
**New Legal Framework
for Cybersecurity**

Transposition of Directive
(EU) 2022/2555 (NIS II)

Decree-Law No. 125/2025,
of 4 December

Main objectives of NIS II

Directive (EU) 2022/2555, commonly referred to as NIS II, repeals the NIS I Directive, establishing a unified legal framework with the purpose of ensuring a high common level of cybersecurity across the European Union.

The aim of this diploma is to increase the level of information sharing between Member States, promoting a coordinated and effective approach in responding to security incidents in cyberspace.

Key time milestones in the implementation of NIS II



16.01.2023

Entry into force of the NIS II Directive.



17.10.2024

Deadline for national transposition of the Directive.



04.12.2025

Transposition of the Directive in Portugal: Publication of [Decree-Law No. 125/2025](#) in the Official Gazette.



03.04.2026

Entry into force of Decree-Law No. 125/2025.



04.05.2026

Deadline for essential and important entities to notify the CNCS of the person designated to act as a cybersecurity officer and permanent point of contact.



60 days after the availability of the CNCS electronic platform

Self-identification on the CNCS platform.



Scope

With the transposition of NIS II into the national legal system, precisely through Decree-Law No. 125/95, of 4 December, and the consequent approval of the New Legal Regime for Cybersecurity, the scope of application of these rules and obligations is significantly expanded.

At the national level, [Law No. 46/2018](#), of 13 August, which transposed the NIS I Directive, limited its scope to:

- to the Public Administration;
- Operators of critical infrastructure and essential services in the energy, transport, banking, financial market infrastructure, health, water and digital infrastructure sectors;
- Digital service providers; and
- To any other entities using networks and information systems.

The New Legal Regime for Cybersecurity not only expands the subjective scope of application but also specifies and classifies the sectors of activity covered into "*essential entities*" and "*important entities*", establishing a specific regime for each.

The New Legal Framework for Cybersecurity applies:

To private entities in sectors of critical importance and other critical sectors that are either (i) classified as medium-sized enterprises (as defined in the applicable legislation) or (ii) companies that:

- Employ more than 250 workers;
- Have an annual turnover equal to or greater than €50 million, or an annual total balance sheet equal to or greater than €43 million; and
- Provide their services or carry out activities within the European Union.

Entities in **sectors of critical importance** and **other critical sectors**, regardless of their size and nature, that are:

- Provider of **public electronic communications networks** or **provider of publicly available electronic communications services**;
- **Trusted service provider**;
- **Top-level domain name registration**, domain name registration service provider, and domain name system service provider.
- The **sole provider** of a service essential for the maintenance of critical social or economic activities.
- The **disruption of the service** provided by you may significantly affect **public safety, public protection or public health** or may generate **considerable systemic risks**.
- Critical due to its **specific importance**, at national or regional level, for the sector or type of service concerned, or for other interdependent sectors.

Public administration;

Ombudsman's Office;

Economic and Social Council;

Technical and administrative services of:

- **Presidency of the Republic;**
- **Assembly of the Republic;**
- **Courts** and secretariats with competence to process judicial procedures;
- **Superior Council of the Judiciary;**
- **Superior Council of Administrative and Tax Courts; and**
- **Superior Council of the Public Prosecutor's Office.**

Entities that, regardless of their size, are identified as **critical entities**;

Higher education institutions.

Territorial delimitation

For the New Legal Regime for Cybersecurity to be applicable, it is also necessary that these entities have an **establishment in national territory** or:

- If they are undertakings that provide **public electronic communications networks** or **provide publicly available electronic communications services**, they make such services available in **national territory**;
- If they are domain name system service providers, top-level domain name registrar, entities providing domain name registration services, cloud computing service providers, **data centre** service providers, **content delivery** network providers, **managed** service providers, managed security service providers, as well as service providers of **online marketplaces**, **online search engines** or **social media service platforms**, they should:
 - Have the principal place of business in the **national territory**; or
 - If not having an establishment in the EU, its **representative** has an establishment in the **national territory**.

Classification of entities

Essential entities

Important entities

Relevant public entities

Group A

Group B

Essential entities

Critical Industries*



Qualified Trust Service Providers and Top-Level Domain Name Registration

Companies offering publicly available electronic communications services

System Service Providers domain names

Public Administration Entities

Companies providing public electronic communications networks

Critical entities pursuant to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022

Any other entity that qualifies as essential based on the degree of exposure of the entity to risks, the size of the entity and the likelihood of occurrence of incidents and their severity.

