# Transposición NIS 2.0.

## Gobernanza y otros retos

Javier Candau
Adjunto al Subdirector
Centro Criptológico Nacional
ccn@cni.es / adjccn@ccn.cni.es

centro criptológico nacional

## CCN / CCN-CERT

- Ley 11/2002 reguladora **del Centro Nacional de Inteligencia.**
- RD 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.

- RD 311/2022 de 4 de mayo, que regula el **Esquema Nacional de Seguridad** para todo el **Sector Público +** sistemas manejan **información clasificada + Sector privado** (preste servicios S. Público). (Antecedentes: RD 3/2010 y RD 951/2015) (Desarrollo: Art 156.2 de la Ley 40/2015)
- RDL 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información. **Coordinación incidentes.**
- RDL 14/2019, de 31 de octubre, Medidas urgentes. **Coordinación CSIRT públicos y enlace con exterior**
- RD 43/2021, de 28 de enero, Desarrollo RDL 12/2018. **Plataforma Nacional**

## MISIÓN

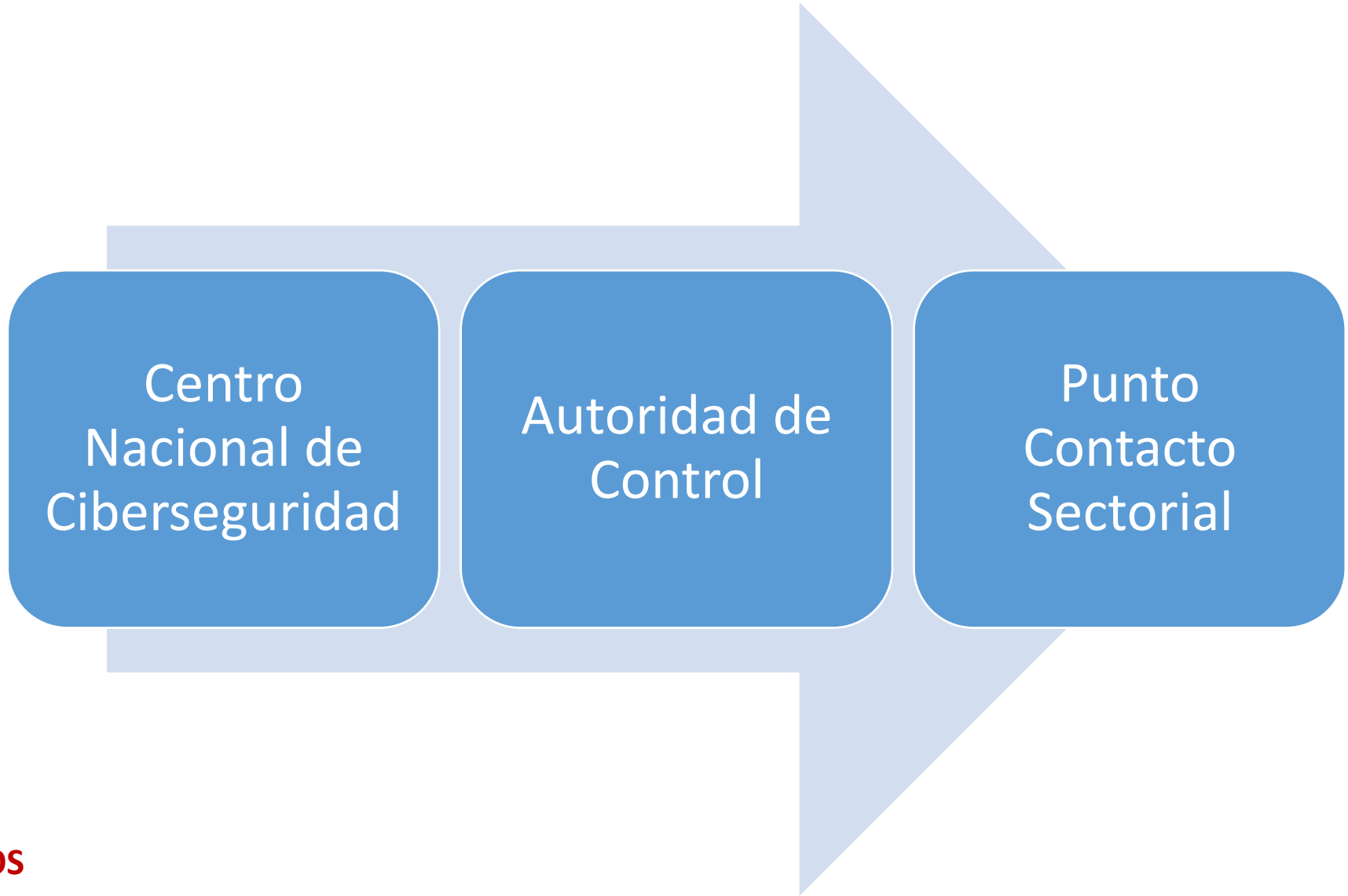
Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

