centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 890

Guía de Adecuación al ENS conforme al Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad

Noviembre 2025

Edita:

centro criptológico nacional

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

ÍNDICE

1. INTRODUCCIÓN

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), da respuesta a la intensificación de las ciberamenazas, los ciberincidentes y los nuevos vectores de ataque desarrollados en el ciberespacio.

El RD 311/2022 del ENS ha supuesto un cambio cultural, una nueva forma de entender la ciberseguridad para prevenir y contrarrestar la amenaza, que se ha plasmado en una evolución del marco legal, la actualización de la terminología (mínimo privilegio), la introducción de nuevos conceptos (vigilancia continua), la extensión del ámbito de aplicación del ENS y la definición de los Perfiles de Cumplimiento Específicos, validados por el Centro Criptológico Nacional (CCN), destinados a grupos de entidades similares desde el punto de vista de los riesgos.

Todo lo anterior ha facilitado la búsqueda de soluciones prácticas a los problemas diarios de los organismos ante la gestión de la ciberseguridad, que den lugar a estrategias simples y creativas que sean escalables. Como resultado de lo anterior, el Centro Criptológico Nacional ha desarrollado una metodología eficiente de certificación en el ENS, µCeENS[1], que facilita la obtención de la Certificación de Conformidad en el ENS en base a un Perfil de Cumplimiento Específico (PCE) y una postura de seguridad inicial adaptada a los recursos de las entidades: el Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (PCE-RFS).

De esta forma, con una metodología consolidada (µCeENS) y una postura de seguridad adaptada al medio (PCE-RFS) se facilita alcanzar una primera Certificación de conformidad en el ENS en categoría BÁSICA para los sistemas de organizaciones que presentan dificultades para adecuarse al Esquema Nacional de Seguridad. Esto se logra con el proceso automatizado en las herramientas de Gobernanza y el acompañamiento necesario para su éxito.

El Perfil de Cumplimiento de Requisitos Fundamentales de Seguridad sustituye al anterior Perfil de Cumplimiento de Requisitos Esenciales de Seguridad que estaba exclusivamente destinado a los sistemas de información que soportan la tramitación de servicios. En esta actualización se ha tenido en cuenta la Directiva 2022/2555 (NIS2) del 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. Los certificados expedidos con anterioridad a la fecha de publicación de la actualización de este PCE-RFS se mantendrán vigentes hasta su fecha de expiración.

2. OBJETO

El objeto de la presente guía es describir el proceso de adecuación al ENS de los sistemas de información de entidades, organismos y organizaciones con el propósito de obtener la Certificación de Conformidad en el ENS para categoría BÁSICA según el Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (PCE-RFS), empleando

[1] Dicha metodología está descrita en el documento *Metodología para alcanzar la Certificación de Conformidad con el ENS en base a un Perfil de Cumplimiento Específico (µCeENS).*

la Metodología Eficiente de Certificación en el ENS, automatizada en la Plataforma de Gobernanza (µCeENS).

El proceso completo aborda la gestión de la ciberseguridad de manera integral. Comienza con un diagnóstico de cumplimiento y continúa con el establecimiento de un Modelo de Gobernanza. Posteriormente, se elabora un Plan de Adecuación que define las tareas para la fase de Implantación. Al finalizar esta etapa, se podrá solicitar la Auditoría de Conformidad.

3. METODOLOGÍA EFICIENTE DE ADECUACIÓN AL ENS (µCeENS) Y EL PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD

El estudio exhaustivo de las amenazas y los principales riesgos a los que están sometidos los sistemas de información de las organizaciones ha dado lugar al PCE-RFS que consta de una Declaración de Aplicabilidad de 38 medidas de seguridad del Anexo II del RD 311/2022 que, una vez implementadas, son salvaguardas para proteger los activos esenciales (información y servicios) en los citados sistemas.

3.1 FASE PREVIA

3.1.1 Diagnóstico de Cumplimiento

Como fase previa, según recoge la metodología µCeENS, es necesario cumplimentar a través del Portal de Gobernanza el diagnóstico de cumplimiento, que evalúa la idoneidad del sistema de información para el empleo de la metodología µCeENS según el grado de cumplimiento de las medidas del PCE-RFS. Esto permitirá tener un punto de partida para establecer la hoja de ruta que finalmente solventará las deficiencias detectadas en los sistemas de información de la entidad, organismo u organización.

3.1.2 Resultados

El resultado del diagnóstico nos proporciona la información para determinar los documentos que son necesarios elaborar y los servicios de seguridad que se podrán solicitar.

3.1.3 Modelo de gobernanza

La gestión de la seguridad de los sistemas de información -definición, implantación y mantenimiento- exige establecer una estructura interna de la Seguridad, que debe determinar con precisión los diferentes actores que la conforman, sus responsabilidades y flujos de interacción considerando las particularidades y estructura de cada organismo, entidad u organización.

