Sete Desafios para a Resiliência das Entidades Críticas: o Contributo do Serviço de Informações de Segurança

Manuel Gonçalves*
Serviço de Informações de Segurança.

Resumo

A conclusão do processo de designação das infraestruturas críticas nacionais, a transposição da Diretiva Europeia de Resiliência de Entidades Críticas, a identificação das novas Entidades Críticas e a elaboração da avaliação nacional de riscos e da estratégia nacional para a resiliência de entidades críticas, num espaço temporalmente curto, são tarefas de monta a que Portugal deve dar resposta para ter serviços essenciais mais seguros, numa conjuntura internacional crescentemente adversa. Subjacente à Diretiva e aos desafios que comporta, está uma visão holística da segurança que o Serviço de Informações de Segurança detém sobre estas matérias e através da qual já contribui para o cumprimento de várias obrigações contempladas na Diretiva.

Palavras-chave: Infraestruturas Críticas; Entidades Críticas; Segurança; Desafios; Avaliação de Riscos; Estratégia; Avaliação das Ameaças.

Abstract

Seven challenges to the resilience of critical entities: the role of the Portuguese Security Intelligence Service

The completion of the process of designation of national critical infrastructures, the transposition of the European Directive on the Resilience of Critical Entities, the identification of the new Critical Entities and the production of the national risk assessment and the national strategy for the resilience of critical entities, in a short period of time, are major tasks that Portugal must answer in order to have safer essential services in an increasingly adverse international situation. Underlying the Directive and the challenges it entails is a holistic view of security that the Portuguese Security Intelligence Service holds on these matters and under which it already contributes to the fulfilment of several obligations set out in the Directive.

Keywords: *Critical infrastructure; Critical entities; Security; Challenges; Risk Assessment; Strategy; Threat Assessment.*

Artigo recebido: 30.10.2024
Aprovado: 27.11.2024
https://doi.org/10.47906/ND2024.169.02

* O autor é o Coordenador do Programa Krítica, programa de sensibilização do SIS, que visa contribuir para a melhoria da proteção das infraestruturas críticas.

Introdução

A recente Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro, relativa à resiliência de entidades críticas (Diretiva REC), cuja transposição para o ordenamento jurídico interno deveria ter sido realizada até 17 de outubro último, consagra uma abordagem holística à segurança das Infraestruturas Críticas (IC). Por um lado, porque integra a "proteção" no conceito mais amplo de resiliência, o qual abarca realidades que são, igualmente, essenciais ao normal funcionamento das IC.

Procura-se, assim, garantir as capacidades de proteção, resposta, resistência, atenuação, absorção, adaptação e recuperação de incidentes, isto é, eventos que "perturbem ou tenham potencial para perturbar significativamente a prestação de um serviço essencial, inclusive quando afetar os sistemas nacionais que salvaguardam o Estado de direito" (art.º 2.º, n.º 3, da Diretiva REC).

Por outro lado, ao criar o conceito de "Entidades Críticas" (EC), a Diretiva REC põe o foco na necessidade de manutenção do serviço essencial prestado pela entidade em causa. Com efeito, a avaliação da Diretiva 2008/114/CE do Conselho de 8 de dezembro, relativa à identificação e designação das infraestruturas críticas (Diretiva DIC), realizada em 2019, concluiu que, "devido à natureza cada vez mais interligada e transfronteiriça das operações que utilizam infraestruturas críticas, as medidas de proteção relativas apenas a ativos individuais são insuficientes para evitar a ocorrência de todas as perturbações".

Esta nova abordagem traz novos desafios que acrescem aos que já decorriam da legislação anterior (e ainda em vigor) relativamente à proteção de IC, alguns inerentes à própria natureza das IC e das EC, outros decorrentes da opção do legislador nacional de, só em 2022, ter optado por alargar a identificação de IC a mais dez setores, em vez dos dois a que a anterior Diretiva de Proteção de IC obrigava.

Com efeito, recorde-se que a Diretiva DIC, constituiu os Estados-Membros na obrigação de identificarem IC nos setores dos Transportes e da Energia, muito embora, à luz do princípio da subsidiariedade, cada Estado fosse (e seja) livre de determinar outros setores onde entenda que devem ser identificadas IC.

A maioria dos nossos parceiros europeus optou por esta última solução, alargando a vários outros setores a obrigação de identificação de IC. O legislador nacional, só em 2022, pelo Decreto-Lei n.º 20/2022, de 28 janeiro (DL 20/2022), alargou o âmbito da identificação de IC para os seguintes setores (para além dos já referidos Transportes e Energia): Comunicações; Infraestruturas digitais e prestadores de serviços digitais; Abastecimento público de água e tratamento de resíduos; Alimentação; Saúde; Indústria; Serviços financeiros; Órgãos de Soberania e Governação; Segurança; e Defesa.