## COMUNIDAD

Responsabilidad en ciberataques sobre:

- **sistemas clasificados**,
- sistemas del **Sector Público**,
- empresas y organizaciones de **sectores estratégicos** para el país en coordinación con el CNPIC.

# NIS 2.0. Gobernanza ciberseguridad




SUJETO A CAMBIOS

# Centro Nacional de Ciberseguridad

Es la **autoridad nacional competente única** en materia de gobernanza de la ciberseguridad, encargada de la **dirección, impulso y la coordinación**, en el ámbito de esta ley, de todas las actividades necesarias para garantizar un elevado nivel de ciberseguridad en España y contribuir a la ciberseguridad de la Unión Europea

**A crear en 12 meses tras la publicación**

- Órgano superior para la gobernanza y **coordinación** de las actividades
- Autoridad Nacional Competente en el ámbito de la ciberseguridad
- Autoridad nacional de gestión de crisis
- Punto de contacto único
- Informar al público sobre incidentes que afecten a más de una autoridad de control
- Establecer, en situaciones de justificada necesidad aprobada mediante **resolución motivada**, con el asesoramiento de las autoridades de control, las **obligaciones específicas necesarias para garantizar la seguridad de las redes y sistemas de información**.
- Promover y aprobar, en su caso, el uso de estándares, guías, especificaciones, instrucciones técnicas

CCN centro criptológico nacional

# Autoridades de Control

- Establecer **canales de comunicación con las entidades esenciales e importantes**, entre los que se incluyen la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes prevista en el artículo 19.**
- Recibir y realizar el **seguimiento de las notificaciones sobre incidentes** que sean presentadas en el marco de esta ley a través de los CSIRT nacionales de referencia.
- **Informar al público sobre determinados incidentes**, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido.
- Participar, de forma voluntaria, en las **revisiones interpares** …
- **Proponer las medidas de gestión de riesgos de ciberseguridad** de obligado cumplimiento para las entidades incluidas en el ámbito de aplicación de esta norma.
- **Potestad sancionadora**
- **Cualquier otra atribuida en esta ley o en su desarrollo reglamentario**.

