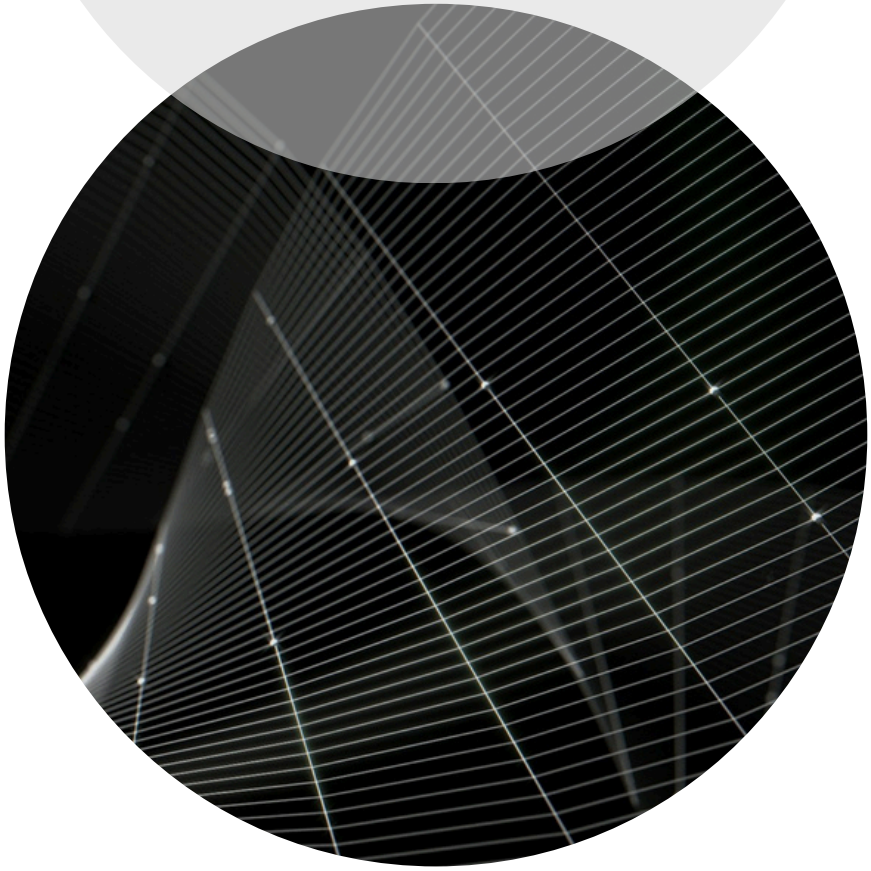
Abreu advogados

National Risk Assessment and National Strategy for the Resilience of Critical Infrastructure

info@abreuadvogados.com
abreuadvogados.com



On June 26, 2026, Council of Ministers Resolution No. 135/2026 was published in the Official Gazette, approving the National Risk Assessment and the National Strategy for the Resilience of Critical Entities ("the Strategy"). These instruments represent an essential step toward the coherent and effective implementation of the national legal framework for the resilience of critical entities and infrastructure, as provided for in Decree-Law No. 22/2025 of March 19 ("the Decree-Law"), which transposed Directive (EU) 2022/2557 of December 14 into national law.
As provided for in the Decree-Law, the National Risk Assessment is classified as "Confidential," and access to and analysis of the document are subject to restrictions.
In turn, the Strategy is a public document that defines the policy measures, strategic objectives, and lines of action to strengthen the resilience of critical entities. Its implementation is accompanied by an Action Plan, which monitors and evaluates the execution of the Strategy for the period 2026–2029.
It is anticipated that the approval and publication of these instruments will trigger the process of designating critical entities and their critical infrastructure, which are now subject to compliance with the Decree-Law, as well as the Legal Framework for Cybersecurity, as defined in Decree-Law No. 125/2025, of December 4.

