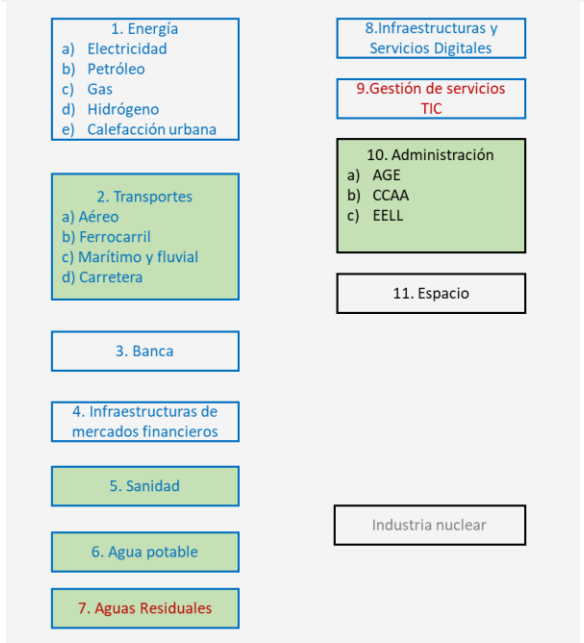
NIS 2.0, CSA y ENS

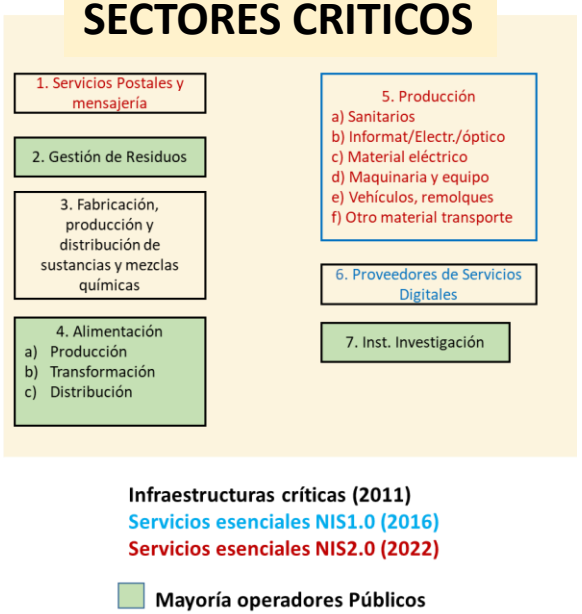
Javier Candau
Centro Criptológico Nacional
ccn@cni.es

NIS 2.0

SECTORES ALTA CRITICIDAD



SECTORES CRITICOS



+ 50 EI
+250 EE

empleados

+8k EI
+3k EE

empresas

1

LISTADO EE/EI

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
Notificar vulnerabilidades

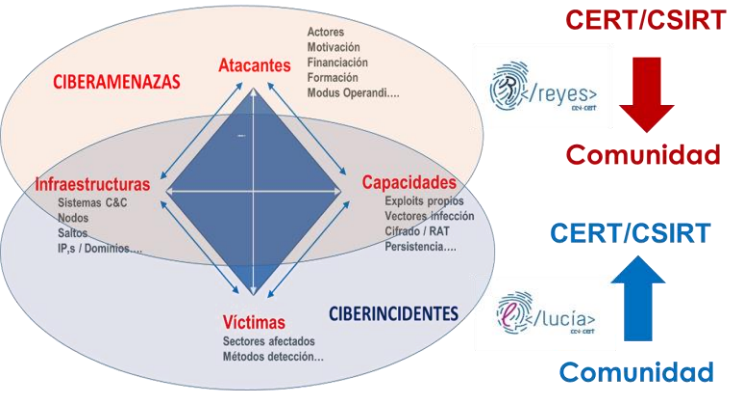
5

GESTIÓN DE CRISIS

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

CCN
centro criptológico nacional

1. OBLIGACIONES. AUTOREGISTRO Y VALIDACIÓN



CERT/CSIRT

</reyes>

Comunidad

CERT/CSIRT

</lucía>

Comunidad

PNNSC

INTERCAMBIAR
+
RESPONDER

SSO
Single Sign On

https://rns.ccn-cert.cni.es/

Red Nacional de SOC

Modulo de Auto registro

</amparo>

</inés>

</pilar>

CNPIC Autoridad Nacional
Autoridades Control
Puntos Control Sectoriales
aepd agencia española protección datos

