# TEMA 48. SEGURIDAD DE SISTEMAS (2). EL ESQUEMA NACIONAL DE SEGURIDAD. ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD. ESTRATEGIA NACIONAL DE SEGURIDAD. CCN-STIC

Actualizado a 15/05/2023

## 1. ESQUEMA NACIONAL DE SEGURIDAD – ENS (RD 311/2022)

**3 principios:**

1) Alineación del ENS con el marco normativo.
2) Introducir la capacidad de ajustar los requisitos del ENS a determinados colectivos o ámbitos tecnológicos.
3) Mejorar la respuesta a incidentes, reducir vulnerabilidades y promover la vigilancia continua, alineado con la directiva NIS2.

**5 dimensiones ACIDT:** Autenticación, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.

**Ámbito subjetivo:**

- AGE + CCAA + EELL + Sector Público Institucional.
- Sistemas que tratan información clasificada.
- Sistemas de entidades del sector privado que presten servicios al sector público.

**7 principios básicos** (capítulo II del ENS):

1. Seguridad como proceso integral.
2. Gestión de la seguridad basada en los riesgos.
3. Prevención, detección, respuesta y conservación.
4. Existencia de líneas de defensa.
5. Vigilancia continua.
6. Reevaluación periódica.
7. Diferenciación de responsabilidades.

**Auditoría** (Cap. IV y Anexo III):

- Mínimo cada 2 años.
- En sistemas de nivel BAJO es suficiente con autoevaluación.
- Con carácter extraordinario, se realiza siempre que se produzcan modificaciones sustanciales en los sistemas de información.

**Estado de Seguridad** (Cap. IV): El Centro Criptológico Nacional (CCN) establece procedimientos para recopilar la información. La Comisión Sectorial de Administración Electrónica (CSAE) elabora el perfil general del estado de seguridad. Se desarrolla en una Instrucción Técnica de Seguridad (ITS).

**Respuesta a incidentes** (Cap. IV): Articulada a través del *Computer Emergency Response Team* del CCN (CCN-CERT), del ESPDEF-CERT y de INCIBE-CERT.

**Normas de conformidad** (Cap. V): Desarrolladas en una ITS.

**Categorización de los Sistemas** (Cap. VII y Anexo I)**:** Se categorizan los activos (información y servicios) de cada dimensión ACIDT en las categorías BÁSICA, MEDIA o ALTA en función del impacto que tendría un incidente de seguridad sobre la capacidad de la organización.

- La categoría de cada dimensión es la mayor de sus activos.
- La categoría del sistema es la mayor de sus dimensiones.

**Medidas de seguridad** (Anexo II)**:** Seleccionadas por la categoría del sistema y sus dimensiones ACIDT.

1) Marco organizativo: relacionado con la organización global de la seguridad.
2) Marco operacional: Protege la operación del sistema.
3) Medidas de protección: Protegen un activo en concreto.

**Declaración de Aplicabilidad** (Art. 28)**:** Obligatoria, formada por las medidas de seguridad seleccionadas.

## 2. GUÍAS CCN-STIC

La serie 800 es la relativa al ENS. Especialmente relevantes las siguientes guías:

- ✓ CCN-STIC-801. Responsabilidades y Funciones en el ENS – Define los diferentes roles.
- ✓ CCN-STIC-802. Auditoría del ENS.
- ✓ CCN-STIC-803. Valoración de Sistemas en el ENS – Desarrolla cómo realizar la categorización.
- ✓ CCN-STIC-804. ENS. Guía de implantación.
- ✓ CCN-STIC-805. Esquema Nacional de Seguridad. Política de seguridad de la información.
- ✓ CCN-STIC-806. Plan de Adecuación al ENS.
- ✓ CCN-STIC-808. Verificación de Cumplimiento del ENS – Publicada en noviembre de 2022.
- ✓ CCN-STIC-823. Utilización de servicios en la nube.
- ✓ CCN-STIC-824. Informe nacional del estado de seguridad de los sistemas TIC.
- ✓ CCN-CSTIC-830. Ámbito de aplicación del ENS.

