Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2026/0011 (COD)

Brussels, 11 September 2026

WK 13873/2026 INIT

LIMITE

CYBER	**IND**
JAI	**CADREFIN**
DATAPROTECT	**FIN**
TELECOM	**BUDGET**
MI	**CSC**
	CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Horizontal Working Party on Cyber Issues
N° Cion doc.:	ST 5611 2026 ADD 1 + ST 5611 2026 ADD 2 + ST 5611 2026 ADD 3 + ST 5611 2026 ADD 4 + ST 5611 2026 INIT
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) – Cyber posture - Presentation by Spain

Delegations will find in the annex a presentation given by Spain at the meeting of the Horizontal Working Party on Cyber Issues on 10 September 2026.

PUBLIC

The Spanish approach to cyberposture and harmonization





centro criptológico nacional

HWPCI- September 2026

Harmonization should build on what works

PUBLIC

Spain supports European harmonisation, but harmonisation should build on mature national capabilities, not replace them.

Europe needs greater convergence, interoperability and trust. But this does not necessarily require replacing national frameworks that already provide a high level of assurance.

Harmonization does not have to mean necessarily uniformity. It can mean complementarity.

Belgium's experience with CyFun, as well as other mature national frameworks developed across the Union, like the Spanish ENS one, illustrates an important point: **Europe is not starting from zero.** We already have mature national capabilities that can become building blocks of European harmonisation.

CCN
centro criptológico nacional

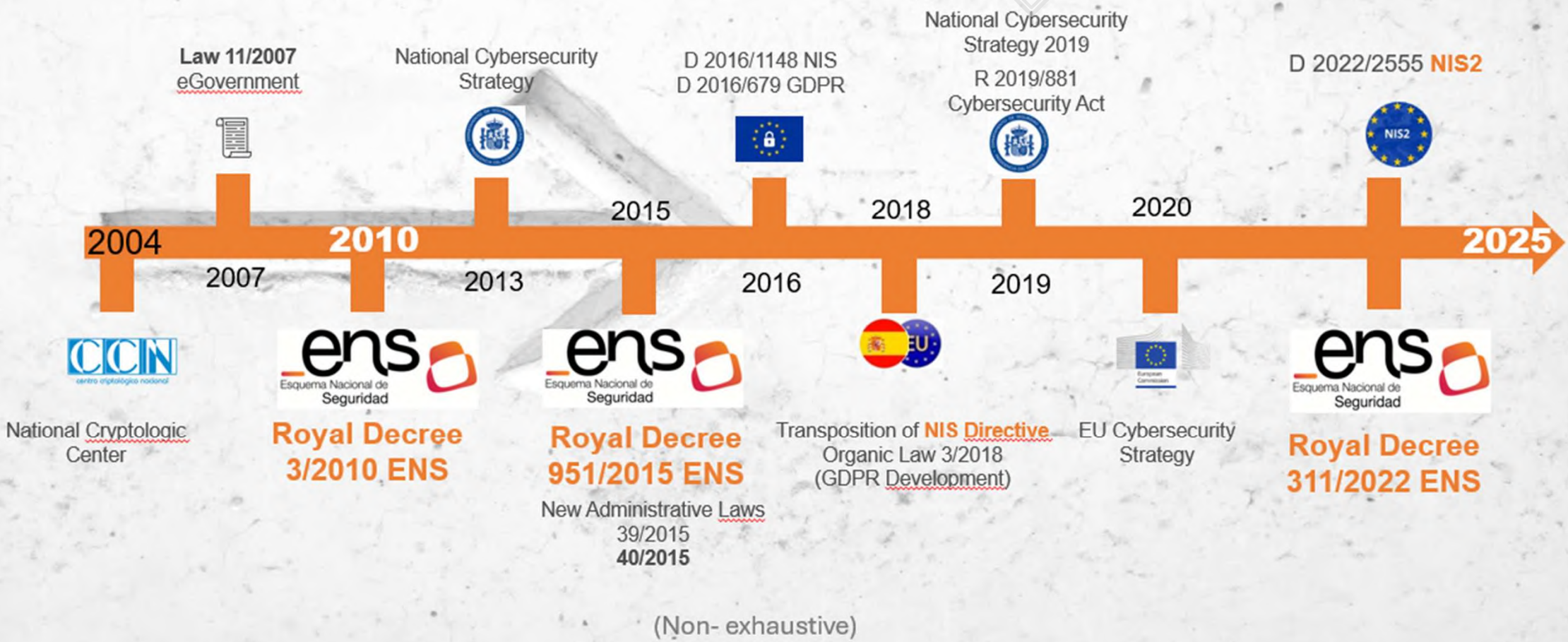
PUBLIC



Spain’s case as a proof of concept

The National Security Framework (ENS)

A collective and multidisciplinary effort, along the time



(Non- exhaustive)

More than 15 years of EXPERIENCE

PUBLIC

FACILITY IN THE COMPLIANCE

Tools and guides made available to the user to facilitate adequacy and compliance.

