SGS Certification Services for the **Spanish National Security Framework (ENS)**

DELIVER SECURE INFORMATION SYSTEMS TO THE SPANISH PUBLIC SECTOR

sgsbrightsight.com

SGS brightsight

Data security is crucial in today's interconnected world.

Without proper protection, sensitive information on your systems is vulnerable to cyberattacks. The Spanish National Security Scheme (Esquema Nacional de Seguridad, or ENS) of Spain provides a framework of security requirements to safeguard information within electronic administration. Its goal is to ensure the protection of personal and confidential data exchanged through online channels, thereby strengthening trust in digital public services. Compliance with ENS standards demonstrates that your information systems are secure, reliable and meet both industry and governmental requirements.

SGS Brightsight offers comprehensive solutions to help you successfully access the Spanish public sector with security-compliant information systems, enabling risk mitigation and market differentiation.

The ENS – security requirements for information systems

The ENS applies to the entire public sector, as well as to suppliers that collaborate with the government. It offers a common framework of basic principles, requirements and security measures for the adequate protection of the information processed and the services provided. This helps to ensure access, confidentiality, integrity, traceability, authenticity, availability and conservation of electronic data, information and services.

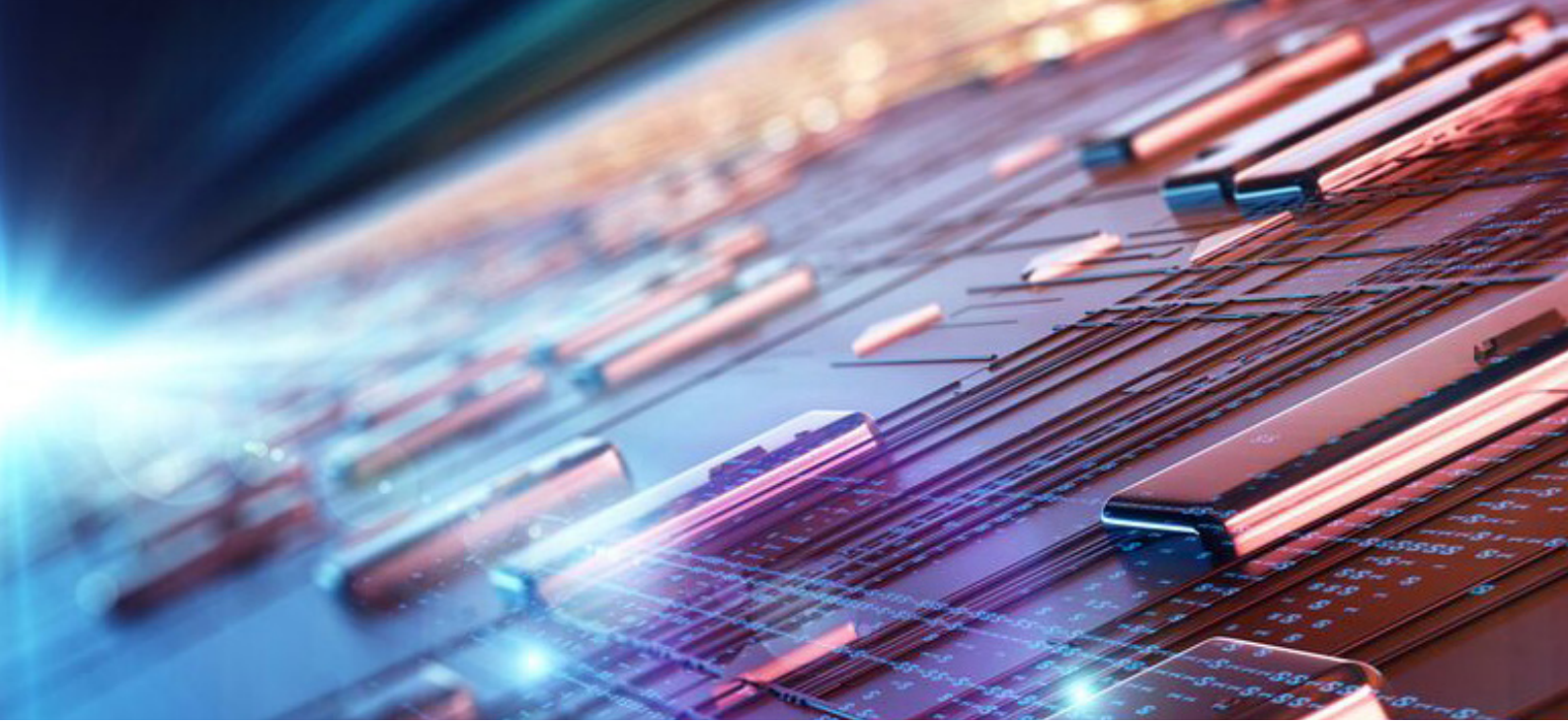
Since its first development in 2010, the ENS has been in constant evolution, with notable modifications in 2015, and was last updated in 2022 (Royal Decree 311/2022).

