# Guía de Seguridad de las TIC
# CCN-STIC 890C

## Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (Entidades de menor tamaño)


Mayo 2026

Edita:





Fecha de Edición: mayo de 2026

**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 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 las amenazas, 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 (µCeENS).

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 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 los comprendidos en el Anexo I y II de la Directiva NIS2[1] independientemente de que se encuentren dentro de su ámbito de aplicación[2], así como del alcance del ENS, ya sean públicas o privadas.

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 Disponibilidad del servicio (agua potable, energía, etc.).

El alcance será el sistema de información que soporta la tramitación de los servicios y la información cuya valoración sea de nivel básico/bajo en todas sus dimensiones:

- Entidades públicas de pequeño tamaño y/o escasos recursos que no se encuentren en el ámbito de aplicación del PCE 890A.
- Pequeñas y medianas empresas[3] del sector privado, que presten dichos servicios al sector público, dentro del alcance del ENS.

Además, el presente PCE podrá utilizarse voluntariamente por aquellas entidades del sector privado que no se encuentren dentro del ámbito de aplicación del ENS.

[1]Directiva 2022/2225 el Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

[2] 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.

[3] La consideración de pequeña y mediana empresa será la establecida en la Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresa.

Las entidades acogidas al PCE podrán englobar los citados servicios en el siguiente: *S100 SERVICIO FINALISTA QUE ENGLOBA LAS FUNCIONES DE LA ORGANIZACIÓN*[4] *(servicio que se ofrece directamente al usuario o cliente final y que, por lo tanto, tiene un impacto directo en sus necesidades y expectativas).*

Para las entidades públicas dependientes, los servicios finalistas serán aquellos que haya sido delegados por la administración pública de la que son dependientes, siempre y cuando sean delegables conforme a lo establecido en el artículo 9 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

## 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[5] | 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 | |
| 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 | |

[4] 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.

[5] 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[5] | Ref |
| 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 | |
| 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 | |

| Dimensiones | | | | | | |
|---|---|---|---|---|---|---|
| Afectadas | CAT B | CAT M | CAT A | | | |
| | | | | Control | Aplicación[5] | Ref |
| 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*[6] 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

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.4] Proceso de gestión de derechos de acceso

[6] Número aproximado de medidas que aplican

[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 controlada[7], 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 se deberán implementar mecanismos efectivos de continuidad que garanticen la disponibilidad y resiliencia de dichos servicios ante incidentes que puedan comprometer su operatividad.

[7] 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.

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.