INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2022/2023

TII

RESILIÊNCIA DE ENTIDADES CRÍTICAS:
CONTRIBUTOS PARA UMA ESTRATÉGIA NACIONAL

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Helder Manuel Gonçalves Garção

MAJOR GNR CAVALARIA

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

RESILIÊNCIA DE ENTIDADES CRÍTICAS: CONTRIBUTOS PARA UMA ESTRATÉGIA NACIONAL

MAJOR GNR CAVALARIA Helder Manuel Gonçalves Garção

Trabalho de Investigação Individual

CEMC 2022/2023

Pedrouços 2023

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

RESILIÊNCIA DE ENTIDADES CRÍTICAS: CONTRIBUTOS PARA UMA ESTRATÉGIA NACIONAL

MAJOR GNR CAVALARIA Helder Manuel Gonçalves Garção

Trabalho de Investigação Individual

CEMC 2022/2023

Orientador: MGEN GNR Pedro Manuel Sequeira Estrela Moleirinho

Coorientador: TCOR GNR ADMIL Carlos Manuel Rodrigues Coelho

Pedrouços 2023

Declaração de compromisso Antiplágio

Eu, **Helder Manuel Gonçalves Garção,** declaro por minha honra que o documento intitulado **"Resiliência de Entidades Críticas: contributos para uma Estratégia Nacional"** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Estado-Maior Conjunto 2022/2023** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 03** de **julho** de **2023**

Assinado por: **Helder Manuel Gonçalves Garção**
Num. de Identificação: 12738675
Data: 2023.07.03 00:02:44+01'00'

CHAVE MÓVEL

Helder Manuel Gonçalves Garção

Agradecimentos

A concretização desta investigação, corolário do Curso de Estado-Maior Conjunto 2022/2023, foi viabilizada com o apoio de diversas pessoas, a quem manifesto o sincero e sentido reconhecimento.

Ao Senhor Major-general Pedro Moleirinho e ao Senhor Tenente-coronel Carlos Coelho, respetivamente orientador e coorientador, pelo inestimável apoio e partilha de visões críticas, que permitiram moldar o rumo e alcance do trabalho, bem como refinar o seu teor.

Ao distinto rol de entrevistados, agradeço pela disponibilidade demonstrada e pela diferenciada qualidade das respostas prestadas, que tanto contribuiram para os resultados alcançados, através da partilha das suas inestimáveis experiências, pareceres e ideias inovadoras.

Ao Senhor Comandante Luís Daniel Carona Jimenez, Diretor do Curso de Estado-Maior Conjunto, em reconhecimento pelo acompanhamento presente e estímulo constante, que imprimiu nos mais diversos momentos deste trajeto.

Aos meus camaradas de curso, pela amizade e entreajuda partilhada ao longo dos meses de trabalho.

Finalmente, uma palavra de especial agradecimento à minha familia e amigos, a quem reconheço a fundamental compreensão e apoio, bem como ao meu filho David, lamentando as ocasiões em que não lhe consegui dedicar a minha atenção, durante os seus três primeiros meses de vida.

A todos, a minha sentida gratidão.

[…] *"National infrastructure is the backbone of a modern economy, and critical infrastructure resilience is essential to develop sustainably.*

Robust and resilient infrastructure is a key driver of local and national economic growth.

The reliability, performance, continuous operation, safety, maintenance, and protection of critical infrastructures are national and local priorities around the world."

United Nations Office for Disaster Risk Reduction (UNDRR) (2022)

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Índice de Quadros

Resumo

Num contexto de profusão de ameaças ciber-físicas, a abordagem europeia à securitização de infraestruturas críticas encontra-se em transformação, visando maior resiliência sistémica.

Realça-se a recente Diretiva 2022/2557, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas que, entre outras inovações geradoras de maior convergência no seio da UE, prescreve a adoção de estratégias nacionais sobre a temática, cuja inexistência em Portugal já havia sido qualificada como vulnerabilidade.

Perante esta conjuntura de oportunidade e utilidade, a investigação procura contribuir para a formulação da estratégia nacional, apontando prioridades a considerar.

Seguindo um raciocínio indutivo e uma estratégia de investigação qualitativa, desenvolveu-se um estudo de caso, com recurso a técnicas de análise documental e entrevistas, estruturado à luz dos ensinamentos da gestão estratégica para que, da análise ao ambiente, se superem os problemas e se explorem as eventualidades.

Conclui-se pela premente edificação de um organismo dedicado e agregador, criando uma plataforma colaborativa estável, à semelhança de outros países, a qual viabilize a prossecução de uma panóplia de objetivos estratégicos interconectados, organizados segundo três vetores fundamentais: inovar e potenciar recursos; maximizar sinergias; e otimizar a governança, conforme esboço do mapa da estratégia sugerido no capítulo 5.

Palavras-chave: Infraestruturas Críticas, Entidades Críticas, Estratégia, Resiliência.

Abstract

Given the profusion of cyber-physical threats, the European approach for the critical infrastructures securitisation is undergoing transformation, aiming for a greater systemic resilience.

The recent Directive 2022/2557, approved on December 14th, 2022, on the resilience of critical entities, should be highlighted, which, among other innovations generating greater convergence within the EU, prescribes the adoption of national strategies on the subject, whose absence in Portugal had already been qualified as a vulnerability.

Given this scenario of opportunity and utility, the research seeks to contribute to the formulation of a national strategy, pointing out priorities to be considered.

Following an inductive reasoning and a qualitative research strategy, a case study was developed, using techniques for document analysis and interview, structured according to the strategic management practices so that, from the environment analysis, problems are overcome and possibilities are explored.

It is concluded that there is an urgent need to establish a dedicated and aggregating agency, creating a stable collaborative platform, as in other countries, which enables pursuing a range of interconnected strategic objectives, in this case organised according to three fundamental areas: innovating and enhancing resources; maximising synergies; and optimising governance, as outlined in the strategy map suggested in chapter 5.

Keywords: *Critical Infrastructures, Critical Entities, Strategy, Resilience.*

Lista de abreviaturas, siglas e acrónimos

A

ALS	Agente de Ligação de Segurança
ANEPC	Autoridade Nacional de Emergência e Proteção Civil
ANS	Autoridade Nacional de Segurança
ANR	Avaliação Nacional de Risco
APC	Agentes de Proteção Civil

B

BCP	*Business Continuity Plan(ning)*
BSC	*Balanced Scorecard*

C

CE	Comissão Europeia
CEDN	Conceito Estratégico de Defesa Nacional
CERT	*Computer Emergency Response Team*
CESP	*Centre for European Policy Studies*
CI	*Critical Infrastructure*
CISA	*Cybersecurity & Infrastructure Security Agency* (integrada no DHS dos Estados Unidos da América [EUA])
CISO	*Chief Information Security Officer*
CNCS	Centro Nacional de Cibersegurança
CNPCE	Conselho Nacional de Planeamento Civil de Emergência
CNPIC	*Centro Nacional de Protección de Infraestructuras Críticas* (de Espanha)
CSIRT	*Computer Security Incident Response Team*
CSPI	Curso de Segurança e Proteção de Infraestruturas
CSSI	Conselho Superior de Segurança Interna

D

DHS	*Department of Homeland Security* (dos EUA)

E

E	Entrevista | Entrevistado
EC	Entidade(s) Crítica(s)
ECI	Elemento de Contacto da Infraestrutura
EM	Estado(s)-Membro(s)
ENCT	Estratégia Nacional de Combate ao Terrorismo

ENISA	Agência da União Europeia para a Cibersegurança
ENPCP2030	Estratégia Nacional para uma Proteção Civil Preventiva 2030
ENSC	Estratégia Nacional de Segurança no Ciberespaço
ERRA	*European Risk & Resilience Assessment and Rating Initiative*
EUA	Estados Unidos da América
F	
FS	Força de Segurança
FSS	Forças e Serviços de Segurança
G	
GCS	Gabinete Coordenador de Segurança
GE	Gestão Estratégica
GNR	Guarda Nacional Republicana
GO2022-2026	Grandes Opções para 2022-2026
GREC	Grupo para a Resiliência de Entidades Críticas
GRRASP	*Geospatial Risk and Resilience Assessment Platform* (da UE)
I	
IC	Infraestrutura(s) Crítica(s)
ICE	Infraestrutura(s) Crítica(s) Europeia(s)
ICN	Infraestrutura(s) Crítica(s) Nacional(s)
I&D	Investigação e Desenvolvimento
ISAC	*Information Sharing and Analysis Centre*
ISO	*International Standardization Organization*
IUM	Instituto Universitário Militar
L	
LNEC	Laboratório Nacional de Engenharia Civil
LSI	Lei de Segurança Interna
N	
NIPP	*National Infrastructure Protection Plan*
O	
OCDE	Organização para a Cooperação e Desenvolvimento Económico
OE	Objetivo Específico
OG	Objetivo Geral
OSCOT	Observatório de Segurança, Criminalidade Organizada e Terrorismo

P

PAPARIC	Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas
PEPC	Plano de Emergência e Proteção Civil
PEPIC	Programa Europeu de Proteção de Infraestruturas Críticas
PIC	Proteção de Infraestruturas Críticas
PM	Polícia Marítima
PNPIC	Plano Nacional de Proteção de Infraestruturas Críticas
PNRRC	Plataforma Nacional de Redução de Risco de Catástrofes
PPI	Plano de Proteção e Intervenção
PRIIC	Plataforma de Registo de Informação de Infraestruturas Críticas
PSIC	Plano de Segurança de Infraestrutura Crítica
PSP	Polícia de Segurança Pública

Q

QC	Questão Central
QD	Questão Derivada

R

RAIC	Rede de Alerta para as Infraestruturas Críticas
RASI	Relatório Anual de Segurança Interna
RCM	Resolução do Conselho de Ministros
RCP	Relatório Cibersegurança em Portugal
REC	Resiliência de Entidades Críticas
RECIPE	*Recommended Elements of Critical Infrastructure Protection for Policy Makers in Europe*
RJSC	Regime Jurídico da Segurança do Ciberespaço

S

SE	Serviços Essenciais
SG-SSI	Secretário-Geral do Sistema de Segurança Interna
SI	Segurança Interna
SIED	Serviço de Informações Estratégicas de Defesa
SIS	Serviço de Informações de Segurança
SRI	Segurança das Redes e da Informação
SSI	Sistema de Segurança Interna

SWOT	*Strengths* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) & *Threats* (ameaças) - Matriz de análise
T	
TII	Trabalho de Investigação Individual
TISN	*Trusted Information Sharing Network* (Austrália)
U	
UE	União Europeia
UNDRR	*United Nations Office for Disaster Risk Reduction*
UNISDR	*United Nations International Strategy for Disaster Reduction Secretariat*
UNOCT	*United Nations Office of Counter-Terrorism*
UR	Unidade(s) de Registo
US	*United States [of America]*
V	
VSF	*Vital Societal Functions*
X	
XPP	*Palladium Execution Premium Process*™

1. Introdução

Decorrente da abordagem holística que o conceito de *segurança humana* impulsionou, conforme consta da Resolução da Assembleia Geral das Nações Unidas n.º 66/290, de 10 de setembro (2012), bem como dos preceitos intrínsecos aos Quadros de Hyogo (2005-2015) e de Sendai (2015-2030) para a redução do risco de catástrofes, advogando estratégias para a resiliência das sociedades, verifica-se a crescente preocupação na implementação de mecanismos mitigadores de riscos em prol da estabilidade social (*United Nations International Strategy for Disaster Reduction Secretariat* [UNISDR], 2015).

Dos ataques terroristas às torres gémeas em Nova Iorque, a 11 de setembro de 2001, à recente sabotagem dos gasodutos *Nord Stream* 1 e 2 no Mar Báltico, a 26 de setembro de 2022, passando pelas múltiplas catástrofes naturais, colapsos de obras de arte, crescente registo de ataques cibernéticos, ou pandemias, como a criada pelo vírus SARS-CoV-2, é árduo quantificar as graves disrupções ocorridas e, ainda mais, os nefastos impactos societais e económicos subjacentes.

Na atual conjuntura da Globalização 4.0, marcada pela transformação digital, dinâmicas aceleradas e tecnologias disruptivas, todavia, também pelo crescente espectro de ameaças híbridas e vulnerabilidades (Schwab, 2018), resulta insofismável que as *Entidades*[1] *Críticas* (EC), enquanto fornecedores de Serviços Essenciais (SE), desempenham um papel nevrálgico na manutenção das funções sociais e das atividades económicas vitais, num ambiente de crescente conectividade de sistemas, pelo que se tornou prioridade da União Europeia (UE) reforçar a sua resiliência, face a toda a tipologia de perigos, de origem natural, humana, acidentais ou intencionais (Conselho da União Europeia, 2022, p. 2-5), procurando mitigar potenciais perturbações, geradoras de efeitos nefastos em cascata, resultantes das interdependências entre as Infraestruturas Críticas (IC) (Comissão Europeia, 2020a; 2020b, pp. 6-7; 2020c).

Conforme Pursiainen e Kytömaa (2022), a crescente profusão de riscos ciber-físicos, a par da consciencialização da problemática, sua complexidade e relevância, alicerçaram a evolução do paradigma na UE, atualmente em transformação, em especial através da substituição da Diretiva respeitante à *Proteção de Infraestruturas Críticas* (PIC) (Diretiva 2008/114/CE, de 08 de dezembro), pela nova Diretiva focada na *Resiliência de Entidades*

[1] Nova designação assumida pela UE, respeitante a prestadores de SE em detrimento da anterior abordagem focada na proteção das Infraestruturas Críticas (IC) (Comissão Europeia, 2019, 2020c; Conselho da União Europeia, 2022)

Críticas (REC[2]) (Diretiva 2022/2557, de 14 de dezembro [Diretiva REC]), fomentando uma abordagem mais holística e integrada (Conselho da União Europeia, 2022).

Os preceitos da proposta da Diretiva REC suscitaram o alargamento dos setores de IC, mas, também, uma abordagem securitária mais ampla e cíclica, baseada no escrutínio prévio das interdependências, na cooperação e mitigação conjunta do risco, bem como na partilha de informação entre atores públicos e privados, em que a profícua articulação entre setores, sistemas e instituições, constitui um fator crítico de sucesso (Buss et al., 2021). Com efeito, considerando que a maioria das IC pertencem ou são operadas pelo setor privado (Oliveira et al., 2017, p.3), as relações de confiança entre atores públicos e privados para a partilha de informações respeitantes à resiliência das IC é crucial (*United States Department of Homeland Security* [DHS], 2016; 2019).

A premência de fomentar a sistemática cooperação entre atores para melhorar a resiliência das IC é indubitável. Esta depende, sobretudo, de plataformas e mecanismos de partilha de informação, que potenciam a monitorização integrada de ameaças ciber-físicas, considerando a análise das interdependências e respetivos riscos, idealmente com recurso a centros de fusão de dados, que potenciem a consciência situacional[3] e permitam um sistema de alertas precoces[4] (Soldatos et al., 2020; 2021).

Entre a panóplia de medidas introduzidas pela Diretiva REC, surge a imperatividade dos Estados-membros (EM) adotarem uma **estratégia nacional** para reforçar a sua resiliência (*ex vi* do artigo 4.º) (Diretiva REC, 2022).

Em Portugal, conforme demonstra Pestana (2016, p. 34-36; 54-62), existem múltiplas referências e atribuições em matéria de IC dispersas pela legislação, porém desarticuladas e pontualmente incoerentes, pelo que se considera importante a promulgação de um documento aglutinador que confira visão estratégica e harmonia ao sistema. Com efeito, atenta a magnitude multissetorial e multidimensional intrínseca à REC, não obstante as recentes atualizações aportadas pelo Decreto-Lei n.º 20/2022, de 28 de janeiro[5], a inexistência de uma estratégia nacional sobre a temática continua a impactar negativamente a implementação dos mecanismos de resiliência.

[2] Tradução do autor de: *Critical Entities Resilience Directive – CER Directive*.
[3] Tradução do autor de: "*situational awareness*".
[4] Tradução do autor de: "*early warnings*".
[5] Revogando o Decreto-Lei n.º 62/2011, de 09 de maio (2011), através do qual foi transposta a Diretiva 2008/114/CE, de 08 de dezembro, no fito de estabelecer os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes, conforme disposições do seu artigo 1.º.

Destarte, é na imperativa edificação do documento estratégico português sobre a temática que reside a justificação deste estudo, fixando-se o objeto da investigação na estratégia nacional para a REC em Portugal.

A investigação delimita-se em três domínios: (i) *temporalmente*, ao hiato entre 08 de dezembro de 2008 e 14 de abril de 2023, correspondendo, respetivamente, à data em que foi publicada a Diretiva 2008/114/CE sobre a temática, e a data até à qual foi exequível carrear dados para a investigação; (ii) *espacialmente*, centra-se em Portugal, sem prejuízo de colher contributos externos, provenientes de países apontados como referência na securitização de IC, a título de *benchmarking*; e, (iii) *quanto ao conteúdo*, cinge-se ao contributo para as prioridades a considerar na formulação estratégica para a REC, à luz da nova Diretiva europeia.

