yolandasabuco.io

Why the Spanish Security Framework (ENS) is a must-to-know in healthcare sector even if you are not based in Spain?

More information

What is it ?

It is the **cornerstone of information security** in Spain and a mandatory legal requirement for any company collaborating with the Public Administration directly or indirectly.

Its **official website managed by Spanish National Cryptologic Centre (CCN-CERT) has documentation and online resources as:**

- security policies templates,
- standard operating procedures (SOPs) templates,
- security guidelines at different levels and adapted to many technologies.

Serving as a valuable source even if you are implementing another type of cybersecurity regulation.

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

Examples of useful resources in healthcare →

Essential Resources for the Healthcare Sector

The Spanish National Cryptologic Centre (CCN-CERT) offers specific guides to facilitate compliance in the health field:

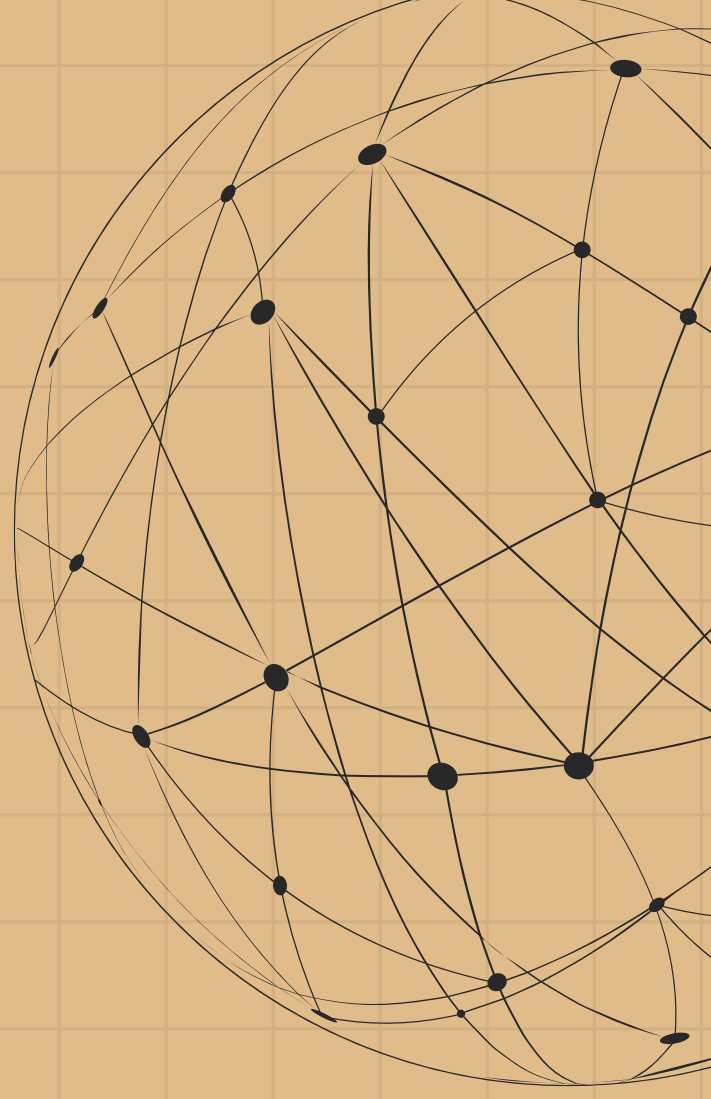
Security requirements for E-health Applications (CCN-STIC 857): For solution providers and healthcare software architects and developers.

Specific Compliance Profile for Health (CCN-STIC 891): Practical guide for adherence to the ENS in the provision of healthcare services to patients (Primary and Specialized Care).

