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 Esenciales de Seguridad

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

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 09:54:20 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-089-0

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

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

El nuevo ENS representa 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 esquema y la definición de los Perfiles de Cumplimiento Específico (PCE), 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 la metodología µCeENS, que hace uso de las novedades del nuevo ENS para facilitar la obtención de la Certificación de Conformidad en el ENS en base a un Perfil de Cumplimiento Específico (PCE).

En base a esta metodología descrita en el Abstract *Metodología para alcanzar la Certificación de Conformidad con el ENS en base a un Perfil de Cumplimiento Específico (PCE)*[1] empleando como instrumento que aporta las debidas medidas de seguridad el Perfil de Cumplimiento Específico de Requisitos Esenciales y como acompañamiento para su implantación, gestión y mantenimiento las soluciones de Gobernanza de la Ciberseguridad INES y AMPARO del Centro Criptológico Nacional, se ha definido un producto básico, mínimo viable, sin sacrificar la funcionalidad en el proceso, adaptado a las necesidades de ciberseguridad de las organizaciones contextualizado por una visión global de la amenaza, dando un apoyo y soporte dimensionado a los recursos y al nivel de madurez para alcanzar los objetivos identificados como prioritarios.

De esta forma, con una metodología consolidada (µCeENS) y una postura de seguridad adaptada al medio (Perfil de Cumplimiento de Requisitos Esenciales de Seguridad) se propicia alcanzar una Certificación en el ENS (categoría BÁSICA) para organizaciones con dificultades para adecuarse al Esquema, automatizada en las herramientas de Gobernanza de la Ciberseguridad, que proporciona el acompañamiento necesario para su consecución y con el principal objetivo de que estas dispongan de sistemas de información seguros para el ejercicio de sus competencias.

[1]https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/12204-nuevo-abstract-sobre-metodologia-para-alcanzar-la-certificacion-de-conformidad-con-el-ens-en-base-a-un-perfil-de-cumplimiento-especifico-pce.html

2. OBJETO

El objeto de la presente Guía es describir el proceso para conseguir la Adecuación al ENS de los sistemas de información de entidades, organismos u organizaciones con el propósito de obtener la Certificación de Conformidad para categoría BÁSICA según el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad empleando la metodología µCeENS.

El proceso completo aborda la gestión de la ciberseguridad de manera integral, partiendo de un diagnóstico de cumplimiento, estableciendo un Modelo de Gobernanza, elaborando el Plan de Adecuación que definirá las tareas a realizar en la fase de Implantación que, una vez finalizada, permitirá solicitar la Auditoría de Conformidad.

Para ello, a través de las soluciones de Gobernanza de la Ciberseguridad INES y AMPARO, y los servicios de seguridad en la modalidad ABS (Análisis y Perfilado Básico de Seguridad), se aporta un conjunto de cinco (5) actuaciones concretas para apoyar el proceso de obtención de Certificación de Conformidad:

(i) Entrega de un Modelo de Gobierno adaptado.

(ii) Entrega de un Plan de Adecuación.

- Carga automática del Plan de Adecuación con los Servicios y el Perfil de Cumplimiento Específico.

(iii) Asistencia técnica para realizar las tareas de la fase de implantación: cumplimentar el Marco Normativo e implementar las medidas técnicas necesarias.

- Documentación de seguridad cumplimentada (a falta de completar y revisar algunos datos por parte de la entidad, organismo u organización).
- Propuesta de medidas técnicas a implementar mediante un plan de acción en base a medidas proporcionadas por servicios de seguridad en modalidad ABS.
- Capacitación para el personal mediante un Plan de Formación a través de la plataforma ÁNGELES.

(iv) Solicitud de la Auditoría de Conformidad y su seguimiento.

(v) Ciclo de Mejora continua: tareas a realizar, frecuencia de las mismas, medidas de resiliencia.