Para o efeito, executa-se um *diagnóstico estratégico*, na esteira do *modelo básico* de Gestão Estratégica (GE) proposto por Ribeiro[6] (2008, pp. 20-25), no desiderato de obter a *clarificação da estratégia*, correspondendo à fase da *análise do ambiente*[7] e ao início da *formulação estratégica*[8].

Decorrente do objeto de estudo e sua delimitação, define-se como **Objetivo Geral (OG)**: *Formular contributos para uma estratégia nacional de REC em Portugal.*

Na prossecução do OG, foram definidos os seguintes **Objetivos Específicos (OE)**:

OE1. Descrever as principais prioridades estratégicas adotadas para a REC por países de referência na temática;

OE2. Examinar o quadro normativo e institucional;

OE3. Avaliar o ambiente estratégico;

OE4. Analisar as perceções dos atores quanto às prioridades estratégicas.

[6] O autor baseia-se sobretudo no modelo de GE proposto pelo *United States (US) Naval War College,* no modelo de 1981 de Hunger e Wheelen (2014), e no *framework* do *Palladium Execution Premium Process* (XPP) de Kaplan e Norton (2008, p. 2), que, no essencial, são semelhantes e se baseiam em quatro questões: «onde se está?» (análise do ambiente); «onde se deverá ir?» (formulação); «como se chega lá?» (operacionalização); «está-se a chegar lá?» (controlo) (Ribeiro 2008, pp. 20-25).

[7] Correspondendo à questão «onde se está?» e, como tal, inclui a análise ao ambiente externo, com recurso nomeadamente à técnica PEST (Johnson e Scholes,1999, p.104, *cit. por* Ribeiro, 2008, p.22) com vista a identificar os fatores estratégicos externos; bem como a análise ao ambiente interno, com recurso à análise funcional. *Ibid*, p.23.

[8] Que responderá à questão «onde se deverá ir», considerando a "melhor conjugação entre os fatores estratégicos externos (problemas e eventualidades) e internos (potencialidades e vulnerabilidades), face à situação corrente, de forma a identificarem um contexto estratégico que permita a melhor promoção do futuro desejado […]. Esse conceito pode ser elaborado com recurso à técnica da matriz *SWOT*." *Ibid*, p.23

No intuito de apoiar a orientação do estudo, sua delimitação e sistematização, definiu-se a seguinte **Questão Central (QC)**: *Quais as prioridades estratégicas a considerar na formulação da estratégia nacional para a REC em Portugal?*

Em linha com o OG e respetivos OE, elencaram-se as **Questões Derivadas (QD)**:

QD1. Quais as principais prioridades estratégicas adotadas para a REC por países de referência na temática?

QD2. Qual o enquadramento normativo e o papel dos atores para a REC?

QD3. Que principais ameaças, oportunidades, potencialidades e vulnerabilidades influem na formulação de uma estratégia para a REC em Portugal?

QD4. Quais são as perceções dos atores quanto às prioridades estratégicas para uma REC?

Além da introdução e conclusões, este trabalho estrutura-se noutros quatro capítulos. O segundo reporta-se ao enquadramento teórico e conceptual, bem como o estado da arte; no terceiro descreve-se a metodologia do trabalho empírico; no quarto analisa-se o ambiente estratégico intrínseco ao objeto de estudo, esboçando-se as estratégias emergentes, sustentadas nos resultados das entrevistas (E); e, no quinto, são sistematizados os contributos para uma estratégia nacional para a REC; seguindo o arquétipo da Figura 1.

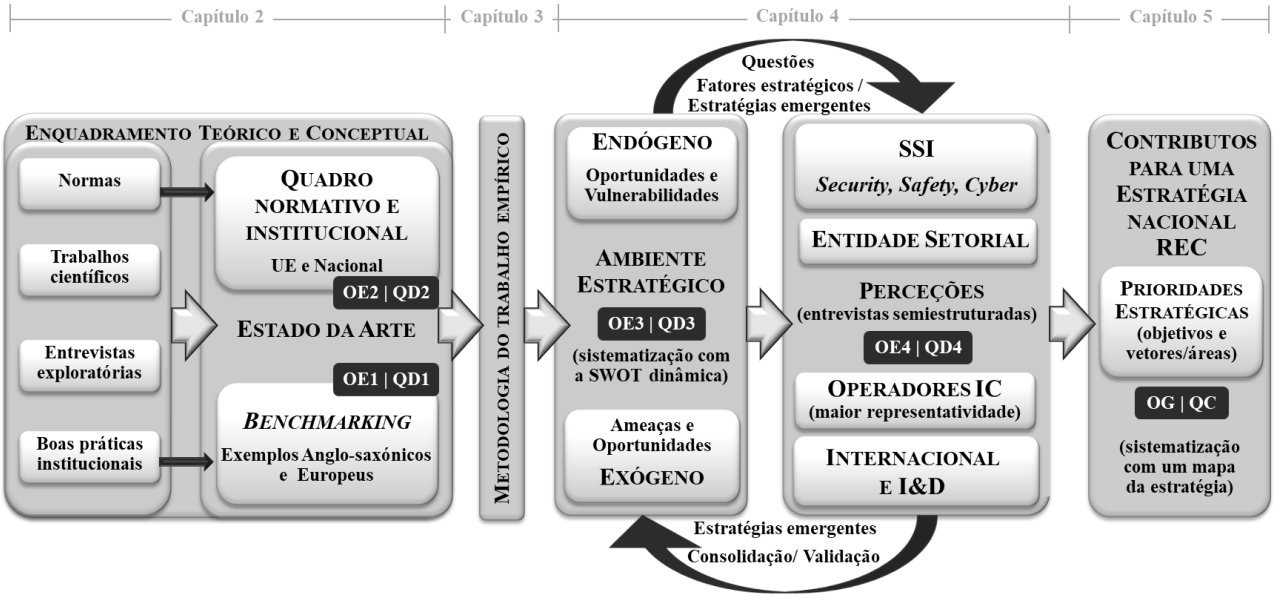

Figura 1 - Estrutura da Investigação

2. Enquadramento teórico e conceptual

No intuito de enquadrar a estratégia para a REC, seus conceitos, princípios, instrumentos, boas práticas hodiernas, bem como o quadro normativo e institucional, procede-se à revisão da literatura de referência, nacional e internacional, privilegiando fontes primárias, para inferir sobre o estado da arte, visando responder às QD1 e QD2.

2.1 Base conceptual

A temática *sub examine* encerra um vasto corpo de conceitos instrumentais, designadamente os constantes do **Apêndice A**.

Como estruturantes para a investigação, destacam-se três: (i) Estratégia; (ii) Entidades e Infraestruturas Críticas; e (iii) Resiliência de Entidades e Infraestruturas Críticas.

2.1.1 Estratégia

Ribeiro (2008, p. 47), define *estratégia* como a "Ciência e arte de edificar, dispor e empregar meios de coação num dado meio e tempo, para se materializarem objetivos fixados pela política, superando problemas e explorando eventualidades em ambientes de desacordo". Conforme os interesses nacionais e necessidades da população, a política garante direção à estratégia, referindo objetivos, métodos e recursos, pelo que a estratégia congrega três ramos: a genética (*means*), a estrutural (*ways*) e a operacional (*ends*) (Barroso, 2008, pp. 402-407), equacionados no respeito pelos critérios da adequabilidade, exequibilidade e aceitabilidade (Yarger, 2006, p. 5).

A estratégia subdivide-se de acordo com os níveis de decisão e execução no processo estratégico, em estratégia integral[9] (ou total) do Estado, as gerais (Ministros) e as estratégias particulares (Secretários-de-Estado), conforme o modelo preconizado por Beaufre (Ribeiro, 2017, pp. 74-86; Barroso, 2008, p. 414).

Conceito indissociável é o de GE, frequentemente entendida por "Política" ou, simplesmente, "Estratégia" (Rumelt et al., 1995). Ansoff (*cit.* por Ribeiro, 2017, p. 63) apresentou a GE com um conteúdo mais amplo que o planeamento estratégico, realçando que a turbulência ambiental é o fator-chave da estratégia.

Na esteira de Hannagan (2002) e Wit e Meyer (1999), Ribeiro (2008, p. 3) esclarece que uma estratégia é traduzida por quatro elementos fundamentais e interdependentes: (i) *contexto estratégico*: conjunto das circunstâncias internas e externas a considerar na formulação, na operacionalização e no conteúdo da estratégia. Responde à pergunta «onde?»; (ii) *processo de formulação*, forma de conceber, comparar e escolher uma

[9] Atribuição do Chefe de Governo.

modalidade de ação estratégica. Responde às perguntas «como?», «quem?» e «quando?»; (iii) *conteúdo estratégico*: produto do processo de formulação estratégica num determinado contexto estratégico, nas suas diferentes fases e aos diferentes níveis de aplicação. Responde à pergunta «o quê?»; e (iv) *processo de operacionalização*, forma de pôr em prática o conteúdo estratégico num determinado contexto estratégico. Concretiza o «como?», «quem?» e «quando?».

Em linha, David (2011) sistematiza um *framework* de GE simplificado, conforme Figura 2.

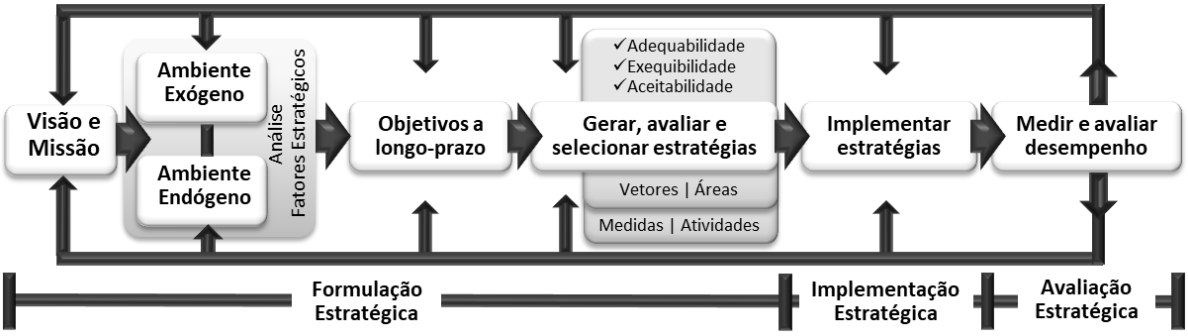

Figura 2 - *Framework* de Gestão Estratégica

Fonte: adaptado a partir de David (2011, p 176).

Segundo Ribeiro (2017b, pp. 31–34), para gerar estratégias, recorre-se à matriz SWOT[10] dinâmica, a qual estimula a correlação de fatores estratégicos, conforme Figura 3.

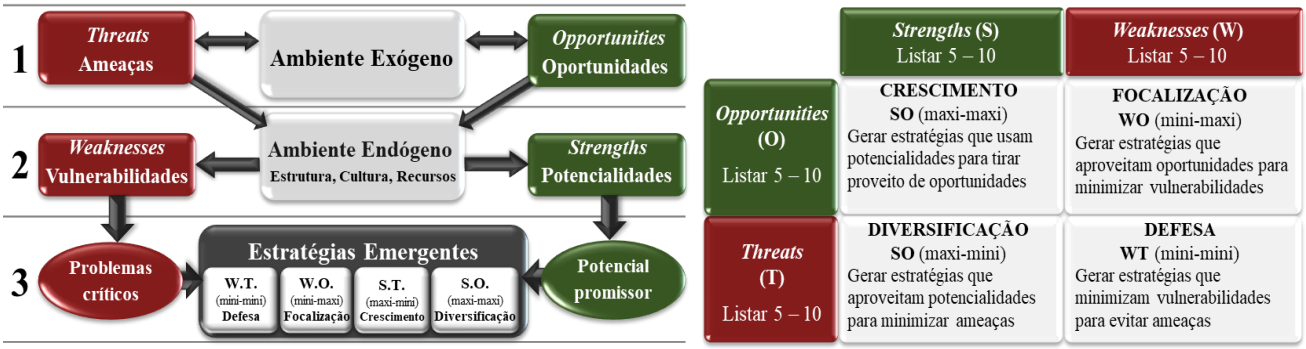

Figura 3 - Interações da análise SWOT dinâmica

Fonte: adaptado a partir de Ribeiro (2017b, p. 31-34), FIEP (2022) e David (2011, p 176-181).

A organização e alinhamento das estratégias geradas é polimorfa, usualmente agregando medidas e/ou ações prioritárias em vetores estratégicos ou áreas de afinidade. Para a clarificação e representação visual, entre outras técnicas, recorre-se ao *Balanced Scorecard* (BSC) apresentado por Kaplan e Norton (1992), adaptável a entidades não-lucrativas (Kaplan, 2010, p. 23), como metodologia que permite alinhar perspetivas e objetivos, associados a indicadores de desempenho, através do *mapa da estratégia*.

[10] *Strengths* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) e *Threats* (ameaças).

2.1.2 Entidades e Infraestruturas Críticas

Conforme artigos 2.º e 6.º da Diretiva REC, a UE define *infraestrutura crítica* como: "um ativo, uma instalação, um equipamento, uma rede ou um sistema, no seu todo ou uma parte […], que seja necessário para a prestação de um *serviço essencial"*[11] e *entidade crítica* como: "uma entidade pública ou privada que tenha sido identificada por um Estado-Membro […], como pertencente a uma das categorias estabelecidas na terceira coluna do quadro constante do anexo", correspondendo às entidades dos 11 setores e respetivos subsetores, num total de 53 categorias, cabendo aos EM a sua identificação, tendo em conta a avaliação dos riscos e a *estratégia nacional*, aplicando todos os seguintes critérios:

> "a) A entidade presta um ou mais serviços essenciais;
>
> b) A entidade opera e as suas infraestruturas críticas estão localizadas no território deste Estado-Membro; e
>
> c) Um incidente teria efeitos perturbadores[12] significativos […], 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."

Em Portugal, à luz do artigo 2.º do Decreto-Lei n.º 20/2022, de 28 de janeiro, (a atualizar[13]), define-se *infraestrutura crítica*[14] 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 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.

No mesmo artigo, adensa-se que *infraestrutura crítica europeia* (ICE) é a infraestrutura crítica nacional cuja perturbação do funcionamento ou destruição teria um

[11] Serviço que é indispensável à manutenção de funções sociais ou atividades económicas vitais, da saúde e segurança pública ou do ambiente. *Ibid*.

[12] Conforme artigo 7.º da Diretiva REC, a importância do efeito perturbador é considerada segundo: número de utilizadores que dependem do serviço essencial; o grau de dependência de outros setores; a intensidade e duração do possível impacto sobre atividades económicas e societais, o ambiente, a proteção e segurança pública ou a saúde da população; a quota e mercado da entidade no respetivo serviço essencial; a zona geográfica suscetível de ser afetada e eventual impacto transfronteiriço; e 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.

[13] Face à entrada em vigor da Diretiva REC, que suscita a imperativa harmonização, nomeadamente quanto aos setores considerados críticos.

[14] A mesma definição consta da alínea d) do artigo 3.º do Regime Jurídico da Segurança do Ciberespaço (RJSC), aprovado pela Lei n.º 46/2018, de 13 de agosto (2018), que transpôs para os preceitos da primeira Diretiva de Segurança das Redes e da Informação (SRI1) da UE.

impacto significativo em, pelo menos, mais um EM da UE; e que a *infraestrutura crítica nacional* (ICN) consiste na IC situada em território português, cuja perturbação do funcionamento ou destruição teria um impacto significativo à escala nacional.

Inexiste definição de EC na legislação nacional. Porém, encontra-se estatuída a definição de *entidade setorial* no artigo 2.º do Decreto-Lei n.º 20/2022, de 28 de janeiro, como "a entidade com funções de regulação, controlo ou fiscalização de cada setor e subsetor relevante" e *operador* como "o proprietário ou a entidade responsável pelo funcionamento de uma infraestrutura crítica, nacional ou europeia".

Verifica-se assim que, para a UE, a designação de EC é análoga à atual designação de operador de IC em Portugal.

De salientar que a categorização detalhada na Diretiva REC quanto aos setores e respetivos subsetores considerados como entidades/infraestruturas críticas é um aspeto essencial para a promoção da homogeneidade entre os países, nomeadamente da UE, atenta a dissonância de abordagens verificada (Comissão Europeia, 2019; OCDE, 2019), conforme patente na Figura 4.

