

PRESIDÊNCIA DO CONSELHO DE MINISTROS**Resolução do Conselho de Ministros n.º 135/2026**

Sumário: Aprova a Avaliação Nacional de Risco e a Estratégia Nacional para a Resiliência das Entidades Críticas.

O Decreto-Lei n.º 22/2025, de 19 de março, transpõe para a ordem jurídica interna a Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à identificação, designação e reforço da resiliência das entidades críticas, estabelecendo um quadro jurídico nacional destinado a assegurar a prestação contínua de serviços essenciais à sociedade e à economia.

Nos termos do referido decreto-lei, incumbe ao Estado proceder à identificação e avaliação dos riscos relevantes para a resiliência das entidades críticas, bem como à definição de uma estratégia nacional que estabeleça objetivos, prioridades e medidas para prevenir, mitigar, responder e recuperar de incidentes que afetem essas entidades.

O artigo 11.º do Decreto-Lei n.º 22/2025, de 19 de março, prevê a elaboração de uma avaliação nacional de risco, enquanto instrumento estruturante de análise das ameaças naturais, acidentais e deliberadas suscetíveis de afetar a prestação de serviços essenciais, sendo esta aprovada por resolução do Conselho de Ministros, sob proposta do Secretário-Geral do Sistema de Segurança Interna com contributos das entidades com competências relevantes nos domínios da segurança, da proteção civil, da cibersegurança, da regulação e da supervisão setorial, bem como de outras entidades públicas com responsabilidades na avaliação de riscos de natureza setorial ou transversal.

Por seu turno, o artigo 12.º do mesmo diploma determina a elaboração de uma estratégia nacional para a resiliência das entidades críticas, a qual estabelece o enquadramento, as medidas de política, os objetivos estratégicos e as linhas de ação nesta matéria, considerando a Avaliação Nacional de Risco. A referida estratégia é aprovada por resolução do Conselho de Ministros, sob proposta da Secretária-Geral do Sistema de Segurança Interna, em colaboração com o Conselho Nacional de Planeamento Civil de Emergência, enquanto órgão de coordenação em matéria de planeamento civil de emergência.

No que se refere à segurança da informação, o artigo 10.º do Decreto-Lei n.º 22/2025, de 19 de março, estabelece ainda que a informação constante da Avaliação Nacional de Risco, no todo ou em parte, se encontra sujeita a classificação de segurança, devendo ser-lhe atribuído, no mínimo, o grau de classificação «Reservado», nos termos da legislação aplicável à proteção da informação classificada, sem prejuízo da disponibilização, às entidades críticas, de elementos pertinentes da referida avaliação que possam ser relevantes para as respetivas avaliações de risco e para a definição das medidas destinadas a reforçar a sua resiliência.

Deste modo, no âmbito da vigência do Decreto-Lei n.º 22/2025, de 19 de março, importa agora proceder à aprovação das primeiras propostas de Avaliação Nacional de Risco e da Estratégia Nacional para a Resiliência das Entidades Críticas, envolvendo as entidades competentes e assegurando a necessária articulação interinstitucional.

Acresce que o Programa «Portugal Transformação, Recuperação e Resiliência» (PTRR) integra, nas medidas que compõem o Pilar «Responder», a elaboração e aprovação da Avaliação Nacional de Risco e da Estratégia Nacional para a Resiliência das Entidades Críticas, enquanto instrumentos essenciais do reforço da capacidade do País para prevenir, mitigar e responder a riscos e crises de natureza diversa. Neste contexto, a presente resolução corporiza a concretização dessas medidas, contribuindo para uma abordagem integrada de identificação, avaliação e mitigação de riscos, bem como para o reforço da continuidade dos serviços essenciais assegurados pelas entidades críticas e da resiliência nacional.

A aprovação destes instrumentos constitui, assim, um passo essencial para a implementação coerente e eficaz do regime jurídico da resiliência das entidades críticas, reforçando a segurança, a continuidade dos serviços essenciais e a proteção dos interesses fundamentais do Estado e da sociedade.

Assim:

Nos termos da alínea g) do artigo 199.º da Constituição, do disposto nos artigos 11.º e 12.º do Decreto-Lei n.º 22/2025, de 19 de março, e sob proposta da Secretária-Geral do Sistema de Segurança Interna, em colaboração com o Conselho Nacional de Planeamento Civil de Emergência, o Conselho de Ministros resolve:

1 — Aprovar a Avaliação Nacional de Risco, prevista no artigo 11.º do Decreto-Lei n.º 22/2025, de 19 de março, constante do anexo I da presente resolução, que dela faz parte integrante.

2 — Aprovar a Estratégia Nacional para a Resiliência das Entidades Críticas, prevista no artigo 12.º do Decreto-Lei n.º 22/2025, de 19 de março, elaborada sob proposta da Secretária-Geral do Sistema de Segurança Interna, em colaboração com o Conselho Nacional de Planeamento Civil de Emergência, constante do anexo II da presente resolução, que dela faz parte integrante.

3 — Determinar que a Avaliação Nacional de Risco, no todo ou nas partes que o integrem, é classificada com o grau de segurança mínimo de «Reservado», nos termos do n.º 3 do artigo 10.º do Decreto-Lei n.º 22/2025, de 19 de março, e da legislação aplicável à proteção da informação classificada, ficando o respetivo acesso, utilização, reprodução e divulgação sujeitos às regras legalmente estabelecidas.

4 — Determinar que a Estratégia Nacional para a Resiliência das Entidades Críticas constitui um documento de natureza pública, devendo ser divulgada nos termos aplicáveis, enquanto instrumento de orientação estratégica para o reforço da resiliência das entidades críticas.

5 — Estabelecer que a presente resolução produz efeitos a partir da data da sua aprovação.

Presidência do Conselho de Ministros, 14 de maio de 2026. — O Primeiro-Ministro, Luís Montenegro.

ANEXO I

Avaliação Nacional de Risco

[Reservado.]

ANEXO II

Estratégia Nacional para a Resiliência das Entidades Críticas

1 — Preâmbulo

A Estratégia Nacional para a Resiliência das Entidades Críticas, adiante designada por Estratégia, é elaborada nos termos e para os efeitos do disposto no Decreto-Lei n.º 22/2025, de 19 de março, que transpõe para a ordem jurídica interna a Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro, relativa à resiliência das entidades críticas.

A Estratégia estabelece o enquadramento, as medidas políticas, os objetivos estratégicos e as respetivas linhas de ação, tendo em consideração a avaliação nacional de risco, e contempla os seguintes elementos estruturantes:

Os objetivos estratégicos no intuito de reforçar a resiliência global das entidades críticas, tendo em conta as dependências e interdependências transfronteiriças e intersetoriais;

O quadro de governação para alcançar os objetivos estratégicos, incluindo uma descrição das funções e responsabilidades das diferentes autoridades, entidades críticas e outras partes relevantes envolvidas na sua execução;

A descrição das medidas necessárias para reforçar a resiliência das entidades críticas;

O processo de identificação e designação das entidades críticas;

A descrição do processo de apoio às entidades críticas, nomeadamente das medidas destinadas a reforçar a cooperação entre o setor público e as entidades públicas e privadas;

As medidas de coordenação com as autoridades competentes em matéria de cibersegurança;

As medidas destinadas a facilitar o cumprimento das obrigações das entidades críticas consideradas pequenas e médias empresas na aceção do anexo da Recomendação 2003/361/CE da Comissão, de 6 de maio.

É concebida de modo a integrar, sem descontinuidades, as políticas existentes, tendo ainda em conta as estratégias nacionais e setoriais, e os planos ou documentos similares pertinentes.

A sua aprovação e sucessivas revisões resultam de resolução do Conselho de Ministros, sob proposta do Secretário-Geral do Sistema de Segurança Interna, em colaboração com o Conselho Nacional de Planeamento Civil de Emergência.

Em anexo à Estratégia, e que dela faz parte integrante, consta o respetivo Plano de Ação, que constitui o instrumento essencial de acompanhamento e avaliação da sua execução para o quadriénio de 2026-2029.

2 — Ancoragem conceptual

Para uma eficaz compreensão e implementação da Estratégia, afigura-se indispensável a definição dos conceitos fundamentais que a sustentam. A explanação conceptual, alinhada com o enquadramento jurídico nacional aplicável, permite estabelecer uma base comum de entendimento, assegurando uma interpretação unívoca dos termos e orientações essenciais. Tal é crucial para garantir a coerência e a eficácia das ações a desenvolver, promovendo a articulação adequada entre as entidades competentes, as entidades setoriais, as entidades críticas e demais partes envolvidas. Com efeito, entende-se por:

«Avaliação de riscos»: o processo geral levado a cabo para determinar a natureza e o alcance de um risco, através da identificação e análise de potenciais ameaças, vulnerabilidades e perigos pertinentes suscetíveis de provocar um incidente, bem como através da avaliação da potencial perda ou perturbação da prestação de um serviço essencial causada por esse incidente;

«Entidade crítica»: entidade pública ou privada, identificada e designada enquanto tal pelo Conselho Nacional de Planeamento Civil de Emergência, que opera uma ou mais infraestruturas críticas localizadas em território nacional, em que um incidente teria efeitos perturbadores significativos sobre a prestação de um ou mais serviços essenciais nos setores da energia; transportes; bancário; infraestruturas do mercado financeiro; saúde; água potável; águas residuais; infraestruturas digitais; Administração Pública; espaço; seguros e fundos de pensões, e produção, transformação e distribuição de produtos alimentares;

«Entidades competentes»: o Conselho Nacional de Planeamento Civil de Emergência, em matéria de identificação e designação das entidades críticas e respetivas infraestruturas críticas, e o Secretário-Geral do Sistema de Segurança Interna, em matéria de reforço de resiliência das entidades críticas;

«Entidades setoriais»: a Comissão de Planeamento de Emergência da Energia; a Comissão de Planeamento de Emergência do Transporte Aéreo; a Comissão de Planeamento de Emergência dos Transportes Terrestres; a Comissão de Planeamento de Emergência do Transporte Marítimo; o Banco de Portugal; a Comissão do Mercado de Valores Mobiliários; a Comissão de Planeamento de Emergência da Saúde; a Comissão de Planeamento de Emergência da Água e Resíduos; a Comissão de Planeamento de Emergência da Cibersegurança; a Comissão de Planeamento de Emergência das Comunicações; o Secretário-Geral do Sistema de Segurança Interna; a Agência Espacial Portuguesa; a Comissão de Planeamento de Emergência da Agricultura e Alimentação, e a Autoridade de Supervisão de Seguros e Fundos de Pensões;

«Incidente»: um evento que perturbe ou tenha potencial para perturbar significativamente a prestação de um serviço essencial, inclusive quando afetar os sistemas nacionais que salvaguardam o Estado de direito;

«Infraestrutura crítica»: o ativo, instalação, equipamento, rede ou sistema, no todo ou em parte, situada em território nacional, identificada e designada enquanto tal pelo Conselho Nacional de Planeamento Civil de Emergência, cuja perturbação do funcionamento ou destruição teria um efeito perturbador significativo na prestação de um serviço essencial;

«Resiliência»: a capacidade de prevenção, proteção, resposta, resistência, atenuação, mitigação, adaptação e recuperação de uma entidade crítica face a incidentes;

«Risco»: o potencial de perda ou perturbação causada por um incidente, expresso pela combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente;

«Serviço essencial»: o serviço indispensável à manutenção de funções societárias ou atividades económicas vitais, da saúde e segurança pública ou do ambiente e que integra uma das categorias constantes do anexo ao Decreto-Lei n.º 22/2025, de 19 de março, e do qual faz parte integrante.

