COUNTRY: **SPAIN**

Spain adopted the National Cyber Security Strategy in 2013. It is a comprehensive document, which sets objectives and targeted lines of actions. It is compatible with, and references, both the National Security Plan and existing security laws; and these plans and laws work together as a package.

Spain has established two computer emergency response teams (CERTs), INTECO-CERT and CCN-CERT, and the National Centre for Critical Infrastructure Protection (CNPIC). The latter appears to be the premier agency for information security and cybersecurity, while the role of the CERTs is limited to dealing with cybersecurity incidents. CNPIC is responsible for ensuring coordination and cooperation between the public and private sector. It also runs sectoral working groups and is working toward the development of sector-specific cybersecurity plans.

Additionally, cooperation with the private sector is formalised through the National Advisory Council on Cybersecurity, established in 2009, whose members are private sector representatives. The council is tasked with providing policy advice to the government, although its current status is somewhat unclear. Private sector associations are also active, with two prominent bodies dedicated specifically to cyber- and information security, as opposed to general IT matters.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Cyber Security Strategy <ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf> was adopted by the Spanish government in 2013. It is a comprehensive document with set objectives and targeted lines of actions. It is compatible with, and references, the National Security Plan and existing security law, and these laws and plans work together as a package.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	Critical infrastructure protection is managed through a package of initiatives, including: • The National Plan for Critical Infrastructure Protection 2007; • The establishment of the National Centre for the Protection of Critical Infrastructure (CNPIC) <cnpic.es>; • The Regulation on Critical Infrastructure Protection 2011 <www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf>; • Law 8/2011 on the Measures for the Protection of Critical Infrastructure 2011 <www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf>; and, • The Royal Decree 704/2011 <www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf>, which gives assent to, and expands on, the framework of Law 8/2011.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Spain that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The classification of information and the handling of such information is covered by: • Law 9/1968 <www.boe.es/boe/dias/1968/04/06/pdfs/A05197-05199.pdf>; • Law 11/2007 <www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>; and, • Royal Decree 3/2010. <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf> Spain classifies information deemed a state secret according to a four-tier classification system. The classification levels are assigned according to the level of risk involved in disclosing the classified information.

COUNTRY: SPAIN

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The classification of information and the handling of such information is covered by: • Law 9/1968 <www.boe.es/boe/dias/1968/04/06/pdfs/A05197-05199.pdf>; • Law 11/2007 <www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>; and, • Royal Decree 3/2010. <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf> Spain classifies information deemed a state secret according to a four-tier classification system. Some security practices are mapped to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	Royal Decree 3/2010 <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>, which regulates e-government within the National Security Framework, requires information security system to be audited at least once every two years, and contains the provision for additional auditing in times of emergency. The act details the necessary standards of such an audit.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or policy in place in Spain that requires a public report on cybersecurity capacity for the government. Royal Decree 3/2010 <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>, which regulates e-government within the National Security Framework, requires an audit of information systems once every two years, however, this isn't a targeted cybersecurity capacity report and it is not required to be made public.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation in place in Spain that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in Spain that requires mandatory reporting of cybersecurity incidents. The National Cyber Security Strategy <ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf>, adopted in 2013, states that enforced incident reporting is a line of action that the Spanish government will pursue.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Centre for the Protection of Critical Infrastructure (CNPIC) <cnpic.es> provides an appropriate definition for critical infrastructure.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	The National security scheme for eGovernment (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica) includes security certification requirement that can be met by reference to international certification or accreditation. <www.boe.es/buscar/doc.php?id=BOE-A-2010-1330> Their stated objective is to: "promote cyber security certification activities in accordance with the internationally recognised norms and standards, incorporating these criteria into processes for the development and acquisition of products or systems".
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	INTECO-CERT <cert.inteco.es> was established in 2008. It is responsible for coordinating incident response measures across all Spanish networks. It also supports entities engaged with critical infrastructure through an agreement with the National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es>. CCN-CERT <www.ccn-cert.cni.es> has jurisdiction over government institutions.
2.	What year was the computer emergency response team (CERT) established?	2008	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> acts as the national competent authority for network and information security in Spain.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	INTECO-CERT <cert.inteco.es>, working in conjunction with the National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es>, is tasked with incident reporting and collecting information about cybersecurity incidents. There is an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Spain has participated in multinational cybersecurity exercises organised by both the European Union and NATO.

COUNTRY: SPAIN

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> acts as the body responsible for coordinating responses to emergency incidents, including cybersecurity incidents. They are responsible for engaging with the relevant stakeholders and government departments in the event of an incident.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> monitors the national critical infrastructure protection system, which includes owners, operators and users of Spanish critical infrastructure. As a result, CNPIC facilitates cooperation between the public and private sectors through initiatives like sectoral working groups. Furthermore, the National Advisory Council on Cybersecurity (CNCCS), whose membership comprised representatives from the information technology and critical infrastructure sectors, was convened by the Spanish government in 2009 to advise the government on future cybersecurity policy directions.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	The Centre for Industrial Cybersecurity (CCI) <www.cci-es.org> is a non-profit organisation with objectives to provide and improve awareness of cybersecurity issues and to facilitate communication channels between industry and lawmakers — to improve cybersecurity outcomes. The Spanish Association for the Promotion of Information Security (ISMS Forum Spain) <www.ismsforum.es> is a non-profit organisation that organises multiple information security initiatives. The Cyber Security Spanish Institute, which publishes reports on cybersecurity in Spain, is one such initiative. In addition to the CCI and the ISMS Forum, AMETIC <www.ametic.es>, the representative body for Spanish electronic technology, information technology and telecommunications companies, engages with cybersecurity issues in the course of its duties.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	Spain already has a public-private partnership dedicated to cybersecurity.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> facilitates cooperation between the public and private sectors through initiatives that include sectoral working groups.
2.	Have sector-specific security priorities been defined?	◑	The National Centre for Critical Infrastructure Protection (CNPIC) is working closely with 12 industry sectors to define sector-specific security priorities. These are expected to be made available following final consultations. Spain has also established the Centre for Industrial Cybersecurity (CCI) which promotes security best practices in the industrial sector. <https://www.cci-es.org>
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been released.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The National Cyber Security Strategy 2013 <ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf> includes a commitment to raising general public awareness. Its focus is on "raising the awareness of citizens, professionals and companies about the importance of cyber security and the responsible use of new technologies and the services of the Information Society". The strategy includes a commitment to "develop education modules for sensitisation in cybersecurity, aimed at all levels of teaching".