A) Strategic Framework

The Decree-Law the national legal framework regarding the resilience of critical entities, covering the energy, transportation, banking, financial market infrastructure, healthcare, drinking water, wastewater, digital infrastructure, public administration, space, food production, processing, and distribution, and insurance and pension funds sectors. The Strategy serves as the policy instrument for framing and implementing the obligations set forth therein.
The Strategy thus incorporates the following key elements:

- Strategic objectives aimed at strengthening the overall resilience of critical entities;
- A governance framework describing the roles and responsibilities of the competent authorities, sectoral authorities, critical entities, and other relevant parties;
- A description of the resilience measures to be implemented;
- A process for identifying and designating critical entities and their respective infrastructure;
- Measures for coordination with the competent cybersecurity authorities;
- Measures to support critical entities, particularly small and medium-sized enterprises.

B) Areas of Intervention and Strategic Objectives

The strategic objectives stem from an analysis of the national and international context and are grouped into three areas of intervention:

- Axis I – Strengthening the Resilience of Critical Entities: encompasses objectives related to the careful identification and designation of critical entities and infrastructure, the systematic assessment of risks, and the adoption of appropriate and proportionate resilience measures;
- Axis II – Cooperation, Oversight, and Institutional Coordination: aims to strengthen national and international cooperation;
- Axis III – Research, Training, Communication, and a Culture of Resilience: focuses on strengthening the technical and operational capabilities of critical entities, conducting exercises, and promoting a national culture of resilience.

C) Resilience Measures: Identification and Designation of Critical Entities and Infrastructure

One of the key measures under Axis I will be the approval, by the National Council for Civil Emergency Planning ("CNPCE"), of the criteria and methodology applicable to identifying and designating critical entities and their critical infrastructure.

D) Process for Designating Critical Entities

The designation process consists of the following sequential phases:

- Proposal by sectoral authorities: sectoral authorities submit a proposal to the CNPCE detailing the identification criteria and applicable thresholds, and identifying the entities eligible for designation;
- Notification of Candidate Entities: The CNPCE notifies the candidate entities of their potential designation, granting them a period of no less than 10 days to submit a statement;
- Review of statements: in the event of an unfavorable statement, the CNPCE forwards it to the sectoral authority, which has 60 days to re-examine and, if necessary, adjust the proposal;
- Formal designation by the CNPCE: Once the procedure is complete, the CNPCE formally designates the critical entities and their respective critical infrastructures within a maximum of 30 days;
- Notification of designation: the critical entity is formally notified within a maximum of 10 days.

E) Obligations of Critical Entities

Upon notification of their designation, critical entities are subject to a set of obligations under the Decree-Law, which are summarized in the following table:

Obligation	**Deadline**
Risk Assessment	9 months after notification of designation
Resilience plan	10 months after notification; reviewed every 4 years
Liaison Officers	10 days after designation as a critical entity
Self-identification as an essential entity on the MyCiber Platform	30 days after designation, if the entity was not already covered by Decree-Law No. 125/2025 of December 4 - Subject to future guidance from the competent authorities

F) Action Plan

The Action Plan comprises 42 measures distributed across the three areas of intervention, with implementation scheduled to begin in January 2026 and, in most cases, extending through December 2029.

The following measures are particularly noteworthy:

- Refinement of the identification criteria by sectoral authorities, with an implementation deadline extending through July 2026;
- Approval by the CNPCE of the criteria and methodology for identifying and designating critical entities and their critical infrastructure, with an implementation deadline also set for July 2026;
- The Action Plan also provides for the development of a common digital platform for incident reporting, to be implemented jointly by the Secretary-General of the Internal Security System and the competent cybersecurity authorities. This platform will cover both incidents related to the resilience of critical entities and incidents falling under the Legal Framework for Cybersecurity, established by Decree-Law No. 125/2025 of December 4.