Cabe destacar la publicación en 2018 de las guías:

- ✓ CCN-STIC-819. Medidas Compensatorias.
- ✓ CCN-STIC-834. Protección ante Código Dañino en el ENS.
- ✓ CCN-STIC-831. Registro de la actividad de los usuarios.
- ✓ CCN-STIC-837. ENS. Seguridad en Bluetooth.

Desde 2018 a 2023 se destacan las siguientes guías:

- ✓ CCN-STIC-888C. Configuración segura para Contenedores.
- ✓ CCN-STIC-809. Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento.
- ✓ CCN-STIC-881. Guía de Adecuación al ENS para Universidades.
- ✓ CCN-STIC-887F. Guía de respuesta a incidentes en AWS.
- ✓ Múltiples guías de configuración segura de servicios en la nube (AWS, Google, Microsoft, Nextcloud).

## 3. MEDIDAS DE SEGURIDAD

El ENS definido en el RD 311/2022 es más exhaustivo que el anterior RD en lo relativo a medidas de seguridad. Son destacables aquellas relacionadas con la protección de servicios en la nube, caracterización del puesto de trabajo, protección de la confiabilidad (teletrabajo), desarrollo de aplicaciones y otros dispositivos conectados a la red (IoT).

## 4. INSTRUCCIONES TÉCNICAS DE SEGURIDAD (ITS)

En el anterior ENS (RD 3/2010) se definía una lista de ITS a desarrollar. En el actual ENS no se especifica, si no que se deja abierta la creación de nuevas y la actualización de las existentes. Se publican por resolución de la SEDIA. Actualmente hay 4:

1) Informe del estado de la seguridad (actualizada en 2020).
2) Notificación de incidentes de seguridad (publicada en 2018).
3) Auditoría de la seguridad de los sistemas de información (publicada en 2018).
4) Conformidad con el ENS (publicada en 2016).

## 5. DIRECTIVA NIS2, UN ALTO NIVEL DE SEGURIDAD COMÚN EN LA UE

Publicada en el DOUE el 27/12/2022, la Directiva (UE) 2022/2555 deroga la anterior Directiva NIS.

NIS2 se fija 3 objetivos fundamentales:

1. Aumentar el nivel de ciberresiliencia.
2. Reducir incoherencias en resiliencia del mercado interior en los sectores cubiertos actualmente en la directiva NIS. Permite establecer sanciones que incluyen multas administrativas de hasta 10 millones de euros o 2% del volumen global del negocio.
3. Mejorar el nivel de conocimiento conjunto de la situación y la capacidad colectiva de prepararse y responder (creación de EU-CyCLONe).

La Agencia de la UE para la Ciberseguridad (ENISA) ve aumentadas sus responsabilidades: supervisión de la aplicación de NIS2; elaboración de un informe bianual sobre el estado de la ciberseguridad; mantenimiento de registros de vulnerabilidades de entidades establecidas en la UE.

## 6. ESTRATEGIA DE SEGURIDAD NACIONAL

Tras la estrategia de 2017, la nueva estrategia fue publicada en 2021. Su desarrollo normativo está en la Ley de Seguridad Nacional 36/2015.

Estructurada en 5 capítulos:

1) Seguridad global y vectores de transformación.
2) Una España segura y resiliente.
3) Riesgos y amenazas.
4) Un planeamiento estratégico integrado.
    - Establece tres objetivos:
        - Avanzar en materia de gestión de crisis.
        - Fortalecer la dimensión de seguridad.
        - Desarrollar la prevención, detección y respuesta frente a estrategias híbridas. Se definen tres ejes (**proteger**, **promover** y **participar**) que estructuran 33 líneas de acción.
5) Un Sistema de Seguridad Nacional y Gestión de Crisis.