



TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

Critical infrastructure resilience: implementation of the Directive in Portugal

European framework

Directive (EU) 2022/2557¹ (Critical Entities Resilience Directive - “**CER Directive**”) aims to strengthen the ability of Member States to protect critical infrastructure from threats such as cyber-attacks, natural disasters, terrorism or public health emergencies. Specifically, this Directive establishes a common legal framework to ensure that critical organisations in strategic sectors adopt appropriate prevention, preparedness, response and recovery measures. The initiative arises from the need to harmonise national legislation and to strengthen cross-border cooperation between competent authorities.²

The CER Directive recognises the growing interdependence of critical sectors and advocates a coordinated approach to identifying vulnerabilities and promoting resilience in the European Union. To this end, Member States must develop a national resilience strategy, carry out risk assessments and identify critical bodies that provide essential services.

This Directive establishes a common legal framework to ensure that critical organisations in strategic sectors adopt appropriate prevention, preparedness, response and recovery measures.

Pedro Lomba
Nádia da Costa
Ribeiro
Inês Cabugueira

Technology,
Media and
Telecommunications
team

¹ Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC of 14 December 2022, available at <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng>.

² Recital 7 of the CER Directive.

National Resilience Framework

In the context of this new legal framework, which addresses the security of critical infrastructure and the need to ensure a coordinated response to threats, Decree-Law 22/2025³ of 19 March 2025 was published, transposing the CER Directive into national law.

Decree-Law 22/2025 establishes a new legal framework to identify, designate and strengthen the resilience of national and European critical facilities in order to guarantee the continuity of essential services.

Chapter II establishes this national framework in three main instruments (Articles 11 to 13):

- National Risk Assessment, approved by a resolution of the Council of Ministers;
- National Strategy for the Resilience of Critical Entities, also approved by a resolution of the Council of Ministers; and
- Objective Criteria for the Identification of Critical Entities.

The National Strategy for the Resilience of Critical Entities, based on the risk assessment, will define the strategic framework, lines of action and policy objectives in this area and will serve as a guiding instrument for the process of identifying critical entities and should reflect an integrated approach to the protection of essential services.

What are critical entities?

Decree-Law 22/2025 provides that a critical entity is any organisation that provides services that are essential for the maintenance of vital societal functions and economic activities.

Although the national risk assessment may justify the inclusion of other entities from other sectors, for the time being critical entities have been identified as those operating in strategic sectors such as:

- Energy (oil, gas, electricity and hydrogen)
- Healthcare
- Transport
- Water and sanitation
- Banking and insurance
- Digital infrastructure
- Public administration

³ Decree-Law 22/2025 of 19 March transposing Directive (EU) 2022/2557, on the identification, designation and resilience-building of critical entities, available at <https://diariodarepublica.pt/dr/detalhe/decreto-lei/22-2025-911488699>.

The assessment also takes into account the role of the entity in ensuring an adequate level of essential service provision based on its resources and infrastructure.

- Food production and distribution
- Space⁴

The **criteria for identifying critical entities** under Article 13 are, in particular,

- i) the provision of essential services
- ii) the location of critical infrastructure in Portugal
- iii) the likelihood of an incident having significant disruptive effects

To determine whether an incident has significant disruptive effects, factors such as the number of users dependent on the essential service, the degree of interdependence with other sectors and sub-sectors⁵, the impact of the incident on the economy, the environment, public safety or health, and the duration of the disruption are taken into account. Other factors include the market share of the entity providing the essential service in question, the geographical area affected, including cross-border effects⁶, and the availability of alternatives to ensure continuity of service.⁷

The assessment also takes into account the role of the entity in ensuring an adequate level of essential service provision based on its resources and infrastructure.

Critical entities in the following sectors are **exempt** from the obligations set out in Chapters III, IV and V of Decree-Law 22/2025 (on resilience, European relevance and supervision).