ECOSYSTEM EXPERT

Auditors with more than 11 years of experience in the certification of the National Security Framework.

MATURE CERTIFICATION AUDIT

Certifying bodies with a track record, aligned criteria and continuous training.

REFERENCE FOR PRIVATE SECTOR

The ENS is one of the **few national security frameworks in Europe** adopted by large technology companies.

360º PUBLIC SECTOR COVERAGE

Practical and real application from the town hall or smaller local entity to the large critical operator.
al operator.

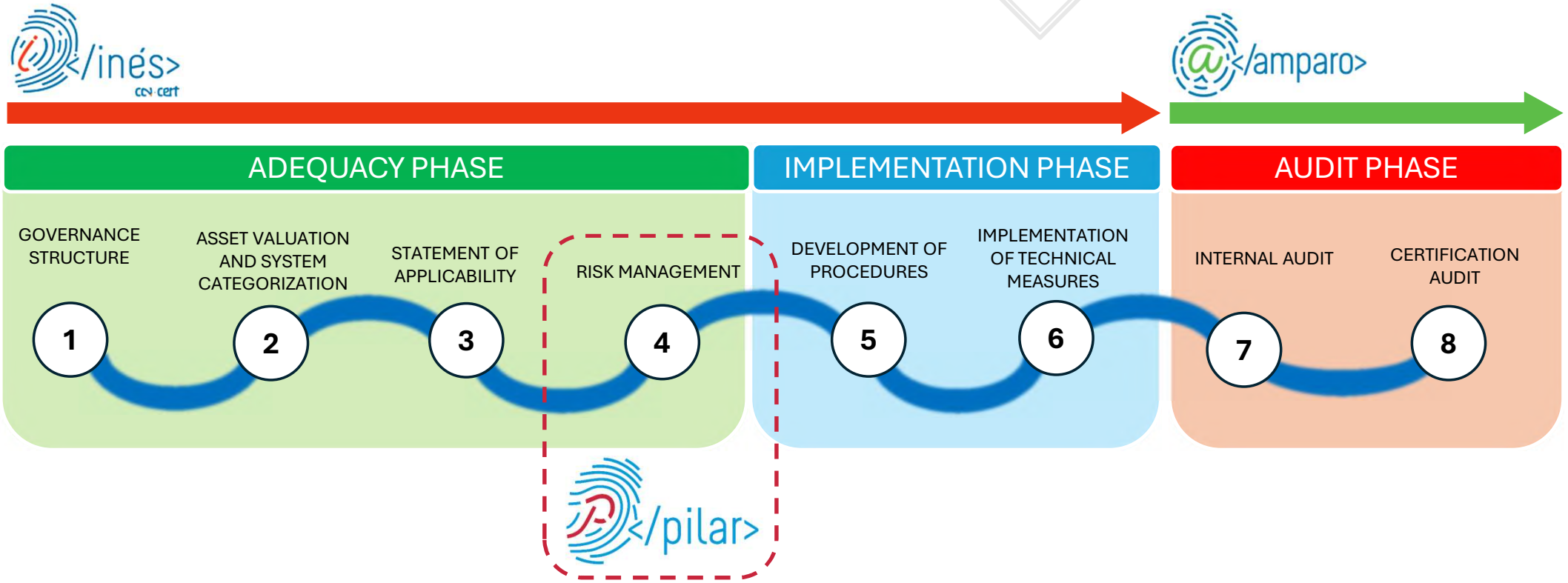
Microsoft
Google Cloud
ORACLE CLOUD
aws
IBM

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN
MINISTERIO DE SANIDAD
MADRID