En este sentido, se parte de un modelo de Política de Seguridad y se propone un modelo de Gobierno por bloques de responsabilidad como se describe en los apartados 5.1.3.1 y 5.1.3.2 de esta Guía para que cada organismo, entidad u organización la adapte en función de su naturaleza y capacidad, designando los roles y constituyendo el Comité de Seguridad.

3.1.3.1 Modelo de gobernanza por bloques de responsabilidad

Destinado a organismos, entidades u organizaciones con dificultades para designar los roles requeridos en el artículo 13 del ENS.

- **Bloque de Gobierno:**
    - **Responsable de Gobierno**, cuyas funciones podrá ejercitar la Presidencia, Gerencia (u órgano similar) de la organización y que integra los siguientes roles y funciones ENS:
        - Comité de Seguridad de la Información.
        - Responsable de la Información.
        - Responsable del Servicio.

Estas competencias se pueden delegar en otros roles/órganos de la organización.

- **Bloque Supervisión:**
    - **Responsable de Supervisión**, cuyas funciones podrá ejercitar la Secretaría General de la Organización (u órgano similar) y que integra el siguiente rol ENS:
        - Responsable de la Seguridad.

En este bloque de supervisión se considerará también la figura del Delegado de Protección de Datos, apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

- **Bloque de Operación:**
    - **Responsable de Operación**, cuyas competencias podrá ejercitar un empleado de la organización y que integra el siguiente rol ENS:
        - Responsable del Sistema.

3.1.3.2 Modelo de gobernanza estándar

En aquellas organizaciones que dispongan de personal suficiente, se designarán los siguientes roles de seguridad y se constituirá un Comité de Seguridad de la información:

- **Roles o perfiles de Seguridad**
    - Responsable/s de Información.
    - Responsable de los Servicios.
    - Responsable de la Seguridad.

- Responsable del Sistema.

- **Comité de Seguridad de la Información**

  Se constituirá como un órgano colegiado, cuyos miembros serán:

  - Presidente/a o Secretario/a.
  - Vocales.
  - Responsable/s de Información.
  - Responsable/s de los Servicios.
  - Responsable de la Seguridad.
  - Responsable del Sistema.
  - Delegado de Protección de datos (DPD) con funciones de asesoramiento y supervisión en materia de protección de datos.

3.2 POLÍTICA DE SEGURIDAD

La organización de la seguridad definida en el apartado anterior se reflejará en la **Política de Seguridad**, documento de alto nivel, mediante el cual la organización define su compromiso respecto a la seguridad de los servicios (trámites electrónicos e información que estos gestionan).

En el Anexo de los PCE-RFS se proporcionan dos (2) modelos de Política de Seguridad en función del modelo de Gobernanza que más se adecúe a la organización.

3.3 CONFORMIDAD Y CUMPLIMIENTO

Gracias a la Metodología Eficiente de Certificación del ENS, aplicada de forma automatizada en la Plataforma de Gobernanza y utilizando los Requisitos Fundamentales de Seguridad, hemos logrado sintetizar y automatizar todo el proceso de Adecuación al ENS y la obtención de la Conformidad.

3.4 PLAN DE ADECUACIÓN

Según recoge la metodología µCeENS, el Plan de Adecuación estará determinado por:

- Alcance: el alcance de esta guía son los sistemas de información desde los que se prestan servicios cuya valoración sea de nivel bajo en todas sus dimensiones de seguridad o que presentan dificultades para adecuarse al Esquema y que se encuentren dentro del ámbito de aplicación del artículo 2 del RD 311/2022. Además, el presente PCE podrá utilizarse voluntariamente por aquellas entidades que no se encuentren dentro del ámbito de aplicación del Real Decreto.

- Categorización del Sistema: nos proporciona el documento de categorización del sistema compuesto por la categorización de los activos de servicios e información. Este requisito se encuentra detallado en el Anexo I del RD 311/2022.

- Declaración de Aplicabilidad: asociada al Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad, compuesto por las 38 medidas de aplicación. Este requisito se encuentra detallado en el Artículo 28 del RD 311/2022.

- Informe de riesgos: que muestra los riesgos residuales que presenta el sistema tras implantar las 38 medidas de seguridad que contempla el PCE. Este proceso de validación del PCE de Requisitos Fundamentales de Seguridad se realiza mediante el Módulo de Verificación de Perfiles de Cumplimiento en cuanto al Riesgo (MVPCR), que nos indica como son mitigados los riesgos que presenta el sistema de información con las mencionadas 38 medidas.

3.4.1 Alcance de los sistemas a certificar

La primera fase del Plan de Adecuación es identificar el alcance de los sistemas a certificar. Para ello, en cada PCE se describe un catálogo de los servicios prestados (junto con la información que manejan) entendiendo que se gestionan, con carácter general, en un único sistema de información.