Sete Desafios para a Resiliência das Entidades Críticas

O enquadramento *supra* descrito traduz-se numa multiplicidade de desafios, por vezes sobrepostos, que têm, impreterivelmente, de ser abordados e superados, não apenas para que o Estado português cumpra com a obrigação formal de respeito pela legislação europeia, mas, sobretudo, para que Portugal consiga garantir o normal funcionamento dos seus serviços essenciais, numa conjuntura cada vez mais instável e de conflitualidade internacional crescente.
Sem prejuízo de outros que possam ser, legitimamente, considerados, elencam-se *infra* os sete desafios que, numa perspetiva estratégica da segurança, se afiguram como os mais prementes.

Primeiro Desafio: transposição da Diretiva REC, conciliando-a com o trabalho já efetuado e em curso no âmbito da proteção de infraestruturas críticas

Um primeiro desafio consiste na transposição da Diretiva REC para o ordenamento jurídico interno, conciliando-a com o trabalho que está a ser realizado na identificação e designação das IC, não apenas nos novos setores introduzidos pelo DL 20/2022 mas, também, nos setores da Energia e Transportes, nos quais ocorreram mudanças nas listas de infraestruturas que devem ser consideradas críticas.
Note-se que, apesar da identificação de uma infraestrutura como crítica ter um carácter estável, essa identificação não é imune a alterações. Com efeito, uma IC pode deixar de o ser devido à criação de redundâncias, com a consequente perda de criticidade, ou por ser desativada, como aconteceu com a Central Termoelétrica de Sines (*Observador*, 2021).
Por outro lado, a eliminação de redundâncias (ou estas serem insuficientes para garantir a função da IC em caso de perda ou perturbação), a redefinição do funcionamento dos operadores setoriais (que serão as novas EC) e a redefinição do funcionamento dos setores de atividade por parte do poder político, ou pelo regulador setorial, podem originar a necessidade de identificação de novas IC, mesmo em setores onde a identificação já tinha sido realizada.
Assim, será fundamental que todo o trabalho efetuado com vista à identificação de IC e à validação dos planos de segurança das IC não seja posto em causa pela transposição da nova Diretiva REC. É que, apesar de esta Diretiva manter o conceito de IC (embora, e bem, alargando o seu escopo para os ativos que sejam necessários para a prestação de um ou mais serviços essenciais[1]), ela deixou de criar obrigações no contexto das IC, transferindo-as para as EC.

1 Até à nova Diretiva, uma IC era definida como "a componente, sistema ou parte deste que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o

Acresce que a Diretiva REC revoga, expressamente, a anterior Diretiva DIC, mas sem estabelecer qualquer ligação com as obrigações anteriormente criadas por esta, concretamente no que respeita ao processo de identificação de IC. De certa forma, é como se o legislador entendesse que o processo de identificação de IC já estivesse concluído e fosse imutável e que, como se revelou insuficiente, também já não seria preciso abordar mais este tema.

Porém, tal entendimento, caso venha a ser o seguido na transposição da nova Diretiva REC, não parece ser o mais correto, por cinco razões.

A primeira razão é que a própria Diretiva REC refere, no parágrafo 13 do seu Preâmbulo, que "cada Estado-Membro deverá dispor de uma estratégia para reforçar a resiliência das entidades críticas" e que "Por razões de coerência e eficiência, a estratégia deverá ser concebida de modo a **integrar sem descontinuidades as políticas existentes**, com base, sempre que possível, nas estratégias nacionais e setoriais, planos ou documentos similares pertinentes existentes" (negrito nosso). Ou seja, dá espaço e incentiva os Estados-Membros a manterem e aprofundarem todo o trabalho já realizado e que contribui para o objetivo de conseguir tornar as suas EC resilientes.

A segunda razão é que, como já foi supra referido, a identificação de IC é uma realidade que não é estática, mas sim dinâmica, e que, naturalmente, continuará a ocorrer ao longo do tempo em virtude das várias mudanças que cada setor poderá sofrer no futuro. E têm de ser os Estados a identificar quais são as IC presentes nos seus territórios, tanto mais que tal identificação implica um dever de proteção acrescida que é partilhado pelo respetivo operador (a EC) e pelo Estado, enquanto detentor e garante das funções soberanas de segurança interna e de defesa.

Acresce que, e esta é a terceira razão, especificamente no caso português, o processo de identificação de IC está longe de estar concluído, pelo que deverá ser mantido o esforço com vista à sua conclusão.