CCN centro criptológico nacional

PUBLIC

ENS lifecycle phases



CCN tools for ENS compliance

PUBLIC

GOBERNANZA de la ciberseguridad nacional

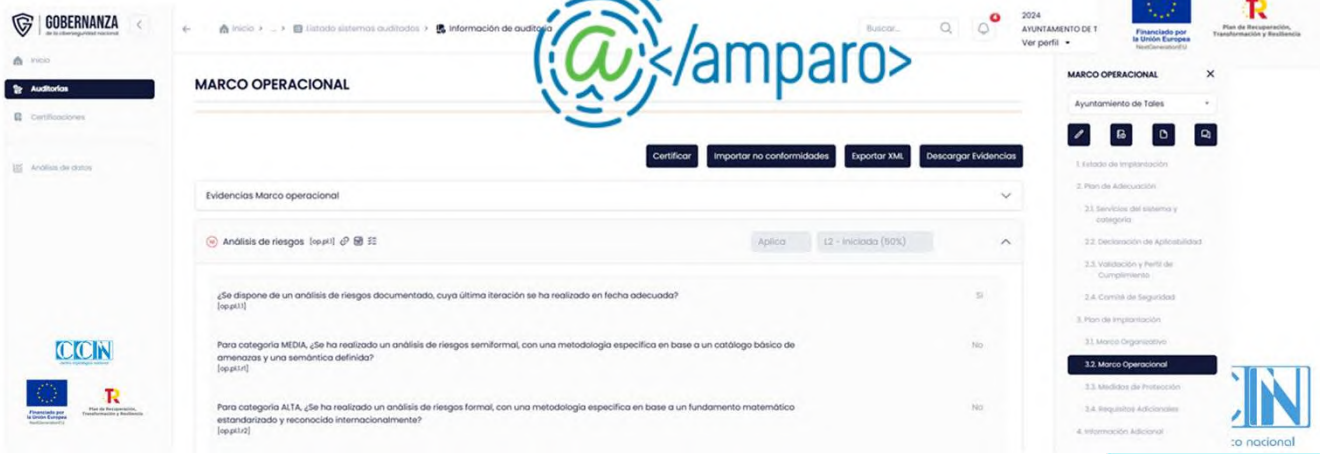
</pilar>



</inés>
CCN-CERT



</amparo>





PUBLIC

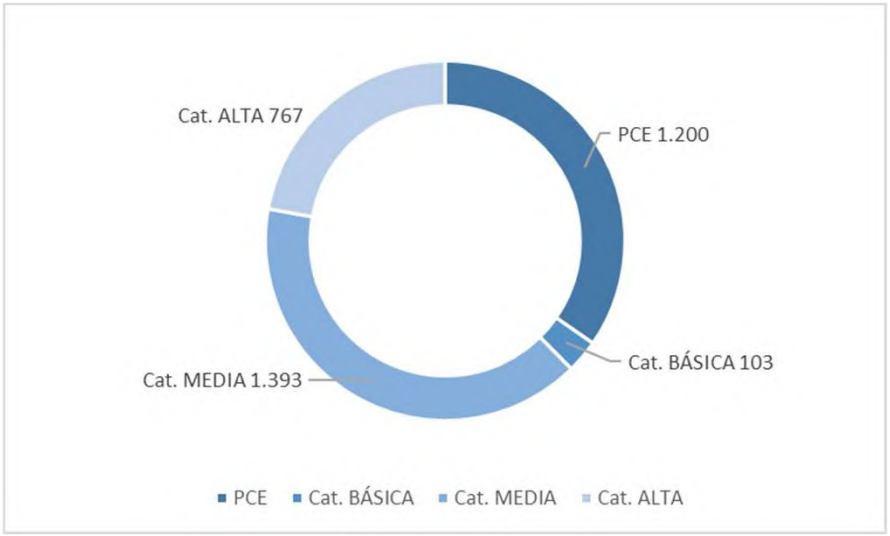
ENS alignment with standards and regulations

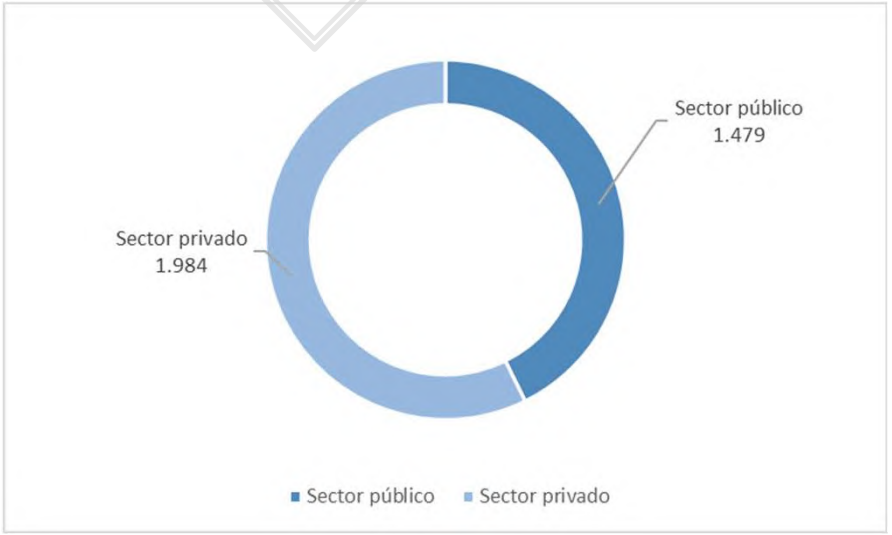
- Aligned with other international standards
  - Facilitates obtaining other certifications