3. METODOLOGÍA µCEENS Y EL PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD

El estudio exhaustivo de las amenazas y de los principales riesgos a los que están sometidos los sistemas de información de las organizaciones, ha dado lugar al Perfil de Cumplimiento Especifico de Requisitos Esenciales de Seguridad: una Declaración de Aplicabilidad de 35 medidas del Anexo II del RD 311/2022 que, una vez implementadas, sirven de salvaguardas para evitar los incidentes de seguridad que podrían

comprometer los activos esenciales (información y servicios) alojados en los citados sistemas.

La aplicación de la metodología µCeENS empleando los requisitos esenciales de seguridad ha permitido sintetizar y automatizar el proceso completo de adecuación al ENS y obtención de la conformidad.

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 Perfil de Cumplimiento Específico (PCE) de Requisitos Esenciales de Seguridad. 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.

A su vez, el uso de la metodología µCeENS exige superar el antedicho diagnóstico de cumplimiento para ser considerado "apto" como se explica en el apartado 3.1.2 ANÁLISIS DIAGNÓSTICO Y SALVAGUARDAS de la presente Guía, y poder continuar con el proceso de adecuación al ENS para obtener la Certificación de Conformidad para categoría BÁSICA según el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

3.1.2 ANÁLISIS DIAGNÓSTICO Y SALVAGUARDAS

Se analizan los **riesgos** y las **deficiencias detectadas,** así como su complejidad, y se valida mediante un sistema de semáforo que:

- Habilita o no los siguientes pasos para la obtención de la certificación de conformidad, en función del resultado.
- Indica qué medidas requieren de una acción compleja para su subsanación.
- Indica qué medidas se pueden subsanar con documentación y/o servicios ABS de seguridad.

Es así como el Portal de Gobernanza permite visualizar en función de los resultados y el sistema de semáforo la posibilidad de continuar con la adecuación como se describe a continuación:

- Rojo: no adecuado y requiere acción compleja.
- Ámbar: adecuado y tiene deficiencia subsanable.
- Verde: adecuado sin desviaciones.

Una vez que el sistema ha sido considerado "adecuado" o haya un compromiso formal de solventar las acciones complejas halladas a corto plazo, el resultado del diagnóstico nos proporciona información sobre los **documentos** que será necesario elaborar y los **servicios de seguridad** en la modalidad **ABS** (Análisis Básico de Seguridad) que subsanan las desviaciones detectadas.

3.2 MODELO DE GOBIERNO

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 3.2.1, 3.2.2 y 3.2.3 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.

Asimismo, y al objeto de facilitar las tareas de gobierno, es posible realizar un análisis de la madurez en ciberseguridad de la organización, mediante la evaluación de sus capacidades en los cinco (5) cinco ámbitos establecidos en el Portal de Gobernanza: Estrategia y política; Cultura; Talento; Cumplimiento normativo; y Marco legal y desarrollo normativo.

3.2.1 Modelo de Gobernanza por bloques de responsabilidad

Destinado a organismos, entidades u organizaciones pequeñas.

- **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.

3.2.2 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 Seguridad.
  - Responsable del Sistema.
- **Comité de Seguridad de la Información**

  Se constituirá como un órgano colegiado, cuyos miembros serán:
  - Presidente/a.
  - Secretario/a.
  - Vocales.
    - Responsable/s de Información.
    - Responsable/s de Servicios.
    - Responsable de Seguridad.
    - Responsable del Sistema.
    - Delegado de Protección de datos (DPD) con funciones de asesoramiento y supervisión en materia de protección de datos.

3.2.3 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).

El Anexo II de la presente guía proporciona dos (2) modelos de Política de Seguridad en función del modelo de Gobernanza que más se adecúe a la organización

- Anexo IIA. Política de Seguridad con modelo de Gobernanza por bloques de responsabilidad.
- Anexo IIB. Política de Seguridad con modelo de Gobernanza estándar.

3.3 CONFORMIDAD Y CUMPLIMIENTO

3.3.1 Plan de Adecuación

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

- Alcance: sistemas que soportan la tramitación de los servicios descritos en el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

- Categorización del Sistema, nos proporciona el documento de categorización del sistema compuesto por la categorización de los activos de servicios e información.