A quarta razão prende-se com um argumento lógico: quando falamos de uma EC referimo-nos a algo imaterial. A materialização da EC é feita pelas suas instalações, pelos seus ativos, pelos seus equipamentos, pelas suas redes e/ou pelos seus sistemas.

bem-estar económico ou social, e cuja perturbação do funcionamento ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções". A nova definição introduzida pela Diretiva REC alarga este conceito para "**um ativo**, uma instalação, um equipamento, uma rede ou um sistema, no seu todo ou uma parte de um ativo, uma instalação, um equipamento, uma rede ou um sistema, que seja necessário para a prestação de um serviço essencial" (negrito nosso), sendo serviço essencial definido como "um serviço que é indispensável à manutenção de funções societais ou atividades económicas vitais, da saúde e segurança pública ou do ambiente". Daqui decorre que uma IC até poderá ser algo que não tenha necessariamente sido construído pelo Homem, sem prejuízo de ações humanas que incidam sobre ela com vista à manutenção da sua funcionalidade como será, por exemplo uma barra de um porto que seja uma IC ou mesmo um aquífero subterrâneo essencial ao abastecimento das populações ou outros serviços essenciais.

Isto é, pelo que pode, eventualmente, ser identificado como IC e pelo que pode (e deve) ser objeto de proteção acrescida para assegurar a manutenção do serviço ou serviços essenciais que presta. Mas, como não é possível proteger tudo de uma entidade e nem tudo é crítico, mesmo numa entidade que seja crítica, a identificação de IC permite definir prioridades na alocação de recursos (que não são ilimitados) na proteção das EC, concretamente nos seus ativos que são críticos.
A quinta e última razão, e que deriva da razão anterior, consiste na necessidade de as Forças de Segurança competentes precisarem de saber, territorialmente o que existe de crítico nas suas áreas de competência e que deve ser, prioritariamente, protegido por elas. Aliás, como decorre do art.º 16.º do DL 20/2022, "o plano de segurança da infraestrutura crítica articula-se com o plano de proteção e intervenção elaborado pelas forças de segurança territorialmente competentes, com o plano de emergência de proteção civil elaborado pela autoridade de proteção civil territorialmente competente e, quando apropriado, com instrumentos setoriais específicos".

Segundo Desafio: concluir a identificação e designação das IC nos novos setores designados pelo DL 20/2022

O alargamento da obrigatoriedade de identificação e designação de IC, para além da Energia e dos Transportes, determinado pelo DL 20/2022, implica um processo moroso que começa com a designação das Entidades setoriais e da criação de grupos de trabalho setoriais coordenados por estas. Este processo inclui não só a designação das IC em cada um dos novos setores visados[2] mas, também, a aprovação dos planos de segurança de cada IC, por parte do Secretário-Geral do Sistema de Segurança Interna. Pelo meio, é necessário que sejam definidos os critérios setoriais que permitam levar à identificação e designação de IC, de acordo com os critérios gerais definidos no art.º 8.º do DL 20/2022, tendo em conta uma apreciação qualitativa das consequências provocadas pela inoperacionalidade de cada infraestrutura, nomeadamente, e numa primeira fase:

a) O impacto económico, estimado em termos de importância dos prejuízos económicos e da degradação de bens ou serviços, incluindo também os potenciais efeitos ambientais;
b) O impacto na sociedade, avaliado em termos de impacto na soberania nacional, na confiança das populações e na perturbação da vida quotidiana, incluindo a perda de serviços essenciais;

2 Os já referidos: Comunicações; Infraestruturas digitais e prestadores de serviços digitais; Abastecimento público de água e tratamento de resíduos; Alimentação; Saúde; Indústria; Serviços financeiros; Órgãos de Soberania e Governação; Segurança; e Defesa.

c) A possibilidade de ocorrência de acidentes, avaliada em termos de número potencial de feridos ou vítimas mortais.

A estes acrescem ainda, num segundo momento, os seguintes critérios:

a) O tipo de bens produzidos ou serviços prestados pela IC;
b) As alternativas disponíveis no fornecimento dos bens produzidos ou serviços prestados pela IC;
c) A população e área geográfica afetada por uma eventual perturbação do funcionamento ou destruição da IC;
d) A duração de uma eventual perturbação do funcionamento da IC e o tempo previsível para a sua recuperação.

No momento atual, sem nos referirmos, expressamente, a nenhum setor em particular, sabe-se que há setores que já estão muito avançados nos seus trabalhos e que já terão uma lista, necessariamente, provisória e informal, de possíveis IC, enquanto existem outros onde ainda não foi realizado qualquer trabalho neste domínio.
Embora se admita que poderá haver algum compasso de espera para se perceber como será feita a transposição da Diretiva REC para o ordenamento jurídico interno e como essa transposição deverá ser compaginada com o trabalho realizado ou a ser realizado, a realidade é que, face aos argumentos expostos *supra* a propósito do primeiro desafio, justifica-se a continuação e a conclusão, tão rapidamente quanto possível, do processo de identificação e designação de IC nos novos setores referidos pelo DL 20/2022.
Enquanto estes trabalhos não estiverem concluídos, não só o nosso país continuará atrasado neste domínio face à generalidade dos seus parceiros europeus, a começar pelos nossos vizinhos mais próximos, como também, e mais importante, não terá as suas EC e os serviços essenciais que prestam tão seguros como poderiam e deveriam estar.