3 – Princípios fundamentais

A Estratégia assenta no quadro político e jurídico que reflete as obrigações e os compromissos assumidos pelo Estado Português, no plano nacional e internacional, em matéria de resiliência das entidades críticas, alicerçando-se nos seguintes princípios fundamentais:

Princípio da proporcionalidade: as medidas adotadas no âmbito da resiliência das entidades críticas devem ser adequadas, necessárias e proporcionais ao contexto de ameaças e riscos emergentes e prospetivos, à sua dimensão e à natureza dos serviços essenciais prestados;

Princípio da subsidiariedade: o papel do Estado e das autoridades competentes é apoiar, colaborar e cooperar com as entidades críticas no reforço da resiliência, sem, contudo, substituí-las quanto às suas responsabilidades legais;

Princípio da complementaridade: as medidas de resiliência devem articular-se e complementar-se com outros instrumentos de política pública, regimes jurídicos setoriais, estratégias nacionais e internacionais, evitando duplicação ou sobreposição de obrigações;

Princípio da cooperação institucional: as entidades competentes, as entidades setoriais, as entidades críticas e demais entidades fundamentais ao seu âmbito de aplicação têm o dever de cooperar entre si, partilhar informação e promover a coordenação de esforços para reforçar as capacidades de resiliência;

Princípio da eficiência: a implementação da Estratégia obedece a critérios de eficiência técnica, administrativa e financeira, assegurando o uso racional dos recursos e a maximização da implementação das medidas adotadas.

4 – Análise do contexto nacional e internacional

A resiliência das entidades críticas afirma-se, no atual contexto global, como um fator essencial da segurança nacional, da estabilidade institucional e da garantia das funções vitais do Estado e da sociedade.

Num cenário internacional marcado pela intensificação de ameaças e riscos complexos, interdependentes, intersetoriais e transfronteiriços, como o terrorismo, as alterações climáticas, a cibercriminalidade, a instabilidade geopolítica, as pandemias, os ataques híbridos, a desinformação e as falhas nas cadeias logísticas, colocam-se inevitavelmente em perspetiva as vulnerabilidades à prestação dos serviços essenciais.

Em particular no contexto da União Europeia, a evolução da resiliência das entidades críticas tem sido acompanhada por um esforço contínuo de harmonização normativa e de reforço da capacidade

coletiva de resposta. A publicação da Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro, relativa à resiliência das entidades críticas, marca um ponto de inflexão nesta matéria. Substituindo a anterior Diretiva 2008/114/CE, adota uma abordagem substancialmente mais abrangente, centrada não apenas na proteção de infraestruturas críticas mas sobretudo na garantia da continuidade da prestação dos serviços essenciais. Abrange um maior número de setores estratégicos, impõe obrigações reforçadas às entidades críticas, requer uma avaliação sistemática de riscos e estabelece deveres de planeamento, notificação e cooperação nacional e transnacional.

A nova diretiva europeia inscreve-se numa política abrangente, coerente e integrada de segurança, proteção e resiliência perante ameaças complexas e crises emergentes, articulando-se com vários instrumentos jurídicos e estratégicos da União Europeia. Entre estes, destacam-se a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança (NIS2); a Estratégia Europeia de Segurança Interna (ProtectEU); a Estratégia da União Europeia para a Preparação (European Preparedness Union Strategy); o Livro Branco da Defesa Europeia — Prontidão 2030 (Readiness 2030); o futuro Escudo Europeu da Democracia (European Democracy Shield); a Recomendação do Conselho (C/2024/4371), de 25 de junho de 2024, sobre o plano de ação para a coordenação da resposta a nível da UE a perturbações em infraestruturas críticas com importante relevância transfronteiriça (Critical Infrastructure Blueprint); a Recomendação do Conselho, de 8 de dezembro de 2022, relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas, e a Comunicação da Comissão Europeia C/2025/4990, de 12 de setembro de 2025, com orientações sobre a resiliência de entidades críticas.

Portugal transpôs a Diretiva (UE) 2022/2557, de 14 de dezembro, através do Decreto-Lei n.º 22/2025, de 19 de março, estabelecendo um novo regime jurídico em matéria de resiliência das entidades críticas que engloba os setores da energia; transportes; bancário; infraestruturas do mercado financeiro; saúde; água potável; águas residuais; infraestruturas digitais; Administração Pública; espaço; produção, transformação e distribuição de produtos alimentares; seguros e fundos de pensões; bem como os subsectores e serviços essenciais constantes do seu anexo, e do qual faz parte integrante.

Sobreleva-se que o seu âmbito não se aplica às entidades da Administração Pública que exerçam as suas atividades nos domínios da segurança nacional, da segurança pública, da defesa nacional, e às demais entidades excluídas no anexo mencionado, salvo aquelas que, em situações excecionais devidamente fundamentadas, venham a ser identificadas no âmbito da continuidade da ação governativa ou da gestão de crises.

Sem prejuízo do disposto, reconhece-se também que a resiliência das entidades críticas e a continuidade da prestação dos serviços essenciais envolve interdependências operacionais com funções vitais do Estado, podendo repercutir-se na capacidade de atuação de entidades daqueles domínios.

O novo regime jurídico substitui o modelo precedente, centrado iminentemente na proteção de infraestruturas críticas nacionais, por um paradigma mais dinâmico e funcional, que atribui relevo à prevenção, resposta e recuperação face a incidentes com impacto potencial na prestação de serviços essenciais. Define também um quadro de governação partilhada, assente na articulação estreita entre o Secretário-Geral do Sistema de Segurança Interna, o Conselho Nacional de Planeamento Civil de Emergência, as entidades setoriais, as entidades críticas e demais entidades fundamentais para o seu escopo.

O enquadramento normativo impõe obrigações concretas às entidades críticas, incluindo, sobretudo, a realização de avaliações de risco, a elaboração de planos de resiliência, a notificação de incidentes relevantes, a realização de exercícios regulares e a designação de agentes de ligação com as entidades legalmente previstas. Em simultâneo, estabelece mecanismos de supervisão, fiscalização e responsabilização, prevendo sanções para situações de incumprimento.

A Estratégia e o seu Plano de Ação consubstanciam o instrumento político de enquadramento e operacionalização destas obrigações, devendo refletir uma visão compreensiva, holística, integrada e orientada para a implementação eficaz de medidas de resiliência adequadas, necessárias e proporcionais.

A nível nacional, subsistem diversos desafios estruturais que exigem resposta estratégica, desde a necessidade de assegurar uma aplicação uniforme do novo regime jurídico entre setores com maturidades distintas até à exigência de desenvolver capacidades técnicas e humanas especializadas, nomeadamente no domínio da cibersegurança, da gestão de riscos sistémicos e da análise de interdependências operacionais. Acresce a complexidade própria da gestão de entidades privadas que operam serviços públicos essenciais, exigindo mecanismos robustos de supervisão, regulação, cooperação e responsabilização partilhada.

Não obstante, Portugal dispõe de um património relevante no domínio da segurança interna, da proteção civil, da cibersegurança, da regulação setorial e da proteção de infraestruturas críticas, bem como de uma crescente maturidade na articulação entre entidades públicas e privadas. Esta capacidade deve ser agora consolidada e ampliada através de uma Estratégia que promova a coerência entre os diversos regimes setoriais, assegure o alinhamento com os compromissos internacionais e fomente uma cultura transversal de resiliência societal. Afigura-se ainda muito relevante que integre, sem descontinuidades, as políticas existentes, tendo em conta outras estratégias nacionais e setoriais e os planos ou documentos similares pertinentes.

O contexto atual impõe, assim, uma visão estratégica que transcende o mero cumprimento normativo e que posicione a resiliência das entidades críticas como um elemento estruturante da segurança nacional, da confiança institucional e da estabilidade socioeconómica.

A Estratégia visa precisamente responder a esse imperativo, procurando estabelecer um quadro coerente, harmonizado e eficaz de reforço da resiliência, com impacto direto na capacidade do País para dirimir ameaças e riscos, proteger os seus cidadãos e garantir a prestação ininterrupta dos serviços essenciais, sobretudo em cenários de emergência ou crise.

5 – Visão

A Estratégia tem a seguinte visão para o quadriénio de 2026-2029:

«Estabelecer um quadro estratégico e operacional coerente e harmonizado que garanta a prestação dos serviços essenciais e reforce a resiliência das entidades críticas, através de uma abordagem holística e integrada.»

6 – Eixos de intervenção e objetivos estratégicos

A definição dos objetivos estratégicos decorre da análise do contexto nacional e internacional, sendo indicados e agregados em eixos de intervenção estruturantes que orientam a prossecução das medidas a implementar, através de uma abordagem integrada e coerente que assegure a articulação institucional e a eficiência e eficácia da sua prossecução, nomeadamente:

Eixo I – Reforço da Resiliência das Entidades Críticas:

Objetivo Estratégico n.º 1 – Estabelecer processos criteriosos para a identificação e designação das entidades críticas e das infraestruturas críticas que operam, incluindo a sua revisão e monitorização periódica, para assegurar a sua atualização e adequação à evolução do contexto de ameaças e riscos.

