COUNTRY: **PORTUGAL**

Portugal has not developed a comprehensive legal and policy framework for cybersecurity, and its cybersecurity strategy has not been elaborated. There is no formalised public-private cooperation in place.

The country does have a national computer emergency response team, CERT-PT, and the National Centre for Cybersecurity. The latter was established by the National Security Authority and is tasked with liaising with the private sector on cybersecurity incidents.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	Draft	Portugal has a proposed national cybersecurity strategy. <www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCiberseguraçaPortuguesa.pdf> This proposal is yet to be adopted by the Portuguese government.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	No	Portugal does not have a critical infrastructure protection strategy or plan in place.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	No	There is no legislation or policy in place in Portugal 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 Act for National Security and the Safeguarding and Defence of Classified Material (SEGNAC 1) 1988 <www.gns.gov.pt/media/1356/SEGNAC1.pdf> requires all information that is that is subject to national or civil security considerations be classified. The four-tiered classification system used is outlined in Chapter 2 of the act, SEGNAC 2 1989. <www.gns.gov.pt/media/1359/SEGNAC2.pdf> Two other laws, SEGNAC 3 1994 <www.gns.gov.pt/media/1362/SEGNAC3.pdf> and SEGNAC 4 1990 <www.gns.gov.pt/media/1365/SEGNAC4.pdf>, provide further classification requirements for information regarding industrial security, telecommunications, and computer security.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The collection of Acts of National Security and the Safeguarding and Defence of Classified Material (SEGNACs) map security requires to assigned classification levels. These levels are set out in SEGNAC 1 <www.gns.gov.pt/media/1356/SEGNAC1.pdf> and are assigned according to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation or policy in place in Portugal that requires an annual cybersecurity audit. The Resolution of the Council of Ministers No. 12/2012 <www.gns.gov.pt/media/1917/rcm-12-2012.pdf> proposes that the National Security Office <www.gns.gov.pt> be responsible for conducting information security audits, however it does not provide a timeframe in which they are to be conducted.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	The Resolution of the Council of Ministers No. 42/2012 <www.gns.gov.pt/media/1924/rcm-42-2012.pdf> requires the Implementation Committee of the National Centre for Cybersecurity to conduct a report into the measures covering the operational needs and capabilities of the National Centre for Cybersecurity. There is, however, no legislation or policy requiring a comprehensive report on cybersecurity capacity. Nor is there a requirement to make any such reporting 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 or policy in place in Portugal 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 Portugal that requires mandatory reporting of cybersecurity incidents.

COUNTRY: PORTUGAL

	QUESTION	RESPONSE	EXPLANATORY TEXT
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	There is no legislation or policy that includes an appropriate definition of critical infrastructure protection.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	Not applicable	There are no specific cybersecurity standards or certification requirements for procurement in Portugal, as of August 2014. This issue may be addressed during the development and implementation of Portugal's proposed national cybersecurity strategy.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-PT <www.cert.pt> was established in 2008. It is responsible for the prevention of incidents and the coordination of incident response measures across all Portuguese networks.
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 Security Office (GNS) <www.gns.gov.pt> acts as the national competent authority for network and information security in Portugal. The GNS is directed by the National Security Authority, who is the sole authority with responsibility for the protection and safeguarding of classified information. The National Centre for Cybersecurity is run under the GNS and is the agency responsible for cybersecurity in particular.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-PT <www.cert.pt> is tasked with managing the reporting of cybersecurity incidents. CERT-PT provides an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Portugal has participated in multi-national cybersecurity exercises organised by both the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	The National Security Office (GNS) <www.gns.gov.pt> operates within a clear organisational structure — however, there is no discrete incident management structure for responding to cybersecurity incidents.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	There is no defined public-private partnership for cybersecurity in Portugal, however, the National Centre for Cybersecurity is tasked with liaising with the private sector in the course of its duties.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	There is no significant industry-led platform for cybersecurity in Portugal.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	There are no new public-private partnerships being planned in Portugal.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Portugal does not have sector-specific joint public-private plans in place.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been defined.
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?	✖	Portugal is preparing a national cybersecurity strategy that may contain education commitments.