**CSIRT de referencia no cambian las funciones respecto RDL 12/2018 Y RD 43/2021**

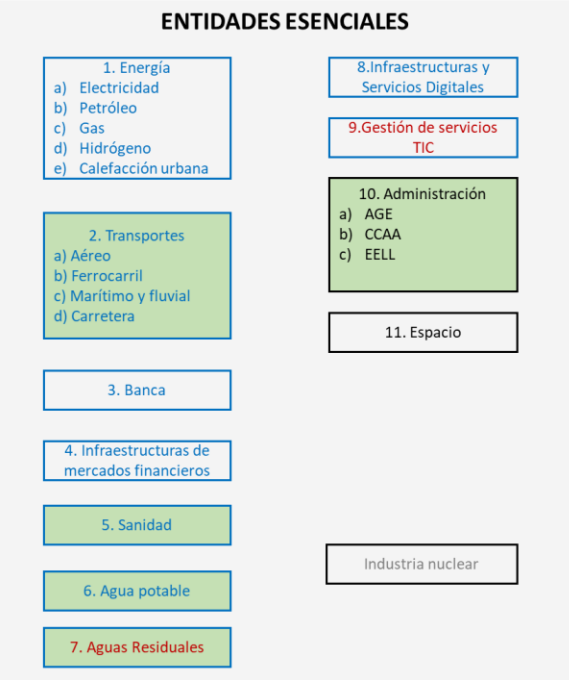
# Puntos Contacto Sectoriales

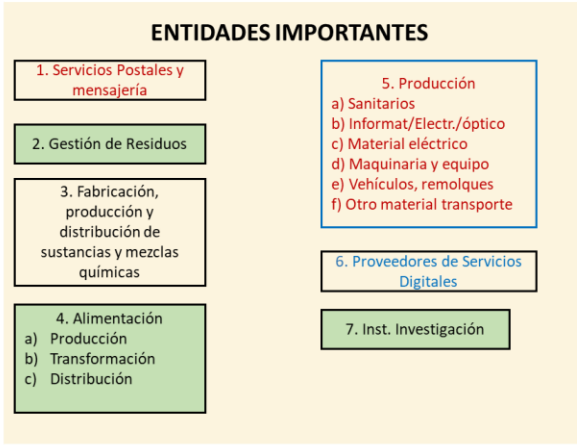
**ARTICULO 7.3** Por cada uno de los sectores relacionados en los anexos I y II, se designará, al menos, un **órgano ministerial u organismo o entidad de derecho público vinculado o dependiente de la Administración General del Estado** que será, en el marco de sus competencias, el punto de contacto especializado con el Centro Nacional de Ciberseguridad y las autoridades de control.

## Funciones

- Impulsar las políticas de seguridad y velar por la aplicación y cumplimiento de las obligaciones derivadas de esta ley
- Identificación y designación de las EE e EI.
- Cualquier otra que se le asigne reglamentariamente.
- Colaborar con el CNC y las AC en el desarrollo de las siguientes actividades
  - Elaboración los perfiles específicos de cumplimiento
  - Informar de incidentes.
  - Supervisión del cumplimiento por parte de las entidades esenciales e importantes de las obligaciones que se determinan en la presente ley
  - Establecimiento de los canales de comunicación oportunos

# RETOS NIS 2.0




**Infraestructuras críticas (2011)**
**Servicios esenciales NIS1.0 (2016)**
**Servicios esenciales NIS2.0 (2022)**

**Mayoría operadores Públicos**

**+ 50 EI**
**+250 EE**
empleados

**+4k EI**
**+1k EE**
empresas

1

## LISTADO OSE/OSI

Auto registro / validación

2

## MEDIDAS DE CIBERSEGURIDAD

Homogéneas que permitan conocer el nivel de ciberseguridad. **Actos de ejecución**

3

## DEMOSTRACIÓN CUMPLIMIENTO

Certificación / Declaración de conformidad

4

## NOTIFICACIÓN INCIDENTES. PNNSC

Conocer todos los incidentes

5

## GESTIÓN DE CRISIS

Reaccionar ante los incidentes críticos
Centro Nacional de Ciberseguridad + CCN-CERT
Red Nacional de SOC,s