* Employing more than 250 people and whose annual turnover exceeds €50 million or whose annual balance sheet total exceeds €43 million.

Important entities

Entities belonging to critical or other critical sectors that are not considered essential entities are considered important entities.

The following entities (from critical or other critical sectors) that justify such classification based on the entity's degree of exposure to risks, the size of the entity and the likelihood of occurrence of incidents and their severity, including their social and economic impact, are also considered to be important entities:

- The entity is the sole provider of a service that is essential for the maintenance of critical social or economic activities.
- The disruption of the service provided by you may significantly affect public safety, public protection or public health or may generate considerable systemic risks.
- Critical due to its specific importance, at national or regional level, for the sector or type of service concerned, or for other interdependent sectors.

Other critical sectors



Relevant public entities


According to the New Legal Framework for Cybersecurity, public entities that are not qualified as essential or important entities are considered relevant public entities, falling into two groups for the purposes of applying specific regimes under the terms of the New Legal Regime for Cybersecurity and other regulations issued by the CNCS.

Group A

- Services of the direct administration of the State, central and peripheral, with 250 or more workers in its staff;
- Direct administration services of the Autonomous Regions, central and peripheral, with 250 or more employees in their staff;
- Entities of the indirect administration of the State, with more than 250 workers in their staff;
- Entities of the indirect administration of the Autonomous Regions, with more than 250 employees in their staff;
- Autonomous administration entities, with more than 250 employees in their staff;
- Large public business entities;
- Independent administrative entities;
- Economic and Social Council, the Ombudsman's Office, the technical and administrative services of the Presidency of the Republic, the Assembly of the Republic, the Courts and the secretariats with competence to deal with procedures, the Superior Council of the Judiciary, the Superior Council of the Administrative and Tax Courts and the Superior Council of the Public Prosecutor's Office.

Group B

- Services of the direct administration of the State, central and peripheral, which have between 75 and 249 employees in their staff.
- Direct administration services of the Autonomous Regions, central and peripheral, which have between 75 and 249 employees in their staff.
- Entities of the indirect administration of the State, which have between 75 and 249 employees in their staff.
- Entities of the indirect administration of the Autonomous Regions, which have between 75 and 249 employees in their staff.
- Autonomous administration entities, which have between 75 and 249 employees in their staff.
- Public business entities qualified as medium-sized companies.



Procedure for qualifying entities

Entities falling within the subjective scope should identify themselves as a relevant essential, important or public entity. This process is done by registering on the digital platform provided by the CNCS.

The CNCS also has the legitimacy to qualify entities on this platform.

If the entity falls into more than one category:

The regime that is most demanding to manage the risks posed to the security of network and information systems shall apply.

If the qualification of the entity is changed, essential and important entities have a period of 6 months to adapt to the new qualification.

Deadline for identification

- **30 days** after the start of your activity or;
- If the entity is already in activity at the time of the entry into force of the Decree-Law, within **60 days** after the availability of the aforementioned electronic platform.

Obligations for essential and important entities

Obligations of the management, management and administration bodies

- Adopt and supervise the adoption of cybersecurity risk management measures.
- Ensure compliance with the supervision and enforcement measures legally required to prevent and resolve incidents.
- Ensure that cybersecurity training is carried out on a regular basis.

Obligation to manage the risks of network and information systems

- Essential and important entities shall adopt appropriate technical, operational and organisational measures to manage the risks to the security of the network and information systems they use in their operations and to prevent or minimise the impact of incidents on the recipients of their services and other services.
- The CNCS may establish minimum security measures taking into account the specificities of the sector and the size of the entity. These measures can be regulated both in the National Reference Framework for Cybersecurity (QNRCS) and through the specific measures for the implementation of the QNRCS.

Cybersecurity Measures

- Cybersecurity measures should be adopted that cover, inter alia, (i) incident handling; (ii) continuity of activities; (iii) supply chain security; (iv) security in the acquisition, development and maintenance of information networks and systems; (v) policies and procedures to assess the effectiveness of cybersecurity risk management measures; (vi) security of human resources; among others.
- Additional cybersecurity measures may be established by means of a CNCS regulation.
- They shall also adopt, without undue delay, all necessary, appropriate and proportionate corrective cybersecurity measures, which are indispensable to remedy failures or omissions in compliance with the measures implemented.