	AUS	AUT	BEL	CAN	CHE	CHL	CZE	DEU	ESP	EST	FIN	FRA	GBR	GRC	IRL	ISL	ISR	ITA	KOR	LAT	LUX	MEX	NLD	NOR	NZL	POL	PRT	SVK	SVN	SWE	TUR	USA
Energy	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Nuclear sector				•			•		•			•	•				•		•				•	•								•
ICT	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•
Transportation	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	
Water	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•	•	•		•				•
Dams & flood defence	•					•	•					•			•	•		•	•	•		•	•	•					•		•	•
Food supply & dist.	•	•		•	•		•	•	•		•	•	•				•				•			•		•				•	•	•
Health	•	•	•	•	•	•	•	•	•	•	•	•	•				•		•	•	•			•		•		•		•	•	•
Finance & banking	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•		•		•		•	•	•
Government		•		•	•		•	•	•			•	•				•		•	•	•			•		•				•		•
Public safety	•	•		•	•		•	•	•				•				•			•	•		•	•						•		•
Law enforcement		•				•		•				•	•				•			•	•		•	•								
Chemical industry	•	•			•				•		•	•	•				•			•	•		•	•		•		•				•
Space sector			•						•			•	•																			
Defence industry	•										•	•	•				•			•												•
Critical manufacturing				•							•	•					•							•							•	•
Other		•	•					•	•	•	•	•	•				•		•	•	•		•	•	•	•				•	•	•

Figura 4 - Setores de IC nos países da OCDE em 2018

Fonte: adaptado a partir do inquérito sobre a REC, aplicado em setembro de 2018, a 22 países da OCDE (2019, p. 67)

2.1.3 Resiliência de Entidades e Infraestruturas Críticas

A *International Standardization Organization* (ISO) define *resiliência*[15] como a capacidade de absorção e adaptação num ambiente em mudança (ISO 22300:2021). Da consulta a enciclopédias, constata-se que a resiliência corresponde a um conceito polissémico, com utilização crescente nas mais diversas áreas do saber, destacando-se a antropologia e a psicologia (Google Trends, 2022) e que, sobretudo nas últimas duas décadas, tem vindo a ganhar popularidade na temática da securitização das IC, face ao reconhecimento que a tradicional abordagem da prevenção e proteção é limitada, atentas as progressivas interdependências, complexidade, não-linearidade e incertezas do ambiente (Ninković, 2021, p. 1207).

No prisma da segurança e proteção às IC e recorrendo à sua origem anglo-saxónica[16], o *U.S. Department of Homeland Security* (DHS) (2013) clarifica, no *National Infrastructure Protection Plan* (NIPP), que a resiliência corresponde à capacidade de preparação e adaptação às condições em mudança e de suportar e recuperar rapidamente de perturbações, nomeadamente de ataques deliberados, acidentais, ou incidentes naturais, sendo fundamental dispor de informações e análises precisas sobre os riscos. Para tal, os bens, sistemas e redes devem ser robustos, ágeis e adaptáveis, associados a atividades de mitigação, resposta e recuperação para reforçar a resiliência de IC.

Para a UE, conforme consta na nova Diretiva REC, resiliência corresponde à "capacidade de uma entidade crítica para prevenir incidentes, se proteger deles, lhes dar resposta, lhes resistir, os atenuar, os absorver, se adaptar a eles e recuperar deles".

Através de uma revisão sistemática da literatura, Ninković (2021) demonstra que, para vários autores, a resiliência consiste na estratégia recomendada para a gestão de riscos que se caracterizam por um elevado grau de incerteza (ou probabilidade muito baixa) e grande impacto, cujas abordagens foram sendo alteradas em função dos eventos:

[15]Do latim *resiliens*, particípio passado de *resalire*, originado pela congregação de "*re*", "para trás", com "*salire*" "pular", motivo pelo qual na literatura anglo-saxónico se recorre, pontualmente, às expressões "*bounce back*" ou "*rebounding*".

[16]A temática da securitização das IC ganhou expressão depois dos ataques de 11 de setembro de 2001, em Nova Iorque, embora o racional ter sido previamente usado nos Estados Unidos da América (EUA), nomeadamente no *President's Commission Report* de 1997, como *"network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services"*.

– De 2001 a 2005, na sequência do ataque às torres gémeas, em 11 de setembro de 2001, com pendor na segurança física (*security*), orientada para soluções técnico-tecnológicas, face a ameaças híbridas e assimétricas;

– De 2006 a 2011, na senda do furacão Katrina, orientada também para os riscos naturais (*safety*), e, logo a partir de 2007, por força de uma série de ataques cibernéticos[17], também para a dimensão *cyber*, levando à abordagem holística a todos os riscos e ameaças (*all-hazards approach*), conforme Quadro 1:

Quadro 1 - Categorização das ameaças a IC

Naturais	Por deterioração	Acidentais	Deliberadas
Externas Terramoto, tornado, inundação, tsunami, tempestade tropical, furacão, tempestade, nevão/neve/tempestade de gelo, granizo, erupção vulcânica, deslizamento de terras, erosão, incêndio, vendaval, temperatura extrema, meteorito, asteroide, biológicos (pandemia)	**Externas** Erosão, ferrugem/corrosão, fadiga pelo tempo **Internas** Desgaste, negligência, stress/fadiga estrutural, envelhecimento do equipamento ou material	**Externas** Corte de cabo ou tubagem, incêndio, derramamento de matérias perigosas, envenenamento **Internas** Erro, perda ou uso indevido de equipamentos, manutenção imprópria, deslizamentos e quedas, derramamentos, inundações, incêndio, intoxicação	**Externas** Terrorismo, criminalidade, sabotagem, subversão, hostilidade, ação militar, insurreição, espionagem estatal ou corporativa, ciberataques, ativismo político, embustes, envenenamento. **Internas** Sabotagem por funcionários, roubo, greve, ações laborais

Fonte: adaptado a partir de Boone (2013).

– A partir de 2011, depois do desastre de Fukushima, o foco transitou para o *fenómeno das interdependências*, *efeitos em cascata* e *crises simultâneas*, passando a *continuidade de atividade*[18] de IC a ser tão importante quanto a sua

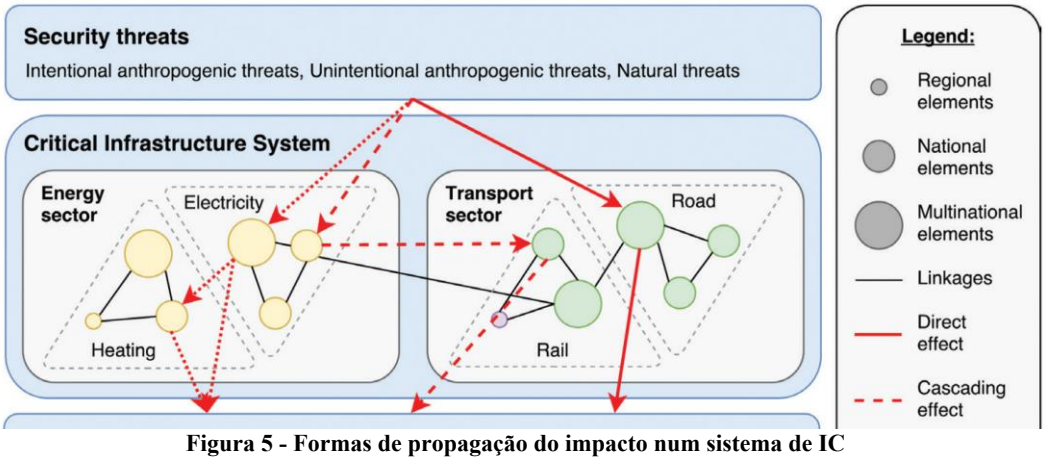

Figura 5 - Formas de propagação do impacto num sistema de IC

Fonte: Rehak e Hromada (2018).

[17]Principalmente relacionado com os ataques à "e-administração" da Estónia em 2007, e o ataque "*Stuxnet*" ao programa nuclear iraniano. Na senda, foram sendo criadas as *Computer Emergency Response Teams* (CERTs).

[18]*Business Continuity Planning* (BCP) (Recommended Elements of Critical Infrastructure Protection for Policy Makers in Europe [RECIPE], 2011).

proteção, contexto em que se passou a analisar a complexidade sistémica, conforme ilustrado através das Figuras 5 e 6.

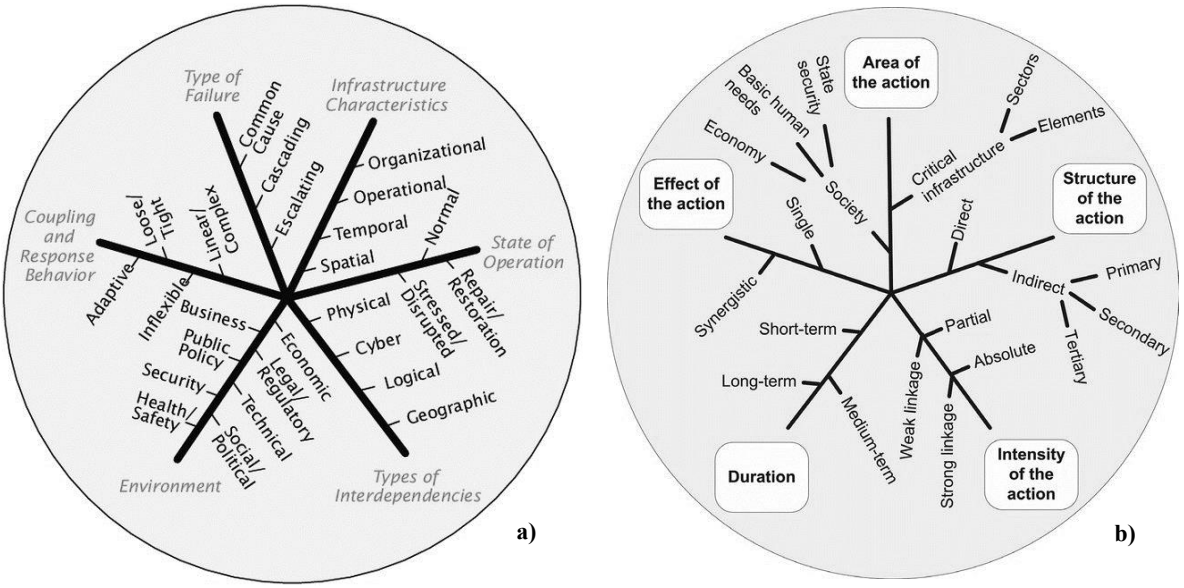

Figura 6 - Dimensões do conceito de dependência (a) e carácter dos impactos num sistema de infraestruturas críticas (b)

Fonte: adaptado a partir de Rinaldi (2001) *cit.* por RECIPE (2011) e Rehak e Hromada (2018).

Para compreensão do conceito de REC importa, também, examinar: (i) as suas *fases*: *ex-ante*, durante e *ex-post* ao evento disruptivo, associadas ao ciclo da catástrofe; as (ii) *capacidades*: preventiva, absortiva, adaptativa e restaurativa; assim como as suas (iii) *dimensões*: técnica / lógica e física, pessoal / humana, organizacional e cooperativa, bem como económica ou ainda outras, embora menos consentâneas, como se sistematiza no **Apêndice B**.

Igualmente importante é o discernimento sobre a tendência para o foco na análise de interdependências e gestão do risco[19] em matéria de REC, o qual é exponenciado em razão da interligação entre IC, conforme se sumariza no **Apêndice C**.

Não obstante, conforme Mentges et al. (2023), enquanto a gestão do risco conhece/aceita a latência do risco residual, a gestão da resiliência é movida pela noção de que nem todos os riscos são previsíveis e evitáveis, pelo que coloca mais ênfase no aumento holístico da capacidade de lidar com as perturbações à medida que estas surgem, enfatizando os processos de recuperação, aprendizagem e adaptação. Portanto, enquanto as abordagens estritamente centradas na gestão do risco se focam na preparação perante eventos que se enquadram num espectro de padrões conhecidos ou familiares, as abordagens centradas na

[19] Processo de Gestão de Risco a desenvolver conforme norma ISO 31000:2018.

resiliência visam permitir que um sistema responda eficazmente a qualquer evento, incluindo aqueles que são inesperados e únicos.

2.2 Estado da arte

2.2.1 Princípios e instrumentos políticos para a Resiliência de Entidades Críticas

A consciencialização do fenómeno das interdependências alavancou uma miríade de investigações, metodologias (Sathurshan et al., 2022), manuais de boas práticas (*Centre for European Policy Studies* [CESP], 2010; RECIPE, 2011; Organização para a Cooperação e Desenvolvimento Económico [OCDE], 2019; DHS, 2019) entre outras iniciativas, enaltecendo sobretudo: (i) a premência de alargar o espectro de setores; (ii) analisar (inter)dependências; (iii) estabelecer parcerias público-privadas; (iv) fomentar a partilha de informação; e (v) desenvolver um processo continuo e integrado de gestão do risco, almejando a crescente agregação de níveis, proporcional à maturidade do sistema, conforme Figura 7.

Figura 7 - Níveis de agregação na Gestão do Risco para IC

Fonte: adaptado a partir de RECIPE (2011, p. 61).

A abordagem anglo-saxónica tende a partir de uma panóplia de princípios fundamentais, no caso dos EUA, indicados como "*core-tenets*" (*vide* Figura 8) no documento estratégico - NIPP (DHS, 2013, p. 13-14):

- O risco deve ser identificado e gerido de uma forma coordenada e holística em toda a comunidade de EC, com partilha de informação, para permitir a atribuição eficaz de recursos de segurança e resiliência;
- Compreender e abordar os riscos advenientes das interdependências sectoriais é essencial para reforçar a segurança e a resiliência das IC baseada na gestão conjunta do risco;

- O intercâmbio de informações sobre os riscos e interdependências das IC entre a comunidade de atores envolvidos é fundamental, sendo necessário promover relações de confiança e o planeamento conjunto;
- As parcerias público-privadas são essenciais para a REC, permitindo reconhecer perspetivas únicas e oportunidades no seio da comunidade de EC, nomeadamente, possibilitando economias de escala na mitigação do risco;
- Parcerias setoriais e regionais permitem a cooperação transversal entre os diversos setores e regiões, possibilitando o desenvolvimento de perspetivas conjuntas sobre vulnerabilidades e melhorias a implementar;
- A REC transcende as fronteiras nacionais, exigindo a colaboração transfronteiriça, a assistência mútua, bem como acordos de cooperação; e
- A segurança e resiliência devem ser consideradas durante a conceção de infraestruturas, sistemas e redes (*security by design*).

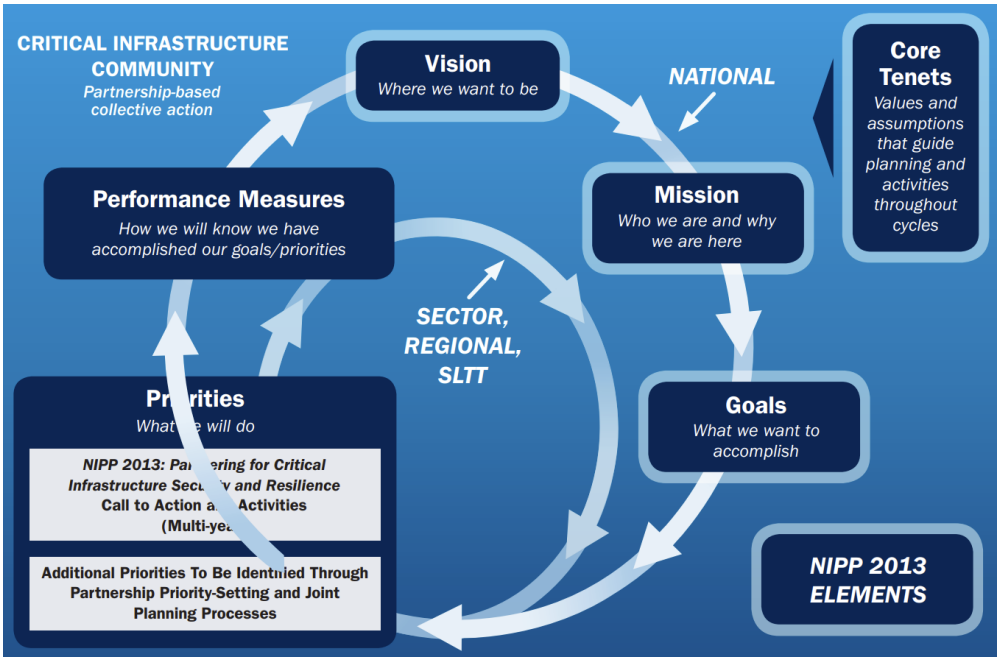

Figura 8 - Abordagem dos EUA com os "*core-tenets*"

Fonte: DHS (2013, p. 6).

Atenta a transversalidade e complexidade da temática, as instituições de referência advogam princípios, objetivos e mecanismos para o aumento da REC, iniciando-se pelo alinhamento estratégico (abordagem *top-down*), mas, simultaneamente, promovendo a congregação das perspetivas operativas e contributos académicos (abordagem *bottom-up*), numa lógica de sistema-de-sistemas, em que as (inter)dependências são fator determinante (Lewis, 2019; OCDE, 2019; DHS, 2019), como sistematizado na Figura 9.

