ManageEngine

A quick guide to Spain's national cyber-incident guide

Approved by Spain's Consejo Nacional de Ciberseguridad, the Guía Nacional de Notificación y Gestión de Ciberincidentes is the national reference for reporting and managing cyber incidents. It defines a shared taxonomy, severity thresholds, and reporting deadlines for public bodies, essential-service and critical operators, and digital service providers, and, on a voluntary basis, the private sector and citizens.

Technical controls checklist

Use the checklist below to assess your organisation's readiness across the guide's key requirement areas.

Sl.no	Requirement area	Section	Controls required
1	Incident classification and taxonomy	§5	• Classify every incident by category • Assign incident type from taxonomy • Align to the ENISA reference taxonomy • Escalate to the highest applicable level
2	Danger and impact assessment	§6.1	• Assign danger level by threat type • Rate impact by consequence • Track share of systems affected • Reassess impact as the case evolves
3	Detection and identification	§7.2	• Monitor networks, systems, and apps • Collect situational data • Detect anomalies promptly • Preserve evidence securely
4	Mandatory notification and deadlines	§6.1.3, §6.5	• Notify high, very high, and critical cases • Send initial notice immediately • Meet intermediate deadlines • Submit the final report on time
5	Incident information and records	§6.3, §6.4	• Record affected assets and IP addresses • Capture the incident origin • Assign a unique case identifier • Document countermeasures taken
6	Containment and mitigation	§7.3, §7.4	• Contain impact quickly • Stop propagation and exfiltration • Remove attacker tools • Recover from a clean backup
7	Recovery and post-incident review	§7.5, §7.6	• Restore under heightened monitoring • Watch for suspicious activity • Capture lessons learned • Report cause, cost, and prevention
8	Metrics and continuous improvement	§8	• Measure service coverage • Track resolution times • Monitor no-response closures • Report metrics on schedule

The national cyber-incident guide and ManageEngine

ManageEngine offers solutions that help organizations detect, report, and manage cyber incidents in line with the guide. AD360, ManageEngine's IAM solution, governs identity and access, while Log360, its SIEM solution, delivers logging, threat detection, and incident response. Together they help you implement the controls the guide expects across the incident life cycle.

How can ManageEngine help you implement the guide?

Real-time threat detection

Detect and classify incidents using MITRE ATTandCK-mapped rules and event correlation.

Helps with §5, §6.1.1.

Behaviour analytics

Baseline user and entity activity to surface anomalies and escalating threats early.

Helps with §7.2.

Centralized log management

Collect, parse, and retain events from networks, systems, and applications.

Helps with §7.2.

Incident management

Register each case with a unique identifier and track it through every state to closure.

Helps with §6.3, §6.6.

Automated containment

Execute response playbooks to limit impact and stop data exfiltration.

Helps with §7.3.

Audit-ready reporting

Generate the incident detail and evidence required for initial, intermediate, and final notifications.

Helps with §6.4, §6.5.

Privileged access oversight

Monitor and alert on elevated-account activity to contain propagation.

Helps with §7.3.

Adaptive MFA and access control

Enforce risk-based authentication and role-based access to affected systems.

Helps with §7.4.

Risk and posture assessment

Scan AD and database configurations to surface exposure for impact rating.

Helps with §6.1.2, §7.1.

For more information, contact sales@manageengine.com