https://plataformanacionalciber.gob.es

CCN centro criptológico nacional

2. OBLIGACIONES. MEDIDAS CIBERSEGURIDAD

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 **[org.1]** Política de Seguridad **[org.2]** Normativa de Seguridad **[op.pl.1]** Análisis de riesgos
Art. 21 b) La gestión de incidentes.	**Art. 25.** Incidentes de seguridad. **[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. **[op.cont.4]** Medios alternativos **[mp.info.6]** Copias de seguridad **[op.cont.1]** Análisis de impacto (BIA) **[op.con.2]** Plan de Continuidad **[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 **[op.ext.1]** Contratación y acuerdos de nivel de servicio **[op.ext.2]** Gestión diaria **[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. **[op.pl.3]** Adquisición de nuevos componentes **[op.pl.5]** Componentes certificados **[mp.sw.1]** Desarrollo de aplicaciones **[mp.sw.2]** Aceptación y puesta en servicio **[op.exp.4]** Mantenimiento y actualizaciones de seguridad **[op.mon.3]** Vigilancia

- Las **entidades esenciales**, con independencia de la categoría del sistema, deberán ser **certificadas** conforme cumplen los requisitos del ENS **por una entidad de certificación(EC) acreditada por ENAC** o por un **Órgano de Auditoría Técnica (OAT)** del sector público reconocido por el CCN.

- Las **entidades importantes**, podrán optar por una **Declaración de Conformidad obtenida mediante la solución INES del Portal de Gobernanza del ENS**, aunque se recomienda una auditoría externa.

- Hoja de ruta a partir del PCE-RFS, solución **automatizada en INES del Portal de Gobernanza del ENS**, con obtención del correspondiente Certificado de Conformidad en base al PCE-RFS. **Durante dos (2) años** aplicar mejora continua para poder alcanzar la categoría adecuada, requiriéndose **acta o documento formal de asunción del compromiso de mejora y del riesgo asumido.**

3. OBLIGACIONES. DEMOSTRACIÓN CUMPLIMIENTO

PCE-RFS: PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD.

Marco Organizativo (4):
[org.1] Política de seguridad
[org.2] Normativa de seguridad
[org.3] Procedimientos de seguridad
[org.4] Proceso de autorización

Marco Operacional (14):
[op.pl] Planificación
[op.pl.1] Análisis de riesgos
[op.pl.3] Adquisición de nuevos componentes
[op.acc] Control de acceso
[op.acc.1] Identificación
[op.acc.2] Requisitos de acceso
[op.acc.4] Proceso de gestión de derechos de acceso
[op.acc.5] Mecanismos de autenticación (usuarios externos)
[op.acc.6] Mecanismo de autenticación (usuarios de la organización)
[op.exp] Explotación
[op.exp.1] Inventario de activos
[op.exp.2] Configuración de seguridad
[op.exp.4] Mantenimiento y actualizaciones de seguridad
[op.exp.6] Protección frente a código dañino
[op.exp.7] Gestión de incidentes
[op.exp.8] Registro de la actividad
[op.exp.10] Protección de claves criptográficas
[op.mon] Monitorización del sistema
[op.mon.2] Sistema de métricas

PCE-RFS
38

Medidas de Protección (19):
[mp.if] Protección de las instalaciones e infraestructuras
[mp.if.1] Áreas separadas y control de acceso
[mp.per] Gestión del personal
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación
[mp.eq] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de dispositivos portátiles
[mp.eq.4] Otros dispositivos conectados a la red.
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.si] Protección de los soportes de información
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.info] Protección de la información
[mp.info.1] Datos de carácter personal
[mp.info.3] Firma electrónica
[mp.info.5] Limpieza de documentos
[mp.info.6] Copias de seguridad (backup)
[mp.s] Protección de los servicios
[mp.si.1] Protección del correo electrónico
[mp.s.3] Protección de la navegación web