Terceiro Desafio: identificar as Entidades Críticas nacionais

O art.º 2.º n.º 1 da Diretiva REC define uma EC como "uma entidade pública ou privada que tenha sido identificada por um Estado-Membro, nos termos do artigo 6.º, como pertencente a uma das categorias estabelecidas na terceira coluna do quadro constante do anexo".
Descodificando o hermetismo desta redação, uma EC é uma entidade que um Estado-Membro considera que:

a) Presta um ou mais serviços essenciais;
b) Opera e as suas IC estão localizadas no território deste Estado-Membro. Este critério implica que uma EC tenha de ter pelo menos uma IC e que esta se localize no território do Estado-Membro que identifica a EC. Tal obrigatoriedade de cumulação de critérios poderá suscitar dificuldades na identificação de uma EC, já que é concebível a existência de EC que, pela sua natureza ou modelo de funcionamento, possam assegurar serviços essenciais a um Estado-Membro sem terem IC no território deste Estado-Membro ou mesmo sem quaisquer IC em qualquer território. Imagine-se, por exemplo, uma companhia aérea de transporte de passageiros e de carga que seja considerada essencial a um Estado-Membro, mas que as IC que utiliza ou de que depende sejam detidas por outras entidades, como por exemplo os aeroportos em que aterra e de onde descola e onde reabastece ou a navegação aérea de que depende para voar;
c) Um incidente teria efeitos perturbadores significativos (nos termos do artigo 7.º, n.º 1)[3] sobre a prestação pela entidade de um ou mais serviços essenciais ou sobre a prestação de outros serviços essenciais nos setores estabelecidos no anexo que dependam desse serviço essencial ou desses serviços essenciais[4].

O art.º 6.º n.º 1 da Diretiva REC estabelece que, até 17 de julho de 2026, cada Estado-Membro identifica as EC para os setores e subsetores estabelecidos no anexo. Dada a realidade *supra* descrita sobre o processo de identificação de IC, admite-se que, no quadro atual, existam dificuldades significativas para o cumprimento desta obrigação, a qual é tanto mais exigente porquanto a mesma norma também determina que, ao identificar as suas EC, o Estado-Membro deve ter em conta os resultados da avaliação dos riscos do Estado-Membro e a sua estratégia de reforço da resiliência das EC, realidades que são outros dois desafios relevantes *infra* abordados.

3 A determinação do efeito perturbador é feita de acordo com os seguintes critérios: O número de utilizadores que dependem do serviço essencial prestado pela entidade em questão; O grau em que outros setores e subsetores estabelecidos no anexo dependem do serviço essencial em questão; O possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais, o ambiente, a proteção e segurança públicas ou a saúde da população; A quota de mercado da entidade no mercado do serviço essencial ou serviços essenciais em questão; 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, as regiões remotas ou as zonas montanhosas; 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.

4 Os setores estabelecidos no anexo da Diretiva REC são os seguintes: Energia; Transportes; Setor bancário; Infraestruturas do mercado financeiro; Saúde; Água potável; Águas residuais; Infraestruturas digitais; Administração pública; Espaço; e Produção, transformação e distribuição de produtos alimentares. Alguns destes setores incluem ainda vários subsetores e em todos eles são designadas as categorias de entidades onde deve ser feita a identificação das EC.

Quarto Desafio: articular a Diretiva REC com 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 na União (Diretiva NIS2), na sua transposição para o ordenamento jurídico interno

Este desafio implica a articulação e a complementaridade entre a segurança física e a cibersegurança, realidades cujos normativos têm, erradamente, evoluído à revelia uma da outra. É disso exemplo cabal a Diretiva (EU) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e informação de toda a União (Diretiva NIS) que, apesar de ter implicações diretas na proteção de infraestruturas críticas, dispõe no seu art.º 1.º n.º 4 que "é aplicável sem prejuízo da Diretiva 2008/114/CE do Conselho", sendo esta a única referência direta ou indireta que é feita a esta diretiva.
Todavia, a Diretiva REC estabelece, e bem, uma articulação e uma visão de complementaridade entre as duas Diretivas. Por curiosidade, refira-se que na Diretiva REC existem trinta referências à Diretiva NIS2. No entanto, na prática, tal articulação e complementaridade implicam primeiro a superação dos vários desafios referidos neste artigo, já que só depois de feito o "trabalho de casa" será possível a articulação com as autoridades competentes referidas na Diretiva NIS2. Para além, claro, do próprio "trabalho de casa" que deve ser realizado pelos Estados-Membros e pelas várias entidades para cumprir o disposto na Diretiva NIS2.
São exemplos da lógica de articulação e complementaridade entre as duas Diretivas, bem como das dificuldades para a sua implementação efetiva, as seguintes normas:

a) O art.º 6.º, n.º 4 da Diretiva REC, que refere que "Os Estados-Membros asseguram que as suas autoridades competentes nos termos da presente diretiva notificam às autoridades competentes nos termos da Diretiva (UE) 2022/2555 a identidade das entidades críticas que tiverem identificado nos termos do presente artigo no prazo de um mês a contar da referida identificação";
b) O art.º 9.º, n.º 6 da Diretiva REC, que determina que "Cada Estado-Membro assegura que a sua autoridade competente nos termos da presente diretiva coopera e partilha informações com as autoridades competentes nos termos da Diretiva (UE) 2022/2555 no que diz respeito aos riscos de cibersegurança, ciberameaças e ciberincidentes, bem como riscos, ameaças e incidentes não relacionados com a cibersegurança, que afetam as entidades críticas, inclusive no que diz respeito às medidas pertinentes que tiverem sido tomadas pela sua autoridade competente e pelas autoridades competentes nos termos da Diretiva (UE) 2022/2555";
c) Na Diretiva NIS2, não há qualquer referência ao conceito de "Entidades Críticas", mas sim a "Entidades Essenciais" e "Entidades Importantes", para além de que

são contemplados mais setores onde estas entidades devem ser identificadas do que os que são referidos na Diretiva REC;

d) Finalmente, e propositadamente deixado para o final desta secção por ser o mais significativo ainda das dificuldades que podem ser encontradas nesta articulação entre as duas Diretivas, é o disposto no art.º 1.º n.º 2 da Diretiva REC, que estabelece que "A presente diretiva não é aplicável às matérias abrangidas pela Diretiva (UE) 2022/2555 (Diretiva NIS2), sem prejuízo do artigo 8.º da presente diretiva[5]. À luz da relação entre a segurança física e cibersegurança das entidades críticas, os Estados-Membros asseguram que a presente diretiva e a Diretiva (UE) 2022/2555 são aplicadas de forma coordenada".

Quinto Desafio: Elaboração da Avaliação Nacional de Riscos

Como foi referido a propósito do terceiro desafio, cada Estado-Membro deve elaborar, até 17 de janeiro de 2026, uma avaliação nacional dos riscos, nos termos do parágrafo 15 do Preâmbulo da Diretiva REC e dos seus artigos 2.º n.º 7 e 5.º.

A Diretiva REC define, no seu art.º 2.º n.º 7, a avaliação dos riscos como "o processo geral levado a cabo para determinar a natureza e o alcance 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". Ou seja, a avaliação dos riscos determina, por um lado, no caso das ameaças humanas intencionais (isto é, no âmbito da *security*), a identificação e avaliação destas, a identificação e avaliação das vulnerabilidades existentes que as ameaças podem explorar e a identificação e avaliação dos impactos resultantes de tais ações. Por outro lado, no caso de ameaças não humanas ou humanas negligentes (portanto no âmbito da *safety*), implica uma avaliação dos perigos pertinentes e dos impactos que a sua materialização poderá causar. É, portanto, uma avaliação global de todos os riscos relevantes para as EC.

Mais concretamente, a Diretiva REC estipula expressamente que cada Estado-Membro deverá realizar "uma avaliação dos riscos naturais e de origem humana pertinentes, incluindo os de natureza intersetorial ou transfronteiriça, que possam afetar a prestação

5 Este artigo determina que "Os Estados-Membros asseguram que o disposto no artigo 11.º (Cooperação entre os Estados-Membros) e nos capítulos III, IV e VI (i.e., Resiliência de Entidades Críticas, Entidades Críticas de Especial Relevância Europeia, Supervisão e Execução Coerciva) não é aplicável às entidades críticas 3, 4 e 8 do quadro constante do anexo (i.e. entidades críticas nos setores dos serviços bancários, das infraestruturas do mercado financeiro e das infraestruturas digitais). Os Estados-Membros podem adotar ou manter disposições de direito nacional destinadas a atingir um nível mais elevado de resiliência das entidades críticas, desde que essas disposições sejam compatíveis com o direito da União aplicável".

de serviços essenciais, nomeadamente acidentes, catástrofes naturais, emergências de saúde pública como as pandemias e as ameaças híbridas ou outras ameaças antagónicas, incluindo infrações terroristas, infiltrações criminosas e sabotagens"[6].
E também determina que, "ao efetuarem avaliações dos riscos do Estado-Membro, os Estados-Membros deverão ter em conta outras avaliações de riscos gerais ou específicas do setor efetuadas nos termos de outros atos jurídicos da União, e deverão ter em consideração em que medida os setores dependem uns dos outros, inclusive setores noutros Estados-Membros e em países terceiros. Os resultados da avaliação dos riscos do Estado-Membro deverão ser utilizados para efeitos da identificação de entidades críticas e para ajudar essas entidades a cumprir os seus requisitos em matéria de resiliência"[7].
Este é um aspeto essencial na avaliação dos riscos, pois implica analisar as dependências e interdependências das EC. Ou seja, a avaliação do risco de uma EC deve ser alargada para além dos seus muros, desde logo, não apenas porque o seu normal funcionamento pode ser prejudicado a montante, mas, também, porque a perturbação do seu normal funcionamento terá consequências a jusante.
Finalmente, refira-se que esta avaliação é fundamental para a elaboração da estratégia nacional de reforço da resiliência de EC, referida *infra*, que cada Estado-Membro está obrigado a elaborar e a implementar[8].
A complexidade desta avaliação nacional dos riscos, bem como o prazo imposto para a sua conclusão – pouco mais de um ano à data da elaboração deste artigo – implicam que a concretização desta avaliação necessitará não só de uma excelente coordenação e supervisão das várias entidades a envolver, mas, também, dos recursos humanos e técnicos adequados para tal.