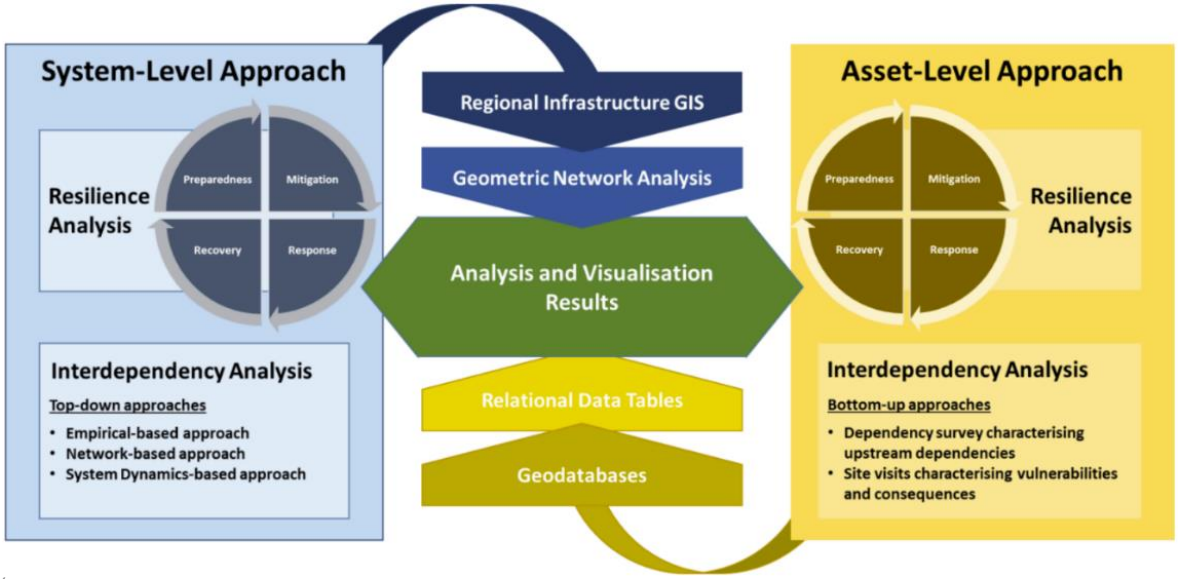

Figura 9 – Exemplo de abordagem enquanto sistema-de-sistemas

Fonte: Lewis (2019, p. 16), seguindo Petit et al., (2017, p. 9).

Segundo a OCDE (2019, pp. 54-55), o incremento da REC resulta do esforço de colaboração entre as várias partes interessadas e requer uma combinação de mecanismos para recolha de informação, priorização dos investimentos em resiliência, assim como o aumento de incentivos transversais, tendo sido identificadas 22 medidas políticas para a resiliência das IC, cujo emprego foi verificado em 2018, resultado nas frequências constantes da Figura 10.

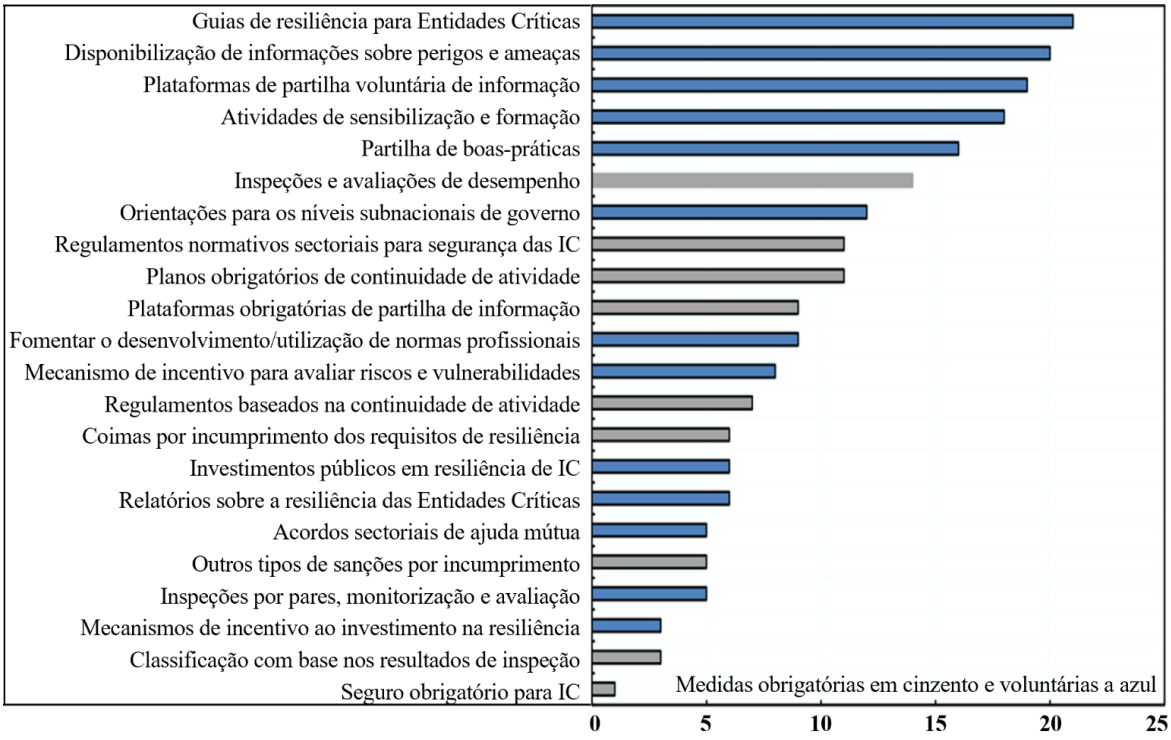

Figura 10 – Aplicação de medidas políticas para a resiliência de IC em países da OCDE

Fonte: adaptado a partir do inquérito sobre a REC, aplicado em setembro de 2018, a 22 países da OCDE (2019, p. 56).

2.2.2 *Benchmarking* de estratégias para a Resiliência de Entidades Críticas

O compêndio de boas práticas sobre a proteção de IC, desenvolvido pela Interpol e pelo Gabinete das Nações Unidas de Combate ao Terrorismo (UNOCT) (2018), evidencia as diferentes abordagens nacionais à temática, enfatizando as dos países anglo-saxónicos, que impulsionaram e se mantêm na vanguarda da securitização de IC, bem como alguns países europeus que se destacam na implementação de políticas e edificação de organismos ou plataformas colaborativas dedicados à resiliência de ativos estratégicos (*e.g.* Alemanha, Bélgica, Espanha, França, Suíça, Suécia, entre outros).

Os anglo-saxónicos fomentam a cooperação mútua sobre IC, designadamente através de iniciativas como a *Critical Five*, integrando: Austrália, Canadá, Nova Zelândia, Reino Unido e EUA (Critical Five, 2015).

Entre os europeus, a cooperação transnacional é eminentemente desenvolvida no quadro da UE. Destaca-se, como referência, o caso de Espanha, não só pela partilha de fronteiras com Portugal, mas, também, enquanto precursor em matéria de segurança de IC no contexto europeu, dispondo do *Centro Nacional de Protección de Infraestructuras Críticas* (CNPIC), em que, para além da *Estrategia de Seguridad Nacional* e do *Plan Nacional de Protección de las Infraestructuras Críticas*, são regularmente atualizados planos estratégicos setoriais para a proteção de IC, conforme definido nos artigos 18.º e 19.º do *Real Decreto 704/2011, de 20 de mayo* (2011), que aprova o *Reglamento de protección de las infraestructuras críticas*. Salienta-se, ainda, o caso da Suécia, que dispõe de um plano nacional para a proteção das funções sociais vitais e IC (Swedish Civil Contingencies Agency, 2014).

Os países tidos como referência, neste âmbito, dispõem de estratégias nacionais securitárias para as IC, as quais são estruturantes e surgem frequentemente associadas a planos de ação monitorizados por organismos dedicados à análise de risco, planeamento, coordenação e partilha de informações (OCDE, 2019; UNOCT, 2018).

Da pesquisa desenvolvida, sistematizam-se exemplos de estratégias nacionais de referência para a proteção ou resiliência de IC, quanto aos objetivos e vetores estratégicos, bem como atividades-chave ou medidas prioritárias, por forma a responder à **QD1**, conforme o Quadro 2.

Quadro 2 – Exemplos de objetivos e prioridades nas estratégias nacionais para a REC

País	Setores	Principais documentos estratégicos
Austrália	**11**	*Critical Infrastructure Resilience Strategy* (2023a) *Critical Infrastructure Resilience Plan* (2023b)
Objetivos estratégicos		1. Apoiar os proprietários de IC e operadores para gerir eficazmente os riscos para os a continuidade das suas operações através da maturação das abordagens baseadas no risco e na resiliência. 2. Apresentar iniciativas através de fortes parcerias entre a indústria e o governo. 3. Apoiar proprietários de IC e operadores a reforçar a sua segurança e resiliência através de estruturas, ferramentas e uma melhor colaboração.
Atividades-chave		1. Alargar e melhorar a *Trusted Information Sharing Network* (TISN) 2. Apoiar os membros da TISN a elevar a segurança e resiliência das suas IC entregáveis 3. Apoiar os proprietários e operadores de IC a cumprir com as suas obrigações legais
Canadá	**10**	*National Strategy for Critical Infrastructure (2009)* *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure (2021)*
Objetivos estratégicos		1. Construir parcerias. 2. Implementar uma abordagem de gestão de riscos "*all-hazards*". 3. Promover a oportuna partilha e proteção de informação entre os parceiros.
Atividades-chave / Medidas prioritárias		1. Abordar questões intersectoriais através de reuniões multi-sectoriais 2. Envolver-se com as províncias e territórios para reforçar a resiliência das IC 3. Colaboração contínua com os principais departamentos federais 4. Envolver-se em vários fóruns internacionais para abordar questões de IC 5. Envolver as partes interessadas dos sectores público e privado na renovação da estratégia e abordagem nacional em matéria de IC 6. Modernização e promoção do Portal de Informação de IC 7. Desenvolver e distribuir produtos de avaliação de impacto, tanto em estado estável como em situação de incidente 8. Apoiar exercícios sectoriais e intersectoriais para reforçar a preparação e capacidade de resposta das IC 9. Utilizar os instrumentos de avaliação existentes para avaliar a resiliência das IC 10. Aumentar a segurança dos Sistemas de Controlo Industrial para a comunidade nacional de IC 11. Renovar a estratégia e a abordagem nacional à resiliência das IC 12. Utilizar um mecanismo de monitorização para avaliar o progresso das atividades do Plano de Ação
Reino Unido	**13**	*National Security Strategy and Strategic Defence and Security Review* (2015) *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* (2010) *Public Summary of Sector Security and Resilience Plans*
Objetivos estratégicos		1. Estabelecer o devido quadro normativo para que as IC nacionais sejam resilientes a futuras ameaças 2. Trabalhar com proprietários e operadores para reforçar a cibersegurança das IC 3. Aumentar a resiliência do Reino Unido
Atividades-chave / Medidas prioritárias		1. Reduzir os riscos mais substanciais para a continuidade da atividade das IC e SE […], através de uma avaliação cuidadosa das vulnerabilidades e de uma atividade prudente e proporcional de mitigação dos riscos, baseada em novas normas definidas a nível central. 2. Criar um quadro comum de apoio à atividade intersectorial para avaliar, melhorar e sustentar a resiliência das IC e dos SE. 3. Aumentar a capacidade coletiva das IC para absorver o choque e agir rapidamente quando confrontadas com eventos inesperados. 4. Assegurar uma resposta de emergência eficaz a nível local através de uma melhor partilha e envolvimento da informação antes, durante e depois das emergências.

EUA	**16**	*Presidential Policy Directive-21 (PPD-21)* (2013) *National Infrastructures Protection Plan* (NIPP2013) *National Security Strategy* (2022)
Objetivos estratégicos		1. Refinar e clarificar as relações funcionais através do Governo Federal para impulsionar a unidade nacional de esforço para reforçar a segurança e resiliência das IC 2. Permitir o intercâmbio eficiente de informações através da identificação de dados de referência e requisitos de sistemas para o Governo Federal 3. Implementar uma função de integração e análise para apoiar o planeamento e as decisões operacionais relativas às IC [...] para: – Ajudar na priorização de ativos e na gestão de riscos para IC; – Antecipar interdependências e impactos em cascata; – Recomendar medidas de segurança e resiliência para IC antes, durante e após um evento ou incidente; e – Apoiar a gestão de incidentes e os esforços de restauração relacionados com IC.
Atividades-chave		1. [Melhorar] Relações Funcionais de Segurança e Resiliência de IC 2. Avaliação do Modelo de Parceria Público-Privada Existente 3. Identificação de Dados de Base e Requisitos de Sistemas para que o Governo Federal Possibilite o Intercâmbio Eficiente de Informações 4. Desenvolvimento de uma Capacidade de Consciencialização Situacional para IC 5. Atualização do NIPP 6. [Implementar um] Plano Nacional de Segurança e Resiliência de IC de Inovação e Desenvolvimento (I&D)
Espanha	**12**	*Estrategia de Seguridad Nacional* (2021) *Reglamento de protección de las infraestructuras críticas* (2011) *Plan Nacional de Protección de las Infraestructuras Críticas* (2016) **(classificado)** *Planes Estratégicos Sectoriales* – **(classificados)**
Objetivos estratégicos		1. Progredir em matéria de gestão de crises com enfoque no princípio da resiliência 2. Promover a dimensão da segurança das capacidades tecnológicas e dos sectores estratégicos 3. Desenvolver a capacidade de prevenção, deteção e resposta face às estratégias híbridas
Atividades-chave		"As infraestruturas críticas são a espinha dorsal da resiliência física de um país. […] É essencial ter um sistema de alerta precoce versátil e digitalizado que permita uma resposta ágil […]. A dimensão preventiva do Sistema Nacional de Proteção de Infraestruturas Críticas deve ser promovida, com especial ênfase na proteção dos sistemas informáticos das IC e dos operadores de SE contra ameaças cibernéticas. Neste sentido, a colaboração público-privada e a I&D para reforçar a resiliência contra ciberataques é fundamental". (Consejo de Seguridad Nacional, 2021, pp. 78–79)
Suécia	**11**	*Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure* (2014)
Objetivos estratégicos		1. Utilizar uma perspetiva de sistema: a estratégia e o plano de acão têm como objetivo garantir a funcionalidade das *Vital Societal Functions* (VSF) & *Critical Infrastructure* (CI) a nível local, regional e nacional. Uma perspetiva de sistema significa que os trabalhos sobre a proteção de VSF & CI são realizados a todos os níveis da sociedade e inclui entidades dos sectores público e privado em todos os sectores da sociedade. A perspetiva do sistema implica também não só assegurar as próprias atividades, mas também perspetivá-las em relação à sociedade em geral. Além disso, deve ter em consideração e retirar lições do trabalho em curso nos países nórdicos, na UE e na ONU, bem como de outros esforços internacionais. Deve ser dada especial atenção ao trabalho no âmbito do Programa Europeu para a Proteção de Infraestruturas Críticas (PEPIC). 2. Medidas antes, durante e depois de uma perturbação: As perspetivas antes, durante e depois de uma perturbação devem ser incluídas no trabalho para que a sociedade seja capaz de resistir, gerir, recuperar, aprender e desenvolver-se a partir de ruturas. Para o conseguir, todos os VSF & CI precisam de implementar uma segurança sistemática. 3. Cobrir todos os tipos de ameaças e riscos: As VSF & CI podem ser afetadas por várias ameaças e riscos, quando muitos riscos são difíceis de prever. É, portanto, crucial que se trabalhe sobre a funcionalidade social, baseada num amplo espectro de ameaças e riscos.
Atividades-chave / Medidas prioritárias		1. Medidas para a melhoria do conhecimento: (i) fundamentos e regulamentos; (ii) investigação; (iii) formação e educação; (iv) exercícios. 2. Atividades para a implementação da segurança sistémica: – Implementação de ferramentas de apoio à Gestão do Risco; Gestão da continuidade da atividade; e Gestão de crises; – Desenvolvimento da cooperação; – Melhorar a análise de risco e vulnerabilidade; – Planos sectoriais; – Feedback de experiências; – Análises de impacto a nível social; – Contratos robustos entre entidades privadas

2.2.3 Quadro normativo e institucional

2.2.3.1 Europeu

Na senda dos ataques terroristas de 2004 em Atocha-Madrid, o Conselho Europeu solicitou à Comissão a elaboração uma estratégia global para a proteção de IC, a qual foi intitulada "proteção de IC no âmbito da luta contra o terrorismo" (Comissão das Comunidades Europeias, 2006). Em 2007, a Comissão aprovou o Livro Verde relativo às opções políticas do subsequente Programa Europeu de Proteção de IC (PEPIC) e, em 2008, criou a Rede de Alerta para as Infraestruturas Críticas (RAIC) (Comissão das Comunidades Europeias, 2008). Não obstante, à época, o ato mais impactante da UE consistiu na promulgação da Diretiva respeitante à PIC em 2008 (Diretiva 2008/114/CE, de 08 de dezembro), através da qual foi definido um conjunto de medidas visando a proteção de infraestruturas dos setores da energia e transportes, deixando à discricionariedade dos EM o alargamento a outros setores (*ex vi* do artigo 3.º).

Num processo integrado na revisão da Estratégia da UE para a União da Segurança, (*vide* Figura 11) (Comissão Europeia, 2020a), a implementação da Diretiva PIC foi alvo de avaliação em 2019 (Comissão Europeia, 2019b), concluindo-se pela necessidade de alargamento dos setores e da harmonização de procedimentos entre EM, a par de uma evolução na abordagem da proteção de ativos específicos para o reforço da resiliência das EC que os operam (Comissão Europeia, 2020c, pp. 2).