- Declaración de Aplicabilidad asociada al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad, compuesto por las 35 medidas de aplicación.

- Informe de Riesgos que muestra los riesgos residuales que presenta el sistema tras implantar las 35 medidas de seguridad que contempla el PCE. Este proceso de validación del PCE de Requisitos Esenciales 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 35 medidas siendo el riesgo residual asumible.

3.3.2 Implantación de seguridad

Una vez finalizado el Plan de Adecuación, se pasará a la Fase de Implantación de la Seguridad, mediante la elaboración de la documentación de seguridad y la implementación de las medidas técnicas junto con el despliegue de los Servicios de Seguridad en la modalidad ABS que sean necesarios.

La documentación de seguridad estará compuesta por:

- Registros de seguridad que facilitan el cumplimiento de las medidas de seguridad relacionadas con el inventario de activos o bien con la existencia de un registro de entrada y salida de soportes.

- Normativa de uso de medios electrónicos, que proporciona la normativa de seguridad, donde se establece la regulación de los recursos tecnológicos puestos a disposición de los usuarios del sistema, incluyendo el acuse de recibo de haberla leído y comprendido.

- El Documento de seguridad, que comprende la relación de todos los procedimientos de seguridad, asociados al cumplimiento de las 35 medidas de seguridad organizados por marco organizativo, marco operacional, medidas de

protección y normas de acceso remoto a formalizar con terceros con acceso al sistema de información, en caso de que fuera necesario.

- Plan de formación, que proporciona un plan de formación-concienciación.

- Política de firma electrónica, que facilita el disponer de una política que regule el uso de la firma electrónica, en este caso mediante la adhesión a la de la Administración General del Estado (AGE).

La implantación de las medidas de seguridad finalizará mediante la aportación de documentos que se han ido completando, debidamente aprobados y la aportación de evidencias de la implantación de las medidas, que se relaciona a continuación:

- Documentos:
  - Política de Seguridad aprobada.
  - Normativa de uso de medios electrónicos aprobada.
  - Documentación de Seguridad aprobado.
  - Informe de análisis de riesgos aprobado.
  - Archivo con el inventario de activos.
  - Informes de CLARA ABS.
  - Declaración de aplicabilidad aprobada.
  - Informe ejecutivo del organismo INÉS.
  - Valoración de servicios e información del sistema aprobada.
  - Categorización del sistema aprobada.
- Evidencias:
  - Acuse de leída la normativa de uso de medios electrónicos por parte de los usuarios.
  - Captura o evidencia del proceso de adquisición de nuevo componente[2].
  - Informe de EMMA ABS[2].
  - Captura o evidencia de solicitud del doble factor de autenticación en el acceso remoto.
  - Captura o evidencia de antivirus.
  - Captura o evidencia de herramienta utilizada para almacenar claves.
  - Plan de formación.
  - Captura o evidencia de borrado seguro.
  - Adhesión a la política de firma electrónica de la AGE.

[2] Opcional.

- Captura o evidencia del almacén de certificados.

También se podrán aportar todas aquellas evidencias adicionales que se consideren oportunas.

3.3.3 Conformidad

Una vez aportados todos los documentos y evidencias necesarias se procederá a iniciar el proceso conformidad del sistema de información en base al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad mediante el desarrollo de las siguientes actividades:

- Actividad 1: Solicitud de la auditoría de conformidad con el ENS. Los organismos entidades u organizaciones que hayan completado el proceso de adecuación a través de las herramientas que constituyen la plataforma de Gobernanza de la Ciberseguridad, estarán en condiciones de solicitar, desde dicha plataforma, la auditoría de conformidad con el ENS en base al Perfil de Cumplimiento Específico.
- Actividad 2: Evaluación documental y de evidencias. La Entidad de Certificación (EC) o el Órgano de Auditoría Técnica del Sector Público (OAT), tras recibir la solicitud de auditoría, procederá a la realización de la evaluación de las evidencias y la documentación aportada.
- Actividad 3: Expedición de la conformidad con el ENS. La EC o el OAT tras resolver acerca de la conformidad del sistema, expedirá la Certificación de Conformidad con el ENS en base al PCE reservándose el derecho a realizar una inspección.