* En rojo: Medidas nuevas respecto al antiguo PCE-RES

¿DISPONE DE CERTIFICADO ENS?

ens Esquema Nacional de Seguridad

SÍ
- ALTA
- MEDIA | BÁSICA

✓ CUMPLE MEDIDAS DE LA NIS2

NO

Entidades **incluidas** en el ámbito del **Reglamento de Ejecución** (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024

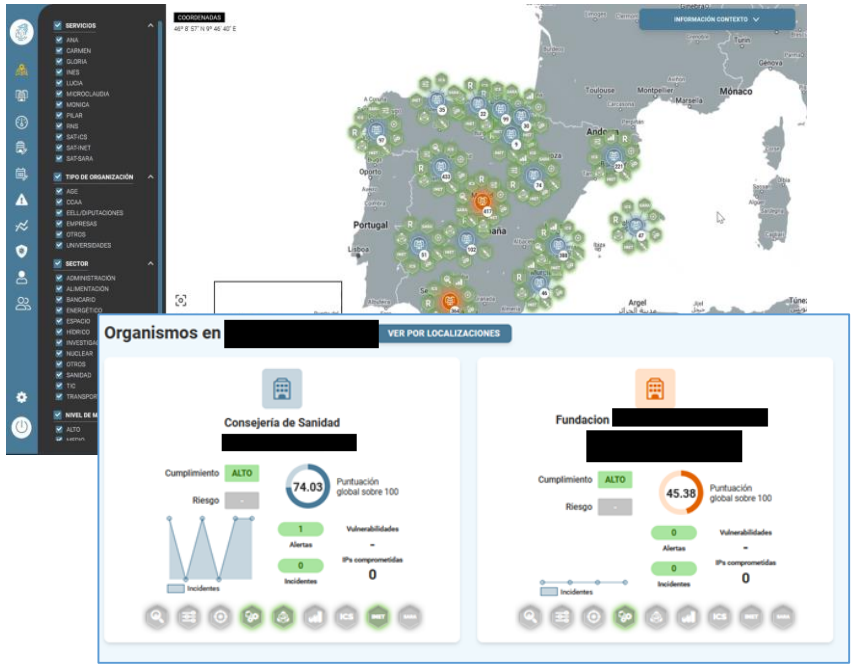
CCN-STIC 892 PCE-Aplicación NIS2

Entidades **no incluidas** en el ámbito del **Reglamento de Ejecución** (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024

ADECUACIÓN ENS / PCE

CCN centro criptológico nacional

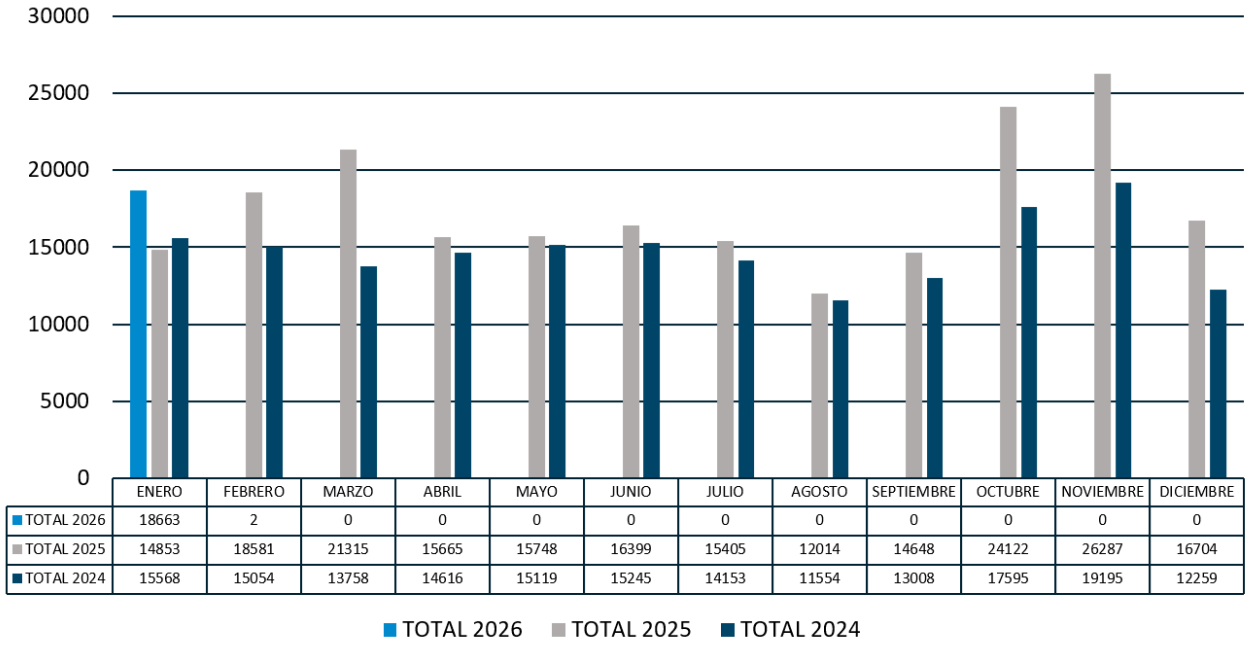
4. OBLIGACIONES. NOTIFICACIÓN CIBERINCIDENTES.