3.4.2 Valoración y Categorización

La categoría de un sistema es el resultado de la valoración de las dimensiones de seguridad de los servicios e información alojados en el mismo, conforme a las instrucciones del Anexo I del RD 311/2022 que regula el ENS y teniendo en cuenta los criterios recogidos en la "Guía CCN-STIC-803 Valoración de Sistemas en el ENS", en el ANEXO III de cada PCE-RFS se encuentra una valoración de impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio, en cada una de las cinco dimensiones de seguridad Confidencialidad [C], Integridad [I], Trazabilidad [T], Autenticidad [A] y Disponibilidad [D]). Este impacto se mide en tres niveles BAJO, MEDIO o ALTO.

3.4.3 Declaración de Aplicabilidad Inicial

En este punto se estaría en condiciones de acogerse al PCE concreto, siendo entonces de aplicación la Declaración de aplicabilidad asociada que tendrá la consideración de inicial.

3.4.4 Análisis de riesgos

El análisis de riesgos será acorde a lo establecido en el Anexo II del RD 311/2022 que regula el ENS. El informe de riesgos se completará con la aceptación de los riesgos residuales del sistema, que serán aceptados formalmente por los Responsables de los Servicios y por los Responsables de la Información. Este proceso de validación del PCE de Requisitos Fundamentales de Seguridad se realiza mediante el Módulo de Verificación de Perfiles de

Cumplimiento en cuanto al Riesgo (MVPCR), que nos indica como los riesgos que presenta el sistema de información a certificar son mitigados con las mencionadas 38 medidas de seguridad.

3.4.5 Compromiso de mejora continua

La Alta Dirección de las entidades que apliquen el presente PCE 890 deberán firmar la asunción del riesgo residual y el compromiso de mejora continua mediante una hoja de ruta, en el Anexo III. Asunción del riesgo y compromiso de mejora de seguridad del sistema de información se aporta un modelo para manifestarlo.

3.4.6 Declaración de Aplicabilidad Definitiva

El análisis de riesgos validará los criterios de aplicación de las medidas del PCE, obteniéndose por tanto de la Declaración de Aplicabilidad Definitiva.

La Declaración de Aplicabilidad Definitiva-PCE se plasmará en un documento que será firmado por el Responsable de la Seguridad.

3.4.7 Elaboración del Plan de Implantación

Partiendo del Perfil de Cumplimiento Específico se elaborará la hoja de ruta con las tareas a realizar.

3.4.8 Ciclo de Mejora Continua

Las medidas de seguridad del sistema se reevalúan y actualizan periódicamente a través de acciones específicas que responden a los cambios del sistema (ej., incorporación de nuevos componentes o personal), y mediante tareas de mantenimiento sistemáticas (como la actualización de servidores, equipos y la revisión de accesos), que también contribuyen a un ciclo de mejora constante.

4. APOYO AL PROCESO DE CONTRATACIÓN PÚBLICA Y CONTROL DE LA CADENA DE SUMINISTRO

Para apoyar a las entidades públicas en sus procesos de contratación, se ofrecen el Anexo V. Modelos de Clausulado para la Contratación y el Anexo VI. Cuestionario de protección de cadena de suministro, disponibles también de forma automatizada en la Plataforma de Gobernanza. Estos documentos facilitan que los servicios y productos contratados cumplan con el Artículo 2 del RD 311/2022, que regula el ENS y estén alineados con Directiva (UE) 2022/2555 (NIS2).

5. ANEXOS

5.1 CCN-STIC 890 PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD

- CCN-STIC-890 Anexo V. Modelos de Clausulado para la Contratación Pública.
- CCN-STIC-890 Anexo VI. Cuestionario de Protección de Cadena de Suministro.

En los siguientes anexos están disponibles todos los documentos que se describen en el Apartado 3.4 PLAN DE ADECUACIÓN.

5.2 CCN-STIC 890A PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD PARA ENTIDADES LOCALES

- CCN-STIC-890 Anexo IA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.
- CCN-STIC-890 Anexo IB. Política de Seguridad según Modelo de Gobernanza estándar.
- CCN-STIC-890A Anexo II. Categorización Sistema.
- CCN-STIC-890A Anexo III. Compromiso Mejora sistema información.
- CCN-STIC-890A Anexo IV. Plan de Continuidad.

5.3 CCN-STIC 890C PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD PARA ENTIDADES DE MENOR TAMAÑO

- CCN-STIC-890 Anexo IA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.
- CCN-STIC-890 Anexo IB. Política de Seguridad según Modelo de Gobernanza estándar.
- CCN-STIC-890C Anexo II. Categorización Sistema.
- CCN-STIC-890C Anexo III. Compromiso Mejora sistema información.
- CCN-STIC-890C Anexo IV. Plan de Continuidad.