ManageEngine

A quick guide to the ENS

The Esquema Nacional de Seguridad (ENS), regulated by Royal Decree 311/2022, is Spain's national security framework for the public sector. Issued by the Government of Spain and overseen technically by the Centro Criptológico Nacional (CCN), it sets the basic principles and minimum requirements for protecting the information and services that public bodies and their suppliers handle by electronic means.

Technical controls checklist

Use the checklist below to assess your organization's readiness across the ENS's key requirement areas.

Sl.no	Requirement area	Measures	Controls required
1	Security governance and organization	org.1–org.4	• Approve a formal security policy • Define security roles and committees • Run a formal authorization process • Separate security from operations
2	Risk analysis and management	op.pl.1	• Identify valuable assets • Assess likely threats • Select proportionate safeguards • Accept residual risk formally
3	Access control and authentication	op.acc.1–op.acc.6	• Assign unique identifiers • Enforce least privilege • Require MFA • Review access rights periodically
4	Secure configuration and maintenance	op.exp.2–op.exp.5	• Remove default accounts • Apply minimum functionality • Install security updates • Control configuration changes
5	Malicious-code protection and monitoring	op.exp.6, op.mon.1–3	• Deploy anti-malware defenses • Detect intrusions • Monitor systems continuously • Track security metrics
6	Activity logging and traceability	op.exp.8–op.exp.9	• Record user activity • Time-stamp and protect logs • Attribute actions to users • Retain the audit trail
7	Incident management and reporting	op.exp.7, Art. 33	• Detect and classify incidents • Contain and investigate • Notify CCN-CERT/INCIBE-CERT • Record for improvement
8	Data protection, backup, and continuity	mp.info, op.cont.2	• Classify sensitive information • Prevent data leakage • Maintain regular backups • Ensure service continuity

The ENS and ManageEngine

ManageEngine offers solutions that can help your organization govern access, monitor activity, and respond to incidents in line with the ENS. AD360, ManageEngine's IAM solution, and Log360, its SIEM solution, together operationalize the framework's access control, logging, monitoring, and data protection measures. With them, you can implement the technical controls required under the ENS in proportion to each system's category.

How can ManageEngine help you implement the ENS?

Identity life cycle management

Automate unique identifiers and account provisioning, and disable accounts on departure or role change.

Helps with op.acc.1.

Adaptive MFA

Enforce a risk-based second factor for internal and external users, including access from uncontrolled networks.

Helps with op.acc.5–op.acc.6.

Role-based access governanc

Restrict privileges to the minimum needed, and recertify access rights on a periodic cycle.

Helps with op.acc.2–op.acc.4.

Malicious code detection and response

Detect and correlate malware indicators across endpoints and servers, and respond automatically to ransomware.

Helps with op.exp.6.

Threat detection and monitoring

Detect intrusions in real time against MITRE ATT&CK®-mapped rules, with continuous surveillance and anomaly detection.

Helps with op.mon.1–op.mon.3.

Audit trails and activity logging

ecord time-stamped user and system activity, attribute actions to identities, and retain a tamper-evident audit trail.

Helps with op.exp.8.

Incident management and response

Detect, classify, contain, and investigate incidents, with automated response and support for CCN-CERT notification.

Helps with op.exp.7 and Article 33.

Cloud security and CASB

Monitor activity across AWS, Azure, GCP, and Salesforce, apply CASB controls over cloud data, and surface shadow IT use.

Helps with op.nub.1.

Configuration and change monitoring

Remove default accounts, monitor secure configuration, and track changes with before-and-after values.

Helps with op.exp.2–op.exp.5.

For more information, contact sales@manageengine.com