MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PUBLICA

SECRETARIA GENERAL
DE ADMINISTRACIÓN DIGITAL

SOCINFO
sociedad de la información digital

Directiva NIS2 para la AAPP: Claves de Cumplimiento y su relación con el ENS

ENS para cumplimiento de NIS2

24 de enero de 2025

Miguel A. Amutio Gómez

Director de Planificación y Coordinación de Ciberseguridad
Secretaría General de Administración Digital
Secretaría de Estado de Función Pública
Ministerio para la Transformación Digital y de la Función Pública

Un marco legal crecientemente exigente

- Reglamento 910/2014 **identidad electrónica**…(eIDAS)
- Reglamento 2016/679 **Protección de datos RGPD**
- Directiva 2016/1148 **NIS Seguridad de las redes y S.I. (NIS)**
- Reglamento 2018/1724 **Pasarela Digital Única (SDG)**
- Reglamento 2018/1807 **Libre circulación datos no personales**
- Reglamento 2019/881 **Ciberseguridad**
- Directiva 2019/1024 **Datos abiertos y reutilización de la información**
- La **Estrategia de ciberseguridad de la UE** (JOIN(2020) 18 final)
- Reglamento 2021/887 **Centro Europeo de Competencias en Ciberseguridad**
- Reglamento 2554/2022 Resiliencia **sector financiero** (DORA)
- Directiva 2022/2555 **nivel común de ciberseguridad (NIS2)**
- Directiva 2022/2557 Resiliencia de **entidades críticas** (CER)
- Conclusiones Consejo sobre seguridad cadena de suministro
- Reglamento 2022/868 de Gobernanza de datos
- EU Policy on Cyber Defence
- Decisión de adecuación sobre el **marco de privacidad de datos entre la Unión Europea y Estados Unidos**
- Reglamento 2023/2841 **ciberseguridad instituciones UE**
- Reglamento 2023/2854 de Datos
- Reglamento 2024/903 **Europa Interoperable**
- Reglamento 2024/1183 **identidad electrónica** (eIDAS 2)
- Reglamento 2024/1689 de **Inteligencia Artificial**
- Esquema Europeo de Certificación **EUCC**
- **Acto de implementación** de la **Directiva NIS2**
- Reglamento 2024/2847**de ciber resiliencia** (CRA)
- Reglamento 2025/37 servicios de seguridad gestionados
- Reglamento 2025/38 de **Cibersolidaridad**
- Propuesta Reglamento **seguridad de la información instituciones UE**
- Propuestas de **Esquemas de Certificación** (EUCS…)

Fuente: Miguel A. Amutio

Contexto estratégico

- Centro Europeo de Competencias en Ciberseguridad (ECCC)
- Red de Centros Nacionales de Coordinación del ECCC
- Grupo de Cooperación NIS
- Red CyCLONe – European cyber Crises Liaison Organisation Network
- Joint Cyber Unit – Cooperación de comunidades de ciberseguridad
- Cooperación internacional en normas y especificaciones de ciberseguridad
- Cooperación con terceros países,
- …
- Multi Stakeholder Platform for ICT Standards
- CIO Network
- Grupo de expertos de Interoperabilidad
- Grupo de Coordinación de la Pasarela Digital Única (SDG)
- European Blockchain
- Grupo de expertos de eIDAS2
- …

- ENISA
- CERT-UE (para Instituciones y agencias de la UE)
- Red de CSIRT.,
- Plataformas transfronterizas intercambio de ciberinteligencia
- Red Transeuropea TESTA
- CEF Building Blocks, …

- Next Generation EU
- Digital Europe Programme - Ciberseguridad
- Horizon Europe
- Otros instrumentos de financiación

- Alineamiento
- Transposición
- Aplicación
- Participación
- Respuesta a monitorización

Directiva NIS2


Photo by Sara Kurfeß on Unsplash

Directiva 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión:

1. Exige a los **Estados miembros que refuercen las capacidades de ciberseguridad,** así como la **cooperación a escala nacional y de la UE.**
2. Introduce la **responsabilidad de los órganos de dirección,** la obligación de aplicar **medidas de gestión de riesgos de ciberseguridad**, de **notificar incidentes** y de uso de Esquemas Europeos de Certificación.
3. Establece normas relativas a **supervisión, ejecución y sanciones**.

NIS2, principales obligaciones para entidades en el ámbito de aplicación

2. Las AA.PP. en ámbito de aplicación de NIS2. Entidades de AGE, CCAA; a determinar EELL

20. Gobernanza: Responsabilidad de los órganos de dirección de las entidades esenciales e importantes.

21. Medidas para gestión de los riesgos de ciberseguridad

23. Obligaciones de notificación: cualquier incidente que tenga un impacto significativo en la prestación de sus servicios.