- Banking
- Financial market infrastructures
- Digital infrastructures

The main obligations of critical entities

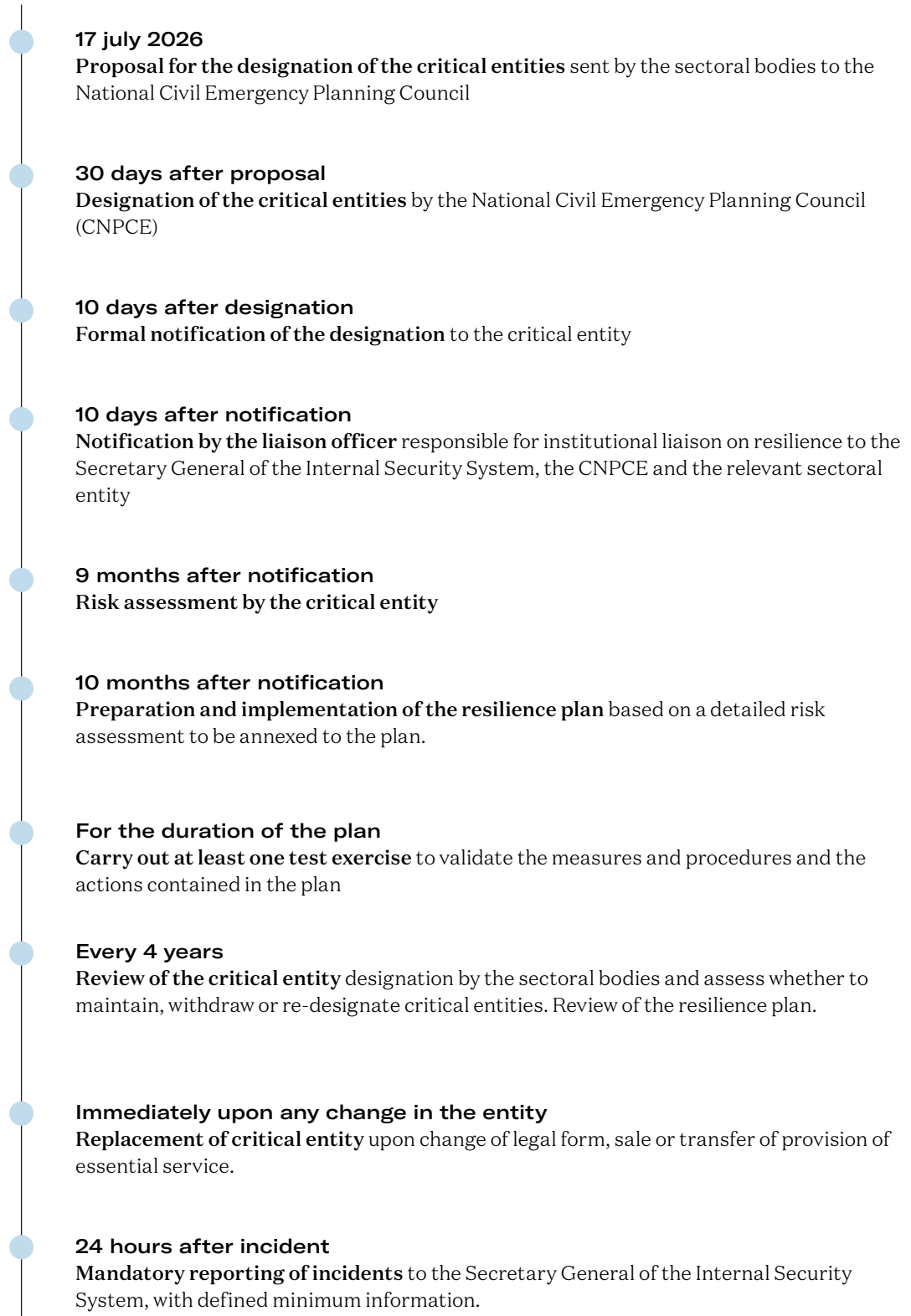
The new legislation sets out a number of specific obligations for entities designated as critical and the respective deadlines for compliance, as detailed below:

⁴ Sectors defined in the Annex to Decree-Law 22/2025.

⁵ Listed in the Annex to Decree-Law 22/2025.

⁶ Particularly in isolated or island regions.

⁷ Article 14 of Decree-Law 22/2025.



The law establishes a coordinated structure for the resilience of critical infrastructures in Portugal.

Entities must draw up security plans⁸ based on a risk assessment, including technical and organisational measures. The liaison officer coordinates communication between critical organisations and the national authorities⁹, ensuring the exchange of information and the implementation of security measures.

The security forces, after consulting the critical entity, may propose measures to restrict the airspace above critical infrastructures and the surrounding area.¹⁰

Institutional Resilience Structure

The law establishes a coordinated structure for the resilience of critical infrastructures in Portugal, made up of the following entities:

National Civil Emergency Planning Council (“CNPCE”)

- Identifies and designates critical entities and their critical infrastructures, in conjunction with the sectoral entities¹¹
- Acts as the national contact point with the European Commission
- Approves the formal designations and notifies the critical entities

Secretary General of the Internal Security System

- Coordinates and supervises resilience building activities
- Approves resilience plans, receives incident notifications, carries out audits and inspections and applies sanctions in accordance with Chapter V¹².

Both entities cooperate with the National Cybersecurity Centre to share information on cybersecurity risks and other risks, threats and incidents not related to cybersecurity.

The sectoral entities and the security forces implement specific measures in conjunction with the above-mentioned entities.

⁸ Article 30 of Decree-Law 22/2025

⁹ National Emergency and Civil Protection Authority, security forces, sectoral organisations.

¹⁰ Article 37 of Decree-Law 22/2025.

¹¹ Article 4 of Decree-Law 22/2025.

¹² Article 5 of Decree-Law 22/2025.

The National Strategy for the Resilience of Critical Entities and the National Risk Assessment must be approved by 17 January 2026. The instruments provided for in Decree-Law 20/2022¹³ will remain in force until then. In addition, an electronic platform will be created to record information on critical entities and infrastructure, which may include classified information.¹⁴

Special regime for European critical entities

Chapter IV regulates critical entities with a European dimension that provide services in six or more Member States, implying transnational cooperation.

Supervision and penalties

Supervision is the responsibility of the Secretary General of the Internal Security System. The law also states that penalties will be defined in a separate law, and Decree-Law 22/2025 also provides for audits and inspections. The offences include failure to comply with any notification from the liaison officer (minor administrative offence), failure to notify incidents (serious administrative offence) or failure to comply with the obligation to draw up and review plans (very serious administrative offence).

Impact on the sector and critical infrastructure

Organisations should start an internal process to assess whether they qualify as a critical entity and prepare to comply with the obligations arising from Decree-Law 22/2025, particularly in terms of operational and security resilience, continuity of service, risk assessment and incident response. Failure to comply could have operational, reputational and legal consequences, exacerbated by the interdependence of systems and the transnational nature of threats.

The implementation of the new legislation has been the subject of extensive institutional consultation, including with the Banco de Portugal, the Portuguese Securities Market Commission, the Insurance and Pension Funds Supervisory Authority, the National Security Office, the security forces and various sectoral emergency planning committees. ■

¹³ Decree-Law 20/2022 of 28 January, available at https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3573&tabela=leis&ficha=1&pagina=1, which approves the procedures for identifying, designating, protecting and increasing the resilience of national and European critical infrastructure.

¹⁴ Article 55 of Decree-Law 22/2025.