Objetivo Estratégico n.º 2 – Avaliar sistematicamente a natureza e o alcance dos riscos que impendem sobre as entidades críticas, através da identificação e análise de potenciais ameaças, vulnerabilidades e perigos suscetíveis de provocar um incidente, incluindo os que incidam sobre as respetivas cadeias de abastecimento, bem como da apreciação da potencial perda ou perturbação da prestação de um serviço essencial.

Objetivo Estratégico n.º 3 – Assegurar que as entidades críticas adotam as medidas necessárias, adequadas e proporcionais para prevenir, proteger, responder, resistir, atenuar, mitigar, adaptar e recuperar de incidentes que possam perturbar significativamente a prestação de serviços essenciais.

Eixo II – Cooperação, Supervisão e Coordenação Institucional:

Objetivo Estratégico n.º 4 – Reforçar a cooperação nacional e internacional entre as entidades competentes, as entidades setoriais, as entidades críticas e demais intervenientes relevantes, promovendo uma abordagem integrada e concertada de reforço da resiliência, alinhada com o quadro jurídico nacional e as políticas e orientações das organizações internacionais de que Portugal faz parte.

Objetivo Estratégico n.º 5 – Robustecer os mecanismos de coordenação e supervisão entre as entidades competentes, as entidades setoriais, as entidades críticas e demais intervenientes relevantes, garantindo a implementação das medidas de resiliência e o cumprimento dos requisitos legais.

Eixo III – Investigação, Formação, Comunicação e Cultura de Resiliência:

Objetivo Estratégico n.º 6 – Reforçar as capacidades técnicas, operacionais e organizativas das entidades críticas, através de ações de formação e exercícios, desenvolvendo estratégias eficazes de comunicação e alerta dirigidas às mesmas e aos utilizadores dos serviços essenciais.

Objetivo Estratégico n.º 7 – Promover uma cultura nacional de resiliência e o potencial nacional de investigação, desenvolvimento e inovação no âmbito da resiliência das entidades críticas, envolvendo os setores público e privado e a academia.

7 – Medidas de resiliência

As medidas de resiliência adiante elencadas prosseguem os objetivos estratégicos e são agrupadas de acordo com os eixos de intervenção identificados, nomeadamente o reforço da resiliência das entidades críticas; a cooperação, supervisão e coordenação institucional, e a investigação, formação, comunicação e cultura de resiliência.

A sua execução e implementação, detalhadas no Plano de Ação em anexo, baseiam-se na definição clara de responsabilidades e na articulação institucional e operacional, visando acautelar os imperativos e idiossincrasias do contexto nacional e internacional.

Eixo I – Reforço da Resiliência das Entidades Críticas:**Objetivo Estratégico n.º 1:**

Medida n.º 1 – Atualizar a avaliação nacional de risco, sempre que necessário, que visa apoiar o processo de identificação das entidades críticas e a adoção de medidas de resiliência.

Medida n.º 2 – Propor para aprovação ao Conselho Nacional de Planeamento Civil de Emergência, através das entidades setoriais, a densificação dos critérios de identificação das entidades críticas, bem como as entidades e respetivas infraestruturas suscetíveis de serem classificadas como críticas, no respetivo setor ou subsetor.

Medida n.º 3 – Avaliar, com as entidades setoriais, a inclusão de novos serviços essenciais, setores ou subsetores, bem como a eventual eliminação de serviços essenciais listados no anexo ao Decreto-Lei n.º 22/2025, de 19 de março, atentas as lições aprendidas e os novos conhecimentos relacionados com as respetivas dependências.

Medida n.º 4 – Aprovar os critérios e metodologia aplicáveis para o efeito, e identificar e designar as entidades críticas e respetivas infraestruturas críticas, através do Conselho Nacional de Planeamento Civil de Emergência.

Medida n.º 5 – Elaborar um referencial de boas práticas na metodologia de identificação de entidades críticas, propondo, caso se justifique, alterações ao Decreto-Lei n.º 22/2025, de 19 de março.

Objetivo Estratégico n.º 2:

Medida n.º 6 – Implementar processos contínuos e sistemáticos de avaliação, análise e mitigação dos riscos, em coordenação com as entidades competentes, considerando dependências e interde-

pendências setoriais, intersetoriais e transfronteiriças, visando uma resposta preventiva e eficaz face a ameaças e riscos que possam comprometer a prestação de serviços essenciais.

Medida n.º 7 — Efetuar a avaliação de risco das entidades críticas, a cargo das próprias, no prazo de nove meses a contar da data da receção da notificação da sua designação, que inclui obrigatoriamente a avaliação dos riscos específicos relativos a cada uma das suas infraestruturas críticas.

Medida n.º 8 — Promover diretamente ou através dos demais órgãos e entidades que integram o Sistema de Segurança Interna, a troca de informações pertinentes relativas às ameaças e riscos para as entidades críticas, sem prejuízo dos regimes legais aplicáveis à proteção e salvaguarda da informação classificada, e aos segredos de Estado e de justiça.

Medida n.º 9 — Desenvolver a taxonomia comum para a classificação dos riscos que impedem sobre as entidades e infraestruturas críticas, através do Secretário-Geral do Sistema de Segurança Interna.

Objetivo Estratégico n.º 3:

Medida n.º 10 — Submeter à aprovação do Secretário-Geral do Sistema de Segurança Interna, após notificação da designação enquanto entidade crítica, o respetivo plano de resiliência, que deve anexar e englobar um plano de segurança por cada infraestrutura crítica.

Medida n.º 11 — Elaborar pareceres emitidos a pedido do Secretário-Geral do Sistema de Segurança Interna com vista à aprovação dos planos de resiliência das entidades críticas.

Medida n.º 12 — Aprovar os planos de resiliência das entidades críticas, através do Secretário-Geral do Sistema de Segurança Interna.

Medida n.º 13 — Elaborar e comunicar ao Secretário-Geral do Sistema de Segurança Interna, através das forças de segurança territorialmente competentes, um plano de intervenção para cada infraestrutura crítica situada na sua área de responsabilidade geográfica.

Medida n.º 14 — Notificar de imediato o Secretário-Geral do Sistema de Segurança Interna e acionar os respetivos planos, através das entidades críticas, perante incidentes que perturbem significativamente, ou sejam suscetíveis de perturbar, a prestação de serviços essenciais ou o funcionamento das infraestruturas críticas que os asseguram.

Medida n.º 15 — Coordenar e comunicar a verificação de antecedentes de segurança humana e a sua implementação, através do Secretário-Geral do Sistema de Segurança Interna e em articulação com as entidades críticas.

Medida n.º 16 — Criar uma unidade orgânica específica em matéria de resiliência e entidades críticas, no âmbito do Sistema de Segurança Interna e na dependência e coordenação do Secretário-Geral do Sistema de Segurança Interna.

Medida n.º 17 — Garantir que as informações relacionadas com a designação e reforço de resiliência das entidades críticas e respetivas infraestruturas críticas são objeto de avaliação com vista à eventual classificação de segurança, bem como que o tratamento da informação classificada respeita a legislação e normas de segurança aplicáveis à proteção e salvaguarda da informação classificada.

Medida n.º 18 — Assegurar que o tratamento da informação classificada, nomeadamente a sua produção, utilização, partilha, arquivo ou armazenamento por parte das entidades críticas, respeita o regime da informação classificada e em particular os requisitos das áreas de segurança da informação e dos sistemas de informação e comunicação.

Eixo II — Cooperação, Supervisão e Coordenação Institucional:

Objetivo Estratégico n.º 4:

Medida n.º 19 — Assegurar a representação nacional e o ponto de contacto único com a Comissão Europeia em matéria de resiliência das entidades críticas, através do Secretário-Geral do Sistema de

Segurança Interna, garantindo a representação de Portugal no Grupo para a Resiliência das Entidades Críticas que assiste a Comissão Europeia no quadro e para os efeitos da Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022.

Medida n.º 20 — Promover a partilha de informação no âmbito da identificação de entidades críticas com os demais Estados-Membros da União Europeia e estimular a assinatura de protocolos de colaboração.

Medida n.º 21 — Garantir a articulação com as entidades congéneres de outros Estados-Membros da União Europeia, ou de países terceiros, em matéria de resiliência das entidades críticas, através do Secretário-Geral do Sistema de Segurança Interna.

Medida n.º 22 — Assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da resiliência das entidades críticas, através do Secretário-Geral do Sistema de Segurança Interna.

Objetivo Estratégico n.º 5:

Medida n.º 23 — Difundir orientações técnicas e outros instrumentos de apoio à elaboração dos planos de resiliência das entidades críticas, dos planos de segurança das infraestruturas críticas, dos mecanismos de notificação de incidentes, dos planos de intervenção das forças de segurança, e de exercícios, apoiando a sua implementação e monitorizando a sua execução, através do Secretário-Geral do Sistema de Segurança Interna.

Medida n.º 24 — Assegurar as competências de fiscalização e de aplicação de sanções previstas no Decreto-Lei n.º 22/2025, de 19 de março, através do Secretário-Geral do Sistema de Segurança Interna.

Medida n.º 25 — Partilhar o acesso às melhores práticas e metodologias disponíveis, assim como, sempre que possível, à informação sobre os novos avanços técnicos relacionados com a resiliência das entidades críticas, incorporando boas práticas e lições aprendidas no plano nacional e internacional.

Medida n.º 26 — Cooperar com as autoridades competentes em matéria de cibersegurança na partilha de informação sobre riscos de cibersegurança, ciberameaças, ciberincidentes, bem como riscos, ameaças e incidentes não relacionados com cibersegurança, e ainda no exercício de funções de supervisão na esfera do Secretário-Geral do Sistema de Segurança Interna.

Medida n.º 27 — Desenvolver uma plataforma digital comum de notificação de incidentes relativos à resiliência das entidades críticas e ao Regime Jurídico da Cibersegurança, envolvendo o Secretário-Geral do Sistema de Segurança Interna e as autoridades competentes em matéria de cibersegurança.