  - Having another certification makes it easier to obtain the ENS certification
- It is aligned with Spanish regulation on data protection
  - Spanish legislation derived from the GDPR requires obligated entities to adopt the security measures established by the ENS (DA1 of LO 3/2018) .

More than 5000 entities certified





PUBLIC

ENS TOOLS



Red Nacional de SOC

PNNSC Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes

- **amparo** — IMPLANTATION AND CONFORMITY ENS
- **ada** — MALWARE ANALYSIS
- **carmen** — DEFENCE AGAINST ADVANCED ATTACKS
- **gloria** — LOGS MANAGER
- **loreto** — CLOUD STORAGE
- **ana** — AUDIT AUTOMATIZATION
- **clara** — DEFENCE AGAINST ADVANCED ATTACKS
- **iris** — STATUS OF CYBERSECURITY
- **pilar** — RISK ANALYSIS
- **lucia** — CYBERINCIDENT MANAGEMENT
- **claudia** — DETECTION OF COMPLEX THREATS
- **marta** — ADVANCED ANALYSIS OF FILES
- **vanesa** — STREAMING VIDEO RECORDS AND EMISSIONS
- **inés** — STATE OF SECURITY REPORT
- **μclaudia** — VACCINATION CENTER
- **elena** — VIDEOVIGILANCE TECHNICAL SIMULATOR
- **elsa** — LOCAL EXPOSURE AND ATTACK SURFACE
- **olvido** — DELETE OF DATA
- **metaolvido** — MANAGEMENT OF METADATES
- **mónica** — EVENT MANAGEMENT AND SECURITY INFORMATION
- **reyes** — EXCHANGE OF CUIBERAMENAZAS INFORMATION

*We do not only offer guides and supporting documentation for compliance with the National Security Framework, but also an **ecosystem of tools** designed to comprehensively strengthen the security of administrations and other public and private entities.*

CCN centro criptológico nacional

CONCLUSIONS ON THE SPANISH ENS

PUBLIC

The ENS is not only a legal framework or a certification scheme for entities.
It is an operational governance ecosystem, supported by tools, guidance, audit mechanisms and measurable evidence.

It is also a living framework, designed to evolve through continuous monitoring, periodic reassessment and the permanent updating of its security requirements.

This makes it a **useful building block** not only for NIS2, but also for providing reusable cybersecurity evidence where requirements overlap with other EU regulatory frameworks.

A mature framework — but also an adaptable one.

And adaptability becomes particularly important when we look at the speed of technological change and AI.

PUBLIC

EU cyberposture: the current logic

CCN
centro criptológico nacional

EU cyberposture: the current logic

1. Under article 86, once a CSA's European certification scheme enters into force, the national certification schemes covering the same subject matter and scope cease to produce effects.

2. The proposed cyber posture framework is intended to facilitate compliance with NIS2 and other relevant Union cybersecurity requirements.

3. In the meantime, Member States are already implementing NIS2 through national regulatory, supervisory and assurance frameworks.

4. Many Member States are already developing or using national frameworks, assurance mechanisms and supervisory arrangements to operationalise NIS2 requirements.

PUBLIC

CCN
centro criptológico nacional

Cyberposture is not product certification

PUBLIC

Assessing the cyber posture of an entity is fundamentally different from certifying a product.

Cyber posture involves:

- **risk-based assessment**, not only compliance with a closed set of requirements;
- **cybersecurity governance**, responsibilities and organisational processes;
- **alternative or compensating measures** that may achieve an equivalent security outcome;
- adaptation to the entity's **changing risks, technologies and threat environment**.

A rigid, closed set of requirements may work for certain product certifications. It is much more difficult to apply to the evolving cyber posture of an organisation.