CCN
centro criptológico nacional

# TAREAS URGENTES

**Auto registro y validación**

**Medidas de seguridad según el análisis de riesgos**

Superficie de exposición

**Esquema de certificación y auditorías de cumplimiento**

**Notificación de ciberincidentes**

Respuesta ante ciberincidentes

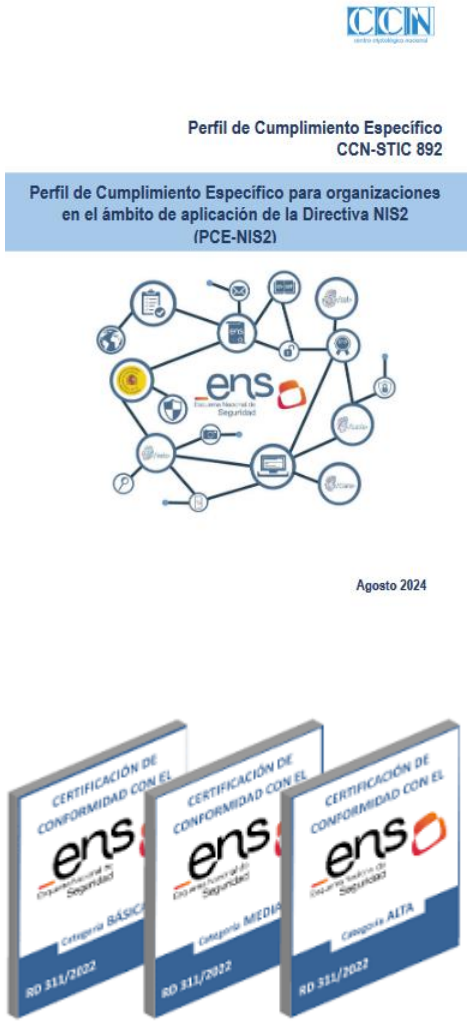
CCN
centro criptológico nacional

# OBLIGACIONES. AUTOREGISTRO Y VALIDACIÓN


https://plataformanacionalciber.gob.es


CCN centro criptológico nacional

# ENS COMO INSTRUMENTO DE CUMPLIMIENTO



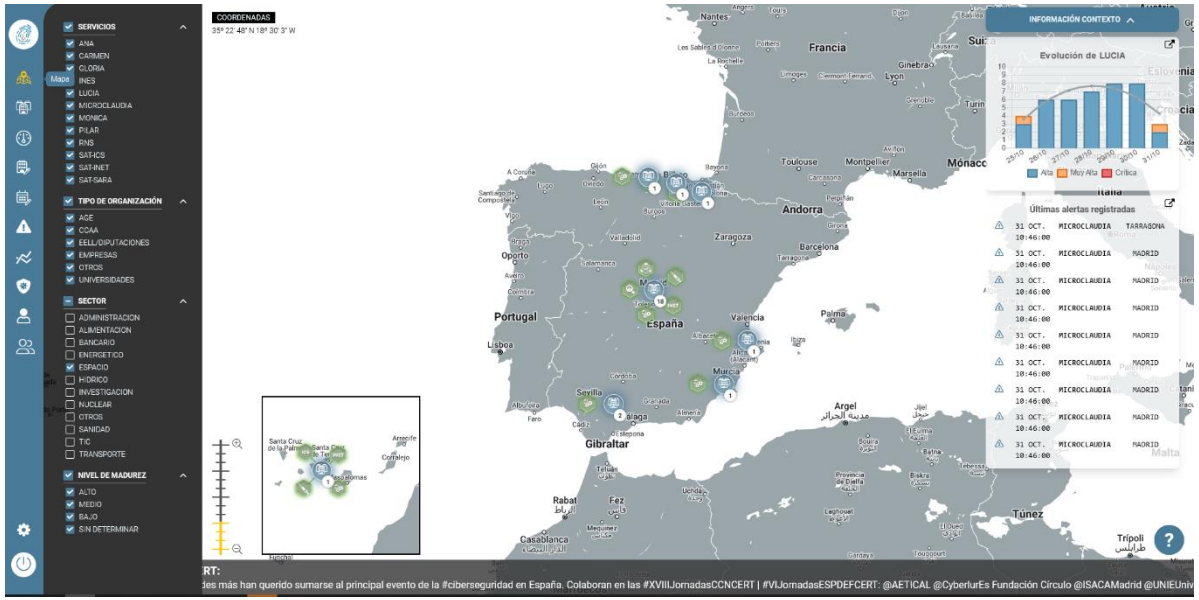

| Medidas generales de la Directiva NIS2 | Medidas de seguridad del ENS relacionadas |
|---|---|
| **Art. 21 a)** las políticas de seguridad de los sistemas de información y análisis de riesgos. | **Art. 12.** Política de seguridad y requisitos mínimos de seguridad<br>**[org.1]** Política de Seguridad<br>**[org.2]** Normativa de Seguridad<br>**[op.pl.1]** Análisis de riesgos |
| **Art. 21 b)** La gestión de incidentes. | **Art. 25.** Incidentes de seguridad.<br>**[op.exp.7]** Gestión de incidentes |
| **Art 21 c)** La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis. | **Art. 26.** Continuidad de la actividad.<br>**[op.cont.4]** Medios alternativos<br>**[mp.info.6]** Copias de seguridad<br>**[op.cont.1]** Análisis de impacto (BIA)<br>**[op.con.2]** Plan de Continuidad<br>**[op.cont.3]** Pruebas periódicas |
| **Art. 21 d)** La Seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos. | **[op.ext.3]** Protección de la cadena de suministro<br>**[op.ext.1]** Contratación y acuerdos de nivel de servicio<br>**[op.ext.2]** Gestión diaria<br>**[op.ext.4]** Interconexión de sistemas |
| **Art. 21 e)** La seguridad en la adquisición, y el desarrollo y mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades. | **Art. 19.** Adquisición de productos de seguridad y contratación de servicios de seguridad.<br>**[op.pl.3]** Adquisición de nuevos componentes<br>**[op.pl.5]** Componentes certificados<br>**[mp.sw.1]** Desarrollo de aplicaciones<br>**[mp.sw.2]** Aceptación y puesta en servicio<br>**[op.exp.4]** Mantenimiento y actualizaciones de seguridad<br>**[op.mon.3]** Vigilancia |

