

CCN-STIC 825

CCN-STIC 825 provides technical guidance and compliance measures to strengthen cybersecurity for Spanish public administrations and critical systems.



What it is

Spain CCN-STIC 825 is a cybersecurity compliance and technical guidance framework that helps organizations in Spain strengthen information security controls and align with national regulatory requirements.

Published by the Centro Criptológico Nacional (CCN), a division of Spain's National Intelligence Centre, CCN-STIC 825 is primarily used by public sector entities, critical infrastructure operators, and organizations handling sensitive government information. The framework covers a broad range of areas, including risk management, implementation of technical security measures, incident response, and compliance with Spanish cybersecurity legislation.

At a glance

PUBLISHER Centro Criptológico Nacional (CCN)	TYPE Guidance	VERSION 2023
EFFECTIVE 21 July 2023	DOMAIN Cybersecurity	FAMILY Other
REGION Spain	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html>

Why it matters

- **Strengthen cybersecurity governance** Establishes clear policies and responsibilities, supporting better oversight and strategic management of cybersecurity across the organization.
- **Enhance regulatory compliance** Aligns security controls with Spanish legal and regulatory requirements, reducing compliance gaps and supporting audit readiness.
- **Improve incident detection and response** Provides structured protocols and technical measures, enabling faster identification and effective management of cybersecurity threats.
- **Support operational resilience** Facilitates continuity planning and incident recovery, minimizing the impact of cyber incidents on business operations and critical services.

How SmartSuite supports CCN-STIC 825

Technical Control Framework Library

Structure CCN-STIC controls aligned to ENS domains with ownership and implementation tracking.

ENS System Level Mapping

Map systems to ENS levels (Basic, Medium, High) and align required technical measures.

CCN-STIC Risk and Control Mitigation

Link risks to CCN-STIC controls and manage mitigation activities across environments.

Secure Configurations and Continuous Monitoring

Track secure configurations, system hardening, and continuous monitoring activities.

Detection, Response, and Incident Documentation

Manage detection, response workflows, and incident documentation aligned to national requirements.

ENS and CCN Audit Readiness Reporting

Provide dashboards showing control coverage, system status, and readiness for ENS/CCN audits.

Common framework mappings

[CIS Controls v8.1](#)
[COBIT 2019](#)
[GDPR](#)
[ISO 27001:2022](#)
[ISO 27002:2022](#)
[NIST CSF 2.0](#)
[NIST 800-53 Rev.5](#)
[PCI DSS 4.0.1](#)
[SOC 2](#)

Official resources

Alaska Consumer Protection Unit

Outlines resources and guidance for compliance with Alaska's data breach laws.

law.alaska.gov/departments/civil/consumer/cpindex.html

ANSSI Cloud Security Guidance

Outlines security principles and recommendations for cloud service providers in compliance with ANSSI standards.

cyber.gouv.fr/enjeux-technologiques/cloud

APEC Privacy Framework Overview

Describes the structure and objectives of the APEC Privacy Framework.

[apec.org/publications/2017/08/apec-privacy-framework-\(2015\)](http://apec.org/publications/2017/08/apec-privacy-framework-(2015))

Frequently asked questions

What is Spain CCN-STIC 825 used for?

Spain CCN-STIC 825 is a cybersecurity guideline designed to help Spanish public sector organizations and service providers comply with the Spanish National Security Framework (ENS). It provides technical and organizational measures to protect information systems handling government data. The framework aims to ensure confidentiality, integrity, availability, and traceability of information.

Is compliance with CCN-STIC 825 mandatory?

Compliance with CCN-STIC 825 is mandatory for government agencies and their service providers operating in Spain. It is not a certifiable standard but rather a comprehensive set of technical controls and best practices for ENS compliance. Failing to adhere can result in regulatory consequences and operational risks.

Who does CCN-STIC 825 apply to?

CCN-STIC 825 applies to public sector bodies, their contractors, and any organization providing services to Spanish government entities. The guidance is relevant for any environment processing, storing, or transmitting government information, particularly where ENS compliance is required by law.

What key concepts or artifacts are required by CCN-STIC 825?

Key concepts include risk management, asset classification, and security controls aligned with ENS categories (basic, medium, high). Required artifacts encompass risk analyses, security plans, evidence of implemented controls, incident response documentation, and continuous monitoring records.

How should organizations implement CCN-STIC 825?

Organizations should adopt a risk-based approach, starting with a thorough risk assessment and asset classification according to ENS levels. Implementation involves mapping ENS requirements to technical controls specified in CCN-STIC 825, followed by rolling out and documenting controls, and preparing evidence for audits.

How does CCN-STIC 825 relate to other cybersecurity frameworks?

CCN-STIC 825 is closely tied to the Spanish National Security Framework (ENS) and complements other CCN-STIC technical guides. While similar in intent to frameworks like ISO 27001 or NIST CSF, it is specifically tailored for compliance with Spanish governmental requirements and may incorporate unique local obligations.

What are the ongoing compliance requirements for CCN-STIC 825?

Ongoing compliance with CCN-STIC 825 requires continual risk assessments, regular reviews and updates of security controls, documented evidence of compliance, incident reporting, and annual or periodic internal audits. Maintenance of up-to-date technical and organizational measures is necessary to remain compliant as threats evolve.

How would SmartSuite support Spain CCN-STIC 825?

SmartSuite can help organizations manage compliance with CCN-STIC 825 by enabling centralized risk tracking, control management, and evidence collection aligned with ENS and CCN-STIC 825 requirements. The platform facilitates audit readiness through task management and workflow automation, and provides robust reporting features to demonstrate compliance and support ongoing monitoring efforts.

License included / downloadable: Yes Spain's CCN-STIC 825 guidance is published by Spain's Centro Criptológico Nacional (CCN) and is publicly available for free on the CCN/CNI website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/spain-ccn-stic-825-cybersecurity-compliance-and-technical-guidance