This challenge becomes even greater in the AI era, where technologies, attack techniques and risks may evolve faster than a European certification scheme can be formally updated.

The risk: harmonization by replacement

PUBLIC

LEVELLING DOWN

- If a future EU cyber posture scheme provides a lower level of assurance than an existing mature national framework, replacing that framework could result in **levelling down rather than levelling up**.

- For Spain, replacing a framework with more than 15 years of experience and more than 5000 public and private entities certified with a lighter scheme, would represent a loss of existing cybersecurity maturity for the whole society making it more vulnerable.

The risk: harmonization by replacement

PUBLIC

TRANSITION COSTS

- Member States may face significant transitional and administrative costs where existing national frameworks overlap with a future EU cyber posture scheme.

Possible consequences:

- re-certification and duplicated assessments;
- adaptation of national legislation;
- transition of existing certificates;
- impact on national auditors/CAB ecosystems;
- adaptation of supervisory processes;
- uncertainty for already certified entities.

PUBLIC

Proposal for the CSA's cyber posture of entities

CCN
centro criptológico nacional

Two ways of harmonize

Harmonization by replacement	Smart Harmonization
Replace national schemes	Build on national frameworks and capabilities
Re-certify	Reuse evidence
Duplicate assessments	Map equivalent requirements
One size fits all	Common outcomes, different mature mechanisms
Risk of levelling down	Preserve higher maturity
Transition costs	Bridging only where gaps exist

PUBLIC

Spain's model for Smart European harmonization

PUBLIC

1. COMMON EUROPEAN OBJECTIVES

Common cybersecurity outcomes and assurance requirements across the EU

→ **Same level of trust, regardless of the mechanism used**

2. RECOGNISE NATIONAL MATURITY

Preserve and recognise mature national frameworks and schemes

→ **Do not replace capabilities that already provide equivalent assurance**

3. REUSE EVIDENCE

Reuse audits, assessments and evidence already produced under national frameworks

→ **Same requirement, same evidence, no unnecessary second audit**

CCN
centro criptológico nacional

Spain's model for Smart European harmonization

PUBLIC

4. RECOGNITION / EQUIVALENCE

Enable mutual recognition or equivalence where national frameworks provide substantially comparable assurance

→ **Towards "certified once, accepted across Europe"**

5. COMPLEMENT, NOT REPLACE, SUPERVISION

European certification can support compliance, but should not replace NIS2 risk-based supervision or national powers

→ **Continuous assurance, not only point-in-time certification**

EUROPEAN ADDED VALUE

Connect national capabilities → create interoperability → increase trust → strengthen the Internal Market

CCN centro criptológico nacional

Cybersecurity harmonization in a fast-changing threat landscape and the impact of AI

PUBLIC

Cybersecurity requirements cannot remain static while technology and threats evolve continuously.

AI is accelerating this challenge:

- new attack techniques emerge faster;
- vulnerabilities can be discovered and exploited more rapidly;
- assurance requirements may need to be adapted before a European certification scheme can be formally revised.

The risk: **A highly rigid European scheme for entities may provide harmonisation, but at the cost of adaptability.**

Cybersecurity harmonization in a fast-changing threat landscape and the impact of AI

PUBLIC

European schemes necessarily require coordination, consultation and formal amendment procedures.

National frameworks can often react faster to:

- emerging threats;
- new technologies;
- sector-specific risks;
- lessons learned from supervision and incidents.

The principle: European harmonisation should establish a common baseline — not a ceiling on cybersecurity maturity.

National flexibility can be a resilience mechanism for Europe.

CCN
centro criptológico nacional

Cybersecurity harmonization in a fast-changing threat landscape and the impact of AI

PUBLIC

Our concern is not only what happens when a European scheme enters into force.

Our concern is what happens five years later, when technology, AI and the threat landscape have evolved, but the scheme has not yet been updated.

This is why we believe that mature national frameworks should not be seen as temporary solutions waiting to disappear. **They can act as laboratories of innovation and resilience, allowing Member States to react to new risks while maintaining a common European baseline.**

In the age of AI, regulatory agility is itself a cybersecurity capability.

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

AEAD
AGENCIA ESTATAL
DE ADMINISTRACIÓN DIGITAL

CCN
centro criptológico nacional



Many thanks

For further information on the ENS:

- serviciosciber@ccn.cni.es
- Alma A. cop.gr@ccn-cert.cni.es
- https://ens.ccn.cni.es/en

Photo by Marvin Meyer on Unsplash