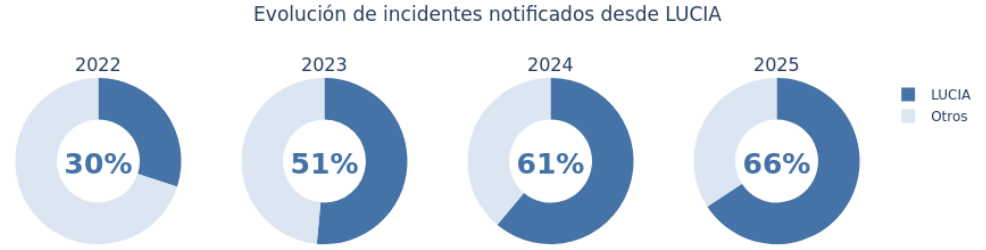
+4700

ENTIDADES EN EL SISTEMA

+211.000 incidentes

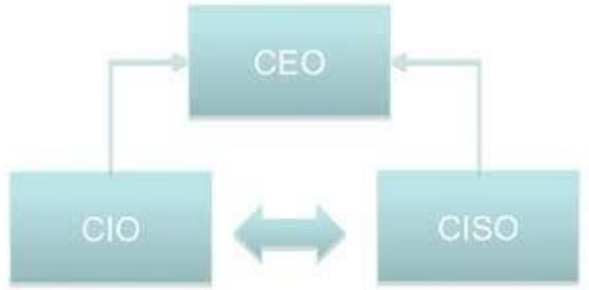


	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
TOTAL 2026	18663	2	0	0	0	0	0	0	0	0	0	0
TOTAL 2025	14853	18581	21315	15665	15748	16399	15405	12014	14648	24122	26287	16704
TOTAL 2024	15568	15054	13758	14616	15119	15245	14153	11554	13008	17595	19195	12259