Medida n.º 28 — Designar um agente de ligação da entidade crítica responsável pela articulação institucional em matéria de resiliência, e um agente de ligação para cada infraestrutura crítica que detém ou explora.

Medida n.º 29 — Assegurar a coordenação com o Secretário-Geral do Sistema de Segurança Interna, as forças e serviços de segurança, a Autoridade Nacional de Emergência e Proteção Civil ou os serviços regionais de proteção civil territorialmente competentes, para obtenção de informações sobre graus de ameaça, estados de segurança e estados de alerta do sistema de proteção civil, através dos agentes de ligação das entidades críticas.

Medida n.º 30 — Assegurar e manter atualizada a plataforma eletrónica de registo das entidades e infraestruturas críticas, através do Secretário-Geral do Sistema de Segurança Interna, que compreende, entre outras informações, a sua catalogação; o elenco de contactos de cooperação institucional e de coordenação operacional; a seriação dos planos de resiliência, segurança e intervenção; a gestão de acidentes e incidentes relevantes, e demais dados que permitam planear e priorizar as medidas de reforço da resiliência.

Medida n.º 31 — Constituir um grupo de trabalho de cooperação e colaboração institucional e operacional, sob a égide do Secretário-Geral do Sistema de Segurança Interna, envolvendo as forças

e serviços de segurança, de emergência e proteção civil, e as autoridades competentes de cibersegurança, no âmbito e para os efeitos estabelecidos no Decreto-Lei n.º 22/2025, de 19 de março.

Eixo III — Investigação, Formação, Comunicação e Cultura de Resiliência:

Objetivo Estratégico n.º 6:

Medida n.º 32 — Realizar pelo menos um exercício durante a vigência do plano de resiliência aprovado, através das entidades críticas, visando testar a adequação das medidas, procedimentos e ações constantes dos mesmos.

Medida n.º 33 — Testar, durante a vigência do plano de resiliência aprovado, através das entidades críticas, todos os planos de segurança das infraestruturas críticas que dele fazem parte, devendo ser envolvidas as forças de segurança e os serviços municipais de proteção civil territorialmente competentes.

Medida n.º 34 — Promover a realização de pelo menos um exercício, ao nível e através das entidades setoriais, envolvendo as entidades críticas, o Secretário-Geral do Sistema de Segurança Interna, o Conselho Nacional de Planeamento Civil de Emergência, e outras entidades relevantes em razão da matéria.

Medida n.º 35 — Promover a realização de pelo menos um exercício transversal, através do Secretário-Geral do Sistema de Segurança Interna e em articulação com o Conselho Nacional de Planeamento Civil de Emergência e as entidades setoriais, podendo envolver entidades críticas e outras entidades relevantes em razão da matéria, assim como, quando pertinente, entidades de outros Estados-Membros da União Europeia.

Medida n.º 36 — Formar e treinar os recursos humanos das entidades críticas, na esfera de responsabilidade das próprias, na implementação das medidas previstas ou implementadas no respetivo plano de resiliência.

Medida n.º 37 — Desenvolver estratégias eficazes de comunicação e alerta dirigidas às entidades críticas e aos utilizadores dos serviços essenciais.

Objetivo Estratégico n.º 7:

Medida n.º 38 — Fomentar uma comunidade de conhecimento e uma cultura nacional de resiliência.

Medida n.º 39 — Apoiar e promover o potencial nacional de investigação, desenvolvimento e inovação no âmbito da identificação e resiliência de entidades críticas, envolvendo o setor público e privado e a academia, através do Secretário-Geral do Sistema de Segurança Interna e do Conselho Nacional de Planeamento Civil de Emergência.

Medida n.º 40 — Desenvolver estudos e formular as propostas consideradas pertinentes para o desenvolvimento e aperfeiçoamento do quadro de governação da resiliência das entidades críticas, no seu âmbito jurídico, político, estratégico e operacional, através do Secretário-Geral do Sistema de Segurança Interna e em articulação com o Conselho Nacional de Planeamento Civil de Emergência.

Medida n.º 41 — Implementar um processo sistemático de recolha e partilha de boas práticas e lições aprendidas nos vários domínios da resiliência, incluindo riscos e ameaças de natureza setorial ou transversal, complementado com sessões de sensibilização dirigidas às entidades críticas.

Medida n.º 42 — Promover ações de formação no âmbito da legislação e normas de segurança aplicáveis à proteção e salvaguarda da informação classificada.

8 — Quadro de governação relativo aos objetivos estratégicos

O quadro de governação para alcançar os objetivos estratégicos contempla uma descrição das funções e responsabilidades das entidades competentes, das entidades setoriais, das entidades críticas e de outras partes relevantes envolvidas na sua execução.

Secretário-Geral do Sistema de Segurança Interna

O Secretário-Geral do Sistema de Segurança Interna é a autoridade nacional competente na coordenação e supervisão das medidas de reforço da resiliência das entidades críticas, face a incidentes, riscos e ameaças que possam comprometer a prestação de serviços essenciais.

Compete-lhe coordenar a elaboração e sucessivas atualizações da avaliação nacional de risco, que visa apoiar a identificação das entidades críticas e a adoção de medidas de resiliência; e a Estratégia Nacional para a Resiliência das Entidades Críticas, e revisões ulteriores, que estabelece as medidas políticas, os objetivos estratégicos e as respetivas linhas de ação.

No âmbito do apoio técnico, o Secretário-Geral do Sistema de Segurança Interna tem a responsabilidade de difundir orientações que facilitem a elaboração dos planos de resiliência das entidades críticas, dos planos de segurança das infraestruturas críticas, dos planos de intervenção das forças de segurança, de notificação de incidentes, e de exercícios, assegurando a sua implementação e monitorização.

Cabe-lhe também aprovar os planos de resiliência das entidades críticas em conformidade com os requisitos estabelecidos. Tal implica a aprovação de cada um dos planos de segurança das infraestruturas críticas que o integram, carecendo dos pareceres da entidade reguladora do setor de atividade em causa, quando exista e tenha atribuições nesta matéria; das forças de segurança territorialmente competentes; da Autoridade Nacional de Emergência e Proteção Civil ou do serviço regional de proteção civil territorialmente competente, e de outras entidades públicas com competência em razão da matéria.

Promove ainda a formação e a qualificação de recursos humanos na área da resiliência das entidades críticas, fomentando uma comunidade de conhecimento e uma cultura nacional de segurança neste domínio.

Em articulação com o Conselho Nacional de Planeamento Civil de Emergência e com as entidades setoriais, realiza exercícios transversais, envolvendo entidades críticas nacionais e outras consideradas relevantes, assim como, quando pertinente, de outros Estados-Membros da União Europeia.

É também responsável pela fiscalização e aplicação das sanções previstas no quadro jurídico aplicável, garantindo o cumprimento das normas e a efetiva implementação das medidas de resiliência. As atividades de supervisão e de execução são orientadas pelos princípios da prossecução do interesse público, da legalidade, da eficiência, da eficácia e da proporcionalidade, devendo minimizar, sempre que possível, o seu impacto nas atividades públicas, sociais e empresariais das entidades supervisionadas. No exercício das suas funções de fiscalização, o Secretário-Geral do Sistema de Segurança Interna é coadjuvado pelas autoridades policiais e outras autoridades ou serviços públicos cuja colaboração solicite.

Além disso, no exercício das suas competências, assegura a verificação de antecedentes de segurança humana e a sua implementação, contribuindo para a resiliência e integridade das entidades críticas.

A articulação com entidades congéneres da União Europeia constitui uma dimensão essencial da sua missão, sobretudo no caso das entidades críticas que utilizem infraestruturas fisicamente ligadas entre dois ou mais Estados-Membros; integrem estruturas empresariais associadas a entidades críticas noutros Estados-Membros; ou tenham sido identificadas como entidades críticas num Estado-Membro e prestem serviços essenciais a outros ou noutros.

É também o ponto de contacto nacional com a Comissão Europeia e o Conselho da União Europeia em matéria de resiliência das entidades críticas.

Assegura ainda e mantém atualizada a plataforma eletrónica de registo das entidades e infraestruturas críticas que compreende, entre outras informações, a sua catalogação; o elenco de contactos de cooperação institucional e de coordenação operacional; a seriação dos planos de resiliência, segurança e intervenção; a gestão de acidentes e incidentes relevantes, e demais dados que permitam planear e priorizar as medidas de reforço da resiliência.

O Secretário-Geral do Sistema de Segurança Interna assegura a articulação entre o Sistema de Segurança Interna e o Sistema Nacional de Planeamento Civil de Emergência, que visa garantir a organização e preparação dos setores estratégicos do Estado para fazer face a situações de crise, tendo como fim assegurar a liberdade e a continuidade da ação governativa; o funcionamento regular dos serviços essenciais do Estado, e a segurança e o bem-estar das populações.

Conselho Nacional de Planeamento Civil de Emergência

O Conselho Nacional de Planeamento Civil de Emergência tem competências fundamentais em matéria de identificação e designação das entidades críticas e das respetivas infraestruturas críticas. Compete-lhe aprovar os respetivos critérios e metodologia aplicáveis, bem como identificar e designar as entidades críticas e respetivas infraestruturas críticas. Para o efeito, pode solicitar parecer às entidades que considere relevantes para a fundamentação das suas deliberações.

No processo que antecede à designação, o Conselho Nacional de Planeamento Civil de Emergência é responsável pela comunicação às entidades candidatas do seu potencial estatuto de entidade crítica, promovendo o contraditório e recolhendo as pronúncias das entidades visadas. Quando necessário, remete essas pronúncias às respetivas entidades setoriais para reanálise e eventual adequação da fundamentação das propostas.

No momento da notificação da designação de uma entidade crítica, o Conselho Nacional de Planeamento Civil de Emergência dá conhecimento simultâneo ao Secretário-Geral do Sistema de Segurança Interna, à respetiva entidade setorial, às autoridades competentes no âmbito da cibersegurança, e aos presidentes de câmara municipal territorialmente competentes.

Procede ainda à designação de entidades críticas para além das propostas pelas entidades setoriais, sempre que disponha de indicadores distintos dos aplicados, ou quando as entidades em causa sejam conexas com outras entidades ou infraestruturas críticas, do mesmo ou de outro setor, nomeadamente por as poderem afetar em caso de perturbação do funcionamento ou destruição.