# ENS. DEMOSTRACIÓN DEL CUMPLIMIENTO

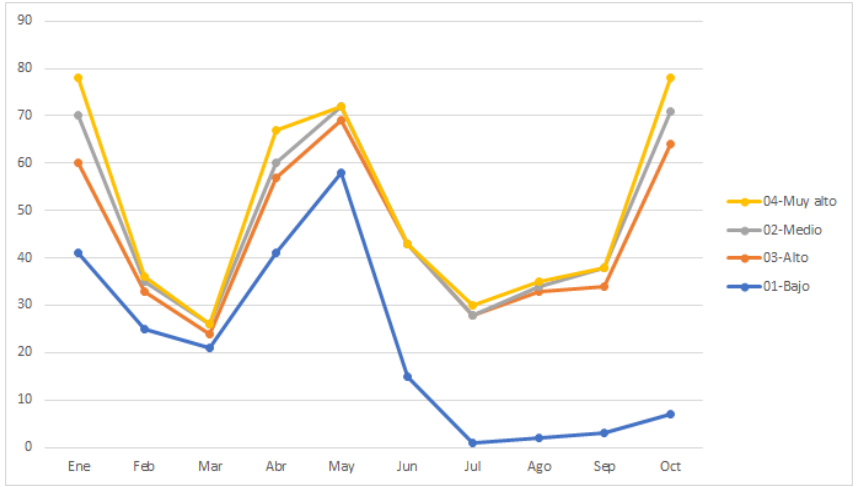


centro criptológico nacional

# OBLIGACIONES. NOTIFICACIÓN CIBERINCIDENTES. EJEMPLO SECTOR ESPACIO




**+500** incidentes

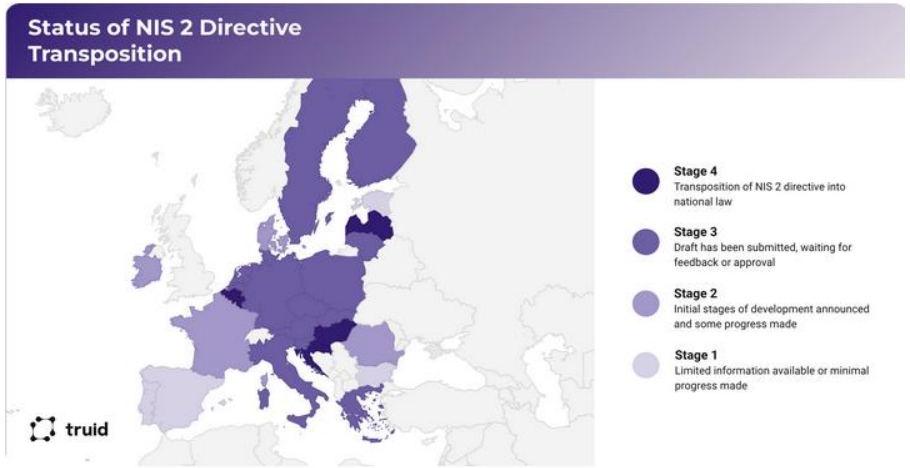



**26 / 75**

ENTIDADES EN EL SISTEMA

CCN centro criptológico nacional

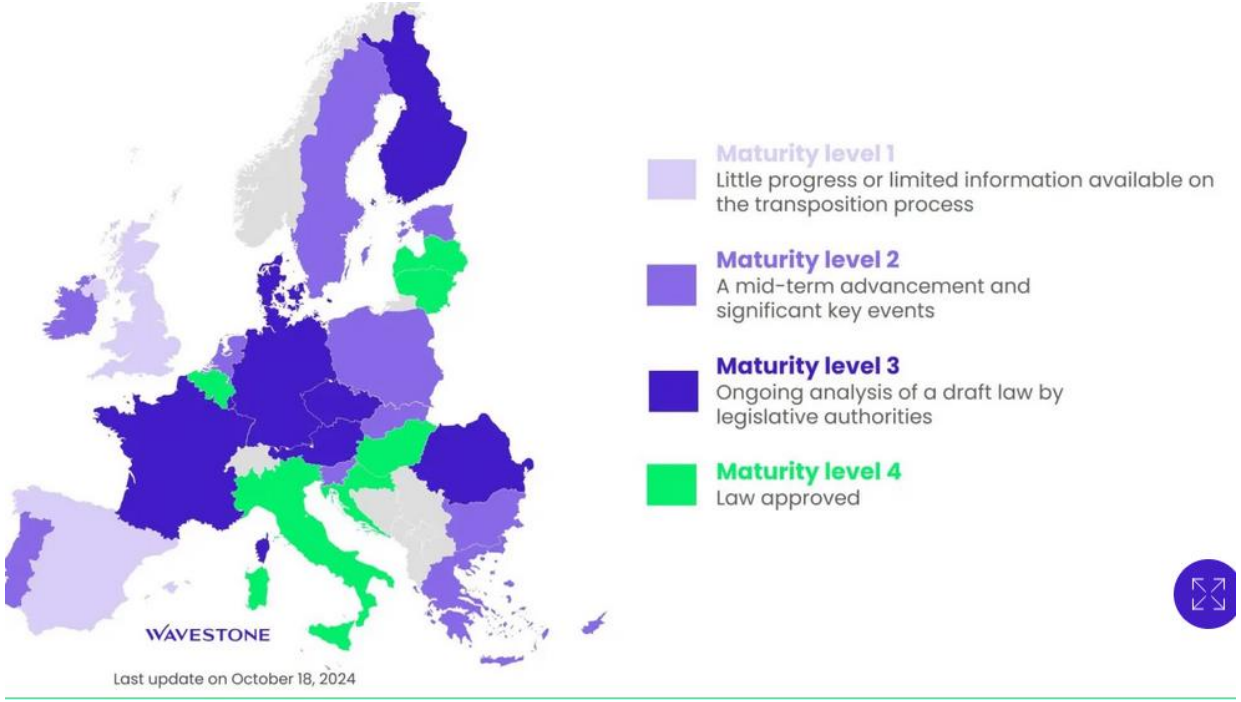
# ESTADO DE LA TRANSPOSICIÓN




**Consulta 12.01.2025**

**Spain**

The legislative process has not started, and there have been no significant updates or public consultations regarding the directive's transposition into Spanish law.




https://www.truid.app/blog/the-nis2-directive-in-eu-a-country-by-country-breakdown

https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive/

# QUÉ APORTA ESPAÑA A LA UE

## GESTIÓN DE RIESGOS

Conjunto armonizado y proporcional de medidas de ciberseguridad con el ENS.

## INTERCAMBIO CONTINUO

Intercambio de incidentes. LUCIA. Sistema conjunto de gestión de incidentes.

## INTELIGENCIA COMPARTIDA

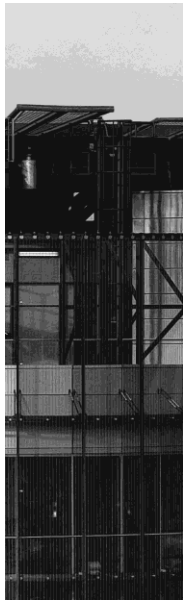
REYES ofrece visión sobre la superficie de exposición y facilita la respuesta.

## RESPUESTA INTEGRADA

La RNS permite disponer de plataformas de intercambio de IOC, IOA e información relevante.

# Muchas

# Gracias



**E-mails**


ccn@cni.es

info@ccn-cert.cni.es

sat@ccn-cert.cni.es

microclaudia@ccn-cert.cni.es

ens@ccn-cert.cni.es

organismo.certificacion@cni.es