centro criptológico nacional

Obligaciones de la dirección

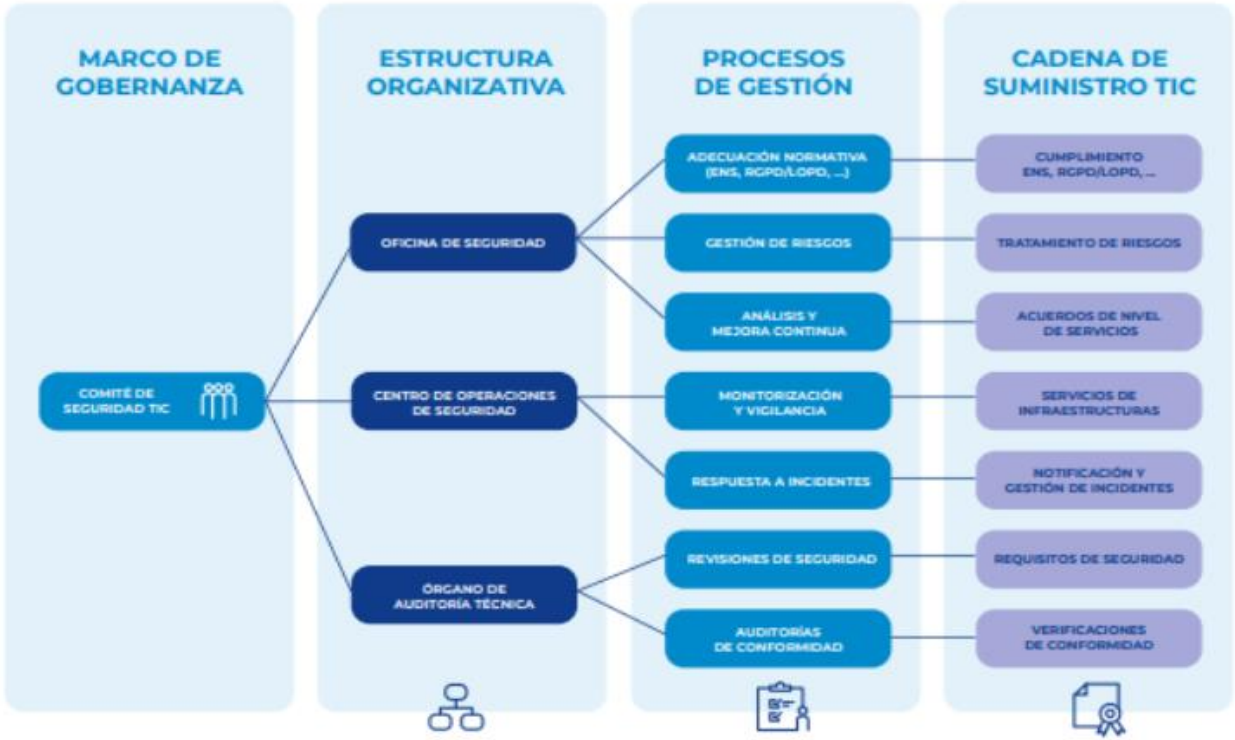


Artículo 14. *Gobernanza*.
Los órganos de dirección de las entidades esenciales e importantes serán responsables de aplicar las medidas para la gestión de riesgos de ciberseguridad, de supervisar su implantación efectiva y, en su caso, asumirán la responsabilidad por su incumplimiento.

Artículo 15. *Medidas generales para la gestión de riesgos de ciberseguridad.*

Artículo 16. *Responsable de la seguridad de la información.*

Artículo 17. *Gestión de incidentes de seguridad*.



Acciones Urgentes:

- **Empoderar al CISO**
- **Certificación ENS. Aceptación de la hoja de ruta y asunción del riesgo**

LEGISLACIONES QUE VIENEN POR EU en 2026

OBLIGACIONES CADENA SUMINISTRO

- Requisitos de soberanía
  - Prohibir proveedores alto riesgo
    - Directiva 2022/2555 **NIS 2**.
    - Reglamento 2024/2690, **desarrolla NIS 2** para ID.
    - Reglamento 2024/2847, **CRA**.
    - Reglamento 2019/881, **CSA**.
    - Reglamento 2024/1689, **AI Act**.
  - Plazos de la CSA JUN2026

REVISIÓN

- Mandato ENISA
- Gobernanza Esquemas. Papel ANCC
- Cadena Suministro
- **Modificaciones NIS 2.0**
- Plazos DIC 2026

- (EU) 2024/1689. Afectará resto normas
- Notificación incidentes
- Esquema Certificación IA ?
- Plazos: APL Gobernanza IA

QUANTUM ACT

- Tecnologías cuánticas CRÍTICAS
- Necesidad de certificación
- Autoridad Nacional en Seguridad Cuántica
- Plazos: Por determinar

- Revisión …NIS, DORA, CRA, GDPR, IA Act
- Simplificación Notificación incidentes
- SEP de ENISA…. A través PNNSC
- Plazos JUN 2026

REVISIÓN

- Esquema Certificación EE e EI
  - Cyber posture
- Notificación incidentes (PNNSC)
- EE y EI y transfronterizas
- PQC
- Plazos DIC 2026