Decorrente da monitorização permanente da atividade dos setores, compete ao Conselho Nacional de Planeamento Civil de Emergência designar novas entidades críticas ou proceder à revogação de entidades designadas, sempre que os critérios estabelecidos deixem de estar cumpridos.

Cabe-lhe também remeter à Comissão Europeia uma proposta fundamentada das entidades críticas com potencial para serem designadas como entidades críticas de especial relevância europeia. Caso a Comissão Europeia determine que a entidade em causa é de especial relevância europeia, compete ao Conselho Nacional de Planeamento Civil de Emergência proceder à notificação da entidade crítica dessa qualidade.

Contribui ainda para a elaboração da avaliação nacional de risco e colabora com o Secretário-Geral do Sistema de Segurança Interna na elaboração da Estratégia, bem como na promoção da realização de exercícios transversais. Fomenta ainda a partilha de boas práticas com as demais entidades competentes, entidades setoriais e entidades críticas.

É também o ponto de contacto nacional com a Comissão Europeia nas matérias relativas à identificação e designação das entidades críticas. Compete-lhe enviar a lista de serviços essenciais não incluídos no regulamento europeu aplicável, o número de entidades críticas identificadas por setor, subsetor e serviço essencial, e os limiares, em separado ou agregados, aplicados para especificar os critérios de designação.

Entidades setoriais

As entidades setoriais são responsáveis por propor ao Conselho Nacional de Planeamento Civil de Emergência a densificação dos critérios de identificação das entidades críticas, incluindo os limiares aplicáveis para especificar os critérios relevantes. Neste âmbito, propõem também as entidades e respetivas infraestruturas suscetíveis de serem designadas e identificadas como críticas, no respetivo setor ou subsetor.

No desempenho das suas atribuições, consultam as entidades com competências de regulação ou supervisão dos setores ou subsetores em causa sempre que estas não integrem as próprias entidades setoriais. Podem ainda solicitar a colaboração de outras entidades consideradas relevantes para o exercício das suas funções. Esta cooperação contribui para garantir uma abordagem articulada e tecnicamente sustentada do processo de designação e identificação das entidades críticas.

Participam ainda na revisão da designação das entidades críticas com uma periodicidade de quatro anos. Esta revisão tem como objetivo identificar as entidades críticas que devem manter essa qualidade, aquelas cuja designação deve ser revogada e, ainda, eventuais novas entidades candidatas para o mesmo efeito. Em paralelo, as entidades setoriais monitorizam em permanência alterações substanciais, em curso ou previstas, que possam ter impacto na prestação de serviços essenciais no respetivo setor ou subsetor. Com base nessa monitorização, procedem à avaliação da existência de entidades candidatas à designação ou à revogação da designação de entidades previamente identificadas.

Para além destas responsabilidades, cooperam com as entidades competentes e com as entidades críticas na capacitação da resiliência. Esta cooperação contempla a partilha de boas práticas, metodologias disponíveis e informação sobre novos avanços técnicos relevantes para o reforço da resiliência, assim como sobre ameaças e riscos emergentes.

Sempre que solicitadas pelo Secretário-Geral do Sistema de Segurança Interna, as entidades setoriais emitem pareceres técnicos no âmbito da elaboração e aprovação dos planos de resiliência e de segurança das entidades críticas. Esta colaboração técnica permite assegurar que as medidas propostas nos planos são adequadas, proporcionais e ajustadas às idiossincrasias de cada setor ou subsetor.

No exercício das suas funções, acompanham o cumprimento das obrigações legais pelas entidades críticas no respetivo setor, promovendo a articulação institucional e apoiando tecnicamente a sua implementação. Esta atividade é exercida em estreita articulação com o Conselho Nacional de Planeamento Civil de Emergência e com o Secretário-Geral do Sistema de Segurança Interna.

Promovem, também, a realização de exercícios ao seu nível, envolvendo as entidades críticas, o Secretário-Geral do Sistema de Segurança Interna, o Conselho Nacional de Planeamento Civil de Emergência, e outras entidades relevantes em razão da matéria.

Mediante avaliação por parte do Secretário-Geral do Sistema de Segurança Interna podem ainda aceder e efetuar registos na plataforma eletrónica de registo de informação de entidades críticas e infraestruturas críticas.

Finalmente, cooperam com o Conselho Nacional de Planeamento Civil de Emergência, o Secretário-Geral do Sistema de Segurança Interna e demais entidades competentes, assegurando a harmonização das abordagens setoriais com o quadro estratégico nacional e europeu de resiliência. Esta cooperação visa garantir a coerência e a eficácia das medidas adotadas, contribuindo para o reforço da segurança das infraestruturas críticas e para a continuidade da prestação dos serviços essenciais.

Autoridades competentes em matéria de cibersegurança

As autoridades competentes em matéria de cibersegurança têm um papel de cooperação e articulação com o Secretário-Geral do Sistema de Segurança Interna e o Conselho Nacional de Planeamento Civil de Emergência, no que se refere à partilha de informação, ao exercício de funções de supervisão, e aos aspetos relevantes da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança (NIS2), transposta para o ordenamento jurídico interno através do Decreto-Lei n.º 125/2025, de 4 de dezembro.

Em particular, cooperam com as entidades competentes mencionadas, através da partilha de informação relativa a riscos de cibersegurança, ciberameaças e ciberincidentes, bem como riscos, ameaças e incidentes não relacionados com a cibersegurança. Esta partilha de informação tem também por objetivo apoiar o exercício das competências de supervisão sobre as entidades críticas, quando aplicável.

Sempre que exerçam as suas competências quanto às entidades dos setores dos serviços bancários, das infraestruturas do mercado financeiro e das infraestruturas digitais, as autoridades competentes

em matéria de cibersegurança devem informar o Secretário-Geral do Sistema de Segurança Interna. Concomitantemente, este pode solicitar a essas autoridades que exerçam as suas competências de supervisão e execução respeitantes às entidades críticas dos setores mencionados.

No quadro da articulação nacional, o Secretário-Geral do Sistema de Segurança Interna, enquanto ponto de contacto nacional com a Comissão Europeia em matéria de resiliência das entidades críticas, assegura a comunicação de elementos que envolvem, entre outros aspetos, a cooperação com as autoridades competentes no domínio da cibersegurança, nomeadamente no contexto da partilha de informações sobre riscos de cibersegurança, ciberameaças e ciberincidentes.

As autoridades competentes em matéria de cibersegurança são também destinatárias das notificações de designação de entidade crítica, quando aplicável, e participam na articulação com os restantes intervenientes do quadro nacional de resiliência, garantindo a integração da dimensão de cibersegurança na proteção das entidades e infraestruturas críticas.

Entidades críticas

As entidades críticas devem realizar, no prazo de nove meses a contar da notificação da sua designação, uma avaliação de risco, que deve ter em conta os elementos pertinentes da avaliação nacional de risco, bem como as relações de interdependência com outros setores, sempre que os serviços essenciais que prestam sejam afetados ou tenham impacto noutros setores. A avaliação de risco inclui, obrigatoriamente, a avaliação dos riscos específicos relativos a cada uma das suas infraestruturas críticas.

Com base nessa avaliação, cada entidade crítica elabora e implementa um plano de resiliência que integra medidas técnicas, de segurança e de organização necessárias para assegurar a sua resiliência. Inclui ainda medidas para prevenir a ocorrência de incidentes, assegurar a adequada proteção física das instalações, resistir e atenuar as consequências dos incidentes, recuperar os serviços afetados, garantir a gestão apropriada da segurança dos recursos humanos, e formar e treinar os mesmos na aplicação das medidas previstas. O plano de resiliência compreende também, como anexo, um plano de segurança por cada infraestrutura crítica.

O plano de resiliência deve ser submetido ao Secretário-Geral do Sistema de Segurança Interna para aprovação no prazo de 10 meses após a notificação da designação dessa qualidade. As entidades críticas devem rever o plano de resiliência no prazo máximo de quatro anos ou sempre que se justifique, nomeadamente em caso de perturbação grave na prestação do serviço essencial, alteração significativa das infraestruturas críticas ou obtenção de novos conhecimentos relevantes.

As entidades críticas devem ainda designar um agente de ligação responsável pela articulação institucional em matéria de resiliência com as entidades competentes. Cabe-lhe, entre outras responsabilidades, assegurar a ligação com o Secretário-Geral do Sistema de Segurança Interna, com as forças e serviços de segurança e com a Autoridade Nacional de Emergência e Proteção Civil ou os serviços regionais de proteção civil territorialmente competentes. Ademais, deve comunicar às entidades competentes as situações anómalas que ocorram e que possam ter impacto na manutenção do serviço ou serviços essenciais que a entidade crítica presta.

As entidades críticas devem também designar um agente de ligação para cada infraestrutura crítica que detêm ou exploram, cabendo-lhes, entre outras competências, agilizar os contactos e a articulação com as estruturas locais das forças de segurança territorialmente competentes e com os serviços municipais de proteção civil.

Em caso de incidentes que perturbem significativamente, ou sejam suscetíveis de perturbar, a prestação de serviços essenciais ou o funcionamento das infraestruturas críticas, as entidades críticas devem notificar de imediato o Secretário-Geral do Sistema de Segurança Interna, fornecendo informação detalhada sobre o incidente no prazo máximo de 24 horas e, depois, um relatório pormenorizado no prazo de um mês.

As entidades críticas realizam, pelo menos, um exercício durante a vigência do plano de resiliência aprovado, visando testar a adequação das medidas, procedimentos e ações constantes dos mesmos. Durante o período referido, são também testados de forma obrigatória todos os planos de segurança,

devendo ser envolvidas as forças de segurança e os serviços municipais de proteção civil territorialmente competentes. A sua realização é objeto de comunicação ao Secretário-Geral do Sistema de Segurança Interna, com a antecedência mínima de 20 dias, sendo depois elaborado relatório que é remetido ao mesmo destinatário no prazo máximo de 30 dias.

Além disso, compete às entidades críticas garantir o cumprimento das medidas de segurança constantes dos seus planos de segurança, designadamente através da nomeação de agentes de ligação das infraestruturas críticas, da implementação de medidas técnicas e organizativas e, quando aplicável, da submissão de pedidos de verificação de antecedentes respeitantes ao pessoal que acede a áreas com medidas especiais de segurança.