24. Utilización de esquemas europeos de certificación de la ciberseguridad

Artículo 20. Gobernanza

1. Los EEMM miembros velarán por que **los órganos de dirección** de las entidades esenciales e importantes **aprueben las medidas para la gestión de riesgos de ciberseguridad** adoptadas por dichas entidades para dar cumplimiento al artículo 21, **supervisen su puesta en práctica** y **respondan por el incumplimiento** por parte de las entidades de dicho artículo…

2. Los EEMM garantizarán que **los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones y alentarán a estas entidades para que ofrezcan formaciones similares a sus empleados periódicamente** ...

RD 311/2022 - ENS

6. La seguridad como un proceso integral.
11. Diferenciación de responsabilidades.
13. Organización e implantación del proceso de seguridad.
15. Gestión de personal.
16. Profesionalidad.
34. Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público – formación a personal especialista
Disposición adicional primera. Formación.

Art. 21 Medidas para la gestión de los riesgos de ciberseguridad

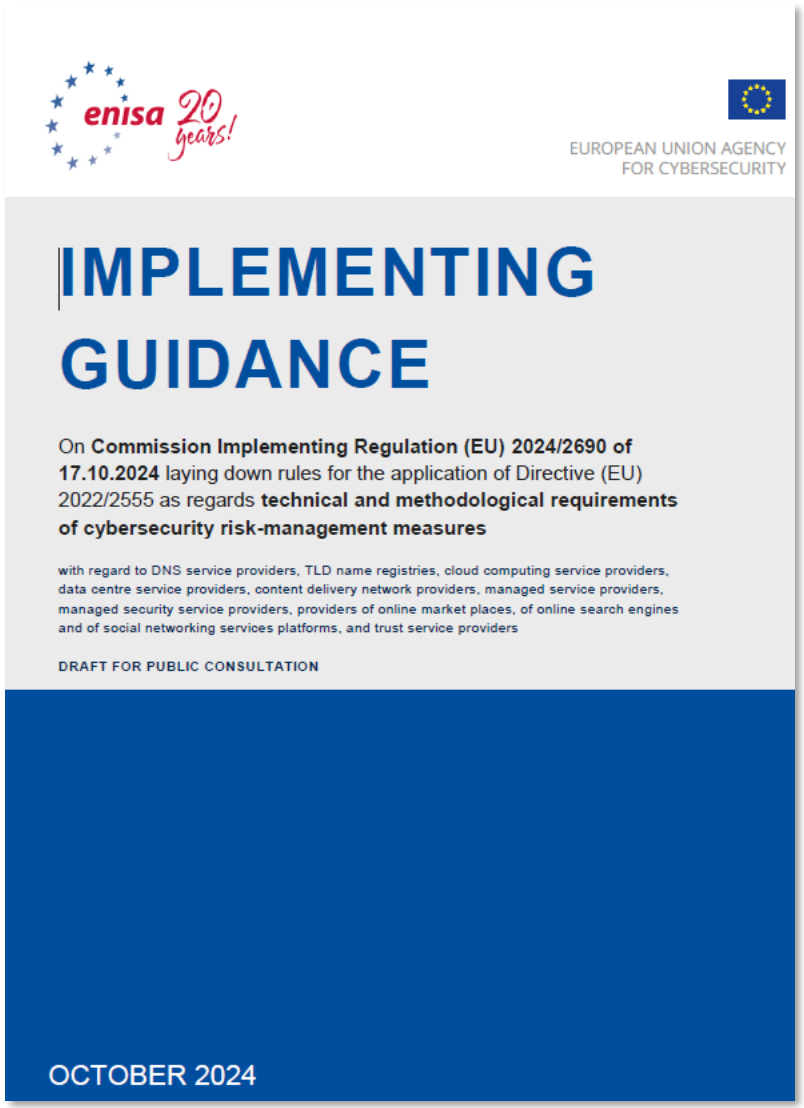
- **Políticas de seguridad y análisis de riesgos**
- **Gestión de incidentes**
- **Continuidad de las actividades (copias, recuperación, gestión de crisis)**
- **Seguridad de la cadena de suministro**
- **Seguridad en adquisición, desarrollo y mantenimiento** de redes y sistemas, incluida gestión y divulgación de vulnerabilidades.
- Políticas y procedimientos para **evaluar la eficacia de las medidas**.
- **Prácticas básicas de ciberhigiene y formación** en ciberseguridad.
- Políticas y procedimientos relativos a **criptografía y de cifrado**
- **Seguridad de recursos humanos**, control de acceso, gestión de activos.
- uso de soluciones de **autenticación multifactorial** o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y **sistemas seguros de comunicaciones de emergencia** en la entidad, cuando proceda.

