Metodología para alcanzar la Certificación de Conformidad con el ENS en base a un Perfil de Cumplimiento Específico (PCE)

Abstract: *µCeENS es una metodología innovadora que se beneficia de las novedades del RD 311/2022, de 3 de mayo, para facilitar la obtención de la Certificación de Conformidad en el Esquema Nacional de Seguridad (ENS) en base a un Perfil de Cumplimiento Específico (PCE).*

Contenido:

1. INTRODUCCIÓN

La publicación del 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, a los ciberincidentes y a los nuevos vectores de ataque desarrollados en el ciberespacio.

El nuevo ENS representa un cambio cultural, una nueva forma de entender la ciberseguridad, que se ha plasmado en una evolución del marco legal mediante 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 Específicos (PCE), validados por el Centro Criptológico Nacional, destinados a grupos de entidades similares desde el punto de vista de los riesgos.

Por otra parte, la acumulación de experiencias y el mejor conocimiento del estado de la seguridad nacional ha hecho necesario definir un modelo que facilite la adecuación al nuevo Esquema y la consecuente obtención de la certificación de conformidad.

Es así como surge **µCeENS, una metodología** innovadora que **se beneficia** 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).**

2. OBJETO

El objeto del presente documento es posibilitar el cumplimiento del ENS de los sistemas de información de organizaciones con limitaciones para abordar por si solas el proceso de adecuación para la obtención de la correspondiente Certificación de Conformidad.

3. DEFINICIÓN

µCeENS es una metodología que facilita alcanzar la Certificación de Conformidad con el ENS en base a un Perfil de Cumplimiento Específico (PCE) validado por el Centro Criptológico Nacional, complementado con servicios de seguridad.

4. METODOLOGÍA Y EXIGENCIA PREVIA

Una implementación factible del ENS para las antedichas organizaciones precisa de tres (3) componentes:

I. Un instrumento que aporte las debidas medidas de seguridad: Perfil de Cumplimiento Específico.

II. Una metodología para su implantación: µCeENS, y

III. Una herramienta que sirva de acompañamiento para su implantación, gestión y mantenimiento.

La metodología µCeENS se basa en proporcionar el **acompañamiento** y la asistencia necesaria para alcanzar la Certificación de Conformidad con el ENS desde la fase previa a la adecuación, hasta después de su obtención, todo ello automatizado en las herramientas de Gobernanza de la Ciberseguridad (INES-AMPARO).

Dentro del análisis previo, un elemento fundamental y discriminante lo constituye el **diagnóstico de cumplimiento**, que identifica las principales carencias de seguridad del sistema de información concernido conforme a un Perfil de Cumplimiento Específico, y que servirá como punto de partida para establecer la hoja de ruta que finalmente solventará las anomalías detectadas.

En definitiva, el uso de la metodología µCeENS exige superar el antedicho diagnóstico de cumplimiento para ser considerado “apto” y poder hacer uso de esta metodología.

4.1 DIAGNÓSTICO DE CUMPLIMIENTO

El objetivo del diagnóstico de cumplimiento persigue evaluar la idoneidad del sistema de información para el empleo de la metodología µCeENS.

Esta aproximación se instrumentaliza en dos (2) secciones: la primera, relativa a la arquitectura de seguridad del sistema de información de que se trate y, la segunda, que

permite evaluar el grado de cumplimiento de las medidas del Perfil de Cumplimiento Específico de aplicación.

Del diagnóstico de cumplimiento se obtiene la relación de desviaciones encontradas y su complejidad, mediante un procedimiento de validación por semáforo: rojo ("no apto": requiere acción compleja), ámbar ("apto": deficiencia subsanable) y verde ("apto": sin desviaciones).

Una vez que el sistema ha sido considerado "apto", o haya un compromiso formal de solventar las desviaciones halladas a corto plazo, se analiza el estado de cumplimiento de las medidas de seguridad y se proporciona la lista de documentos y/o servicios de seguridad que corrigen las desviaciones detectadas.

4.2 GOBIERNO

Para implementar la Gobernanza de la Ciberseguridad se elabora la Política de Seguridad y se define el modelo de Gobierno que mejor se adapte a la entidad de que se trate, designando los roles y responsabilidades, y constituyendo el Comité de Seguridad.

Asimismo, y al objeto de facilitar las tareas de gobierno, siempre es posible realizar un análisis de la madurez de la organización en dicho ámbito, mediante la evaluación de sus capacidades en cinco (5) dimensiones: estrategia y política, cultura, talento, marco legal y desarrollo normativo e implantación.

4.3 PLAN DE ADECUACIÓN

De cara a la implementación de medidas de seguridad y gestionar las expectativas asociadas, se aborda el plan de adecuación al ENS, que incluye:

- Alcance, identificando los servicios prestados y la información tratada por los mismos.
- Categoría del sistema, tras la valoración de las dimensiones de seguridad de los servicios e información identificados.
- Declaración de aplicabilidad asociada al Perfil de Cumplimiento Específico.
- Validación de la Declaración de Aplicabilidad, en base a un riesgo residual asumible, mediante MVPCR (Módulo de Verificación del PCE en cuanto al Riesgo).

4.4 IMPLANTACIÓN DE SEGURIDAD

La fase de implantación comprende la elaboración de la normativa y procedimientos de seguridad que constituyen el Marco Normativo en materia de ciberseguridad de la organización, la implementación de las medidas técnicas y el despliegue, si procede, de los servicios de seguridad.

5. PROCESO DE VERIFICACIÓN DE LA CONFORMIDAD

5.1 FASE 1. SOLICITUD DE LA AUDITORÍA DE CONFORMIDAD CON EL ENS

Las 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 asociado.

5.2 FASE 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.

5.3 FASE 3. EXPEDICIÓN DE LA CONFORMIDAD CON EL ENS

La EC o el OAT, y 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.

6. CICLO DE MEJORA CONTINUA

La gestión continua de la seguridad exigida por el ENS implica realizar tareas de mantenimiento y evaluaciones periódicas para vigilar los sistemas y mantener la correcta protección de los mismos. Asimismo, requiere que todo el personal que accede, opera o administra el sistema, así como los responsables definidos en el modelo de gobierno, se mantengan en formación constante.

La Plataforma de Gobernanza facilita dicha mejora continua, proporcionando listas de mantenimiento y asistencia para la formación y la evaluación de la capacidad de resiliencia de los sistemas ante las ciberamenazas.