CYBERDIPLOMACY TOOLBOX

- Atribución en UE
- Incremento actividad
- MAEUC alineado?
- Plazos: ACTIVO

SPACE ACT

- Ciberseguridad infraestructura espacial
- Segmento terrestre
- Segmento espacial (satélites)
- Plazos: SEPT 2026

CCN
centro criptológico nacional

NIS 2.0 vs Digital Omnibus

(EU) 2022/2555 NIS 2
(EU) 2022/2554 DORA
(EU) 2022/2557 CERN
(EU) 910/2014 / (UE) 2024/1183 eIDAS
(EU) 2016/679 GDPR

CCN
centro criptológico nacional

El Reglamento sobre la Ciberseguridad (*Cybersecurity Act*)

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019

- **ENISA, la Agencia de la Unión Europea para la Ciberseguridad**
  - Nueva denominación y mandato permanente
  - Objetivos, tareas y aspectos organizativos
  - Competencias en certificación de ciberseguridad

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

- **MARCO DE CERTIFICACIÓN DE LA CIBERSEGURIDAD**
  - Define un mecanismo para instaurar Esquemas Europeos de Certificación de la Ciberseguridad
  - Con el objetivo de incrementar el nivel de ciberseguridad de la Unión
  - Los certificados serán reconocidos en todos los Estados miembros
  - Certificación voluntaria, salvo disposición contraria en el Derecho de la Unión o de los EEMM

Supply Chain Security ……REQUISITOS DE SOBERANÍA.

ANCC Autoridad Nacional de Certificación de la Ciberseguridad

CCN centro criptológico nacional

Los Esquemas Europeos de Certificación de la Ciberseguridad

El Marco Europeo de Certificación de la Ciberseguridad

European Commission

Comisión Europea

solicita

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA

publica

prepara

Programa de trabajo evolutivo de la Unión

Esquema candidato

European Commission

Acto de ejecución

Esquema europeo

dictaminan

dictamina

asesoran

Grupo de las Partes Interesadas sobre Certificación

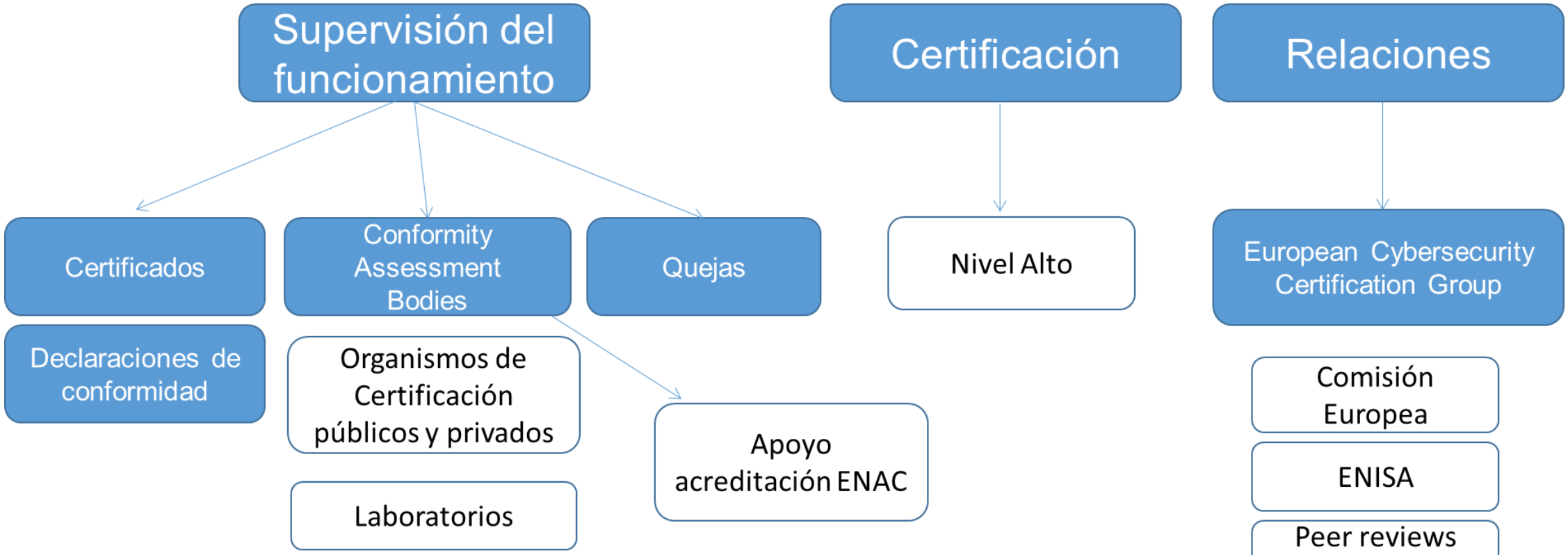
Grupo Europeo de Certificación de la Ciberseguridad