Relation with other European Legal Frameworks →

yolandasabuco.io

Synergies with the European Legal Framework

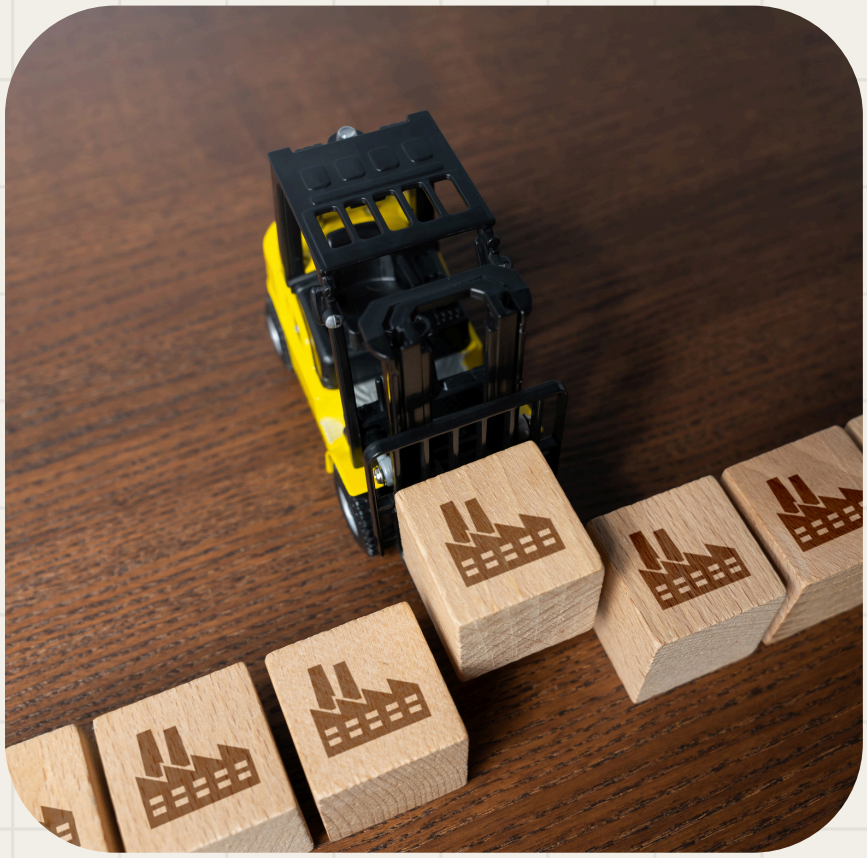


A good model to implement NIS2 ?

ISO 27001	The ENS is inspired by the ISO 27000 family of standards, making it easier for companies to integrate both security management frameworks. **Mapping between the ISO 27001:2022 Standard and the RD 311/2022 (ENS)**
NIS / NIS2 & Cybersecurity Act	The ENS is the primary security framework in Spain. Its compliance lays the foundation security requirements mandated by the NIS and NIS2 Directive. **Spain presents to the European Union the alignment of the National Security Scheme with the requirements of the NIS2 Directive**
GDPR	The ENS demands the rigorous technical measures necessary to protect personal data and, thus, is the mechanism for materializing the security obligation established by the GDPR.

Scope in Spain →

Mandatory Scope



- **Public Sector**: It is mandatory for all General State Administration, Autonomous Communities, and Local Entities.
- **Collaborating Suppliers**: It applies to all suppliers and companies that collaborate with the Public Sector.

It affects you even without a direct contract with the Spanish Public Administration because a key feature is its ***strong focus on supply chain security.***