As entidades críticas devem assegurar a cooperação com as entidades competentes, manter atualizada a informação relevante, cumprir os prazos legais e colaborar nos processos de fiscalização, auditoria ou inspeção que visem verificar a conformidade e a efetiva implementação das medidas adotadas para reforço da sua resiliência.

Forças e serviços de segurança, de emergência e proteção civil

As forças e serviços de segurança, a Autoridade Nacional de Emergência e Proteção Civil e os serviços regionais de Proteção Civil contribuem para a elaboração e sucessivas revisões da avaliação nacional de risco, que é coordenada pelo Secretário-Geral do Sistema de Segurança Interna visando apoiar o processo de identificação das entidades críticas e a adoção das respetivas medidas de resiliência.

Contribuem, também, para o esforço coletivo da avaliação sistemática da natureza e o alcance dos riscos que impendem sobre as entidades críticas, através da identificação e análise de potenciais ameaças, vulnerabilidades e perigos suscetíveis de provocar um incidente, bem como da avaliação da potencial perda ou perturbação da prestação de um serviço essencial.

Integram ainda um grupo de trabalho de cooperação e colaboração institucional, operacional e estratégica, sob a égide do Secretário-Geral do Sistema de Segurança Interna e em articulação com o Conselho Nacional de Planeamento Civil de Emergência, envolvendo as forças e serviços de segurança, os serviços de proteção civil e as autoridades nacionais de cibersegurança, no âmbito e para os efeitos estabelecidos no Decreto-Lei n.º 22/2025, de 19 de março.

A aprovação dos planos de resiliência das entidades críticas carece, entre outros, do parecer das forças de segurança territorialmente competentes, da Autoridade Nacional de Emergência e Proteção Civil ou do serviço regional de proteção civil territorialmente competente, emitido a pedido do Secretário-Geral do Sistema de Segurança Interna, podendo, para o efeito, efetuar visitas técnicas para verificação das medidas previstas nos mesmos.

Cabe à força de segurança territorialmente competente a elaboração de um plano de intervenção para cada infraestrutura crítica situada na sua área de responsabilidade, o qual deve ser comunicado ao Secretário-Geral do Sistema de Segurança Interna. Os respetivos conteúdos são definidos por este, ouvidas as primeiras, com vista à sua uniformidade.

Além disso, podem, no âmbito da elaboração do respetivo plano de intervenção, e após auscultação da entidade crítica, propor ao Secretário-Geral do Sistema de Segurança Interna a implementação de medidas restritivas do espaço aéreo situado por cima das respetivas infraestruturas críticas e área envolvente, que remete a proposta para avaliação da Autoridade Aeronáutica Nacional.

Os planos de intervenção elaborados pelas forças de segurança, e os planos municipais de emergência e proteção civil elaborados pela autoridade de proteção civil territorialmente competente, têm em conta a existência de infraestruturas críticas localizadas nas áreas geográficas da sua competência.

Durante a vigência do plano de resiliência aprovado, é obrigatória a realização de pelo menos um exercício por parte das entidades críticas, devendo ser testados todos os planos de segurança e obrigatoriamente envolvidas as forças de segurança e os serviços municipais de proteção civil territorialmente competentes.

Os agentes de ligação da entidade crítica devem assegurar a ligação com as forças e serviços de segurança e com a Autoridade Nacional de Emergência e Proteção Civil ou os serviços regionais de proteção civil territorialmente competentes para obtenção de informações sobre graus de ameaça, estados de segurança e estados de alerta do sistema de proteção civil.

Compete aos agentes de ligação da infraestrutura crítica assegurar a comunicação local e a articulação com as estruturas locais das forças de segurança territorialmente competentes e com os serviços municipais de proteção civil.

Sem prejuízo da plataforma eletrónica de registo de informação de entidades críticas e infraestruturas críticas, as forças e serviços de segurança devem manter atualizada a informação relativa às infraestruturas críticas existentes nas respetivas áreas de competência territorial, tendo em vista a execução tempestiva dos necessários procedimentos policiais, aquando da declaração de um Estado de Segurança ou na sequência da elevação do grau de ameaça, nos termos e para os efeitos estabelecidos no Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança.

9 – Processo de identificação e designação das entidades críticas

A identificação e designação das entidades críticas decorre de forma transparente, estruturada e fundamentada, envolvendo a participação de diferentes entidades e fases bem definidas, tendo em consideração a avaliação nacional de risco e a presente Estratégia.

O seu processo tem início com a aplicação cumulativa de três critérios fundamentais:

A entidade presta um ou mais serviços essenciais;

A entidade opera e as suas infraestruturas críticas estão localizadas em território nacional; e

A ocorrência de um incidente teria efeitos perturbadores significativos na prestação desses serviços ou noutros serviços essenciais que deles dependam.

Para determinar a importância de um efeito perturbador significativo produzido por um incidente, são considerados os seguintes critérios:

O número de utilizadores que dependem do serviço essencial prestado pela entidade;

O grau em que outros setores e subsectores dependem de determinado serviço essencial;

O possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e sociais, o ambiente, a proteção e segurança públicas ou a saúde da população;

A quota da entidade no mercado do serviço essencial ou serviços essenciais;

A zona geográfica suscetível de ser afetada por um incidente, incluindo um eventual impacto transfronteiriço, tendo em conta a vulnerabilidade associada ao grau de isolamento de determinados tipos de zonas geográficas, como sejam as regiões insulares;

A importância da entidade na manutenção de um nível de serviço essencial suficiente, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço essencial.

Com base nestes critérios, as entidades setoriais submetem ao Conselho Nacional de Planeamento Civil de Emergência uma proposta com a densificação dos critérios de identificação e os limiares a aplicar. Em caso de aprovação, remetem seguidamente ao Conselho Nacional de Planeamento Civil de Emergência uma proposta fundamentada quanto às entidades que devem ser designadas como críticas.

Após avaliação e aprovação das propostas, o Conselho Nacional de Planeamento Civil de Emergência procede à notificação das entidades candidatas, informando-as da sua possível designação como entidades críticas e concedendo-lhes um prazo não inferior a 10 dias para se pronunciarem.

Se a entidade se pronunciar de forma desfavorável, o Conselho Nacional de Planeamento Civil de Emergência remete a pronúncia à respetiva entidade setorial para que esta reanalise e, se necessário, adequa a proposta no prazo de 60 dias.

Concluído este procedimento, o Conselho Nacional de Planeamento Civil de Emergência designa formalmente as entidades críticas e respetivas infraestruturas críticas, num prazo máximo de 30 dias, podendo também designar outras entidades críticas além das propostas pelas entidades setoriais, se possuir indicadores distintos ou se verificar que a entidade a designar está conexas com outras entidades críticas já identificadas.

Após a designação, notifica formalmente a entidade crítica no prazo máximo de 10 dias, informando-a das obrigações a que fica sujeita. Em simultâneo, dá conhecimento da designação ao Secretário-Geral do Sistema de Segurança Interna, à entidade setorial competente, às entidades com competências de regulação ou supervisão que não integrem as entidades setoriais, às autoridades de cibersegurança e aos presidentes de câmara municipal territorialmente competentes.

10 – Apoio às entidades críticas

O apoio às entidades críticas encontra-se estruturado como um instrumento transversal de suporte técnico, institucional e cooperativo, visando a garantia da efetiva implementação das obrigações legais, do reforço da resiliência operacional e da continuidade da prestação dos serviços essenciais.

O apoio assume, desde logo, uma vertente técnica, centrada na difusão de orientações e outros instrumentos de apoio. Esta tarefa é da responsabilidade do Secretário-Geral do Sistema de Segurança Interna que assegura a disponibilização de documentos e diretrizes relacionados com a elaboração e implementação dos planos de resiliência, dos planos de segurança das infraestruturas críticas, dos mecanismos de notificação de incidentes, bem como dos planos de intervenção das forças de segurança e dos exercícios de resiliência. Este apoio não se limita à simples emissão de orientações mas compreende também a monitorização e acompanhamento da sua aplicação pelas entidades críticas, promovendo a uniformização de critérios e a adoção de boas práticas.

Adicionalmente, encontra-se consagrada uma lógica de partilha de informação e cooperação contínua entre os diferentes intervenientes. As entidades competentes, as entidades setoriais e as entidades críticas estão obrigadas a partilhar o acesso às melhores práticas e metodologias disponíveis, à informação sobre novos avanços técnicos relevantes para a resiliência e a indícios relativos a ameaças e riscos. Esta partilha tem por finalidade reforçar a capacidade de adaptação e resposta coordenada face a incidentes com impacto significativo nos serviços essenciais.

Outro aspeto estruturante do apoio reside na preocupação com a previsibilidade e proporcionalidade das exigências, garantindo que o apoio técnico e institucional seja ajustado à capacidade instalada e à dimensão de cada entidade crítica.

Durante o processo de aprovação dos planos de resiliência, o Secretário-Geral do Sistema de Segurança Interna carece dos pareceres técnicos das entidades reguladoras, das forças de segurança territorialmente competentes e da Autoridade Nacional de Emergência e Proteção Civil ou do serviço regional de proteção civil territorialmente competente, podendo ainda solicitar a colaboração de outras entidades públicas com competência em razão da matéria. As entidades referidas podem, com vista à emissão do respetivo parecer, efetuar visitas técnicas à entidade para verificação das medidas previstas nos respetivos planos de resiliência.

Além disso, as entidades críticas beneficiam de apoio durante os processos de planeamento e execução de exercícios para testar a adequação das medidas de resiliência e segurança previstas nos planos, devendo envolver as forças de segurança e os serviços municipais de proteção civil territorialmente competentes. Após a realização de exercícios, é elaborado um relatório técnico, o qual pode incluir recomendações úteis à melhoria contínua da resiliência.

Em matéria de fiscalização, o Secretário-Geral do Sistema de Segurança Interna pode realizar auditorias, inspeções e ações de supervisão remota, mas também pode prestar apoio, emitir instruções e sugerir medidas corretivas sempre que detete falhas na implementação das obrigações legais por parte das entidades críticas. Esta supervisão prudencial assume, assim, um caráter preventivo, pedagógico e corretivo, com o objetivo de promover a conformidade sustentada e não apenas a aplicação sancionatória.

