

THE NEW RULES FOR THE IDENTIFICATION, PROTECTION, AND RESILIENCE OF CRITICAL ENTITIES

Decree-Law No. 22/2025, of March 19, implements Directive (EU) 2022/2557 into national law and establishes new rules for the identification, protection, and resilience of entities operating in essential sectors such as electricity, transport, and health, which are therefore considered critical.

Critical entities will be required to comply with certain obligations, including conducting a risk assessment, developing resilience plans, and performing periodic tests, with sanctions applicable in case of non-compliance.

By 2026, the national resilience strategy and national risk assessment will be defined, and the designation of critical entities must be completed by July 2026.

The new rules for the identification, protection, and resilience of critical entities aim to ensure that entities providing essential services for maintaining social functions and vital economic activities can prevent, protect, respond, manage, and recover from incidents such as terrorist threats or public health emergencies.

In this regard, [Decree-Law No. 22/2025, of March 19](#), establishes (i) the terms and procedures for identifying critical entities pursuant to the national resilience strategy and the national risk assessment, (ii) the obligations of critical entities, and (iii) the sanctions for non-compliance with these obligations.

The identification of critical entities will be carried out by the National Council for Civil Emergency Planning according to the following criteria:

- The entity in question provides an essential service.
- The entity operates and its critical infrastructure (asset, facility, equipment, network, or system located in Portuguese territory, whose disruption or destruction would significantly impact the provision of an essential service) is situated in Portugal.
- An incident would have significant disruptive effects on the provision of one or more essential services, considering factors such as the number of users, the entity's market share, and the geographical area that could be affected.

The essential services include (non-exhaustive list):

- Energy: Production, supply, transportation, distribution, and storage of electricity, gas, and oil.
- Air, rail, and maritime transport: Transport services and management of infrastructure and traffic.
- Road transport: Traffic management control within intelligent transport systems.
- Banking: Acceptance of deposits, lending, and payment services.
- Financial markets: Operation of trading platforms and clearing systems.
- Health: healthcare services, research and development of medicines, manufacturing of basic pharmaceutical products and preparations, production of medical devices considered critical during a public health emergency, and storage and distribution of medicines.
- Drinking water: Supply and distribution of potable water.
- Wastewater: Collection, treatment, and disposal of wastewater.
- Digital infrastructures: Cloud computing services, data centres, content distribution

CONTACTS

SUSANA VIEIRA

SVIEIRA@MACEDOVITORINO.COM

RITA COELHO

RCOELHO@MACEDOVITORINO.COM

networks, trust services, public electronic communications services, and public electronic communication networks.

- Food production, processing, and distribution.
- Insurance and pension funds.

Entities identified as critical will be notified and given 15 days to answer, after which they may be considered designated as such. The identification of critical entities must be reviewed every four years.

Critical entities will be subject to several obligations, including:

1. Appointment of a liaison officer responsible for institutional coordination and a liaison officer for each critical infrastructure and notice of such appointment to the competent authorities within 10 days.
2. Conducting a risk assessment within 9 months. The risk assessment must be updated every four years or whenever necessary.
3. Development and implementation of a resilience plan based on the risk assessment and submission for approval by the Secretary-General of the Internal Security System within 10 months. This plan must include the technical, security, and organizational measures necessary to ensure the resilience of the entity and its critical infrastructures, including physical protection, security plan for each infrastructure, identification of categories of personnel with critical functions, and training and exercises for human resources. The resilience plan must be reviewed every four years or whenever necessary.
4. Notification of incidents that disrupt or may disrupt the provision of essential services or the operation of critical infrastructures within 24 hours.
5. Conducting at least one exercise under the approved resilience plan to test the adequacy of its measures, procedures, and actions.
6. Prior notification of changes in legal status and the sale or transfer of the essential service, including identification of the purchaser and assurance that the relevant information of the resilience plan is conveyed to the purchaser.
7. Prior notification of the sale or transfer of critical infrastructures, with at least 30 days' notice before the transaction takes effect, including identification of the purchaser.

Failure to comply with these obligations constitutes an administrative offense subject to fines and other penalties.

The obligations outlined in points 1 to 5 above and the penalty regime do not apply to critical entities in the banking, financial markets, insurance, pension funds, and digital infrastructure sectors.

The national resilience strategy for critical entities and the national risk assessment must be defined by January 17, 2026. The current regime (Decree-Law No. 20/2022, of January 28) will remain in force until then. The designation of critical entities in the essential sectors must be completed by July 17, 2026.

