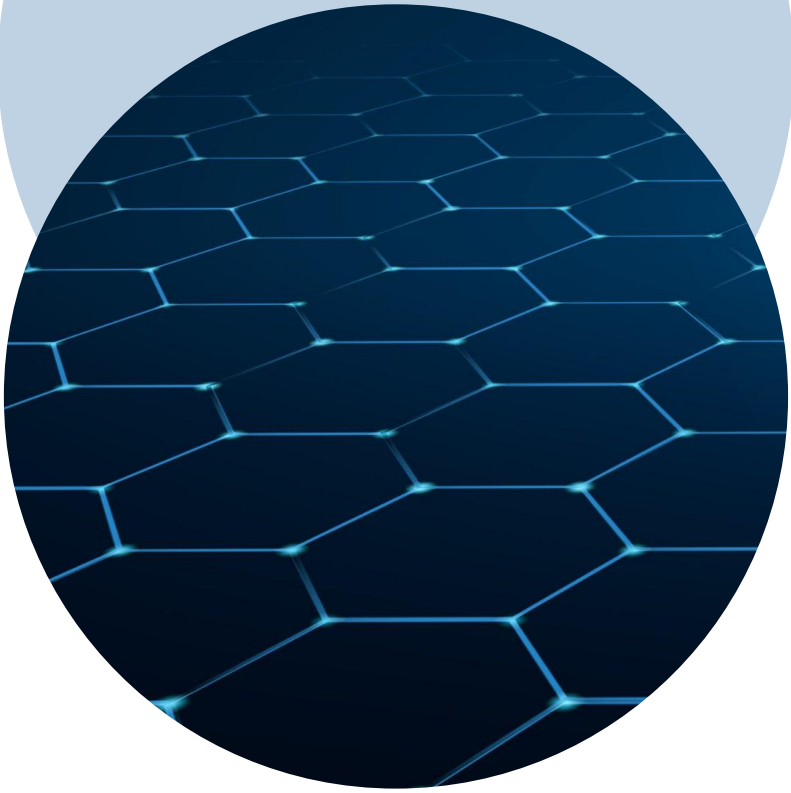
NIS 2 Radar

Public Consultation by the National Cybersecurity Centre

abreuadvogados.com



The National Cybersecurity Centre (CNCS) has launched a public consultation, open until 22 April 2026, on a draft Regulation on the Legal Framework for Cybersecurity (the "**Draft Regulation**"). This Draft develops and elaborates on Decree-Law no. 125/2025 of 4 December, which transposes the NIS2 Directive into national law.

1. **Electronic Platform**

All entities within scope must register and interact with the competent authority through a centralised electronic platform. Through this platform, entities shall: (i) carry out self-identification, qualification and registration; (ii) designate a Cybersecurity Officer and a Permanent Point of Contact; (iii) submit annual reports; and (iv) notify cybersecurity incidents. Authentication requires high-level Portuguese electronic identification, namely the Citizen Card or Digital Mobile Key. Official notifications are deemed received on the third day after being sent to the reserved area.

2. **Risk Matrix and Compliance Levels**

The Draft establishes a reference framework with risk values for scenarios applicable to each sector and sub-sector of activity. This model leads to a three-tier compliance classification system: Basic, Substantial and High. The levels are cumulative: an entity at the Substantial level must implement all Basic measures plus the additional Substantial ones, while an entity at the High level must implement measures across all three levels. This proportionate approach ensures that obligations are calibrated to reflect the risk profile inherent to the entity's sector, its size and systemic importance.

3. **Minimum Cybersecurity Measures**

The minimum measures apply to essential and important entities according to the three compliance levels, and to relevant public entities according to their classification as A or B. The measures cover the following areas: identification of critical services; risk management processes; asset inventory; incident response and recovery plan; incident handling and business continuity; supply chain security; acquisition, development and maintenance of networks and systems; cyber hygiene practices and training; cryptography and multi-factor authentication policies; and asset management and access control.

4. **Incident Notification Procedures**

Organisations must notify significant incidents through the Electronic Platform, following these stages: (i) initial notification immediately upon detection; (ii) communication of the cessation of significant impact; and (iii) final or interim reports after resolution of the incident.

5 **Voluntary Certification**

The Draft provides for a presumption of compliance for organisations holding valid certificates under: QNRCS Certification Scheme; ISO/IEC 27001; DNP TS 4577-1 (Digital Maturity Seal) for public entities; and other schemes approved by the CNCS. Changes to the certificate status (revocation, suspension or expiry) must be communicated within 20 working days.

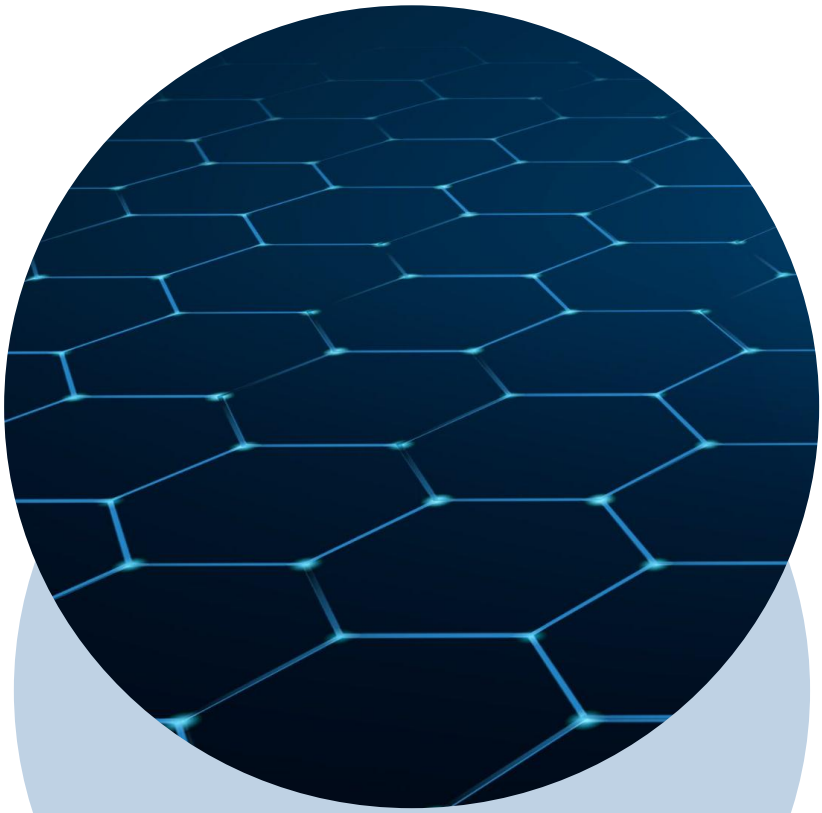
6. **List of Publicly Accessible Assets**

Essential, important and relevant public entities must prepare, keep updated and communicate to the competent authority a list of all assets essential for the provision of their respective services that are directly accessible via the Internet.

7. **Key dates and next steps**

Milestone	**Date**
Public consultation period	Until 22 April 2026
Entry into force	5th day after publication in Official Gazette (*Diário da República*)

The Abreu Advogados team is available to assist with the analysis and application of these matters, including providing support in connection with the public consultation process.



Thinking about tomorrow? Let's talk today.

Ricardo Henriques – Partner
ricardo.henriques@abreuadvogados.com

Catarina Mascarenhas – Of Counsel
catarina.mascarenhas@abreuadvogados.com

Marta Boura – Of Counsel
marta.boura@abreuadvogados.com