G) Next Steps

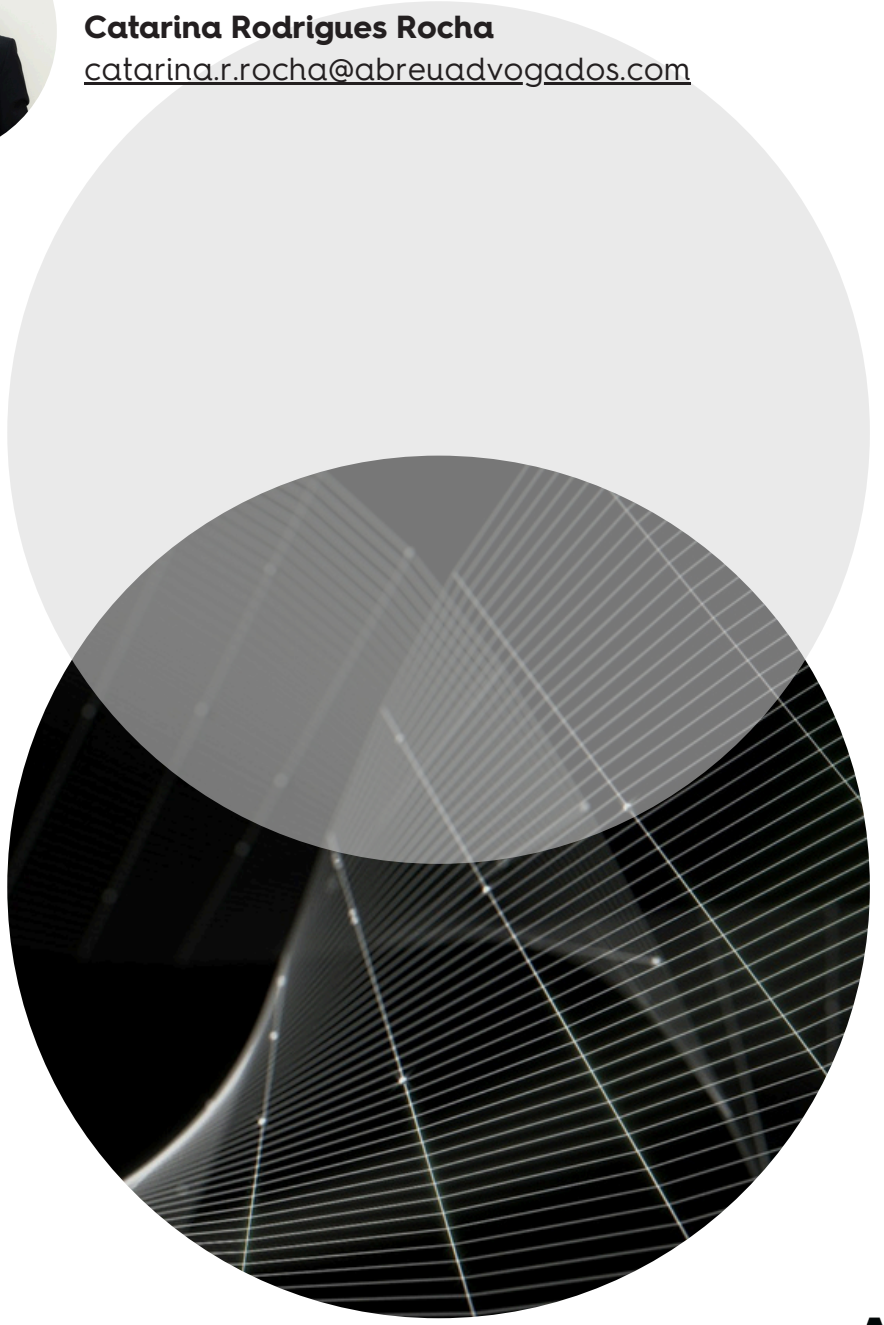
The approval of the National Risk Assessment and the National Strategy for the Resilience of Critical Entities marks the beginning of the operational phase of the legal framework for the resilience of critical entities, with the designation of these entities and their critical infrastructure expected in the second half of 2026.

For more information, please contact our Data Protection and Cybersecurity Service.

Thinking about tomorrow? Let's talk today.

Ricardo Henriques
ricardo.henriques@abreuadvogados.com

Catarina Rodrigues Rocha
catarina.r.rocha@abreuadvogados.com



info@abreuadvogados.com
abreuadvogados.com

Abreu advogados