

ENS (Esquema Nacional de Seguridad) — RD 3/2010 (as amended by RD 951/2015)



Spain's national cybersecurity and digital regulation sets legal requirements for managing cybersecurity risks, reporting incidents, and protecting essential

What it is

The Esquema Nacional de Seguridad (ENS) is the Spanish National Security Framework that establishes cybersecurity and data protection requirements for public sector organizations and service providers handling government information. ENS aims to promote a consistent and robust approach to managing information security risks and safeguarding critical public data.

Published by the Spanish government, specifically the Ministry for Digital Transformation and Public Service, ENS applies to national, regional, and local public administrations, as well as private entities delivering services to the public sector. The framework covers key areas such as cybersecurity controls, risk management, operational resilience, and regulatory compliance, aligning with both European and international standards.

At a glance

PUBLISHER Centro Criptológico Nacional (CCN)	TYPE Regulation	VERSION ENS — Royal Decree 311/2022
EFFECTIVE April 29, 2022	DOMAIN Cybersecurity	FAMILY Other
REGION Spain	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://ens.ccn.cni.es/es/>

Why it matters

- Strengthen national cybersecurity posture** Enable organizations to proactively identify and mitigate evolving threats targeting Spain's critical digital and information systems.
- Enhance regulatory compliance** Support organizations in meeting national and European cybersecurity and privacy obligations, reducing legal liabilities and non-compliance risks.
- Promote coordinated incident response** Facilitate faster, more cohesive response to incidents by defining communication protocols and reporting requirements across sectors.
- Protect sensitive digital assets** Safeguard personal data, intellectual property, and critical business processes from unauthorized access, loss, or manipulation.

How SmartSuite supports ENS

System Classification and Scope

Track ENS security level classification and define boundaries with clarity.

ENS Control Library and Ownership

Manage ENS controls with owners, procedures, and implementation evidence.

Evidence and Audit Trail

Centralize policies, configurations, and proof tied to each ENS requirement.

Monitoring and Vulnerability Cadence

Schedule scanning, patching, and monitoring activities with evidence of execution.

Supplier and Service Provider Oversight

Track vendor safeguards, contracts, and ongoing monitoring evidence.

Audit and Review Readiness Reporting

Report control status, gaps, exceptions, and progress for audits and reviews.

Common framework mappings

CIS Controls v8.1

ENS RD 311/2022

GDPR

ISO 27001:2022

ISO 27002:2022

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

Esquema Nacional de Seguridad (ENS) Framework

Defines cybersecurity and data protection requirements for public sector in Spain.

ens.ccn.cni.es/es

Guía de Seguridad de las TIC: ENS Guide

Provides implementation guidance for applying ENS within organizations.

ccn.cni.es

ENS Control Catalog

Outlines technical requirements and controls for compliance with ENS.

ens.ccn.cni.es/es/normativa

Frequently asked questions

What is the Spain BOE-A-2022-7191 National Cybersecurity and Digital Regulation used for?

This regulation establishes the minimum cybersecurity requirements for critical infrastructures and essential digital services in Spain. Its purpose is to strengthen national resilience against cyber threats and ensure continuity of critical digital operations.

Is compliance with the Spain BOE-A-2022-7191 National Cybersecurity and Digital Regulation mandatory?

Yes, compliance is mandatory for all operators of essential services and digital service providers defined under Spanish law. Regulatory enforcement includes significant penalties for non-compliance and periodic supervisory assessments.

Who must comply with the Spain BOE-A-2022-7191 Regulation?

The regulation applies to operators of critical infrastructure, essential service providers (such as energy, transport, and health sectors), and digital service providers operating within Spain. Organizations must determine their status as defined by the regulation to assess applicability.

What are the key concepts and requirements of the Spain BOE-A-2022-7191 Regulation?

Key concepts include risk management, incident reporting, secure system design, and operational control implementation. Organizations must establish cybersecurity policies, conduct regular risk assessments, and maintain evidence of compliance through documentation and technical controls.

