N/A	Expedientes de obras solicitudes de reparación
S02	Control de espacios públicos	La policía de caminos rurales, montes, fuentes y ríos	N/A	Gestión de permisos de paso y control
S03	Gestión medioambiental	La limpieza de calles	N/A	Expedientes de obras solicitudes de reparación Solicitudes Control y gestión de aprovechamientos comunales
		La mera administración y conservación de su patrimonio, incluido el forestal, y la regulación del aprovechamiento de sus bienes comunales	N/A	
S04	Obras menores	La ejecución de obras y la prestación de servicios comprendidos en la competencia municipal	N/A	Expedientes de obras solicitudes de reparación

2.4 Servicios prestados por Ayuntamientos (o agrupaciones) de hasta 5.000 habitantes con valoración más elevada en alguna de sus dimensiones

En este apartado, se relacionan a modo de ejemplo, servicios valorados en algunas de sus dimensiones de nivel medio/alto.

2.4.1 Servicios de competencia municipal

A continuación, se describen aquellos servicios que pueden prestar los Ayuntamientos (o agrupaciones de estos) cuya valoración en alguna de sus dimensiones puede ser media/alta, por disponer de especiales requisitos sobre la confidencialidad, integridad o autenticidad o por tratarse categorías especiales de datos según la legislación que los regula.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S09	Padrón de habitantes	Gestión del Padrón	No aplica subservicio	Altas, bajas y modificaciones
S10	Servicios sociales de primera intervención	Asistencia urgente	No aplica subservicio	Expedientes de gestión de ayudas de primera intervención con personas del municipio

2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2

A continuación, se describen los servicios prestados por las Entidades Locales de pequeño tamaño que se encuentran incluidos¹ en los anexos I y II de la Directiva NIS2 y la norma de transposición.

SERVICIO EELL	Descripción del servicio	COD	SERVICIOS NIS2	NIS2
Medioambiente Urbano	Gestión de los expedientes relacionados entre otros con la Gestión y tratamiento de residuos	S21	Gestión de residuos	ANEXO II
Abastecimiento de agua potable a domicilio y evacuación y tratamiento de aguas residuales	Abastecimiento de agua y saneamiento que garantiza el consumo de agua en los hogares. (El ciclo se inicia con la captación y potabilización del agua, posteriormente es distribuida para su consumo y finalmente, las aguas residuales son depuradas en la EDAR para que puedan ser devueltas al río sin contaminar)	S22	Gestión agua potable	ANEXO I
		S23	Gestión aguas residuales	ANEXO I
Tráfico, estacionamiento de vehículos y movilidad. Transporte colectivo urbano	Gestión del área de tráfico (multas, alegaciones, pago) y del transporte público	S24	Transporte por carretera: autoridades viarias	ANEXO I

A continuación, se detallan los servicios e información.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S21	Gestión de residuos	Recogida, el transporte, la valorización y la eliminación de los residuos, incluida la vigilancia de estas operaciones, así como el mantenimiento posterior al cierre de los vertederos	No aplica subservicio	Gestión de expedientes relacionados con el servicio

¹ Aunque ciertos servicios puedan estar incluidos en los Anexos I y II de NIS2, esto no implica necesariamente que la entidad quede bajo su alcance, ya que factores adicionales, como el tamaño de la población u otros criterios, también determinan dicha aplicabilidad.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que <u>podrían</u> incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S22	Agua potable	Suministradores y distribuidores de aguas destinadas al consumo humano	No aplica subservicio	Gestión de expedientes relacionados con el servicio
S23	Alcantarillado	Recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales	No aplica subservicio	Gestión de expedientes relacionados con el servicio
S24	Transporte por carretera: autoridades viarias	Planificación, el control o la gestión de las carreteras en el ámbito territorial de su competencia; control de la gestión del tráfico	No aplica subservicio	Información sobre la gestión del tráfico y videovigilancia

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 ²	Ref
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	4.1
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	

² 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				Control	Aplicación ²	Ref
Afectadas	CAT B	CAT M	CAT A			
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	BAJO	
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	BAJO	4.2
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	4.3
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 (*)	4.4
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	BÁSICA	4.5
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	MEDIO	
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	BÁSICA	
C	aplica	+ R1	+ R1	mp.eq.4	BAJO	
Categoría	aplica	aplica	Aplica	mp.com.1	BÁSICA	4.6
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	

Dimensiones				Control	Aplicación ²	Ref
Afectadas	CAT B	CAT M	CAT 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	
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	BAJO	
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	4.7
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	

■ Detalles del criterio específico de aplicación de la media en el apartado 4 de este documento

■ Se considera que la medida no será de aplicación al PCE RFS

3.1 MEDIDAS DE APLICACIÓN

De las 73 medidas de seguridad definidas en el Anexo II del ENS, **aplican un total de 38^{*3} 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 (15):

- [op.pl] Planificación
- [op.pl.1] Análisis de riesgos
- [op.pl.3] Adquisición de nuevos componentes
- [op.acc] Control de acceso

³ Número aproximado de medidas que aplican

- [op.acc.1] Identificación
- [op.acc.2] Requisitos de acceso
- [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.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 (19):

- [mp.if] Protección de las instalaciones e infraestructuras
 - [mp.if.1] Áreas separadas y control de acceso
- [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.2] Bloqueo de puesto de trabajo
 - [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 el Portal de Gobernanza (<https://gobernanza.ccn-cert.cni.es/>). 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)

Se recomienda que, aunque el acceso al equipo se realice desde una zona controlada⁴, se implemente el Refuerzo R2 – Contraseña más otro factor de autenticación (múltiple factor de autenticación –MFA–), con el fin de incrementar el nivel de protección frente a accesos no autorizados, especialmente en aquellas entidades que presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2 (véase apartado del presente PCE “**2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2**”).

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 [op.cont.2] Plan de continuidad

En el caso de que las entidades a las que sea de aplicación el presente PCE presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2 (véase

⁴ Se entiende por zona controlada aquella en la que al usuario se le ha requerido una autenticación previa, mediante un control de acceso formalizado a las instalaciones, y en la que se han aplicado los requisitos de seguridad necesarios antes de permitir el acceso al equipo.

apartado del presente PCE “**2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2**”) se deberán implementar mecanismos efectivos de continuidad que garanticen la disponibilidad y resiliencia de dichos servicios ante incidentes que puedan comprometer su operatividad.

El modelo de referencia para el desarrollo de estos planes puede encontrarse en la Guía CCN-STIC-890 Anexo IV. Plan de Continuidad, el cual debe ser adaptado por cada entidad según su estructura y necesidades específicas. Este modelo proporciona una base para diseñar e implementar un plan de continuidad robusto, abarcando todas las acciones necesarias para garantizar que los servicios esenciales puedan mantenerse operativos o recuperarse en el menor tiempo posible.

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

En caso de que no se disponga de Centro de Proceso de Datos (CPD), el equipamiento se instalará, en la medida de lo posible, en áreas que aseguren que solo el personal autorizado tenga acceso a ellas.

4.6 [mp.com.1] Perímetro Seguro

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

4.7 [mp.info.6] Copias de seguridad

Para dar cumplimiento a los requisitos de la medida para nivel BAJO y el artículo 26. Continuidad de la actividad, existirá alguna copia de seguridad *offline* que se mantendrá actualizada y almacenada en un lugar seguro.