Risk analysis and management

- Essential and important entities must carry out risk analysis and management in relation to all assets that ensure the continuity of the operation of the networks and information systems they use.
- This risk analysis should serve as a basis for determining the security measures to be adopted, and therefore should serve the objective of complying with the obligation to implement cybersecurity measures.

Annual Report

- Essential and important entities must prepare a report each year, which must contain certain mandatory elements. This report must be signed by the cybersecurity officer and sent to the competent cybersecurity authority.
- The CNCS may, at any time, request the important entities to deliver the report.

The annual report must be submitted:

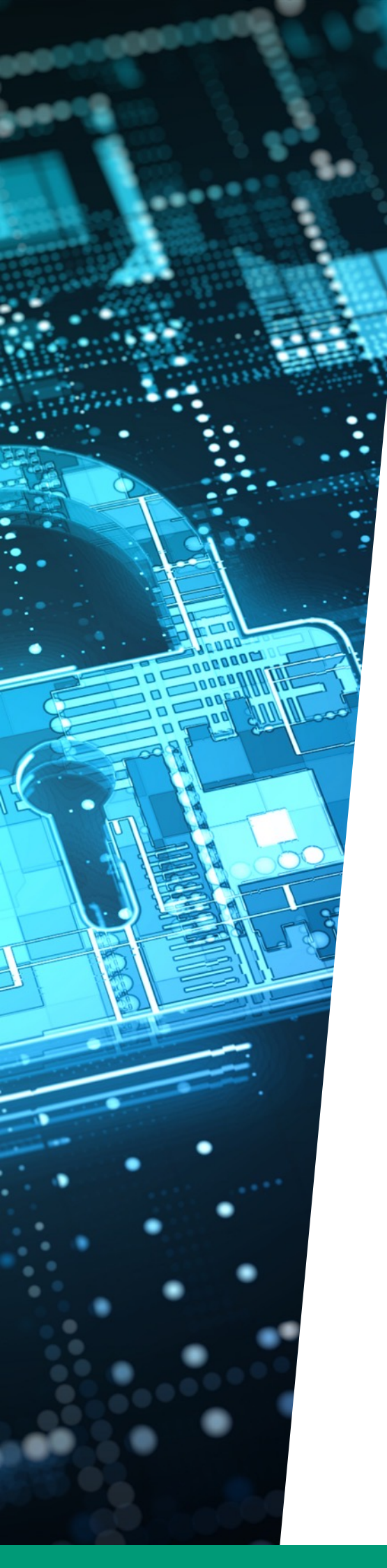
- Until the last working day of January of the calendar year following the first calendar year of activity, when it has started in the first half of the year.
- Until the last working day of January of the second calendar year following the first calendar year of activity, when it began in the second half of the year.
- Subsequent annual reports are submitted by the last working day of January of the following calendar year to which they refer.

Cybersecurity Manager

- The person designated by the essential and important entities for the management of cybersecurity and information security, who is the head of the management, management or administration bodies or reports organically and directly to them.
- The communication of the appointment to the CNCS must be made within 20 working days, counted from the beginning of his duties or the entry into force of the New Legal Regime for Cybersecurity.

Permanent point of contact

- Essential and important entities ensure the function of the permanent point of contact with continuous 24/7 availability.
- Essential and important entities must communicate to the CNCS at least 1 permanent point of contact, which can be provided by an element or a team.
- The communication of the appointment must be made within 20 working days, counted from the beginning of his duties or the entry into force of the New Legal Regime for Cybersecurity.



Specific obligations

Relevant Public Entities

The relevant public entities have the obligation to comply with the additional security measures established by the CNCS in a specific regulation for this purpose.

Entities that provide domain name registration services

The registry of top-level domain names and the entities that provide domain name registration services:

- They shall collect and maintain accurate and complete data relating to the registration of domain names in databases created specifically for that purpose.
- They guarantee free access to specific data relating to the registration of domain names to those who submit a duly substantiated request for access and who meet the legal requirements.

Cybersecurity Certification

- The CNCS may require relevant essential, important and public entities to obtain certification in matters of national, European or international cybersecurity, to prove and certify that the entities comply with the obligations established in the New Legal Framework for Cybersecurity. This certification can also be done on a voluntary basis.
- The CNCS may also require entities to use ICT products, services and ICT processes, developed or provided by entities certified under national and European cybersecurity certification schemes.

