Novo Regime Jurídico da Cibersegurança (NIS II)
New Cybersecurity Legal Framework (NIS II)

Carina Branco
Adriana Alves Henriques
António Seixas Barata
Equipa de TMT da pbbr | pbbr TMT team

O QUÊ?

Decreto-Lei n.º 125/2025 de 4 de dezembro, que aprova o regime jurídico da cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, para a garantia de um elevado nível comum de cibersegurança em toda a União (adiante o "Novo Regime Jurídico da Cibersegurança" ou "RJC") .

OBJETO

O RJC introduz um conjunto de alterações a diversos diplomas legais, com o objetivo de fazer face às múltiplas ciberameaças existentes e ao elevado potencial disruptivo das ações hostis dirigidas contra ativos digitais. Pretende-se reforçar a capacitação nacional em matéria de prevenção, deteção e resposta a incidentes, bem como, assegurar a salvaguarda da segurança e do interesse nacional e das dinâmicas funcionais e produtivas da sociedade portuguesa.

COMO?

O RJC aprofunda instrumentos fundamentais para as políticas públicas de Cibersegurança:

- A Estratégia Nacional de Segurança do Ciberespaço;
- O Plano Nacional de Resposta a Crises e Incidentes de Cibersegurança, e;
- Quadro Nacional de referência para a Cibersegurança.

WHAT?

Decree-Law No. 125/2025 approves the legal framework for cybersecurity, transposing Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, which aims to ensure a high common level of cybersecurity across the Union (hereinafter "New Legal Framework for Cybersecurity" or "CLF")) .

OBJECT

The CLF introduces a series of amendments to several pieces of legislation, with the aim of addressing the multiple cyber threats that exist and the high disruptive potential of hostile actions directed against digital assets. The aim is to strengthen national capacity in terms of prevention, detection and response to incidents, as well as to ensure the safeguarding of national security and interests and the functional and productive dynamics of Portuguese society.

HOW?

The CLF strengthens three key instruments of public cybersecurity policy:

- the National Cybersecurity Strategy;
- the National Plan for Responding to Large-Scale Cybersecurity Crises and Incidents; and
- the National Cybersecurity Reference Framework.

Reforça as competências da CNPD e implementa um sistema de maior cooperação entre as entidades públicas e privadas, estabelecendo ainda, um modelo de gestão de riscos, baseado em padrões pré-definidos, aplicáveis a cada setor e tipo de entidade, com medidas de prevenção proporcionais e uma avaliação do risco residual.

O RJC incentiva ainda, a certificação em cibersegurança e prevê um modelo de supervisão dual, distinguindo o tratamento das entidades essenciais e importantes, de acordo com os riscos de cibersegurança associados a cada categoria, em respeito pelo princípio da proporcionalidade.

QUEM?

O novo RJC aplica-se a**:**

Entidades Essenciais:

- Entidades dos tipos referidos no anexo I ao RJC, que excedam os limiares para as médias empresas previstos na Recomendação 2003/361/CE da Comissão;
- Prestadores de serviços de confiança qualificados, registo de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio, independentemente da sua dimensão;
- Empresas que oferecem redes públicas de comunicações eletrónicas ou serviços de comunicações eletrónicas acessíveis ao público, que sejam consideradas médias empresas;
- Entidades da Administração Pública com atribuições na prestação de serviços nas áreas de desenvolvimento, manutenção e gestão de infraestruturas de TIC ou com elevado grau de integração digital, e a entidade pública responsável pela avaliação educativa;
- Entidades identificadas como entidades críticas, nos termos da Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas, independentemente da sua dimensão.

CLF also reinforces the powers of the CNPD and establishes a system of enhanced cooperation between public and private entities whilst introducing a risk management model based on predefined standards, applicable to each sector and type of entity, with proportionate preventive measures and an assessment of residual risk.

The CLF promotes cybersecurity certification and provides for a dual supervisory model, distinguishing between essential and important entities according to the cybersecurity risks associated with each category, in line with the principle of proportionality.

TO WHOM?

The new CLF applies to:

Essential Entities:

- Entities of the types referred to in Annex I to the CLF that exceed the thresholds for medium-sized enterprises set out in Commission Recommendation 2003/361/EC;
- Qualified trust service providers, top-level domain name registrars and domain name system service providers, regardless of their size;
- Companies offering public electronic communications networks or publicly available electronic communications services that are considered medium-sized enterprises;
- Public administration entities with responsibilities in the provision of services in the areas of ICT infrastructure development, maintenance and management or with a high degree of digital integration, and the public entity responsible for educational assessment;
- Entities identified as critical entities under Directive (EU) 2022/2557 on the resilience of critical entities, regardless of their size.

Entidades importantes:

• Entidades dos tipos referidos nos anexos I e II ao RJC, que não sejam consideradas entidades essenciais;
• Entidades dos tipos constantes nos anexos I ou II ao RJC, que justifiquem tal qualificação com base no respetivo grau de exposição aos riscos, na dimensão da entidade e na probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico.

Entidades Públicas Relevantes:

– Grupo A inclui:
  • Serviços da administração direta do Estado e das Regiões Autónomas, com 250 ou mais trabalhadores;
  • Entidades da administração indireta e autónoma, com mais de 250 trabalhadores;
  • Entidades públicas empresariais que excedam os limiares para médias empresas;
  • Entidades administrativas independentes e órgãos como o Conselho Económico e Social, Provedoria da Justiça, e serviços técnicos da Presidência da República, Assembleia da República e tribunais.

– Grupo B inclui:
  • Serviços da administração direta do Estado e das Regiões Autónomas, com uma dimensão de 75 a 249 trabalhadores;
  • Entidades da administração indireta e autónoma com com uma dimensão de 75 a 249 trabalhadores;
  • Entidades públicas empresariais qualificadas como médias empresas.

QUANDO?

O RJC entra em vigor 120 dias após a sua publicação, i.e., em 3 de abril de 2026.

Important Entities:

• Entities of the types referred to in Annexes I and II to the CLF that are not considered essential entities;
• Entities of the types listed in Annexes I or II to the CLF that justify such classification based on their degree of exposure to risks, the size of the entity, and the likelihood and severity of incidents, including their social and economic impact.

Relevant Public Entities:

– Group A includes:
  • Direct administration services of the State and Autonomous Regions with 250 or more employees;
  • Indirect and autonomous administration entities with more than 250 employees;
  • Public business entities that exceed the thresholds for medium-sized companies;
  • Independent administrative entities and bodies such as the Economic and Social Council, the Ombudsman, and technical services of the Presidency of the Republic, the Assembly of the Republic and the courts.

– Group B includes:
  • Direct administration services of the State and Autonomous Regions with a size from 75 to 249 employees;
  • Indirect and autonomous administration entities with a size from 75 to 249 employees;
  • Public business entities classified as medium-sized companies.

WHEN?

The CLF enters into force 120 days after its publication, i.e., 3 April 2026.