Esquema Nacional de Seguridad
Aproximación al µCeENS

David Marciel Fernández

Abogado – Cumplimiento normativo
Compliance Officer – CESCOM®
Delegado de Protección de Datos – Esquema AEPD
Experto en ciberseguridad

Unive abogados
Una nueva forma de asesoramiento

conecta.unive.es / compliance@unive.es / info@unive.es

1. ¿Qué es µCeENS?

Definición:

- Es un **modelo, una metodología** que facilita la obtención de la Certificación de Conformidad en el ENS.
- Tiene en cuenta los **Requisitos de Seguridad definidos en un Perfil de Cumplimiento Específico** validado por el Centro Criptológico Nacional.

Acompañamiento en base a fases y actuaciones durante el proceso de la Certificación de Conformidad:

1. **Definición de un Modelo mínimo viable**.
2. **Diagnóstico de cumplimiento** en base a **Perfiles de Cumplimiento Específicos**.
3. **Gobierno**: Política de Seguridad, Gobernanza y Marco Normativo necesario.
4. **Herramientas de perfilado básico de seguridad (soluciones ABS)** como apoyo a la implementación técnica de seguridad, tareas de mantenimiento y recogida de evidencias.
5. **Mejor Continua** al propiciar el progreso y avance del nivel de implantación de la seguridad en las Organizaciones.

Desarrollo de la Metodología:

- **Automatización de los procesos en las herramientas de Gobernanza** para obtener la adecuación y la correspondiente Certificación de Conformidad en el ENS, conforme a un **Perfil de Cumplimiento Específico**, que se complementa con los servicios básicos de seguridad proporcionados por las soluciones del CCN en la modalidad ABS:.

Herramientas de Gobernanza:

Soluciones ABS:

David Marciel Fernández - valladolid@unive.es - 670 440 127

2. ¿Quienes puede beneficiarse de µCeENS?

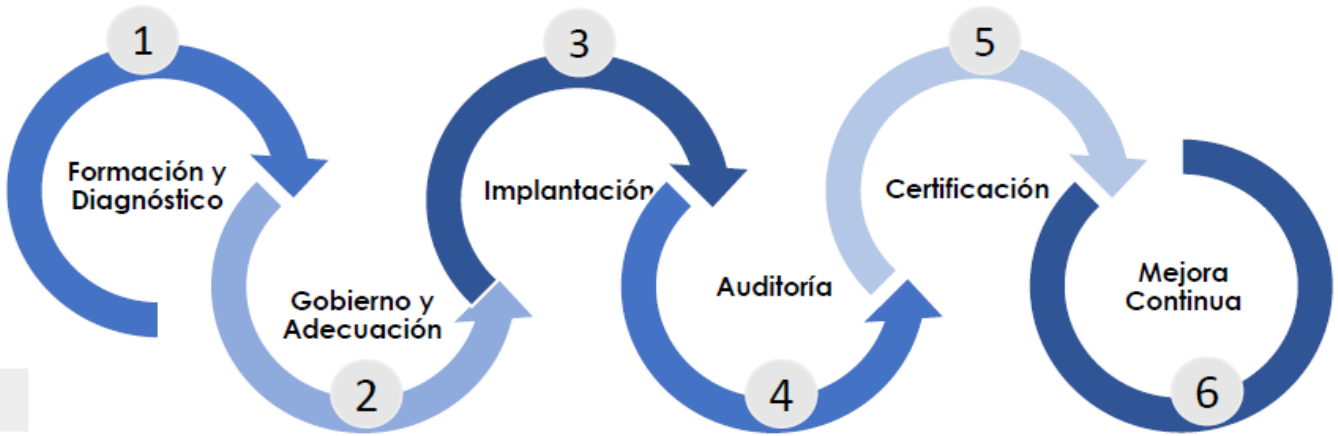
Alcance determinado para Entidades u Organizaciones con las siguientes características:

- **Dificultades para abordar la Adecuación al ENS**, tras analizar los riesgos y amenazas a los que están sometidos los sistemas.
- **Superar el Diagnóstico de Cumplimiento** del ENS (validación por semáforo)
- Cuyos **riesgos identificados** son **mitigados** con la implementación de un Perfil de Cumplimiento Específico (validación mediante el Módulo de Verificación de Perfiles de Cumplimiento en cuanto al Riesgo – **MVPCR**)

3. ¿Cómo se aplica µCeENS? (fases)

Implantación de la Metodología µCeENS mediante seis (6) fases

Planificación aproximada de cuatro (4) a seis (6) meses.



Alcance determinado para cada fase:

1. Formación en el ENS, de manera asíncrona, a través de la plataforma ÁNGELES

1.1 Diagnóstico de Cumplimiento para determinar la situación y posibilidad de abordar un proceso de adecuación al ENS.

2. Gobierno y Adecuación. Política de seguridad, establecer una estructura, determinar roles asignando responsabilidades y flujos de relación, inventario de activos, categorización, declaración de aplicabilidad e informe de riesgos.

3. Implementación de medidas, marco normativo, desarrollo procedimental, adopción de soluciones técnicas, recogida de evidencias y registros.

4. Auditoría de Certificación

5. Obtención de la certificación.

6. Mejora continua, progreso y avance del nivel de implantación, tareas de mantenimiento y acciones puntuales del sistema.

3. ¿Cómo se aplica µCeENS? (entregables)

Durante las fases de µCeENS se generan diferentes entregables:

1 Perfil de Cumplimiento Específico (PCE)

- Conjunto de medidas de seguridad 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

2 Informe de Resultados del Diagnóstico de cumplimiento

- Análisis de desviaciones indicando las medidas que requieren de una acción compleja para su subsanación o bien son subsanables con una implementación procedimental y/o servicios ABS de seguridad.

3 Modelo para la designación de Roles y Política de Seguridad

- Designación de los Responsables de Gobierno, Supervisión y Operación. Asignación de responsabilidades y establecimiento de flujos de interrelación.
- Aprobación de la Política de Seguridad de la Información.

4 Plan de Adecuación (Categorización del Sistema y Declaración de Aplicabilidad)

- **Categorización del Sistema**: propuesta de inventario de servicios-información y su valoración.
- **Declaración de Aplicabilidad**.
- **Informe de riesgo residual**.

5 Normativa de uso de medios electrónicos

- Regulación del uso de los recursos puestos a disposición del personal.

6 Marco Normativo de Seguridad

- Procedimientos que soportan el cumplimiento de las medidas.

7 Registro de Seguridad

- Modelo de registro de seguridad para el inventario de activos y de entrada y salida de soportes.

8 Lista de mantenimiento del sistema y acciones puntuales

- Medidas y acciones puntuales que propicien el mantenimiento y mejora continua de la seguridad.