11 – Medidas de apoio às pequenas e médias empresas

Em conformidade com o disposto no anexo da Recomendação 2003/361/CE da Comissão, de 6 de maio, as medidas destinadas a facilitar o cumprimento das obrigações por parte das pequenas e médias empresas (PME) designadas como entidades críticas devem respeitar os princípios da proporcionalidade, exequibilidade e não comprometimento dos objetivos de resiliência. Para o efeito, encontra-se previsto:

Apoio técnico diferenciado e ajustado à escala das PME, através da disponibilização de orientações técnicas, metodologias simplificadas e instrumentos de apoio à elaboração dos planos de resiliência e de segurança, promovidos pelo Secretário-Geral do Sistema de Segurança Interna;

Promoção da cooperação entre entidades públicas e privadas, incluindo a partilha de melhores práticas, informação sobre riscos, ameaças e soluções técnicas adequadas, permitindo às PME aceder ao conhecimento e à experiência acumulada de outras entidades críticas e autoridades competentes;

Medidas específicas, avaliadas casuisticamente, que permitam a adoção gradual e proporcional das obrigações, em particular no que respeita à avaliação de risco, à notificação de incidentes, à realização de exercícios e à verificação de antecedentes de segurança humana, sem prejuízo dos objetivos de proteção e continuidade dos serviços essenciais;

Estabelecimento de canais de comunicação eficazes e acessíveis, que garantam que as PME designadas como entidades críticas tenham contacto direto e apoio das entidades competentes e setoriais, facilitando o esclarecimento de dúvidas e a execução atempada das obrigações legais;

Possibilidade de recurso a instrumentos partilhados ou serviços comuns, quando adequado, no que respeita à formação de recursos humanos, testes de resiliência ou plataformas tecnológicas, para reduzir encargos excessivos e garantir a conformidade.

12 – Avaliação e revisão

A natureza e o contexto das ameaças e riscos à resiliência das entidades críticas exigem que a Estratégia seja objeto de avaliação regular e periódica, quer no que diz respeito ao grau de implementação do seu plano de ação quer no que concerne à verificação da adequação dos objetivos estratégicos à evolução das circunstâncias.

A avaliação do grau de implementação das medidas do plano de ação é efetuada com periodicidade semestral, pelo Secretário-Geral do Sistema de Segurança Interna, em colaboração com o Conselho Nacional de Planeamento Civil de Emergência, devendo o 1.º ciclo de avaliação ser efetuado em dezembro de 2026. O conteúdo dos relatórios é aferido com vista à eventual classificação de segurança da informação.

Sem prejuízo de processos extraordinários sempre que as circunstâncias o exijam, a revisão da estratégia deve ocorrer no prazo máximo de quatro anos.

ANEXO
Plano de Ação

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 1	Medida n.º 1 — Atualizar a avaliação nacional de risco, sempre que necessário, que visa apoiar o processo de identificação das entidades críticas e a adoção de medidas de resiliência.	Coordenação da atualização a cargo do SGSSI em colaboração com o CNPCE Presidência do Conselho de Ministros (aprovação)	Forças e serviços de segurança, ANEPC, serviços regionais de proteção civil, autoridades competentes em matéria de cibersegurança, entidades setoriais, entidades com competências de regulação ou supervisão, e outras entidades relevantes.	Janeiro de 2026	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 1	Medida n.º 2 — Propor para aprovação ao CNPCE, através das entidades setoriais, a densificação dos critérios de identificação das entidades críticas, bem como as entidades e respetivas infraestruturas suscetíveis de serem classificadas como críticas, no respetivo setor ou subsetor.	Entidades setoriais	CNPCE	Janeiro de 2026	Julho de 2026
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 1	Medida n.º 3 — Avaliar, com as entidades setoriais, a inclusão de novos serviços essenciais, setores ou subsetores, bem como a eventual eliminação de serviços essenciais listados no anexo ao Decreto-Lei n.º 22/2025, de 19 de março, atentas as lições aprendidas e os novos conhecimentos relacionados com as respetivas dependências.	CNPCE	Entidades setoriais	Julho de 2027	Dezembro de 2028
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 1	Medida n.º 4 — Aprovar os critérios e metodologia aplicáveis para o efeito, e identificar e designar as entidades críticas e respetivas infraestruturas críticas, através do CNPCE.	CNPCE	Entidades setoriais e outras entidades que considere relevantes	Janeiro de 2026	Julho de 2026
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 1	Medida n.º 5 — Elaborar um referencial de boas práticas na metodologia de identificação de entidades críticas, propondo, caso se justifique, alterações ao Decreto-Lei n.º 22/2025, de 19 de março.	CNPCE	Entidades setoriais e outras entidades que considere relevantes	Janeiro de 2026	Dezembro de 2028

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 2	Medida n.º 6 — Implementar processos contínuos e sistemáticos de avaliação, análise e mitigação dos riscos, em coordenação com as entidades competentes, considerando dependências e interdependências setoriais, intersetoriais e transfronteiriças, visando uma resposta preventiva e eficaz face a ameaças e riscos que possam comprometer a prestação de serviços essenciais.	SGSSI, entidades nacionais e internacionais competentes	CNPCE, ANEPC, entidades setoriais, entidades críticas, forças e serviços de segurança, entidades com competências de regulação ou supervisão e outras entidades relevantes em razão da matéria.	Janeiro de 2026	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 2	Medida n.º 7 — Efetuar a avaliação de risco das entidades críticas, a cargo das próprias, no prazo de nove meses a contar da data da receção da notificação da sua designação, que inclui obrigatoriamente a avaliação dos riscos específicos relativos a cada uma das suas infraestruturas críticas.	Entidades críticas	Outras entidades relevantes	Após receção da notificação da sua designação como entidade crítica.	Nove meses a contar da data da receção da notificação da sua designação como entidade crítica.
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 2	Medida n.º 8 — Promover, diretamente ou através dos demais órgãos e entidades que integram o Sistema de Segurança Interna, a troca de informações pertinentes relativas às ameaças e riscos para as entidades críticas, sem prejuízo dos regimes legais aplicáveis à proteção e salvaguarda da informação classificada, e aos segredos de Estado e de justiça.	SGSSI	Entidades que integram o SSI e entidades críticas	Janeiro de 2026	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 2	Medida n.º 9 — Desenvolver a taxonomia comum para a classificação dos riscos que impendem sobre as entidades e infraestruturas críticas, através do SGSSI.	SGSSI	Entidades que considere relevantes para o efeito	Janeiro de 2026	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 10 — Submeter à aprovação do SGSSI, após notificação da designação enquanto entidade crítica, o respetivo plano de resiliência, que deve anexar e englobar um plano de segurança por cada infraestrutura crítica.	Entidades críticas	SGSSI	Após receção da notificação da sua designação como entidade crítica.	10 meses a contar da data da receção da notificação da sua designação como entidade crítica.

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 11 — Elaborar pareceres emitidos a pedido do SGSSI com vista à aprovação dos planos de resiliência das entidades críticas.	Entidade reguladora do setor de atividade, forças de segurança territorialmente competentes, ANEPC ou serviço regional de proteção civil territorialmente competente, e outras entidades públicas com competência em razão da matéria (e. g. entidades setoriais).	SGSSI	Prazos constantes do Decreto-Lei n.º 22/2025, de 19 de março.	Prazos constantes do Decreto-Lei n.º 22/2025, de 19 de março.
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 12 — Aprovar os planos de resiliência das entidades críticas.	SGSSI	Com o parecer da entidade reguladora do setor de atividade em causa, forças de segurança territorialmente competentes, ANEPC ou serviço regional de proteção civil territorialmente competente e outras entidades públicas com competência em razão da matéria.	Prazos constantes do Decreto-Lei n.º 22/2025, de 19 de março.	Prazos constantes do Decreto-Lei n.º 22/2025, de 19 de março.
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 13 — Elaborar e comunicar ao SGSSI, através das forças de segurança territorialmente competentes, um plano de intervenção para cada infraestrutura crítica situada na sua área de responsabilidade geográfica.	Forças de segurança territorialmente competentes	SGSSI e forças de segurança	N/A	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 14 — Notificar de imediato o SGSSI e acionar os respetivos planos, através das entidades críticas, perante incidentes que perturbem significativamente, ou sejam suscetíveis de perturbar, a prestação de serviços essenciais ou o funcionamento das infraestruturas críticas que os asseguram.	Entidades críticas	SGSSI e órgãos de polícia criminal competentes sempre que existam suspeitas da prática de crime.	Após receção da notificação da sua designação como entidade crítica.	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 15 — Coordenar e comunicar a verificação de antecedentes de segurança humana e a sua implementação, através do SGSSI e em articulação com as entidades críticas.	SGSSI	Autoridades nacionais e internacionais competentes, e entidades críticas.	N/A	Dezembro de 2029

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 16 — Criar uma unidade orgânica específica em matéria de resiliência e entidades críticas, no âmbito do SSI e na dependência e coordenação do SGSSI.	SGSSI	SGSSI	Janeiro de 2026	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 17 — Garantir que as informações relacionadas com a designação e reforço de resiliência das entidades críticas e respetivas infraestruturas críticas são objeto de avaliação com vista à eventual classificação de segurança, bem como que o tratamento da informação classificada respeita a legislação e normas de segurança aplicáveis à proteção e salvaguarda da informação classificada.	SGSSI, CNCPE, GNS	Forças e serviços de segurança, CNCS, entidades setoriais e entidades críticas.	Julho de 2026	Dezembro de 2029
I — Reforço da Resiliência das Entidades Críticas	Objetivo Estratégico n.º 3	Medida n.º 18 — Assegurar que o tratamento da informação classificada, nomeadamente a sua produção, utilização, partilha, arquivo ou armazenamento por parte das entidades críticas, respeita o regime da informação classificada e em particular os requisitos das áreas de segurança da informação e dos sistemas de informação e comunicação.	Entidades críticas	SGSSI, GNS	Julho de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 4	Medida n.º 19 — Assegurar a representação nacional e o ponto de contacto único com a Comissão Europeia em matéria de resiliência das entidades críticas, através do SGSSI, garantindo a representação de Portugal no Grupo para a Resiliência das Entidades Críticas que assiste a Comissão Europeia no quadro e para os efeitos da Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022.	SGSSI	Entidades que considere relevantes para o efeito	Janeiro de 2026	Dezembro de 2029