The ENS creates the legal framework for Spain to align with the European Directive on network and information system security, as well as national and European cybersecurity strategies. It addresses different standards such as the General Data Protection Regulation (GDPR), ISO 22301 (Business Continuity), ISO 27001 and a wide range of 70 technical measures to protect networks and information systems to enable interaction with Spanish public sector organizations. The three system categories under the ENS scheme are Basic, Medium, and High. The Basic category can be achieved by a self-declaration. The Medium and High categories require certification from an accredited Certification Body (CB).

BASIC

MEDIUM

HIGH



Security regulatory landscape in Spain

CCN

The National Cryptologic Center (CCN) is the organization responsible for coordinating the activities of the public sector entities that use resources or encryption procedures, ensuring the security of information technologies across all areas. The CCN also oversees the coordinated acquisition of cryptology materials and provides training for public sector personnel specializing in this field.

The CCN was created in 2004 by a Spanish Royal Decree 421/2004, assigned to the CNI (National Centre of Intelligence). Spain's Act 11/2002 of May 6 regulates the CNI and entrusts it with all functions regarding the security of information technologies and protection of classified information. The Secretary of State Director is responsible for running the National Cryptology Center. The CCN shares environments, procedures, regulations and resources with the CNI.

CPSTIC PRODUCT CATALOGUE

The CPSTIC is the CNN's catalog. It helps public and private entities find security products and services for information and communication technology (ICT) systems under the ENS. These products have certified security functionalities and are suitable for use in systems affected by the ENS, in any of its categories (High, Medium and Basic). The classification field in each product's file indicates the highest ENS category (High or Medium) for which the product is suitable. Products classified as High may be used in systems categorized as ENS High, Medium, or Basic, while products classified as Medium may be used in systems categorized as ENS Medium or Basic.

COMMON CRITERIA

Common Criteria, or CC, (ISO/IEC 15408) is the most comprehensive and widely recognized set of standards for IT security certification. This standard is essential for IT systems and devices providing security functions, and has been adopted by more than 25 countries. Specific national requirements often require a CC certificate before product launch, especially for national identification documents, such as e-passports and national ID cards. In Spain, the CCN is the national scheme for Common Criteria.

LINCE

LINCE, developed by the CCN, is a cybersecurity evaluation and certification methodology in Spain. It is part of the National Evaluation and Certification Scheme of Spain (ENECSTIC). The LINCE methodology is intended specifically for ICT products and services that need to demonstrate a medium or basic level of security. As a result, LINCE security evaluations are shorter, leading to reduced processing times and lower costs.

Our Services

We offer comprehensive services through our ENS Certification Body (CB) to support you throughout all phases of the ENS certification process, enabling you to fast-track your products and services to market.

Additionally, our IT Security Evaluation Facility (ITSEF) provides a full range of supplementary services, including developer support, pre-assessment and evaluation services for the Spanish Common Criteria (CCN) and the LINCE methodology.

CERTIFICATION BODY SERVICES FOR ENS

As an ENAC-accredited Certification Body (Accreditation No: 220/C-PR466), we offer comprehensive certification services for information systems to ensure compliance with the ENS.

ENS certification is valid for up to two years. According to Article 38 of the ENS, information systems must be subject to a regular audit at least every two years, to verify compliance with the requirements of the ENS. The certification process includes the following stages:

- **Audit -** assessment of the basic principles and minimum requirements defined in Annex II of Royal Decree 311/2022
- **Audit report**
- **Technical review**
- **Decision**
- **Certificate issuance**

SUPPLEMENTARY ITSEF SERVICES FOR SPANISH CC

PRE-EVALUATION

Our comprehensive ITSEF pre-evaluation training and developer support services help developers gain a better understanding of the Spanish CCN and LINCE methodology requirements for their products. This will reduce the potential for failure during formal security evaluations

- **Workshops/training**
- **Ongoing developer advisory support**

SECURITY EVALUATION

- **Security evaluation for CCN/LINCE**
- **Evaluations for entry in the CPSTIC catalog**
- **Product security testing:**
  - Product analysis
  - Code analysis
  - Vulnerability analysis
  - Penetration testing

WHY SGS BRIGHTSIGHT?

With 40 years of experience in cybersecurity and a growing global network of specialist testing facilities, we are the world's number one security evaluation service provider with over 700 security evaluations completed every year.

We are also an accredited certification body, offering comprehensive certification services to help you prove compliance with a wide range of security requirements.

We understand the market and the technical requirements relevant to your component, device or system. Our dedicated team of security experts supports the streamlining of evaluation criteria into a single assessment process that incorporates all relevant global, regional and vendor requirements – one evaluation, multiple certifications. We are your first choice for independent testing, developer support and certification services, when you want to efficiently deliver secure information systems that comply with Spanish security legislation.

When you need to be sure

SGS Brightsight
Brassersplein 2
2612CT Delft
The Netherlands

+31 (0)15 269 2500

brs.sales@sgs.com

sgsbrightsight.com