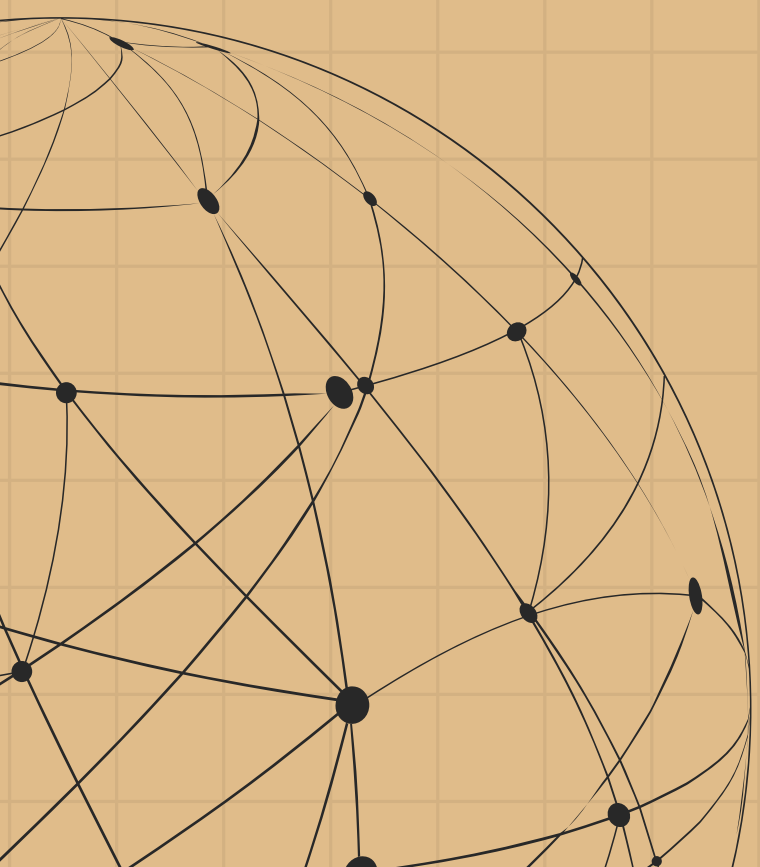
Scope in Healthcare

yolandasabuco.io

Critical Focus: The ENS in the Healthcare Sector

Compliance is required from:

- **Health Services**: Hospitals, health centers and regional health services.
- **Healthcare Information Technology Providers**: Any company that manages, processes, or maintains patient information (electronic health record systems, appointment platforms, laboratory information systems etc.).



Certification requirement

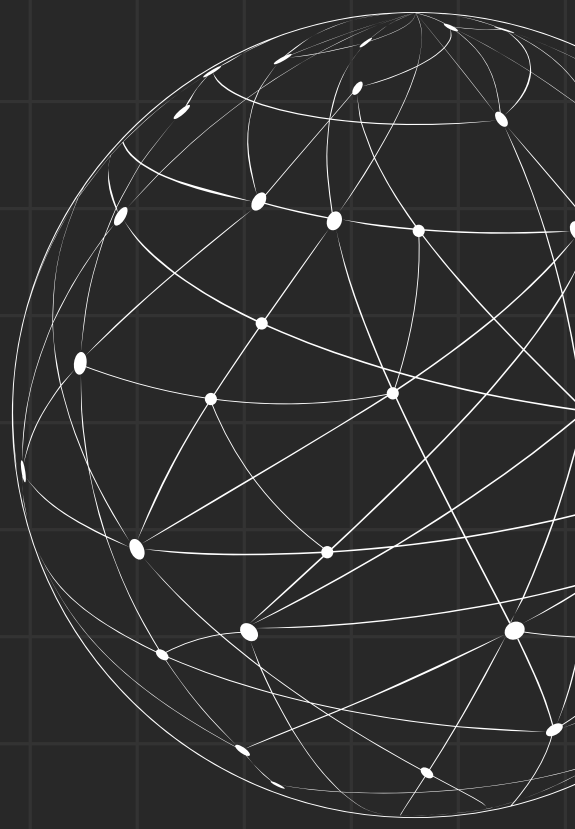
Certification Requirement

Since health data is a special category of data, systems must be categorized as minimum **MEDIUM** or **HIGH** security category.

For Medium and High-category systems, the ENS requires the implementation of a Security Management System that must be validated through an **external audit, with a minimum frequency of every two years.**

From theory to practice: sharing direct lessons to drive digital health.

More information at yolandasabuco.io



Was this post **Helpful?**

Contact me:

yolandasabuco.io

yolanda-sabuco-garcia

yoliyu

info@yolandasabuco.io