Incident Notification

Relevant essential, important and public entities

Relevant essential, important and public entities shall report any significant incident to the competent cybersecurity authority.

Guiding criteria for determining whether the incident had a significant impact:

- Number of users affected by the service disruption.
- Total number of users of the disturbed service.
- Duration of the incident.
- Level of severity of the disruption to the operation of the service.
- Dimension of the impact on economic and social activities.

For each incident subject to mandatory notification, the following shall be submitted:

- Initial notification: up to 24 hours after verification.
- Notification of the end of significant impact: up to 24 hours after the end of the significant impact.
- The final report: within 30 working days from the date of notification of the end of significant impact.

NOTE: Entities may also be notified to submit a progress report.

When the incident is resolved within two (2) hours of its detection, entities are only required to send the notification of the end of the significant impact.

Without prejudice to mandatory notifications, any natural or legal person may report incidents, cyber threats or vulnerabilities that it detects.

Significant incidents and cyber threats that may have significant impacts on service recipients shall be notified to the latter.

Supervision

Competent cybersecurity authority:

- CNCS or;
- National sectoral cybersecurity authority.

Supervisory powers:

inspections, audits, security checks, requests for access to data, information and evidence demonstrating compliance with cybersecurity measures.

Specific supervisory measures for essential entities

Specific supervisory measures for relevant important and public entities in the event of evidence, indications or information regarding the potential non-compliance of these entities

Implementing Measures

Blocking and redirecting measures

Sanctioning regime

Administrative offence

Very serious

Practiced by an **essential entity**:

- From €2,000.00 to €10,000,000.00 or up to 2% of the annual worldwide turnover, in the previous financial year;
- From €350.00 to €200,000.00, if practised by a natural person.

Practiced by an **important entity**:

- From €1,250.00 to €7,000,000.00 or a maximum amount of not less than 1.4% of the annual turnover worldwide;
- From €350.00 to €200,000.00, if practised by a natural person.

Practiced by a **relevant public entity** (depending on whether it is part of Group A or B): From €8,000.00 to €4,000,000.00.

Serious

Practiced by an **essential entity**:

- From €1,250.00 to €5,000,000.00 or 1% of the annual worldwide turnover, in the previous financial year;
- From €250.00 to €125,000.00, if practised by a natural person.

Practiced by an **important entity**:

- From €875.00 to €3,500,000.00 or a maximum amount of not less than 0.7% of the annual turnover worldwide;
- From €250.00 to €125,000.00, if practised by a natural person.

Practiced by a **relevant public entity** (depending on whether it is part of Group A or B): From €5,000.00 to €225,000.00.

Lightweight

- From €875.00 to €45,000.00, if practised by a legal person;
- From €250.00 to €3,750.00, if practised by a natural person.

Note: Any essential, important and relevant public entity that is subject to the application of fines resulting from very serious or serious administrative offences, may, upon duly substantiated request, request the competent cybersecurity authority to waive the application of fines on the grounds that there is no internal procedure for adapting these entities to the new legal regime, for 12 months from the entry into force of the New Legal Regime for Cybersecurity.

In certain circumstances, the imposition of fines may also be cumulated with:

Personal responsibility of the members of the management, direction and administration bodies of essential and important entities:

- They may be liable, by action or omission, with intent or gross negligence, for the infractions provided for in the New Legal Regime for Cybersecurity.
- They may be temporarily banned from performing their duties.

Ancillary sanctions:

- Publication of the conviction decision in the Official Gazette and in one of the newspapers with the largest national circulation, at the expense of the offender.
- Prohibition of participation in public procurement procedures, where applicable.
- Suspension of the provision of the service until the fulfilment of the omitted duties.
- Adoption and implementation of a cybersecurity training plan, to be implemented within 6 months.
- Adoption or amendment of a security plan, to be implemented within 6 months.

Contacts



**Manuel Liberal
Jerónimo**

Partner – Digital and Corporate Department
manuel.liberal.jeronimo@garrigues.com



**Luisa
Cyrne**

Senior Associate – Digital Department
luisa.cyrne@garrigues.com



**Matilde
Bettencourt**

Associate – Digital Department
matilde.bettencourt@garrigues.com

GARRIGUES

garrigues.com

Síguenos



IS 685586