3.4 MEJORA CONTINUA

3.4.1 Ciclo de Mejora Continua

La reevaluación y actualización periódica de las medidas de seguridad del sistema se consigue mediante acciones puntuales que se presentan cuando haya cambios en el sistema (nuevo componente en el sistema, nuevo personal, etc.) y la realización de tareas de mantenimiento del sistema (actualización de servidores, equipos, revisión de accesos, etc.) que incluye también tareas que garantizan el ciclo de mejora, como pueden ser las que se proporcionan en el Anexo VIII. Lista de Mantenimiento y Acciones Puntuales.

4. ANEXOS

En los Anexos de la presente guía están disponibles todos los documentos que se describen en el Apartado 3. Metodología µCeENS y el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

Se han clasificado en función del tipo de entidad y del Modelo de Gobierno (Bloques de Responsabilidad o Estándar).

4.1 CCN-STIC 890A PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD PARA ENTIDADES LOCALES.

4.1.1 Anexo I. Diagnóstico ENS.

4.1.2 Anexo IIA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.

Anexo IIB. Política de Seguridad con modelo de Gobernanza Estándar.

4.1.3 Anexo III. Categorización del Sistema.

4.1.4 Anexo IV. Declaración de Aplicabilidad.

4.1.5 Anexo V.A. Documento de Seguridad (para modelo de Gobernanza por Bloques de Responsabilidad).

Anexo V.B. Documento de Seguridad (para modelo de Gobernanza Estándar).

4.1.6 Anexo VI. Normativa de Uso de Medios electrónicos.

4.1.7 Anexo VII. Plan de Concienciación-Formación.

4.1.8 Anexo VIII. Lista de Mantenimiento y Acciones Puntuales.

4.1.9 Anexo IX. Adhesión a la Política de Firma electrónica de la AGE.

4.2 CCN-STIC 890B PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD PARA ORGANISMOS DEL SECTOR PÚBLICO.

4.2.1 Anexo I. Diagnóstico ENS

4.2.2 Anexo IIA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.

Anexo IIB. Política de Seguridad con modelo de Gobernanza Estándar.

4.2.3 Anexo III. Categorización del Sistema.

4.2.4 Anexo IV. Declaración de Aplicabilidad.

4.2.5 Anexo V.A. Documento de Seguridad (para modelo de Gobernanza por Bloques de Responsabilidad).

Anexo V.B. Documento de Seguridad (para modelo de Gobernanza Estándar).

4.2.6 Anexo VI. Normativa de Uso de Medios electrónicos

4.2.7 Anexo VII. Plan de Concienciación-Formación

4.2.8 Anexo VIII. Lista de Mantenimiento y Acciones Puntuales

4.2.9 Anexo IX. Adhesión a la Política de Firma electrónica de la AGE

4.3 CCN-STIC 890C PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD.

4.3.1 Anexo I. Diagnóstico ENS

4.3.2 Anexo IIA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.

Anexo IIB. Política de Seguridad con modelo de Gobernanza Estándar.

4.3.3 Anexo III. Categorización del Sistema.

4.3.4 Anexo IV. Declaración de Aplicabilidad

4.3.5 Anexo V.A. Documento de Seguridad (para modelo de Gobernanza por Bloques de Responsabilidad).

Anexo V.B. Documento de Seguridad (para modelo de Gobernanza estándar).

4.3.6 Anexo VI. Normativa de Uso de Medios electrónicos

4.3.7 Anexo VII. Plan de Concienciación-Formación

4.3.8 Anexo VIII. Lista de Mantenimiento y Acciones Puntuales

4.3.9 Anexo IX. Adhesión a la Política de Firma electrónica de la AGE

PUBLICACIONES DE DEFENSA

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