Figura 11 - Âmbito da Estratégia da UE para a União da Segurança

Fonte: Comissão Europeia (2020b)

Conforme consta da Resolução legislativa P9_TA(2022)0394, de 22 de novembro (2022), da qual resultou a Diretiva REC, o acordo político sobre a proposta foi alcançado em 28 de junho de 2022, abrangendo 11 setores, e, das entidades da administração pública, foram excluídos os parlamentos, o poder judicial e os bancos centrais, bem como os setores da defesa e segurança pública.

Nos termos da Diretiva REC, os EM passam a identificar as EC, **adotam uma estratégia nacional** (artigo 4.º) e realizam avaliações de risco regulares (artigo 5.º), enquanto às EC cabe conduzir as suas avaliações de risco próprias (artigo 12.º), tomar medidas de resiliência (artigo 13.º), relatando incidentes e perturbações (artigo 15.º), prevendo-se também inspeções no local e sanções por incumprimento (artigos 21.º e 22.º).

A Diretiva REC, centrada na resiliência contra riscos físicos, foi apresentada em conjunto com a revisão da Diretiva de Segurança das Redes e da Informação (SRI2[20]), tendo por objetivo reforçar a ciber-resiliência, aplicável ao espectro ora alargado de EC identificadas na Diretiva REC (Voronova, 2022).

Destaca-se, ainda, o mecanismo de cooperação melhorado através da criação do Grupo para a Resiliência de Entidades Críticas (GREC), visando o intercâmbio de informações e boas práticas respeitantes à REC (artigo 19.º), bem como de recursos e soluções disponíveis, nomeadamente, os emergentes de projetos como o *SmartResilience* (*SmartResilience*, s.d.), a *Geospatial Risk and Resilience Assessment Platform* (GRRASP) (*GRRASP*, s.d.) ou a *European Risk & Resilience Assessment and Rating Initiative* (ERRA) (*ERRA*, s.d.).

As principais alterações introduzidas pela Diretiva REC sistematizam-se na Figura 12.

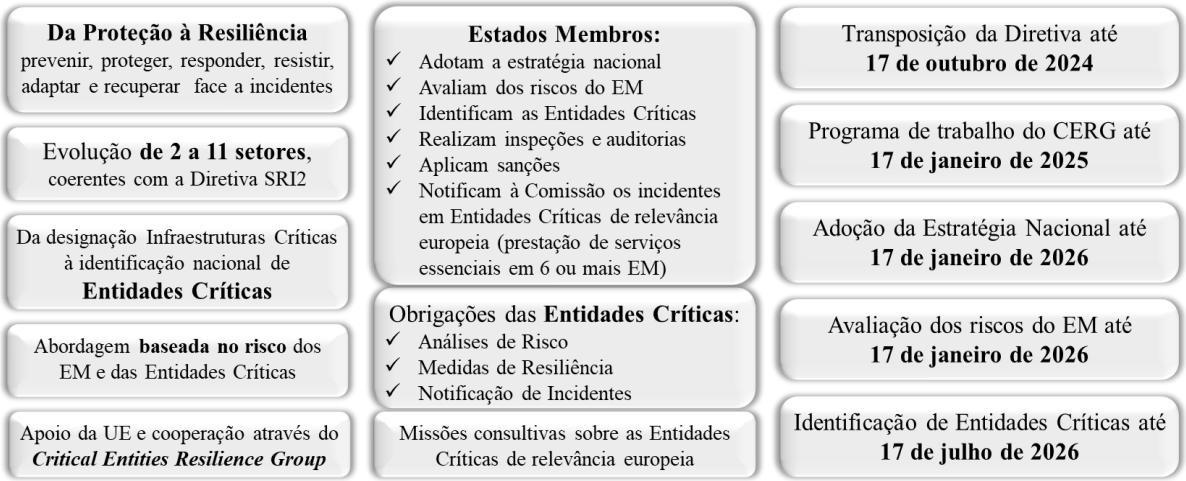

Figura 12 - Principais alterações introduzidas pela Diretiva REC

[20] O texto da Diretiva SRI2 (tradução do autor de *Network and Information Security Directive 2 – NIS2 Directive*) foi aprovada em 10 de novembro de 2022, enquanto o da Diretiva REC foi aprovado em 22 de novembro de 2022, pelo Parlamento Europeu.

2.2.3.2 Português

Ex vi da transição de paradigma da PIC para a REC, o Governo português antecipou-se, aprovando o Decreto-Lei n.º 20/2022, de 28 de janeiro[21], que, não obstante ainda se reportar "à consolidação no direito nacional da transposição da Diretiva 2008/114/CE", materialmente, visa "a identificação, designação, proteção e aumento da resiliência" das ICN e ICE. Neste diploma enfatiza-se a colaboração entre entidades, "através da partilha de informações relevantes à proteção e aumento da resiliência das infraestruturas críticas", nomeadamente, através da Plataforma de Registo de Informação de Infraestruturas Críticas (PRIIC)[22], além da inclusão de mais dez setores (total de 12) face ao anterior enquadramento do Decreto-lei 62/2011, de 09 de maio, que havia transposto a Diretiva 2008/114/CE, conforme cotejo do Quadro 3:

Quadro 3 - Evolução dos setores críticos conforme a legislação europeia e nacional

Diretiva 2008/114/CE (PIC)	Decreto-lei 62/2011, de 09 de maio	Decreto-lei 20/2022, de 28 de janeiro	Diretiva 2022/2557 (REC)
2 setores (mínimo)	**2 setores**	**12 setores**	**11 setores**
– Energia – Transportes	– Energia – Transportes	– Energia – Transportes	– Energia – Transportes
		– Saúde	– Saúde
		– Comunicações – Infraestruturas Digitais e prestadores de serviços digitais	– Infraestruturas digitais
		– Serviços financeiros	– Bancário – Infraestruturas do mercado financeiro
		– Abastecimento público de água e tratamento de resíduos	– Água potável – Águas residuais
		– Alimentação	– Produção, transformação e distribuição de produtos alimentares
		– Indústria	
		– Órgãos de Soberania e Governação	*Conforme. n.º 10) do artigo 2.º: "excluindo os tribunais, os parlamentos ou os bancos centrais"*
		– Segurança – Defesa	*Conforme. n.º 6 do artigo 1.º: "não se aplica às entidades da administração pública que exerçam as suas atividades nos domínios da segurança nacional, da segurança pública, da defesa ou da aplicação da lei"*
			– Administração Pública *(conforme definido pelos EM, excluindo segurança e defesa)*
			– Espaço

[21] Revogando o anterior Decreto-Lei n.º 62/2011, de 09 de maio (2011), através do qual foi transposta a Diretiva 2008/114/CE, de 08 de dezembro, no fito de estabelecer os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes, conforme disposições do seu artigo 1.º.

[22] Prevista no artigo 22.º do Decreto-Lei n.º 20/2022.

Não obstante, à data da investigação, vigoram, ainda, os efeitos práticos do Decreto-Lei n.º 62/2011, de 09 de maio (2011), pelo que, em Portugal, se mantém a identificação formal de 163 ICN, somente nos setores da energia e transportes. Nesta fase, as entidades setoriais[23] equacionam os critérios de criticidade e a lista de infraestruturas a propor ao Conselho Nacional de Planeamento Civil de Emergência (CNPCE)[24], *ex vi* dos artigos 6.º a 8.º do Decreto-Lei n.º 20/2022 (C. Costa; R. Mendes; R. Póvoa, entrevistas exploratórias, 10NOV2022; D. Gomes, entrevista exploratória, 10JAN2023).

Sintomático da relevância da temática no contexto nacional é o Programa do Governo 2022-2026, através do qual se define como uma das prioridades para proporcionar níveis mais elevados de segurança:

> […] Estabelecer um plano anual dirigido à preservação da segurança das infraestruturas críticas do Estado[25], em articulação com as estruturas homólogas do setor da Defesa Nacional, sob coordenação do Sistema de Segurança Interna e envolvendo o Sistema Nacional de Planeamento Civil de Emergência; […] (XXIII Governo Constitucional, 2022, pp. 62-63)

No plano da documentação estratégica nacional conexa, salienta-se que:

- Nos termos da Resolução de Conselho de Ministros (RCM) n.º 19/2013, de 05 de abril (2013), o Conceito Estratégico de Defesa Nacional (CEDN), enfatiza que "adquire grande acuidade a implementação de um Programa Nacional de Proteção das Infraestruturas Críticas" (PNPIC), no quadro da linha de ação estratégica "1.4.2 Responder às ameaças e riscos";
- De acordo com a RCM n.º 7-A/2015, de 20 de fevereiro (2015), a estratégia nacional de combate ao terrorismo (ENCT) visa detetar, prevenir, proteger, perseguir e responder ao combate ao terrorismo, nomeadamente, através do desenvolvimento do "plano de ação para a proteção de aumento da resiliência das IC nacionais e europeias" (PAPARIC);

[23] Conforme Anexo ao Decreto-lei n.º 20/2022, são entidades setoriais as Comissões Nacionais de Emergência da: Energia; Transportes terrestres; Transporte Aéreo; Transporte Marítimo; Comunicações; Cibersegurança; Água e Resíduos; Agricultura e Alimentação; Saúde; Secretaria-Geral da Economia; Banco de Portugal; Comissão do Mercado de Valores Mobiliários (CMVM); Autoridade de Supervisão de Seguros e Fundos de Pensões (ASSFP); SG-SSI; Direção-Geral de Recursos da Defesa Nacional (DGRDN); e Estado-Maior General das Forças Armadas (EMGFA).

[24] Cujas atribuições, composição e articulação decorrem do Decreto-Lei n.º 43/2020, de 21 de julho (2020).

[25] É de considerar, supletivamente, o Decreto-Lei n.º 138/2014, de 25 de setembro (2014), respeitante ao regime de salvaguarda de ativos estratégicos essenciais para garantir a defesa e segurança nacional e a segurança do aprovisionamento do País em serviços fundamentais para o interesse nacional, nas áreas da energia, dos transportes e comunicações, enquanto interesses fundamentais de segurança pública.

- Conforme a RCM n.º 92/2019, de 05 de junho (2019), a estratégia nacional de segurança do ciberespaço (ENSC) visa, entre outros propósitos, "garantir a segurança do ciberespaço, (..) incluindo ações de cibersabotagem destinadas a atingir infraestruturas críticas e a provocar a disrupção de serviços essenciais para o regular funcionamento da sociedade", constituindo-se como Autoridade Nacional de Cibersegurança;
- Através da RCM n.º 112/2021, de 11 de agosto (2021) foi aprovada a estratégia nacional para uma Proteção Civil preventiva 2030 (ENPCP2030) enfatizando a vertente preventiva e a gestão do risco face a riscos de origem natural, tecnológica ou mista, através da qual são definidos cinco objetivos estratégicos, dez áreas prioritárias e um plano de ação com 136 objetivos operacionais, incluindo a respetiva calendarização e a entidade coordenadora, cuja ampla maioria tem relação, mais ou menos direta, com os preceitos intrínsecos à REC, sempre na vertente *safety*; e que
- A Lei n.º 24-C/2022, de 30 de dezembro (2022), que aprova as Grandes Opções para 2022-2026 (GO2022-2026), apesar de não acautelar a imperatividade de dispor de uma estratégia nacional para a REC[26], sublinha a importância de melhorar as infraestruturas (energéticas, de transportes; digitais; saúde, militares, e das forças de segurança), bem como de promover a resiliência (energética, económica, dos serviços públicos, das respostas sociais, dos sistemas e infraestruturas digitais, da saúde, face a alterações climáticas, a catástrofes, dos recursos hídricos, ou dos sistemas de abastecimento).

No plano institucional, face à crescente complexidade, interdependências e conectividade física e digital, a contínua sinergia de esforços entre entidades críticas e os atores públicos com responsabilidade nos domínios *security*, *safety* e *cyber*, torna-se cada vez mais fundamental para garantir a resiliência sistémica, contexto em que as Forças e Serviços de Segurança (FSS), os Agentes de Proteção Civil (APC) e o Centro Nacional de Cibersegurança (CNCS) assumem papéis essenciais para a REC em Portugal e cujos esforços são coordenados através do Sistema de Segurança Interna (SSI) (Buss et al., 2021; Martinho, 2017; Pereira, 2022).

[26] Conforme se extrai do quadro 7 da Lei n.º 24-C/2022, de 30 de dezembro, respeitante aos instrumentos de planeamento e de políticas públicas associadas ao desafio estratégico transversal «Boa governação».

O SSI, criado através da Lei de Segurança Interna[27] (LSI), constitui-se como um "sistema de geometria variável" que integra e promove a coordenação dos organismos com responsabilidades securitárias, nomeadamente as FSS, APC, e CNCS, através dos seus três órgãos: Conselho Superior de Segurança Interna (CSSI); Secretário-Geral (SG-SSI); e Gabinete Coordenador de Segurança (GCS) (Letras, 2022), cuja organização se ilustra através da Figura 13.

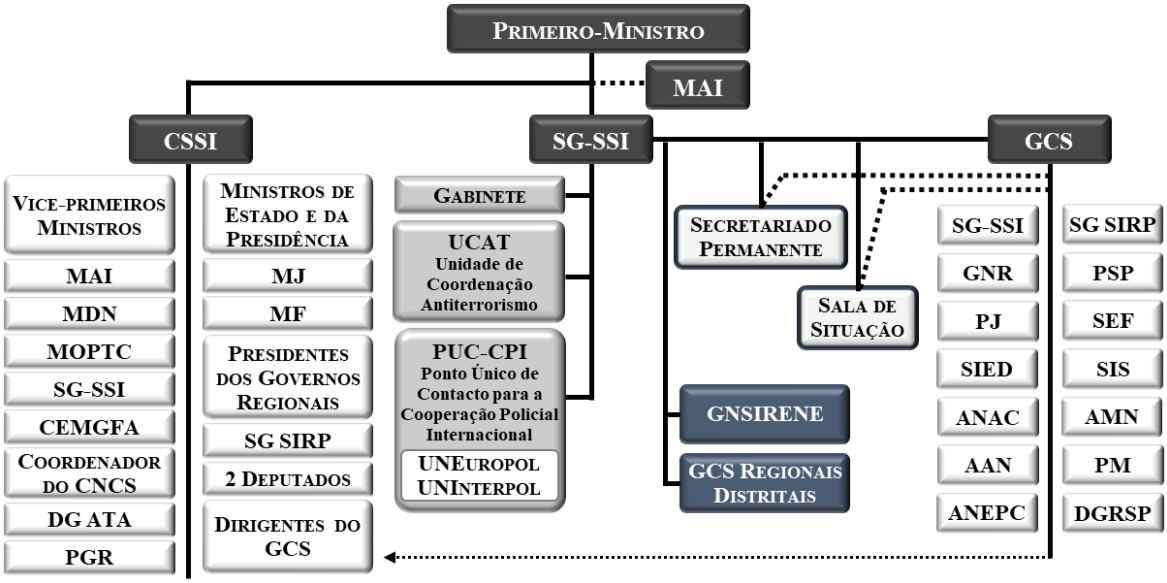

Figura 13 - Organização do SSI

Fonte: adaptado e atualizado a partir de Letras (2022, p. Apd C-3).

O SG-SSI constitui-se na entidade agregadora da segurança nacional, que se encontra:

> […] num plano político facilitador da comunicação e articulação entre a definição dos objetivos estratégicos da Segurança Interna (SI), estratégia total na esfera de responsabilidade do Primeiro-Ministro, e a sua materialização na estratégia setorial, ao nível dos Ministérios e, ainda, elemento essencial na coordenação e colaboração próxima dos dirigentes máximos das FSS, no âmbito da estratégia operacional. Acrescendo também, constituir-se como elemento simplificador da comunicação e articulação com os demais Subsistemas das diferentes tutelas políticas, designadamente, justiça, defesa e proteção civil, além da sua intervenção ao nível da cooperação e coordenação policial europeia e internacional, nas diferentes plataformas e âmbitos, designada de dimensão externa da SI. (Letras, 2022, p. 20)

[27] Aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua atual redação decorrente da Lei n.º 59/2015, de 24 de junho (2015).