How should organizations implement the Spain BOE-A-2022-7191 Regulation?

Implementation involves conducting a risk analysis, identifying relevant assets and threats, establishing technical and organizational security measures, and training staff on compliance requirements. Regular monitoring, incident response planning, and maintaining audit trails are essential steps.

How does Spain BOE-A-2022-7191 relate to other cybersecurity frameworks?

Spain BOE-A-2022-7191 aligns with broader European frameworks such as the NIS Directive and GDPR, while providing country-specific requirements. Compliance may leverage ISO 27001 or NIST standards, but organizations must ensure they meet the unique obligations specified in the regulation.

What are the ongoing compliance requirements for Spain BOE-A-2022-7191?

Ongoing requirements include periodic risk assessments, continuous monitoring of security controls, prompt incident reporting to competent authorities, and regular internal or external audits. Documentation and evidence retention are critical for demonstrating compliance.

How would SmartSuite support Spain BOE-A-2022-7191 (National Cybersecurity and Digital Regulation)?

SmartSuite can streamline compliance by enabling organizations to track risks, map and manage required controls, collect relevant evidence, and automate audit workflows. It supports continuous monitoring, facilitates incident reporting, and provides comprehensive reporting for regulatory reviews.

What is the Spain ENS used for?

The Spain ENS establishes cybersecurity and data protection requirements for public sector organizations and service providers handling government information. It aims to protect critical public data, ensure consistent approaches to information security, and mitigate cyber risks across all levels of Spain's public administration.

Is compliance with the Esquema Nacional de Seguridad required?

Yes, compliance with the ENS is mandatory for national, regional, and local public administrations in Spain, as well as for private entities delivering services to the public sector. The framework is enforced by regulatory authorities to ensure uniform security standards are maintained within the public sector ecosystem.

Who does the Spain ENS apply to?

Spain ENS applies to all public sector organizations, including ministries, agencies, and local governments, in addition to private companies that manage or process government information or provide services to public bodies. The scope covers both IT systems and supporting infrastructure handling government data.

What are the core concepts and required artifacts in the ENS?

Key ENS concepts include system classification (basic, medium, or high assurance), risk assessment, and implementation of security controls across several domains. Required artifacts typically include risk registers, security policies, operational procedures, incident response plans, audit logs, and records demonstrating ongoing compliance.

How do organizations implement the Spain ENS?

Organizations implement ENS by classifying information systems based on criticality and risk, conducting impact and risk assessments, and selecting the appropriate set of mandatory security controls corresponding to their assurance level. Regular audits, internal monitoring, and continuous improvement processes are integral to sustained compliance.

How does the Spain ENS relate to other frameworks like ISO 27001?

The ENS aligns with ISO 27001 by incorporating risk-based methodologies, control catalogs, and information security management principles. However, ENS includes specific requirements tailored to the Spanish public sector and introduces three assurance levels, mapping controls to national legal and regulatory mandates.

What are the ongoing compliance requirements for ENS?

Ongoing ENS compliance requires periodic risk assessments, regular self-assessments or third-party audits, continuous monitoring of control effectiveness, incident management, and maintaining thorough documentation as evidence of compliance. Organizations must keep policies current and demonstrate timely remediation of identified risks.

How would SmartSuite support Spain ENS (Esquema Nacional de Seguridad)?

SmartSuite supports ENS management through centralized risk registers, configurable control libraries mapped to assurance levels, and automated compliance tracking. It enables evidence collection, stores audit-ready documentation, and provides dashboards for real-time visibility of control status, outstanding risks, and remediation progress, supporting continuous compliance and reporting

License included / downloadable: Yes Spain's BOE publishes BOE-A-2022-7191; the National Cybersecurity and Digital Regulation is publicly available via the official BOE website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/spain-ens-esquema-nacional-de-seguridad