Sexto Desafio: elaboração e implementação da Estratégia Nacional de Reforço da Resiliência das Entidades Críticas

No Parágrafo 2 do Preâmbulo da Diretiva REC estabelece-se que as EC deverão estar em condições de poder reforçar a sua capacidade para prevenir incidentes com potencial para perturbar a prestação de serviços essenciais, para se protegerem desses incidentes, lhes dar resposta, lhes resistirem, os atenuarem, os absorverem, se adaptarem a eles e recuperarem deles.
Com vista à concretização destes objetivos, mais adiante, no Parágrafo 13 do mesmo Preâmbulo, determina-se que, para assegurar uma abordagem abrangente à resiliên-

6 Diretiva REC, parágrafo 15 do Preâmbulo.
7 *Idem*.
8 Art.º 5.º n.º 2 c) da Diretiva REC.

cia das EC, os Estados-Membros deverão dispor de uma estratégia para reforçar a resiliência das EC localizadas nos respetivos territórios.
Esta estratégia deverá estabelecer objetivos estratégicos e medidas políticas a aplicar e, por razões de coerência e eficiência, deverá ser concebida de modo a integrar, de forma contínua, as políticas existentes, com base, sempre que possível, nas estratégias nacionais e setoriais, planos ou documentos similares pertinentes existentes.
Os desafios para a elaboração e implementação desta estratégia não acabam aqui. Com efeito, é também determinado que os Estados-Membros assegurem que as suas estratégias prevejam um quadro político para o reforço da cooperação entre as autoridades competentes, ao abrigo da Diretiva REC, e as autoridades competentes ao abrigo da Diretiva NIS2, no contexto da partilha de informações sobre os riscos de cibersegurança, as ciberameaças e os ciberincidentes, bem como sobre os riscos, ameaças e incidentes não relacionados com a cibersegurança, e no contexto do exercício de funções de supervisão.
Finalmente, ao aplicar as suas estratégias, os Estados-Membros deverão ter, devidamente, em conta a natureza híbrida das ameaças às EC.
Saliente-se que a elaboração desta estratégia deverá estar concluída até 17 de janeiro de 2026, ou seja, em simultâneo com a conclusão da avaliação nacional de riscos, o que constitui desafios acrescidos à significativa complexidade da produção daquele documento.

Sétimo Desafio: apoio dos Estados-Membros às Entidades Críticas

O último desafio, significativo para a proteção das IC e das EC, é o apoio que os Estados-Membros devem prestar às IC. Com efeito, no parágrafo 8 do Preâmbulo da Diretiva REC, determina-se que, a fim de alcançar um elevado nível de resiliência, os Estados-Membros deverão identificar as EC que ficarão sujeitas a requisitos específicos e a uma supervisão determinada e que receberão apoio e orientações face a todos os riscos pertinentes.
Esta obrigação é concretizada no art.º 10.º da Diretiva REC, relativo ao apoio dos Estados-Membros às EC no reforço da sua resiliência. A redação desta norma impõe algumas formas concretas de prestação deste apoio e sugere possibilidades adicionais, como por exemplo as seguintes:

a) Obrigação dos Estados-Membros assegurarem que a sua autoridade competente coopera e troca informações e boas práticas com as EC;
b) Obrigação dos Estados-Membros facilitarem a partilha voluntária de informações entre EC sobre as matérias abrangidas pela Diretiva REC;
c) A possibilidade de o apoio prestado pelos Estados-Membros incluir o desenvolvimento de documentação e metodologias de orientação, ajuda à organização de

exercícios para testar a sua resiliência e a prestação de aconselhamento e formação ao pessoal das EC;