O SG-SSI tutela a temática da securitização de IC em Portugal, nos termos do Decreto-Lei n.º 20/2022[28], cabendo-lhe, nomeadamente, emanar orientações (n.º 3 do artigo 13.º), coordenar a partilha de informação e garantir o acesso às melhores práticas e metodologias disponíveis (n.º 3 e n.º 4 do artigo 17.º), avaliar ameaças (artigo 19.º), proceder a verificações de segurança (artigo 20.º), promover a realização de exercícios (artigo 21.º), criar e atualizar a plataforma de registo de informação de infraestruturas críticas (PRIIC) (artigo 22.º), fiscalizar o cumprimento das normas e aplicar eventuais coimas por contraordenação (artigos 23.º e 24.º), garantir a comunicação com a Comissão Europeia nas matérias relativas à segurança, proteção e resiliência de IC (n.º 2 do artigo 19.º e artigo 26.º), bem como a aprovação dos planos de segurança (artigo 14.º), em articulação com as Forças de Segurança (FS) territorialmente competentes, a Autoridade Nacional de Emergência e Proteção Civil (ANEPC), o CNCS, e as entidades setoriais, conforme se sistematiza através da Figura 13:

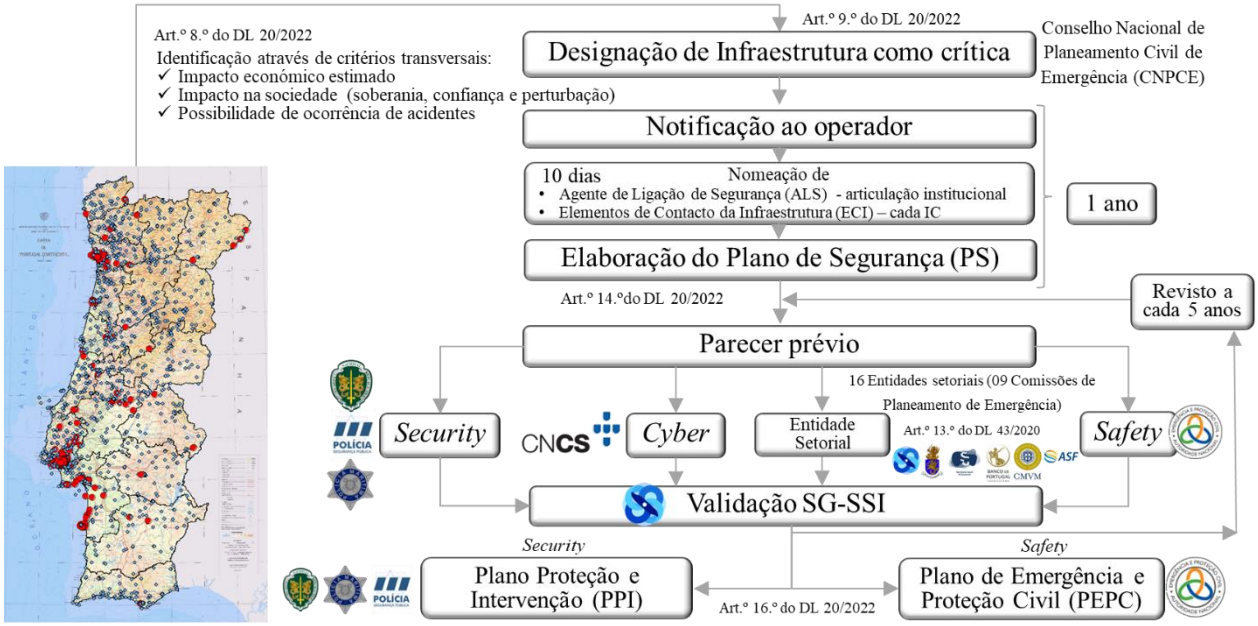

Figura 14 - Articulação para aprovação de planos de segurança de IC

Fonte: Autor, como base no Decreto-Lei n.º 20/2022, de 28 de janeiro (2022).

Em matéria de informações, além das geradas pelas FS territorialmente responsáveis, particularmente pela Guarda Nacional Republicana (GNR), Polícia de Segurança Pública (PSP) e Polícia Marítima (PM), o Serviço de Informações de Segurança (SIS) e o Serviço de Informações Estratégicas de Defesa (SIED), nos termos das respetivas atribuições[29], contribuem para monitorizar potenciais ameaças a IC, destacando-se o programa *Kritica* do SIS, executado em apoio às EC desde 2013 (SIS, s.d.; Martinho, 2017, pp. 36–37).

[28] Mantendo a linha das anteriores disposições do Decreto-lei 62/2011, de 09 de maio.
[29] Conforme n.º 3 do artigo 3.º da Lei n.º 50/2014, de 13 de agosto (2014), alterando a Lei n.º 9/2007, de 19 de fevereiro.

Por outro lado, também a Autoridade Nacional de Segurança (ANS) tem atribuições em matéria de segurança a IC, enquanto órgão responsável pela credenciação "de entidades públicas e privadas para o exercício de atividades industriais, tecnológicas e de investigação, quando tal seja exigido por disposição legal ou regulamentar"[30].

Quanto à análise de riscos, esta é desenvolvida de forma segmentada, destacando-se três documentos: (i) os Relatórios Anuais de Segurança Interna (RASI), que caracterizam as ameaças globais à segurança interna, enfatizando eminentemente o prisma *security* (SSI, 2022; 2021); (ii) no âmbito *safety*, a ANEPC publicou a Avaliação Nacional de Risco (ANR) em 2014 e a atualização em 2019, abrangendo 23 riscos, 11 dos quais de origem natural e os restantes tecnológicos (ANPC, 2019); e (iii) no plano *cyber*, o CNCS divulga, anualmente, o Relatório Cibersegurança em Portugal (RCP), cuja terceira edição foi publicada em junho de 2022, incluindo análise prospetiva de ameaças (CNCS, 2022).

Além da complexidade decorrente das múltiplas referências e atribuições em matéria de IC dispersas pela legislação nacional, Pestana (2016, p. 34-36; 54-62) salienta, também, a inexistência de recursos humanos dedicados à temática[31] e a carência de um organismo interministerial que exerça o planeamento e a coordenação eficazes, de forma transversal às diversas tutelas setoriais, pelo que propõe a elaboração de um documento aglutinador (plano ou estratégia) que permita a clarificação e a estabilização do panorama jurídico.

As estratégias e legislação, europeias e nacionais, têm alavancado os desenvolvimentos na temática, verificando-se, porém, a necessidade de harmonização do quadro normativo nacional, em consonância com os novos preceitos da Diretiva REC, conforme se sistematiza no **Apêndice D.**

Finalmente, é de sublinhar que, face às transformações em curso ao nível da UE sobre a temática, o SG-SSI anunciou em 22 de novembro de 2022 a criação de uma "pequena unidade especializada", na sua dependência direta, para alavancar a coordenação da REC (P. Pinheiro, Conferência do Observatório de Segurança, Criminalidade Organizada e Terrorismo [OSCOT], 22NOV2022).

Considera-se, assim, respondida a **QD2**.

[30] Conforme alínea i) do n.º 2 do artigo 2.º do Decreto-Lei n.º 3/2012, de 16 de janeiro (2012).
[31] Caso único na UE, conforme acerva o autor.

3. Metodologia e método

3.1 Metodologia

Na esteira de Creswell & Creswell (2018, p.41) e Santos e Lima (2019, p. 36), o desenho da pesquisa assentou num estudo de caso único, concretamente o de Portugal e as respetivas idiossincrasias intrínsecas à temática da REC.

Seguiu-se um raciocínio indutivo, na procura de contributos para um arquétipo, e uma estratégia de investigação qualitativa (Santos & Lima, 2019, p. 18), sustentada na hermenêutica, face ao desiderato de compreender dinâmicas complexas, num estudo holístico de uma realidade hodierna, triangulando diferentes perspetivas e dados, no intuito de estabelecer um conjunto de factos baseado na convergência de fontes de referência (Yin, 2018, p.18).

A estrutura, bem como o percurso metodológico desenvolvido em duas fases, subsumem-se às normas vigentes no Instituto Universitário Militar (2020a, 2020b).

A primeira fase, de natureza exploratória, atinente ao enquadramento e delimitação, concorreu para a definição do objeto de estudo e subsequente revisão preliminar da literatura, assim como do quadro normativo relevante. Foram analisadas as fontes primárias e secundárias de referência, que permitiram a aproximação à base conceptual e ao estado da arte, auxiliando na definição do OG e respetivos OE, bem como da QC e das quatro QD em que se estrutura a investigação.

Visando obter uma perspetiva atual sobre as dinâmicas inerentes à problemática, recorreu-se, ainda, à realização de entrevistas abertas e exploratórias a oficiais da GNR que diariamente a trabalham, nos níveis estratégico e operacional, conforme Quadro 4.

Quadro 4 – Entrevistas exploratórias

POSTO	NOME	FUNÇÃO	DATA
Coronel	Carlos Soares da Costa	Diretor de Informações da GNR	10NOV22
Major	David Gomes	Coordenador Setorial do CNPCE na ANEPC	Várias – NOV22 a MAR23
Major	Rui Póvoa	Chefe da Repartição de Segurança da DI/GNR	10NOV22
Major	Ricardo Mendes	Oficial de Ligação no SSI	10NOV22

Na segunda fase operacionalizou-se o modelo de análise preconizado (*vide* **Apêndice E**), à luz dos conceitos estabelecidos, recolhendo, interpretando e consolidando os conhecimentos obtidos durante a revisão bibliográfica.

A investigação sustentou-se na pesquisa bibliográfica e análise documental, assim como na recolha de dados e informações, conjugando valores conhecidos e articulados, com o conhecimento e a experiência proveniente das entrevistas, no intuito de obter simultaneamente a verificação e aprofundamento dos dados (Santos & Lima, 2019, p. 102).

3.2 Método

3.2.1 Participantes e procedimentos

Considerando a natureza do estudo e a arquitetura de segurança nacional, entrevistaram-se peritos (*experts*) e pessoas em posições-chave (*elite interviewing*), no fito de percecionar as suas visões e conhecimentos privilegiados (Litting, 2009; O'Sullivan et al., 2017, p. 189; Richards, 1996; Van Audenhove & Donders, 2019).

Paralelamente, as entrevistas visaram a validação da pré-análise prospetiva realizada com recurso à análise SWOT dinâmica constante do subcapítulo 4.3, consolidando o escrutínio desenvolvido, num processo dinâmico de construção.

Face à panóplia de entrevistados, seus conhecimentos, experiência e funções desempenhadas no quadro da temática, confere-se a imprescindível visão holística à investigação, congregando diferentes prismas, conforme sistematizado no Quadro 5.

Quadro 5 – Entrevistas

E	Nome	Função	Prismas	Data/meio
E1	Gabinete do Embaixador Paulo Viseu Pinheiro*	– SG-SSI	– Nível político-estratégico	25MAR23 E-mail
E2	Tenente-general José Manuel Lopes dos Santos Correia	– Comandante-Geral da GNR	– *Security* – Militar / Policial – Nível Operacional – FSS (SSI)	19MAR23 E-mail
E3	Dra. Isabel Pais	– Chefe da Delegação Nacional ao PROCIV-CER do Conselho da UE – Secretária da Subcomissão da Plataforma Nacional para a Redução do Risco de Catástrofes (UNDRR)	– *Safety* – UE – Nível operacional – ANEPC (SSI) – Académico	05ABR23 Presencial
E4	Dra. Isabel Baptista	– Coordenadora do Departamento de Desenvolvimento e Inovação do CNCS	– *Cyber* – Nível operacional – CNCS (CSSI)	12ABR23 MSTeams
E5	Dr. Manuel Gonçalves	– Técnico Coordenador de Informações Coordenador do programa Kritica do SIS	– Sistema de informações	11MAR23 E-mail
E6	Eng. Manuela Seixas Fonseca	– Comissão de Planeamento de Emergência da Energia – Direção Geral de Energia e Geologia (DGEG) – Diretora de Serviços de Planeamento Energético e Estatística	– Setor da Energia – Entidade setorial	21MAR23 MSTeams
E7	Eng. Leonel Salvado	– Agente de Ligação de Segurança da NAV Portugal	– Setor dos Transportes – Entidade Crítica – Académico	21MAR23 E-mail
E8	Eng. José Alegria	– *Chief Security Officer* & *Chief Information Security Officer* do Grupo Altice; – Assessor, *European Cybercrime Centre* (EC3) da EUROPOL	– Setor das infraestruturas digitais – Entidade Crítica – *Cyber*	17MAR23 MSTeams
E9	Eng. Maria Luísa Sousa	– Laboratório Nacional de Engenharia Civil (LNEC)	– I&D	27MAR23 E-mail
E10	José Luís Perez Pajuero	– Diretor do CNPIC de Espanha	– Externo (internacional)	13MAR23 E-mail

*Nota: por indicação do Exmo. SG-SSI, a entrevista foi concedida pelo seu Gabinete.

Através desta amostragem não-probabilística intencional (Vilelas, 2009, p. 248), colheram-se as múltiplas perspetivas envolvidas no estudo, aos níveis político-estratégico e operacional da arquitetura de segurança nacional, maximizando a recolha das visões dos setores de IC mais representativos[32], bem como a abordagem aos prismas securitários: *security*, *safety* e *cyber*, assim como os domínios público e privado.

3.2.2 Instrumentos de recolha e tratamento de dados

Recorreu-se à observação não-estruturada, à análise documental e a entrevistas semiestruturadas (Santos & Lima, 2019, p. 29; p. 73-74; p. 102-103).

As entrevistas tiveram por base um guião previamente remetido (**Apêndice F**), com sete perguntas[33], em consonância com o modelo de análise definido.

A aplicação das entrevistas decorreu entre 04 de março e 12 de abril de 2023, presencialmente ou *online*, através da plataforma *Microsoft Teams*® e/ou por correio eletrónico[34], consoante a conveniência para cada um dos entrevistados.

Na esteira de Bardin (2020, pp. 121–154), executou-se uma análise temática ou categorial ao conteúdo das entrevistas, em três fases: organização da análise; codificação; e categorização. Através de uma leitura flutuante, realizou-se uma pré-análise e exploração dos conteúdos[35]. Considerando a problemática, estabeleceram-se as unidades de registo (UR), salientando os segmentos de resposta e os «temas» da categorização, *in casu*, pré-alinhados pelo guião de entrevista. Finalmente, na enumeração, foi registada a *presença* em razão do critério do *léxico*.

O tratamento dos dados obtidos resultou na elaboração dos quadros 6 a 9 constantes do capítulo seguinte que, seguindo o guião estruturado de acordo com as dimensões e variáveis em análise, permitiram sistematizar e gradualmente consolidar ideias sobre as prioridades a considerar na formulação da Estratégia Nacional para a REC.

[32] A conjugação dos setores da energia, transportes e comunicações correspondem a mais de metade do total de IC em Portugal, segundo dados de trabalho da ANEPC (D. Gomes, entrevista exploratória, 20JAN2023).
[33] A pergunta n.º 7 visou obter sugestões ou comentários adicionais associados à problemática que não tivessem sido abordados aquando das anteriores respostas, razão pela qual os dados obtidos foram paulatinamente integrados nas partes relevantes das anteriores respostas, não tendo originado uma codificação isolada.
[34] As respostas prestadas por *e-mail* foram consolidadas telefonicamente.
[35] Através da ligação constante do **Apêndice G** viabiliza-se o acesso aos conteúdos das entrevistas, agrupados por respostas.

4. Formulação de uma Estratégia para a Resiliência de Entidades Críticas

Neste capítulo apresentam-se os dados e discutem-se os resultados do estudo de caso aplicado, consolidando a revisão da literatura com o conhecimento adveniente das entrevistas realizadas, visando responder à **QD3** e à **QD4**.

4.1 Avaliação do ambiente estratégico

No contexto nacional vigente no início de 2023, respeitante ao período da investigação, salientam-se, de seguida, os principais fatores do ambiente estratégico português para a REC, nos planos exógeno e endógeno, cuja apreciação foi maturada através do conhecimento transmitido pelos atores do sistema, contribuindo, ulteriormente, para a consolidação da análise SWOT dinâmica constante do subcapítulo 4.3.

4.1.1 Ambiente exógeno – ameaças e oportunidades

A caracterização do ambiente estratégico exógeno apresenta-se em linha com os resultados da análise de conteúdo às entrevistas, conforme sistematizados no Quadro 6.

Quadro 6 – Ambiente exógeno – UR das entrevistas

Cod.	Segmento e Unidade de Registo (UR)	Entrevistados										Resultados	
		1	2	3	4	5	6	7	8	9	10	∑ UR	%
Ambiente Exógeno – Ameaças e Oportunidades													
1.1 Ameaças													
1.1.1	Ciberataques (*e.g.* cibercriminalidade, hacktivismo)	X	X	X	X	X	X	X	X	X	X	10	100%
1.1.2	Conflitualidade económica e social (*e.g.* ecoactivismo)	X	X	X		X	X	X	X		X	8	80%
1.1.3	Terrorismo	X	X	X		X	X		X	X	X	8	80%
1.1.4	Espionagem, sabotagem ou ingerência		X		X	X	X		X	X	X	7	70%
1.1.5	Naturais (*e.g.* sismos, eventos climáticos extremos)	X		X			X			X		4	40%
1.1.6	Criminalidade organizada				X			X	X		X	4	40%
1.1.7	Ameaça interna (maioritariamente negligente)				X		X		X			3	30%
1.1.8	Acidentais (*e.g.* avarias técnicas, acidentes, incêndios)			X						X		2	20%
1.2 Oportunidades													
1.2.1	Transposição da Diretiva REC permite reequacionar o quadro normativo e a arquitetura institucional	X	X	X	X	X	X	X	X		X	9	90%
1.2.2	Incremento da cooperação entre *stakeholders*	X		X	X	X	X		X	X		7	70%
1.2.3	Maior partilha de informação, boas práticas e exercícios	X		X	X	X	X		X	X		7	70%
1.2.4	Criação de organismos focados na REC (UE e/ou nacional)		X	X		X	X		X		X	6	60%
1.2.5	Sinergias da convergência e uniformização na UE	X		X	X		X				X	5	50%
1.2.6	Sensibilização para a problemática (*e.g.* Guerra na Ucrânia)		X	X	X					X	X	5	50%
1.2.7	Estudo das interdependências em prol da resiliência			X		X		X		X		4	40%
1.2.8	Fundos para projetos visando a REC				X						X	2	20%

Em consonância com as principais ameaças enfatizadas, no contexto da exponencial digitalização e crescente interligação transfronteiriça, salienta-se a preponderância que o domínio cibernético vem adquirindo como principal vetor de ameaças às IC. Importa sublinhar que, mesmo as ameaças deliberadas mais prementes, como é o caso do terrorismo, espionagem, sabotagem, ingerência ou criminalidade organizada, podem ser perpetradas

pela via cibernética, razão pela qual é particularmente pertinente a harmonia entre a Diretiva REC e a Diretiva SRI2, a preservar aquando da sua transposição para o ordenamento interno.