Grupo Ad Hoc de ENISA

CCN
centro criptológico nacional

Autoridad Nacional de Certificación de la Ciberseguridad

Funciones de la Autoridad Nacional Certificación de la Ciberseguridad



CCN centro criptológico nacional

Estado Esquemas Europeos de Certificación

EUCC

Activo

REGLAMENTO DE EJECUCIÓN (UE) 2024/482

Nivel sustancial

- 2 CBs notificados
- 2 ITSEFs notificados

Nivel elevado

- OC/ANNC pendiente acreditar (Audit. Julio 2025)
- 3 laboratorios con autorización en curso

EUCS

Borrador de esquema candidato enviado a CE en mayo 2024

A la espera de la revisión de la CE para desarrollo del reglamento de ejecución

Última versión elimina requisitos de soberanía

Requisitos en norma CEN TS-18026

EUC5G

EU NESAS – en revisión

EUCC – certificación eUICC

GSMA – TSP provisioning

EUDIW

Ad-Hoc WG creado en enero de 2025

Fase de definición esquema europeo. Entrega prevista por ENISA para finales de junio de 2026

EUMSS

Creación de AHWG en septiembre de 2025. Trabajando en la definición del esquema. Entrega por ESNISA esperada para Q3 2026

ciclon
CERTIFICACIÓN ITERATIVA CLOUD NACIONAL

IA

Vehículos

Cyber-Posture

Red Nacional de SOC

CCN
centro criptológico nacional

NIS 2.0 vs Cyber posture

CYFUN

SMALL	BASIC	IMPORTANT	ESSENTIAL
Basic security measures, 6 requirements	34 requirements	133 requirements	218 requirements

ESQUEMA NACIONAL DE SEGURIDAD

	PCE- RFS	BASIC Category	MEDIUM Category	HIGH Category
	109 requirements	178 requirements	283 requirements	360 requirements

- 40 ENS controls PCE-RFS 38 controls + contracting and cloud services (contract -covered)
- 65 ENS controls + 2 considerations
- 65 ENS controls + 4 considerations

Difference between IMPORTANT and ESSENTIAL regarding the ENS is that it includes more requirements.

PCE
By sectors

- CLOUD
- HEALTH
- ENERGY
- DIGITAL INFRASTRUCTURE
- MANAGED SECURITY SERVICES
- TRANSPORT RAIL
- LOCAL ENTITIES
- WATER
- UNIVERSITIES
- SPACE
- SMALL ENTITIES
- JUSTICE

CATEGORY	BASIC	MEDIUM	HIGH
EVALUATION TYPE	SELF-ASSESSMENT-CERTIFICATION AUDIT	CERTIFICATION	CERTIFICATION
METHOD OF EVALUATION	SELF-ASSESSMENT OR CERTIFICATION AUDIT >=1,5d	CERTIFICATION AUDIT >=2,5 d	CERTIFICATION AUDIT >=3,5d
PERFORMED BY	ACCREDITED CERTIFICATION BODY OR OR OAT	ACCREDITED CERTIFICATION BODY OR OR OAT	ACCREDITED CERTIFICATION BODY OR OR OAT
MARKS IN ACCORDANCE WITH THE NSF	DECLARATION OF CONFORMITY OR CERTIFICATE OF CONFORMITY	CERTIFICATE OF CONFORMITY	CERTIFICATE OF CONFORMITY

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.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%)