Acto de implementación dirigido a: DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

(7) ...**Frameworks, guidance or other mechanisms provided by Member States' national law,** as well as relevant European and international standards, can also support relevant entities in demonstrating compliance with this Regulation. ...

+ Guía de implementación de ENISA (*Draft for consultation*). **Incluye correspondencia con el ENS.**

Guía de orientación de ENISA para el acto de implementación



Correspondencia de las medidas con el ENS. Ejemplo:

1.1 POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

MAPPING TO STANDARDS & FRAMEWORKS

European and international frameworks		National Frameworks	
ISO 27001:2022	5.2, A.5.1, A.5.36, A.5.4, 9.3	**BE-CyFun®2023**	BASIC: ID.GV-1.1
			IMPORTANT: ID.GV-1.2, PR.IP-5.1, PR.IP-6.1, PR.PT-2.1, PR.AT-4.1
			ESSENTIAL: PR.PT-3.3, PR.PT-4.3
NIST CSF v2.0	PR.AT-02, GV.PO-01, GV.PO-02, GV.OC-03, GV.RM-03, GV.OC-02, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	**FI-Kybermittari**	WORKFORCE-3, PROGRAM-1, PROGRAM-2, Management activities, CRITICAL-2, ARCHITECTURE-1,
ETSI EN 319 401	REQ 6.1-02, REQ 6.1-06, REQ 6.1-07, REQ 6.1-08, REQ 6.3	**EL – Ministerial decision 1027/2019 Article 2 - paragraph 2, Article 3**	Cybersecurity handbook: Part A: 2, Part B: 1.1, 1.5, 2.1, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1
			Self assessment tool: 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, 1.13, 2.1, 2.2, 3.1, 4.1, 5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1, 12.1, 13.1, 14.1, 15.1, 16.1, 17.1, 18.1, 19.1
CEN/TS 18026:2024	ISP-01, ISP-02, OPS-01, OPS-02, OPS-03	**ES- Royal Decree 311/2022**	Article 5, Article 6, Article 10, Article 12, Annex II: 3.1 Security policy

Perfil de Cumplimiento Específico para entidades en el alcance de NIS2

Esquema Nacional de Seguridad

Instrumento para implementar NIS2 de forma ágil, eficaz y eficiente.

Perfil de Cumplimiento Específico para organizaciones en el ámbito de aplicación de la Directiva NIS2 (**PCE-NIS2**):

- Correspondencia entre NIS2 y ENS
- Recopilación de obligaciones para entidades incluidas en alcance NIS2
- Detalle de correspondencia entre medidas NIS2 y medidas ENS
- Detalle de la Declaración de Aplicabilidad
- Criterios de aplicación de las medidas

A evolucionar en función de la transposición de NIS2, de posibles actos de implementación de la Comisión.

Utilización de esquemas europeos de certificación de la ciberseguridad

ENS, art. 19: Uso de **productos certificados** conforme al principio de proporcionalidad.

ENS, [op.pl.5]: Se utilizará el **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación** (CPSTIC).

CPSTIC: ofrece un conjunto de productos de referencia cuyas medidas de seguridad han sido verificadas y certificadas:

- Aprobados: para manejo de información clasificada.
- Cualificados: para ámbito ENS.

Los instrumentos de contratación centralizada se refieren al ENS en cuanto a los requisitos de seguridad y a la forma de demostrar o acreditar su cumplimiento.

ej. SISTEMA DINÁMICO DE ADQUISICIÓN DE SUMINISTRO DE SOFTWARE DE SISTEMA, DESARROLLO Y APLICACIÓN (**SDA 25/2022**)
Las especificaciones para las adquisiciones **incluyen**:

- **Requisitos de Seguridad**
- **Cómo demostrar el cumplimiento de los requisitos de seguridad mediante referencias a:**
  - Conformidad con el Esquema Nacional de Seguridad (ENS)
  - Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) o equivalente
  - **Referencia a esquemas de certificación europeos (EUCC, EUCS).**

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PUBLICA

SECRETARIA GENERAL
DE ADMINISTRACIÓN DIGITAL

SOCINFO
sociedad de la información digital

Directiva NIS2 para la AAPP: Claves de Cumplimiento y su relación con el ENS

Muchas gracias

24 de enero de 2025

Miguel A. Amutio Gómez

Director de Planificación y Coordinación de Ciberseguridad
Secretaría General de Administración Digital
Secretaría de Estado de Función Pública
Ministerio para la Transformación Digital y de la Función Pública