Spain

Your local contact

Fernando Fernandez-Miranda Vidal
Partner, PwC Spain
+34 620 03 00 64
fernando.fernandez-miranda.vidal@pwc.com

Samanta Murillo Geiser
Manager, PwC Spain
+34 618 74 71 86
samanta.murillo.geiser@pwc.com

Status	As of today (July 01, 2025), the only reference to this transposition work by the Government of Spain is the approval of an "Anteproyecto de Ley" which is a draft of the future transposition law (Law on Cybersecurity Coordination and Governance) that is not yet even in parliamentary procedure.
Name of National Law	Law on Cybersecurity Coordination and Governance
Entered into force	Expected 2025, draft bill not yet in parliamentary procedure
Link to current draft or equivalent	https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf
Scope (deviating from NIS-2-Directive)	(Additional) categories of entities in scope: (i) companies with significant public participation; (ii) universities and research centers; (iii) large municipalities and municipalities with more than 20.000 inhabitants; (iv) private security companies and detective agencies; (v) entities with impact on National Defense; (vi) foreign companies with a permanent establishment in Spain (under certain decision-making or operational volume criteria); (vii) any other entity identified as essential or important by the supervisory authority applying the criteria of Article 3 of the law, by reasoned resolution.
Registration	Entities potentially within the scope of the law must self-assess their inclusion as essential or important. Once identified, they are required to submit a set of information to the supervisory authorities within a maximum period of three months from acquiring such status to proceed with their registration. We understand that such registration can be done through the National Platform for Notification and Monitoring of Cyber Incidents, which on its website has a section called "NIS-2" that can be accessed through a link named "NIS-Registration", which is still under construction and not available.
Information Security Standards referenced	Entities within the scope of the National Security Framework must comply with the standard and security measures described therein.
Incident reporting	Essential and important entities must notify the supervisory authority without undue delay, through their national reference CSIRT, of any significant incidents that have occurred in their operations or service provision, as determined by regulation according to their severity and impact. The national reference CSIRTs will use the National Platform for Notification and Monitoring of Cyber Incidents to facilitate and automate notification processes. This platform will be adapted, maintained, and managed by the National Cryptologic Center (CCN-CERT) under the direction of the National Cybersecurity Center. The notification deadlines are as follows: (i) within 24 hours, an early warning; (ii) within 72 hours, incident notification; (iii) within one month, a final report.

Spain

Your local contact

Fernando Fernandez-Miranda Vidal
Partner, PwC Spain
+34 620 03 00 64
fernando.fernandez-miranda.vidal@pwc.com

Samanta Murillo Geiser
Manager, PwC Spain
+34 618 74 71 86
samanta.murillo.geiser@pwc.com

Authority / CSIRT	The Cybersecurity Coordination and Governance Law establishes the National Cybersecurity Center as the sole national competent authority for cybersecurity governance. However, this administrative body has not yet been created in Spain (pending approval of the Law) and a transitional regime is foreseen whereby the supervisory authorities will continue to be, until the National Cybersecurity Center begins its activities, various ministries depending on the sector of each essential or important entity. Regarding the reference CSIRTs, the following are designated: (i) CCN-CERT, for public sector entities; (ii) INCIBE-CERT, for private law entities and citizens; (iii) Joint Cyber Space Command, for the Armed Forces. Fines (deviating from NIS-2-Directive): The Cybersecurity Coordination and Governance Law provides the following additional regime regarding sanctions imposed under Articles 34.4 and 34.5 of NIS-2: (i) minor infringements: fine between EUR 10.000 and EUR 100.000; (ii) serious infringements: fine between EUR 100.001 and EUR 500.000; (iii) very serious infringements: fine between EUR 500.001 and EUR 2.000.000.
Fines (deviating from NIS-2-Directive)	The Cybersecurity Coordination and Governance Law provides the following additional regime regarding sanctions imposed under Articles 34.4 and 34.5 of NIS-2: • minor infringements: fine between EUR 10.000 and EUR 100.000; • serious infringements: fine between EUR 100.001 and EUR 500.000; • very serious infringements: fine between EUR 500.001 and EUR 2.000.000.
Worth mentioning	As noted, the draft Cybersecurity Coordination and Governance Law complements the NIS-2-Directive by: (i) expanding the scope to additional entities; (ii) strengthening institutional coordination through the creation of the National Cybersecurity Center as a single authority; (iii) establishing procedures for the identification of essential and important entities.