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 4	Medida n.º 20 — Promover a partilha de informação no âmbito da identificação de entidades críticas com os demais Estados-Membros da União Europeia e estimular a assinatura de protocolos de colaboração.	CNPCE	Entidades que considere relevantes para o efeito	Janeiro de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 4	Medida n.º 21 — Garantir a articulação com as entidades congéneres de outros Estados-Membros da União Europeia, ou de países terceiros, em matéria de resiliência das entidades críticas, através do SGSSI.	SGSSI	Entidades que considere relevantes para o efeito	Janeiro de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 4	Medida n.º 22 — Assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da resiliência das entidades críticas, através do SGSSI.	SGSSI	Intervenientes e responsáveis nacionais na área da resiliência das entidades críticas.	Janeiro de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 23 — Difundir orientações técnicas e outros instrumentos de apoio à elaboração dos planos de resiliência das entidades críticas, dos planos de segurança das infraestruturas críticas, dos mecanismos de notificação de incidentes, dos planos de intervenção das forças de segurança, e de exercícios, apoiando a sua implementação e monitorizando a sua execução, através do SGSSI.	SGSSI	Entidades que considere relevantes para o efeito	Janeiro de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 24 — Assegurar as competências de fiscalização e de aplicação de sanções previstas no Decreto-Lei n.º 22/2025, de 19 de março.	SGSSI	Autoridades policiais e outras autoridades ou serviços públicos cuja colaboração solicite.	Prazos constantes do Decreto-Lei n.º 22/2025, de 19 de março.	Prazos constantes do Decreto-Lei n.º 22/2025, de 19 de março.
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 25 — Partilhar o acesso às melhores práticas e metodologias disponíveis, assim como, sempre que possível, à informação sobre os novos avanços técnicos relacionados com a resiliência das entidades críticas, incorporando boas práticas e lições aprendidas no plano nacional e internacional.	SGSSI, CNPCE, entidades setoriais	Entidades críticas	Janeiro de 2026	Dezembro de 2029

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 26 — Cooperar com as autoridades competentes em matéria de cibersegurança na partilha de informação sobre riscos de cibersegurança, ciberameaças, ciberincidentes, bem como riscos, ameaças e incidentes não relacionados com cibersegurança, e ainda no exercício de funções de supervisão na esfera do SGSSI.	SGSSI	Autoridades competentes em matéria de cibersegurança (CNCS) e Serviço de Informações de Segurança	Janeiro de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 27 — Desenvolver uma plataforma digital comum de notificação de incidentes relativos à resiliência das entidades críticas e ao Regime Jurídico da Cibersegurança, envolvendo o SGSSI e as autoridades competentes em matéria de cibersegurança.	SGSSI e autoridades competentes em matéria de cibersegurança (CNCS)	Outras entidades consideradas pertinentes na sua esfera de cooperação e colaboração.	Janeiro de 2026	Dezembro de 2026
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 28 — Designar um agente de ligação da entidade crítica responsável pela articulação institucional, em matéria de resiliência, e um agente de ligação para cada infraestrutura crítica que detém ou explora.	Entidades críticas	SGSSI, CNPCE e respetiva entidade setorial	Após receção da notificação da sua designação como entidade crítica.	No prazo de 10 dias após a designação da entidade como entidade crítica.
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 29 — Assegurar a coordenação com o SGSSI, as forças e serviços de segurança, a Autoridade Nacional de Emergência e Proteção Civil ou os serviços regionais de proteção civil territorialmente competentes, para obtenção de informações sobre graus de ameaça, estados de segurança e estados de alerta do sistema de proteção civil, através dos agentes de ligação das entidades críticas.	Entidades críticas	SGSSI, forças e serviços de segurança, ANEPC ou serviços regionais de proteção civil territorialmente competentes.	Após receção da notificação da sua designação como entidade crítica.	Dezembro de 2029

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 30 — Assegurar e manter atualizada a plataforma eletrónica de registo das entidades e infraestruturas críticas que compreende, entre outras informações, a sua catalogação; o elenco de contactos de cooperação institucional e de coordenação operacional; a seriação dos planos de resiliência, segurança e intervenção; a gestão de acidentes e incidentes relevantes, e demais dados que permitam planear e priorizar as medidas de reforço da resiliência.	SGSSI	CNPCE, forças de segurança, Serviço de Informações de Segurança, ANEPC, serviços regionais de proteção civil, CNCS, entidades setoriais e outras entidades que se afigurem relevantes.	Janeiro de 2026	Dezembro de 2029
II — Cooperação, Supervisão e Coordenação Institucional	Objetivo Estratégico n.º 5	Medida n.º 31 — Constituir um grupo de trabalho de cooperação e colaboração institucional e operacional, sob a égide do SGSSI, envolvendo as forças e serviços de segurança, de emergência e proteção civil, e as autoridades competentes de cibersegurança, no âmbito e para os efeitos estabelecidos no Decreto-Lei n.º 22/2025, de 19 de março.	SGSSI	Forças e serviços de segurança, ANEPC e CNCS	Janeiro de 2026	Dezembro de 2029
III — Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 6	Medida n.º 32 — Realizar pelo menos um exercício durante a vigência do plano de resiliência aprovado, através das entidades críticas, visando testar a adequação das medidas, procedimentos e ações constantes dos mesmos.	Entidades críticas	Na sua esfera de responsabilidade e cooperação institucional.	Após aprovação do plano de resiliência pelo SGSSI.	Durante a vigência do plano de resiliência.
III — Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 6	Medida n.º 33 — Testar, durante a vigência do plano de resiliência aprovado, todos os planos de segurança das infraestruturas críticas que dele fazem parte, devendo ser envolvidas as forças de segurança e os serviços municipais de proteção civil territorialmente competentes.	Entidades críticas	Forças de segurança e serviços municipais de proteção civil territorialmente competentes.	Após aprovação do plano de resiliência pelo SGSSI.	Durante a vigência do plano de resiliência.
III — Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 6	Medida n.º 34 — Promover a realização de pelo menos um exercício, ao nível e através das entidades setoriais, envolvendo as entidades críticas, o SGSSI, o CNPCE e outras entidades relevantes em razão da matéria.	Entidade setoriais	SGSSI, CNPCE, entidades críticas e outras entidades relevantes em razão da matéria.	Janeiro de 2027	Dezembro de 2029

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 6	Medida n.º 35 – Promover a realização de pelo menos um exercício transversal, através do SGSSI e em articulação com o CNPCE e as entidades setoriais, podendo envolver entidades críticas e outras entidades relevantes em razão da matéria, assim como, quando pertinente, entidades de outros Estados-Membros da UE.	SGSSI	CNPCE, entidades setoriais e outras entidades relevantes em razão da matéria.	Janeiro de 2027	Dezembro de 2029
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 6	Medida n.º 36 – Formar e treinar os recursos humanos das entidades críticas, na esfera de responsabilidade das próprias, na implementação das medidas previstas ou implementadas no respetivo plano de resiliência.	Entidades críticas	Entidades críticas e outras entidades na sua esfera de cooperação e colaboração.	Após aprovação do plano de resiliência pelo SGSSI.	Dezembro de 2029
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 6	Medida n.º 37 – Desenvolver estratégias eficazes de comunicação e alerta dirigidas às entidades críticas e aos utilizadores dos serviços essenciais.	SGSSI, ANEPC ou serviços regionais de proteção civil	Entidades críticas e utilizadores dos serviços essenciais	Janeiro de 2026	Dezembro de 2029
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 7	Medida n.º 38 – Fomentar uma comunidade de conhecimento e uma cultura nacional de resiliência.	SGSSI, CNPCE, entidades setoriais	Entidades críticas, forças e serviços de segurança, ANEPC, serviços regionais de proteção civil, outras entidades relevantes em razão da matéria e a sociedade civil.	Janeiro de 2026	Dezembro de 2029
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 7	Medida n.º 39 – Apoiar e promover o potencial nacional de investigação, desenvolvimento e inovação no âmbito da identificação e resiliência de entidades críticas, envolvendo o setor público e privado e a academia, através do SGSSI e do CNPCE.	SGSSI, CNPCE	Setor público e privado e a academia	Janeiro de 2026	Dezembro de 2029
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 7	Medida n.º 40 – Desenvolver estudos e formular as propostas consideradas pertinentes para o desenvolvimento e aperfeiçoamento do quadro de governação da resiliência das entidades críticas, no seu âmbito jurídico, político, estratégico e operacional, através do SGSSI e em articulação com o CNPCE.	SGSSI, CNPCE	Outras entidades relevantes em razão da matéria	Janeiro de 2027	Dezembro de 2029

Eixo de intervenção	Objetivos estratégicos	Ações e medidas	Entidade responsável	Entidades envolvidas	Início de implementação	Prazo de implementação
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 7	Medida n.º 41 – Implementar um processo sistemático de recolha e partilha de boas práticas e lições aprendidas nos vários domínios da resiliência, incluindo riscos e ameaças de natureza setorial ou transversal, complementado com sessões de sensibilização dirigidas às entidades críticas.	SGSSI, CNPCE, forças e serviços de segurança, ANEPC, serviços regionais de proteção civil, entidades setoriais, entidades com competências de regulação ou supervisão, autoridades competentes em matéria de cibersegurança.	Entidades críticas	Janeiro de 2026	Dezembro de 2029
III – Investigação, Formação, Comunicação e Cultura de Resiliência	Objetivo Estratégico n.º 7	Medida n.º 42 – Promover ações de formação no âmbito da legislação e normas de segurança aplicáveis à proteção e salvaguarda da informação classificada.	GNS	SGSSI, CNPCE, entidades críticas e outras entidades relevantes em razão da matéria.	Janeiro de 2028	Dezembro de 2029

Siglas:

ANEPC – Autoridade Nacional de Emergência e Proteção Civil.

CNCS – Centro Nacional de Cibersegurança.

CNPCE – Conselho Nacional de Planeamento Civil de Emergência.

GNS – Gabinete Nacional de Segurança.

SGSSI – Secretário-Geral do Sistema de Segurança Interna.

119948664