Também de realçar que, entre as ameaças naturais, se verifica a crescente tendência para a ocorrência de fenómenos meteorológicos extremos associados às alterações climáticas, bem como a ocorrência de sismos, sendo crucial aplicar soluções de engenharia adequadas logo na projeção de IC, em linha com o princípio *"security by design"* (E3 e E9).

Não obstante, importa garantir a abordagem *all-hazards* à securitização das IC, com a cada vez mais importante integração de todos os riscos, em detrimento de visões segmentadas (E1, E2, E5, E6, E9).

Quanto a oportunidades, destaca-se a perspetiva transversal de que a atual conjuntura é fértil à introdução de melhorias na arquitetura nacional de segurança, resultante do novo paradigma suscitado pela Diretiva REC e a sua subsequente transposição, permitindo reequacionar soluções do quadro normativo e institucional, em prol da criação e/ou aprofundamento de canais de cooperação, partilha de informação e de boas-práticas, nomeadamente as decorrentes de mais exercícios conjuntos (E1,E3, E5, E6 e E8).

Com efeito, o contexto de transformação e convergência no seio da UE permite alavancar sinergias, sendo a criação de organismos focados na REC, como o GREC, ao nível da UE, bem como a possível criação de um organismo agregador dedicado às IC, em Portugal, percecionados como oportunidades para a desejável melhoria (E3, E6 e E10).

Destaca-se, ainda, que a mudança em curso poderá alavancar o cabal estudo das (inter)dependências, beneficiando a resiliência do sistema (E3, E5, E7, E9).

4.1.2 Ambiente endógeno – vulnerabilidades e potencialidades

A análise ao ambiente estratégico endógeno apresenta-se em consonância com os resultados organizados no Quadro 7.

Quadro 7 – Ambiente endógeno – UR das entrevistas

Cod.	Segmento e Unidade de Registo (UR)	Entrevistados										Resultados	
		1	2	3	4	5	6	7	8	9	10	∑ UR	%
Ambiente Endógeno – Vulnerabilidades e Potencialidades													
2.1 Vulnerabilidades													
2.1.1	Parca cultura de segurança e formação	X		X	X	X	X	X	X	X		8	80%
2.1.2	Complexidade na articulação/competências das entidades	X	X	X	X		X	X			X	7	70%
2.1.3	Falta de estratégia e/ou ineficiência das disposições legais			X	X		X	X	X		X	6	60%
2.1.4	Inexistência de organismo agregador dedicado às IC	X	X	X	X			X				5	50%
2.1.5	Controlo de cadeias de abastecimento por outros países			X	X	X	X				X	5	50%
2.1.6	Resistência à partilha de informação e colaboração		X			X	X				X	4	40%
2.1.7	Escassa sensibilidade social e política para a problemática	X		X				X		X		4	40%
2.1.8	Crescentes interdependências pouco estudadas e vulneráveis			X	X	X		X				4	40%
2.1.9	Elevado número de IC (método de designação inadequado)		X			X						2	20%
2.1.10	Constrangimentos legais (RGPD, *vettings* de segurança, etc.)						X		X			2	20%

2.2 Potencialidades												
2.2.1	Aproveitar o conhecimento de entidades especializadas			**X**	**X**	**X**	**X**		**X**	**X**		**6**	**60%**
2.2.2	Panorama securitário nacional estável e favorável		**X**	**X**	**X**		**X**	**X**				**5**	**50%**
2.2.3	Transformação tendo por base a experiência de outros EM	**X**		**X**	**X**						**X**	**4**	**40%**
2.2.4	Existência de *fora* de partilha de conhecimento e informação		**X**	**X**	**X**	**X**						**4**	**40%**
2.2.5	Crescente preocupação com a temática		**X**	**X**	**X**						**X**	**4**	**40%**
2.2.6	Cooperação internacional e/ou académica (*e.g.* I&D)			**X**	**X**		**X**				**X**	**4**	**40%**
2.2.7	Lições do anterior enquadramento normativo	**X**						**X**			**X**	**3**	**30%**
2.2.8	Fácil operacionalização de um organismo agregador, tendo por base as estruturas do SSI e CNPCE	**X**		**X**								**2**	**20%**

No que concerne a vulnerabilidades nacionais, realça-se a parca formação e cultura de segurança, associada à escassa sensibilidade social e, sobretudo, política para a problemática, efusivamente sublinhada por parte dos 40% de entrevistados que a destacam. A este contexto associa-se a dispersão e complexidade do quadro normativo e institucional, além da inexistência de uma estratégia nacional que sirva de referência orientadora. O cenário é sintomático da limitada governança na securitização de IC, agravado por resistências à partilha de informação e colaboração, sobretudo no plano intersetorial, tornando-se alvo de crítica a falta de um organismo agregador dedicado à temática, especialmente perante um panorama de crescentes interdependências, pouco estudadas e vulneráveis.

Negativamente, salienta-se, também, a crescente dependência de cadeias de abastecimento controladas por entidades externas, a incoerente e excessiva identificação de IC à luz da anterior metodologia aplicada aos setores da energia e transportes, bem como as limitações legais à implementação de medidas de segurança mais eficazes e os constrangimentos no oportuno acesso a informação crucial, nomeadamente no que respeita a dados que facilitam a mitigação de ameaças, particularmente as internas.

Em antagonismo, destaca-se, como potencialidade nacional, a cabal rentabilização do saber detido por entidades com forte cultura de segurança, porquanto o conhecimento existe, embora seja pouco aproveitado face à escassa sensibilidade dominante (E3, E5, E6, E8), a qual, axiomaticamente, advém da histórica estabilidade contextual em termos securitários.

Face ao atual contexto de transformação, em que se verifica a crescente preocupação com a temática, realça-se, também, o potencial aproveitamento das lições resultantes do anterior quadro normativo, da experiência de outros EM, bem como da cooperação internacional e do envolvimento do meio académico como aspetos a rentabilizar.

Finalmente, sublinha-se o potencial intrínseco à existência de *fora* de partilha de conhecimento e informação (*e.g.* PEPIC e PNRRC) e à operacionalização de um organismo agregador, a edificar a partir dos atuais recursos do SSI e CNPCE.

Face à panóplia de fatores estratégicos expostos, considera-se respondida a **QD3**.

4.2 Perceções sobre as prioridades estratégicas

4.2.1 Problemas críticos, potenciais promissores e medidas prioritárias

Na esteira do método estratégico sustentado por Ribeiro (2008, pp. 21-27; 2017a, pp. 41-47), partindo da turbulência do ambiente, é na ponderação sobre a superação de problemas e exploração de eventualidades que reside o âmago da formulação estratégica. Assim, apelando à correlação de fatores, colheram-se as perceções dos atores sobre os aspetos prioritários a ponderar na formulação da estratégia, aglutinando os diversos prismas envolvidos, por forma a responder à **QD4**. Os resultados sistematizam-se no Quadro 8.

Quadro 8 – Prioridades estratégicas – UR das entrevistas

Cod.	Segmento e Unidade de Registo (UR)	Entrevistados										Resultados	
		1	2	3	4	5	6	7	8	9	10	∑ seg.	%
3 Problemas críticos													
3.1	Reduzida cultura de segurança	X		X	X	X	X	X	X	X		8	80%
3.2	Capacidades face às crescentes ameaças cibernéticas	X	X		X		X		X		X	6	60%
3.3	Poder limitado para coordenar a partilha de informações e assegurar a aplicação de medidas determinadas às IC	X	X				X	X			X	5	50%
3.4	Inexistência de organismo agregador dedicado às IC		X	X	X		X	X				5	50%
3.5	Desconhecimento das interdependências				X	X	X	X				4	40%
3.6	Escassa cooperação intersectorial e internacional			X		X	X					3	30%
3.7	Inexistência de uma estratégia nacional			X	X			X				3	30%
3.8	Controlo de cadeias de abastecimento por outros países				X	X	X					3	30%
3.9	Inexistência de sistemas de alerta precoce e testes sistemáticos de vulnerabilidades				X				X	X		3	30%
3.10	Falta de formação e treinos sistemáticos				X				X	X		3	30%
3.11	Arquitetura complexa e burocrática			X				X				2	20%
3.12	Excessivo número de IC					X						1	10%
3.13	Crescente ameaça terrorista e instabilidade económica										X	1	10%
4 Potenciais promissores													
4.1	Criação de organismo agregador dedicado às IC permite melhorar processos, colaboração e partilha de boas práticas	X	X	X	X	X	X	X	X	X	X	10	100%
4.2	Convergência e maior cooperação no seio da UE	X	X	X	X		X		X	X	X	8	80%
4.3	Diretiva REC criou contexto para implementação de melhorias e o panorama securitário nacional é favorável		X	X	X	X	X	X		X	X	8	80%
4.4	Reformular a *governance* tendo por base uma Estratégia Nacional			X	X		X	X	X		X	6	60%
4.5	Formar e reter especialistas na securitização de IC			X	X				X		X	4	40%
4.6	Uso de novas tecnologias para proteção e alerta precoce		X	X					X			3	30%
4.7	Aprender com os melhores exemplos internacionais			X	X	X						3	30%
4.8	Fundos para projetos visando a REC				X						X	2	20%
5 Medidas prioritárias													
5.1	Criação de organismo agregador dedicado às IC	X	X	X	X	X	X	X		X	X	9	90%
5.2	Criar formação universitária para a gestão de riscos e securitização de IC			X	X		X		X	X	X	6	60%
5.3	Implementar mecanismo de intercambio de informações	X			X		X	X		X		5	50%
5.4	Estabelecer e/ou incentivar a adesão a normas internacionais						X	X	X	X	X	5	50%
5.5	Fomentar sensibilização (política e sociedade em geral)			X	X		X		X	X		5	50%
5.6	Formação comum a todas as EC (*e.g.* CSPI da GNR)		X				X				X	3	30%
5.7	Estratégia nacional e harmonização de normas (*governance*)			X	X						X	3	30%
5.8	Criar *ratings* de segurança de entidades (*e.g.* cibersegurança)				X				X			2	20%
5.9	*Upskilling* e *reskilling* de pessoas para a cibersegurança				X				X			2	20%
5.10	Fomentar colaboração e exercícios conjuntos				X					X		2	20%
5.11	Reconhecer infraestruturas hipercríticas								X			1	10%

Como problemas críticos, os entrevistados reiteram a parca cultura de segurança, bem como um conjunto de disfunções na governança da temática, entre as quais a incapacidade de coordenar atividades, suscitar a partilha de informações e promover a colaboração (sobretudo intersetorial), de assegurar a aplicação de medidas determinadas às IC e de apoiar tempestivamente a resposta a incidentes (nomeadamente no âmbito cibernético [E8]).

Sublinha-se, ainda, o desconhecimento das interdependências, a carência de testes sistemáticos de vulnerabilidades e de exercícios conjuntos, a falta de formação, a inexistência de sistemas de alerta precoce e a dependência de cadeias de abastecimento.

Estes problemas espelham a ausência de uma estratégia nacional e de um organismo agregador. Refletem, também, a complexidade e ineficiência da atual arquitetura, agravada pela segmentação e dispersão normativa. Trata-se, enfim, de um cenário contra-indicado que, no contexto da transposição da Diretiva REC, pode beneficiar de uma transformação substancial (E1, E2, E3, E5, E6, E7, E8 e E10).

No espectro da exploração de eventualidades, destaca-se a perceção inequívoca de que urge criar um organismo aglutinador dedicado (*e.g.* agência ou centro nacional), num patamar transversal às diversas áreas governativas, que promova sinergias, o planeamento integrado, a coordenação geral das atividades atinentes à resiliência sistémica e se constitua como ponto único de intercâmbio com os demais EM e instâncias europeias.

Face ao contexto de convergência e maior cooperação europeia, tirando partido da conjuntura estável, importa reformular a arquitetura nacional e a respetiva governança, tendo por base uma estratégia nacional e colhendo lições das melhores soluções implementadas por outros países de referência na temática. Considera-se fundamental aprofundar os mecanismos de cooperação, exercícios conjuntos, monitorização e sistemática testagem de vulnerabilidades, com a eventual instituição de *ratings*, que fomentem a consciencialização dos decisores, bem como o intercâmbio de informações, pelo que a operacionalização da PRIIC e de outras soluções promotoras da integração é essencial, a par do emprego de novas tecnologias para proteção e alerta precoce, preferencialmente de implementação conjunta e abrangente, idealmente com o apoio de fundos para projetos visando a REC.

Além da sensibilização geral da população, considera-se importante apostar na formação e retenção de especialistas na securitização de IC, nomeadamente através da criação de formação universitária específica, com forte pendor na gestão de riscos. Também é de considerar a formação conjunta entre elementos de segurança da EC, como é o caso do CSPI, no âmbito da qual é promovida a visão holística, métodos e técnicas comuns, o

networking e a realização de exercícios. Face à crescente carência de especialistas em cibersegurança, é de promover programas para o *upskilling* e *reskilling* de pessoas, bem como a constituição de uma *Computer Security Incident Response Team* (CSIRT) nacional, dedicada às EC e, idealmente, ainda, um observatório de *Chief Information Security Officers* (CISO) de referência, que pudesse contribuir para a *governance* da cibersegurança (E8).

Finalmente, "se tudo é crítico, nada é crítico" (P. Pinheiro, Conferência do OSCOT, 22NOV2022). Logo, é de ponderar a hierarquização da criticidade de IC, reconhecendo as "hipercríticas" (E8) ou a definição de critérios de identificação mais seletivos, visando reduzir a quantidade de IC (E5).

4.2.2 Objetivos e vetores estratégicos

Apontando à consolidação dos dados, colheram-se ainda as perceções dos diversos atores quanto aos objetivos e vetores estratégicos, simultaneamente, no fito de extrair ideias sobre a estrutura/organização das prioridades a considerar na estratégia nacional. Os resultados sistematizam-se no Quadro 9.

Quadro 9 – Objetivos e vetores estratégicos – UR das entrevistas

Cod.	Segmento e Unidade de Registo (UR)	Entrevistados										Resultados	
		1	2	3	4	5	6	7	8	9	10	Σ seg.	%
Objetivos e vetores estratégicos													
6.1 Objetivos estratégicos													
6.1.1	Coordenação e cooperação (inter/intra setorial e multinível)		X		X		X		X	X	X	6	60%
6.1.2	Fomentar partilha de conhecimento e informações		X	X	X			X	X		X	6	60%
6.1.3	Aumento da resiliência de EC e do sistema na globalidade		X		X	X		X	X			5	50%
6.1.4	Quadro legal e estratégico coerente/integrador (*governance*)	X			X					X	X	4	40%
6.1.5	Visão agregada do risco e da resiliência			X	X						X	3	30%
6.1.6	Aumentar conhecimento/sensibilização sobre proteção de IC (seminários, publicações, formação, etc.)	X									X	2	20%
6.1.7	Fomentar a prevenção e sistemas de alerta precoce			X				X				2	20%
6.1.8	Intensificar atividades de proteção e resiliência de EC/IC	X										1	10%
6.1.9	Identificação e redução de IC					X						1	10%
6.1.10	Otimizar dependências e interdependências						X					1	10%
6.1.11	Melhorar resposta a incidentes							X				1	10%
6.1.12	Reforçar quadro legal para a supervisão de ativos críticos							X				1	10%
6.1.13	Criar e reter competências									X		1	10%
6.2 Vetores estratégicos													
6.2.1	Promover cooperação baseada nas interdependências	X	X	X	X	X			X			6	60%
6.2.2	Reorganização e criação de organismo agregador dedicado			X				X	X		X	4	40%
6.2.3	Melhorar comunicação e partilha de informação				X		X			X	X	4	40%
6.2.4	Desenvolvimento tecnológico para a prevenção, alerta precoce e recuperação		X	X					X			3	30%
6.2.5	Aumentar a resiliência						X				X	2	20%
6.2.6	Criação de doutrina comum		X		X							2	20%
6.2.7	Aumentar conhecimento/sensibilização sobre proteção de IC	X										1	10%
6.2.8	Fomentar atividades e formações conjuntas (exercícios)	X										1	10%
6.2.9	Atualização continua de IC e respetivas interdependências					X						1	10%
6.2.10	Diminuição gradual e consistente do número de EC/IC					X						1	10%
6.2.11	Cibersegurança (ciber-higiene, proteção de credenciais)									X		1	10%

Não obstante a maior dispersão de ideias obtidas, salientam-se como principais objetivos e áreas/vetores estratégicos nos **domínios organizacional e cooperativo**: o fomento de sinergias através de mais comunicação e coordenação, bem como da partilha de conhecimento e informações entre *stakeholders* (inter/intra setorial e multinível), nomeadamente através de um *Information Sharing and Analysis Centre* (ISAC) (E4), para a qual contribuem as atividades e formações conjuntas, nomeadamente, através de exercícios e a criação de doutrina comum. Reforça-se, também, a premência de reformular e fortalecer o quadro normativo para a supervisão de ativos críticos, incluindo a promulgação de uma estratégia que contribua para a governança coerente e holística, em consonância com a Diretiva REC. Destaca-se, ainda, a otimização de (inter)dependências, em prol do aumento da resiliência sistémica. Para a cabal operacionalização dos objetivos elencados, considera-se premente a criação de um organismo agregador dedicado à temática.

