Spanish sheme for MSS

+ CCN-STIC 896

1 SPANISH APPROACH

1 Model Basis

- Based on the National Security Framework (**ENS**).(16 years old)

+

- MSS certification is carried out using the **CCN-STIC 896**.

2 Alignment with Europe

- Aligned with the **NIS2**
- Aligned with the **CSA+**

3 Scope of application

- **Public Sector** Providers (mandatory).
- **Private providers** that provide services to the public sector.
- **Private sector** in general (voluntary/recommended).

4 Key Principle: Dual Assurance Model

- **Security of the infrastructure** supporting the services (ENS certification and Guide 896 specific mandatory requirements).
- **Operational capacity and capabilities of the service** (resources, skills, processes, procedures, and technology).

Esquema Nacional de Seguridad

Spanish scheme is not **certifying** only the service provider, but **the complete service** supply and its environment.

2 HOW DOES THE 896 MODEL WORK?

CCN-STIC 896 (Certi MSS) defines how to structure, evaluate, protect and certify MSS services.

Security Controls (Horizontal layer)

- Based on the **ENS, reinforced** with specific and **mandatory requirements** for MSS services. (36 controls)

Certified Services (Vertical layer)

The model covers the entire cybersecurity life cycle:

- These services reflect the **complete lifecycle of incident management** as well as cybersecurity **capacities and capabilities on execution**.
- Each service is broken down into specific capacities and capabilities (e.g., monitoring, threat hunting, incident response).
- The model is not solely about regulatory compliance; it evaluates and evidence real operational execution.

SOCs Maturity Level

ENS + Guide CCN-STIC896 combination **helps to move forward higher maturity level** of operations.

3 CONTRIBUTION FOR EUROPE

Spain already implemented **a proven model** that combines regulation, security, and real-world operation.

Value of the Model

- **Integrates** regulatory compliance, operation, reliability, and service quality.
- **Evaluates**:
  - **Operational Capabilities**
  - **Technical competencies of personnel.**
  - **System security**

Spain is not in the model design phase, but rather in the phase of **real and consolidated operation**.

3 CONTRIBUTION FOR EUROPE

ENS is not just a national framework — it is already adopted by leading **global and European** industry players.

ENS Adoption Across Global & European Leaders

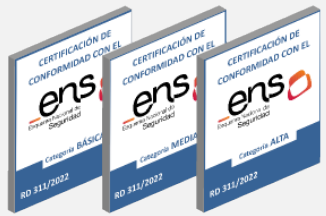
Global Cloud & Technology
Microsoft (USA)
AWS (USA)
Google Cloud (USA)
IBM (USA)
Oracle (USA)
SAP (Germany)
OVHcloud (France)

Global Consulting & Cyber MSS
Accenture (Ireland)
Deloitte (UK)
PwC (UK)
EY (UK)
Capgemini (France)
Atos (France)

European Industry & Defence
Thales (France)
Airbus (EU)
Siemens (Germany)

Telecommunications
Telefónica (Spain)
Orange (France)
Vodafone (UK)

Spanish Ecosystem (Other Sectors)
Santander, BBVA (Banking)
Iberdrola, Repsol, Endesa (Energy)
Indra, GMV (Cyber & Defence)



https://ens.ccn.cni.es/

https://www.ccn.cni.es

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

Thanks for your attention