d) A possibilidade de os Estados-Membros proporcionarem recursos financeiros às EC, sempre que necessário e justificado por objetivos de interesse público;
e) A obrigatoriedade, prevista no art.º 13.º da Diretiva REC, de os Estados-Membros partilharem informações pertinentes com as EC sobre a avaliação dos riscos do Estado-Membro e sobre os resultados da avaliação dos riscos de EC. Estas informações visam capacitar as EC para:
   a. Prevenir a ocorrência de incidentes;
   b. Assegurar uma proteção física adequada das suas instalações e IC;
   c. Dar resposta, resistir e atenuar as consequências dos incidentes;
   d. Recuperar de incidentes, tendo devidamente em conta a adoção de medidas de continuidade das atividades e a identificação de cadeias de abastecimento alternativas, a fim de retomar a prestação do serviço essencial;
   e. Assegurar uma gestão adequada das questões de segurança relacionadas com o pessoal, tendo devidamente em conta medidas como a definição das categorias de pessoal, incluindo pessoal de prestadores externos, que exercem funções críticas, o estabelecimento de direitos de acesso a instalações, IC e informações sensíveis, o estabelecimento de procedimentos para a realização de verificações de antecedentes e a designação das categorias de pessoas obrigatoriamente sujeitas a tais verificações de antecedentes;
   f. Sensibilizar o pessoal competente, incluindo o pessoal de prestadores externos, para as medidas referidas nas alíneas *supra* tendo devidamente em conta formações, documentação informativa e exercícios;
f) A realização de verificações de antecedentes (ou de segurança), atualmente já prevista no art.º 20.º do DL n.º 20/2022, mas mais aprofundado no Parágrafo 32 do Preâmbulo e no art.º 14.º da Diretiva REC.

Concretamente, sendo considerada uma preocupação crescente a possibilidade de trabalhadores de EC ou dos respetivos prestadores externos fazerem uma utilização abusiva, por exemplo, dos seus direitos de acesso no seio da organização da EC para prejudicar e causar danos, determina-se que os Estados-Membros deverão especificar as condições em que as EC estão autorizadas a apresentar pedidos de verificação de antecedentes relativos a pessoas pertencentes a categorias específicas do seu pessoal e que seja dada uma resposta no prazo de dez dias úteis.
Salienta-se que, para as verificações de antecedentes, os Estados-Membros deverão recorrer ao Sistema Europeu de Informação sobre Registos Criminais e poderão também, se necessário e aplicável, recorrer ao Sistema de Informação de Schengen de Segunda Geração, a informações provenientes dos serviços de informações e de segurança, bem como a quaisquer outras informações objetivas disponíveis que possam

ser necessárias para determinar a adequação da pessoa em causa para ocupar o cargo em relação ao qual a EC solicitou a realização de uma verificação de antecedentes.

Por fim, refira-se que também está prevista a possibilidade de a Comissão Europeia apoiar os Estados-Membros e as EC no cumprimento das suas obrigações decorrentes da Diretiva REC. Este apoio pode incluir: a elaboração de uma panorâmica a nível da União dos riscos transfronteiriços e intersectoriais para a prestação de serviços essenciais; a organização de missões consultivas; a facilitação do intercâmbio de informações entre Estados-Membros e peritos de toda a União; o desenvolvimento de boas práticas, documentação e metodologias de orientação, bem como atividades de formação e exercícios transfronteiriços para testar a resiliência das EC, em complemento dos Estados-Membros; e a prestação de informação aos Estados-Membros sobre os recursos financeiros a nível da União que lhes são disponibilizados para reforçarem a resiliência das EC.

O Contributo do Serviço de Informações de Segurança

Os sete desafios acima elencados não são os únicos que devem ser considerados na resiliência das EC. De facto, as obrigações que decorrem da Diretiva REC para as EC são também significativas, a começar pelo facto de elas terem o dever de proceder às respetivas avaliações de riscos e de elaborarem planos e procedimentos com vista à sua resiliência, aspetos que não são especificamente abordados neste artigo.
Porém, os desafios referidos são os que, na perspetiva do Serviço de Informações de Segurança (SIS), têm impactos mais significativos e imediatos para os Estados-Membros no âmbito da Diretiva REC. Recordemos que esta Diretiva impõe prazos curtos para a execução dos atos mais essenciais à sua efetiva execução:

- 17 de outubro de 2024: transposição da Diretiva REC para o ordenamento jurídico interno (prazo ultrapassado à data da elaboração do presente artigo);
- 17 de janeiro de 2026: elaboração da avaliação nacional dos riscos;
- 17 de janeiro de 2026: adoção da estratégia nacional de reforço da resiliência das EC.

Acresce que, pelas razões *supra* expostas, todo este trabalho assenta, ou deverá assentar, na prévia identificação e designação das IC nacionais nos setores considerados no DL n.º 20/2022, realidade em que o nosso país está, desde há vários anos, muito atrás de vários dos seus parceiros europeus, a começar pelos nossos vizinhos mais próximos.
Aqui chegados, e por este artigo pretender partilhar a visão do SIS sobre a resiliência das EC, importa também abordar o papel que este Serviço tem e irá ter nesta matéria.
De acordo com a Lei n.º 30/84, de 5 de setembro, é missão do SIS a produção de informações que contribuam para a salvaguarda da segurança interna e a pre-

venção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido.