# RD 311/2022 Esquema Nacional de CiberSeguridad

**7 Principios básicos**

a) Seguridad como proceso integral
b) Gestión de seguridad basada en riesgos
c) Prevención, detección, respuesta y conservación
d) Existencia de Líneas de defensa
e) Vigilancia Continua
f) Reevaluación periódica
g) Diferenciación de responsabilidades

**73 Medidas de seguridad**

a) Marco organizativo (4)
b) Marco operacional (33)
c) Medidas de protección (36)

**15 Requisitos mínimos**

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de riesgos
c) Gestión del personal
d) Profesionalidad
e) Autorización y control de accesos
f) Protección de las instalaciones
g) Adquisición de productos y contratación de servicios seguridad
h) Mínimo privilegio
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de actividad y detección de código dañino
m) Incidentes de Seguridad
n) Continuidad de la actividad
o) Mejora continua del proceso de seguridad

1. Los **Principios básicos**, que sirven de guía.
2. Los **Requisitos mínimos**, de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS. **Sellos de conformidad.**
5. La **respuesta a incidentes de seguridad**. Papel del CCN- CERT. **Notificación y auditoria**
6. El uso de **productos certificados**. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.
8. Serie 800 Guías CCN-STIC (**+90 documentos**)

**Categoría BÁSICA: 52 / 45 controles (70%)**
**Categoría MEDIA: 68 / 63 controles (93%)**
**Categoría ALTA: 73 / 75 controles (100%)**

CCN centro criptológico nacional