O contributo prestado pelo SIS para a prevenção de tais atos é feito mediante a partilha das suas informações com vários destinatários (Governo, Forças e Serviços de Segurança, Forças Armadas e outras entidades) para que estes possam, no âmbito das suas capacidades e competências, robustecer a sua capacidade de decisão com vista a tomarem as medidas adequadas e necessárias: para que os atos acima referidos não ocorram; para que o país e as suas várias entidades se possam proteger o melhor possível de tais atos; para que o país e as suas várias entidades respondam da melhor forma possível em caso de ocorrência de alguns desses atos.

Neste âmbito, deve ser salientada a produção de avaliações de ameaça. Como sabemos, o risco é o resultado da equação Probabilidade x Consequência. No âmbito da *security*, a Probabilidade é constituída pela Ameaça e pela Vulnerabilidade, cabendo ao SIS a avaliação da Ameaça, concretamente, das ameaças especialmente graves acima mencionadas. A partilha destas informações com as demais entidades públicas competentes e com as EC, de acordo com as regras relativas à segurança das matérias classificadas, é fundamental para uma correta avaliação e gestão dos riscos, tanto a nível nacional, como pelas EC.

Mas o contributo do SIS para a resiliência das EC não se esgota aqui. A colaboração na verificação de antecedentes, *suprarreferida*, é um outro aspeto fundamental com vista à prevenção das ameaças, neste caso de ameaças internas nas EC.

Um outro contributo relevante consiste na participação em exercícios e simulacros com vista ao reforço da resiliência das EC, sendo este contributo orientado para a criação de cenários e incidentes que sejam os mais adequados, tendo em conta a manifestação das ameaças mais prováveis.

Num outro plano, a Diretiva REC, em articulação com o Regulamento (UE) 2019/452 do Parlamento Europeu e do Conselho, de 19 de março de 2019, que estabelece um regime de análise dos investimentos diretos estrangeiros na União, reconhece que a propriedade estrangeira de infraestruturas críticas na União representa uma potencial ameaça, pois os serviços, a economia, a livre circulação e a segurança dos cidadãos da União dependem do bom funcionamento das IC. Neste contexto, o SIS contribui, no âmbito da sua missão, para a análise dos investimentos diretos estrangeiros em EC presentes em território nacional.

Por fim, mas não menos relevante, o SIS, através dos seus programas de sensibilização Krítica (KRÍTICA, 2015) e Programa de Proteção do Conhecimento e da Informação Sensível (PPC, 2015), já contribui e continuará a contribuir para o disposto nos artigos 10.º e 13.º da Diretiva REC, melhorando a cultura de segurança das EC através da sensibilização do seu pessoal com vista à sua capacitação para a adoção de procedimentos e medidas de prevenção e proteção das EC e respetivas IC e outras

instalações, bem como, de uma forma genérica, para a redução dos respetivos riscos securitários que sejam decorrentes das ameaças tratadas por este Serviço.

Conclusão

Para terminar, uma consideração final para uma última reflexão do leitor: A segurança, pois é de segurança que falamos quando falamos da proteção de IC e da resiliência de EC, é algo que só se nota quando deixa de existir.
Como diz Giovanni Manunta, segurança é "a condição imaginada de ausência de, ou liberdade de perigo e preocupação, relativamente a um valor. [Porém] Tal resulta da implementação de medidas destinadas a evitar, prevenir, minimizar ou proteger da ocorrência de um dano, que pode ser intencionalmente causado ao valor" (Manunta, 1998).
A proteção de IC, agora incluída na resiliência das EC, é uma componente essencial na Segurança dos Estados. Por este motivo, é fundamental que os desafios referidos neste artigo – e também os outros que os demais autores contribuintes desta edição refiram – não sejam apenas superados. Devem, ou melhor ainda, têm, de ser bem superados e essa superação deverá ocorrer sem mais delongas para garantir a segurança do nosso país face a ameaças reais que põem em causa o Estado de direito e a sociedade.

Bibliografia

Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho.

Directiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção.

Decreto-Lei n.º 20/2022, de 28 de janeiro, que aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias.

Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.o 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148.

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

KRÍTICA, 2015. SIS. [em linha] Disponível em: https://www.sis.pt/pagina/132/programa-kritica-o-que-e [acedido 25 10 2024].

Lei n.º 30/84, de 5 de setembro, que estabelece as bases gerais do Sistema de Informações da República Portuguesa.

Manunta, G., 1998. Security: An Introduction. s.l.:Cranfield University.

Observador, 2021. Observador. [em linha] Disponível em: https://observador.pt/2021/01/15/central-de-sines-encerra-esta-sexta-feira-antes-do-previsto-devido-a-evolucao-do-mercado/ [acedido 25 10 2024].

PPC, 2015. SIS. [em linha] Disponível em: https://ppc.sis.pt/o-programa [acedido 25 10 2024].

Regulamento (UE) 2019/452 do Parlamento Europeu e do Conselho, de 19 de março de 2019, que estabelece um regime de análise dos investimentos diretos estrangeiros na União.