No **domínio técnico**, enfatiza-se a visão integrada do risco e a crescente importância das ciberameaças, a par da atualização e redução do número de IC ou estratificação da sua criticidade. Sublinha-se a aposta na prevenção e intensificação de atividades de proteção, bem como na implementação de sistemas de alerta precoce e otimização da resposta/recuperação perante incidentes, as quais dependem, também, da dimensão cooperativa.

No **domínio humano**, destaca-se a sensibilização/conhecimento sobre a proteção de IC, bem como a criação e retenção de peritos na securitização de IC e gestão do risco.

Face às perceções expostas e sistematizadas, respondeu-se à **QD4**.

4.3 Análise SWOT Dinâmica

Tendo por base a análise ao ambiente, consolidada pelas perceções colhidas, os fatores estratégicos são correlacionados na matriz SWOT dinâmica do Quadro 10, conforme o método da GE abordado no subcapítulo 2.1.1., no intuito de extrair estratégias emergentes.

Quadro 10 – Análise SWOT dinâmica

Fatores Endógenos ➡ / Fatores Exógenos ⬇	POTENCIALIDADES | *STRENGTHS (S)*	VULNERABILIDADES | *WEAKNESSES* (W)
	– Aproveitar conhecimento de entidades especializadas – Panorama securitário favorável e estável – Lições do anterior enquadramento normativo – Transformação baseada na experiência de outros EM – Existência de *fora* que possibilitam a partilha de conhecimento e informação – Crescente preocupação com a temática – Cooperação internacional e académica (I&D) – Fácil operacionalização de um organismo agregador, tendo por base as estruturas do SSI e CNPCE	– Parca cultura de segurança e formação – Complexidade na articulação/competências das entidades – Inexistência de estratégia para a REC – Resistência à partilha de informação e colaboração – Visão segmentada do risco e dos atores – Ineficiência das disposições legais – Inexistência de organismo agregador dedicado – Escassa sensibilidade política e social para a problemática – Controlo externo das cadeias de abastecimento – Crescentes interdependências pouco estudadas e vulneráveis – Elevado número de IC – Constrangimentos legais no acesso a dados
OPORTUNIDADES | *OPPORTUNITIES (O)*	**SO – CRESCIMENTO**	**WO – FOCALIZAÇÃO**
– Transposição da Diretiva REC (e SRI2) cria contexto fértil à transformação – Incremento da cooperação entre *stakeholders*, com maior partilha de informação, boas práticas e exercícios – Estudo das interdependências em prol da resiliência sistémica – Criação de organismos focados na REC – Sinergias da convergência e uniformização na UE, a par da disponibilização de recursos e soluções – Sensibilização para a problemática (*e.g.* Guerra na Ucrânia) – Evolução tecnológica – Fundos para projetos visando a REC	– Melhorar governança: reformular quadro normativo e arquitetura institucional – Criar uma agência dedicada e agregadora, que promova sinergias, desenvolva planeamento e análise, coordene atividades e audite EC/IC (analisar exemplos externos como o CNPIC) – Maximizar cooperação internacional – Selecionar e incentivar a aplicação de soluções e recursos da UE (*e.g.* GRRASP, ERRA, *SmartResilience*) – Incentivar I&D e parcerias académicas – Incentivar o desenvolvimento e emprego de soluções tecnológicas robustas na securitização de IC – Promover o recurso a fundos	– Promover formação universitária para a securitização de IC e gestão de risco (*e.g.* pós-graduação específica para ALS) – Promover atividades intersectoriais (*e.g.* formações e exercícios conjuntos), análises de interdependências e processos de comunicação e consulta – Desenvolver doutrina conjunta (inter/intra setorial) – Criar agência dedicada e agregadora – Promulgar uma estratégia nacional, orientadora da reformulação do quadro normativo interno – Fomentar consciencialização política e sensibilização geral – Reduzir a quantidade de IC e/ou hierarquização da sua criticidade – Promover a diversificação de cadeias de abastecimento
AMEAÇAS | *THREATS (T)*	**ST – DIVERSIFICAÇÃO**	**WT - DEFESA**
– Crescentes ciberameaças (*e.g.* cibercriminalidade, *hacktivismo*) – Conflitualidade económica e social – Terrorismo – Espionagem, sabotagem ou ingerência – Criminalidade organizada – Naturais (*e.g.* sismos, eventos climáticos extremos) – Ameaça interna (maioritariamente negligente) – Acidentais (*e.g.* avarias técnicas, acidentes, incêndios) – Crescente transnacionalidade dos vetores de ameaças	– Agregar *expertise* das entidades envolvidas (SSI, CNPCE, CNCS, SIS, FSS, ANEPC, LNEC, Entidades Setoriais, EC) através de agência dedicada à temática – Promover o *upskilling*/*reskilling* de pessoas para a cibersegurança – Criar CSIRT nacional dedicada às EC – Criar fórum de CISO para apoiar a governança da cibersegurança – Implementar sistemas de alerta precoce	– Intensificar capacitação de entidades, ações de proteção e medidas de resiliência – Promover sistemática análise e testagem para conhecer e mitigar vulnerabilidades (*stress tests*) – Desenvolver avaliações nacionais periódicas com agregação de riscos (*security*, *safety* e *cyber*) – Reforçar quadro normativo para a supervisão de ativos críticos e flexibilização do acesso a dados por parte dos atores nevrálgicos – Otimizar interdependências com redundâncias e atividades de resiliência – Dinamizar partilha e análise de informações, conhecimento e boas práticas (*e.g.* ISAC) – Adotar normas técnicas na construção (*e.g.* Eurocódigos) e a aplicação de medidas de segurança em projeto (*security by design*)

5. Contributos para a Estratégia Nacional de Resiliência de Entidades Críticas

Congregando o enquadramento teórico e conceptual com os resultados obtidos da análise ao ambiente, o presente capítulo visa responder à **QC**, ao apontar *prioridades estratégicas a considerar na formulação da Estratégia Nacional para a REC em Portugal*.

Tendo como finalidade o aumento da resiliência sistémica, no prisma da **estratégia operacional** (*ends*), destaca-se a imperatividade de exponenciar sinergias e confiança entre todos os atores, públicos e privados, reforçando capacidades, a cooperação e partilha de informação, no fito de viabilizar a otimização de interdependências e a gestão holística do risco, partindo da sua visão agregada, ao combinar as dimensões *security*, *safety* e *cyber*.

Também para adequar as ações de proteção e priorizar a implementação de medidas ciber-físicas, torna-se crucial a análise e testagem sistemática de vulnerabilidades, a qual permite monitorizar os níveis de resiliência, a mensurar e integrar em *ratings*, visando despertar a consciência situacional dos *stakeholders*, mormente dos decisores, e, assim, fomentar a melhoria contínua.

Em linha, na perspetiva da **estratégia estrutural** (*ways*), salienta-se a aposta na prevenção e sistemas de alerta precoce, beneficiando do emprego de soluções tecnológicas robustas, agregadoras e interoperáveis, possibilitando o fluxo seguro de dados para centros de fusão que promovam a consciência situacional e a oportuna tomada de decisão, através de ISACs, conforme recomendado pela Agência da União Europeia para a Cibersegurança [ENISA] (2017). Como tal, a génese e capacidades da atual PRIIC devem ser reequacionadas em consonância, no sentido da criação de um ISAC nacional agregador. Para este e outros propósitos subjacentes à REC, torna-se oportuno explorar aprendizagens e recursos disponibilizados no seio da UE, cuja implementação conjunta pode ser potenciada pelo financiamento através de fundos, bem como envolvendo órgãos de I&D e o meio académico.

Também estruturante é o cabal estudo e monitorização das (inter)dependências, perspetivando efeitos em cascata, o qual é potenciado pela execução de exercícios e outras interações entre *stakeholders*, a par da agilização da tomada de decisão na gestão integrada da REC, acompanhada pelo reforço do quadro normativo para a supervisão de ativos críticos, bem como pela flexibilização do acesso a dados por parte de atores nevrálgicos e pela aplicação de normas que fomentem a segurança em projeto.

Por sua vez, no âmbito da **estratégia genética** (*means*), realça-se a promoção da formação, designadamente de peritos na securitização de IC e gestão de risco, bem como a capacitação de pessoas, sobretudo no domínio cibernético, aos diferentes níveis, visando

desenvolver recursos e mitigar as ameaças emergentes no espaço virtual, cada vez mais transversal e complexo. Neste particular, a constituição de uma CSIRT nacional exclusivamente dedicada às EC, capacitada para testar vulnerabilidades, monitorizar e prestar apoio na resposta a incidentes, permitiria alavancar a resiliência cibernética das EC. Paralelamente, é desejável a criação de um fórum de CISO de referência, no fito de prestar assessoria em prol da governança da cibersegurança nacional.

Concomitantemente, urge desenvolver a linguagem securitária comum, nomeadamente, através de doutrina conjunta, em prol de maior reciprocidade.

De enfatizar como ponto de partida, na medida em que permite alavancar a prossecução dos demais desideratos, simultaneamente nos planos **genético e estrutural**, a consciencialização política e sensibilização geral para a problemática, a par da premente criação de um organismo agregador dedicado (centro ou agência nacional), integrando recursos especializados dos *stakeholders* (SSI, CNPCE, CNCS, SIS, FSS, ANEPC, LNEC, Entidades Setoriais, EC) para viabilizar sinergias, fomentar planeamento e análise multissetorial, promover partilha de informação, fiscalizar o cumprimento de normas e coordenar todas as atividades de resiliência.

A constituição deste organismo, na dependência do SG-SSI ou de outro órgão inter/supraministerial, abrangendo a multiplicidade de tutelas setoriais, permite estabelecer a crucial plataforma colaborativa permanente, criando condições para a gradual mitigação das disfunções verificadas e, assim, contrariar a visão segmentada vigente em Portugal. Para o efeito, contribui a implementação e subsequente monitorização da estratégia nacional para a REC, a qual deve, ulteriormente, ser incumbência do organismo agregador, em linha com os preceitos advogados pela ENISA (2023). Para a edificação deste organismo unificador importa, também, analisar as boas práticas internacionais, entre as quais se destaca o caso de Espanha e o seu CNPIC, desde logo, para alavancar a desejável interoperabilidade, face às interdependências entre os dois países.

De notar que a interdependência de objetivos é profunda e, do seu alinhamento, podem ser apontados três vetores/áreas estratégicas: (i) inovar e potenciar recursos; (ii) maximizar sinergias; e (iii) otimizar a governança, conforme resulta da articulação constante do esboço parcial[36] do *mapa da estratégia* sugerido na Figura 15, que, simultaneamente, sistematiza a resposta à **QC**.

[36] Sem indicadores de desempenho, os quais devem ser definidos para permitir a ulterior avaliação estratégica.

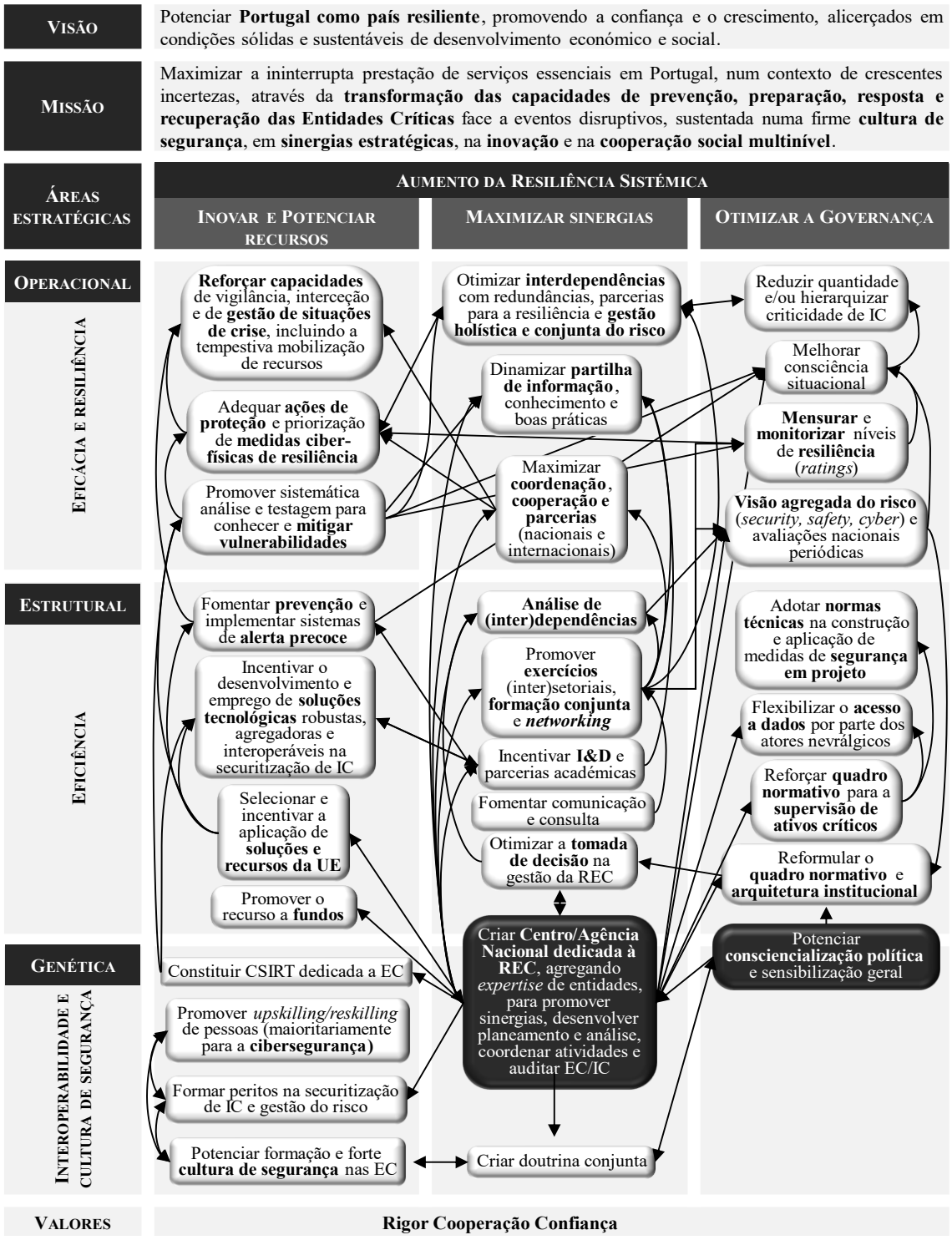

Figura 15 – Esboço parcial do *mapa da estratégia*

Finalmente, de salientar que a estratégia nacional para a REC deverá ser coerentemente articulada com os preceitos de outras estratégias nacionais associadas, mormente da ENCT, ENSC e ENPCP2030, num documento de divulgação pública, sem prejuízo da preparação detalhada de planos estratégicos setoriais, eventualmente classificados, em linha com o modelo espanhol.

6. Conclusões

A estabilidade social e económica depende do ininterrupto funcionamento de uma rede interconectada de IC e respetivos sistemas, em diferentes setores, que garante a prestação de SE. Em razão das (inter)dependências, uma perturbação no funcionamento de uma IC pode gerar efeitos disruptivos em cascata, inclusive transnacionais, pelo que se tornou prioridade da UE reforçar a sua resiliência, perante um ambiente de crescente incerteza.

Decorridos catorze anos da Diretiva 2008/114/CE, de 08 de dezembro, sobre a PIC, que ditou a aplicação de medidas de segurança nos setores da energia e transportes, a publicação da Diretiva 2022/2557, de 14 de dezembro, sobre a REC, transforma o paradigma, gerando maior convergência entre EM, de forma concertada com a Diretiva SRI2, em prol do aumento da resiliência da União.

Além do alargamento a onze setores, a Diretiva REC suscita uma abordagem securitária mais holística e cíclica, sustentada na avaliação de riscos e análise de (inter)dependências, bem como na maior cooperação entre *stakeholders*. Visa-se maior robustez e resiliência, mitigando os efeitos de potenciais disrupções na atividade das IC, alicerçadas na capacitação dos seus operadores, enquanto EC, para prevenir incidentes e proteger-se deles, dar-lhes resposta, resistir-lhes, os atenuar, os absorver, adaptar-se a eles e recuperar deles.

Tal abordagem materializa a estratégia recomendada para a gestão de riscos com elevado grau de incerteza e grande impacto, decorrentes de ameaças naturais, por deterioração, acidentais ou deliberadas, acervando a perspetiva *all-hazards* na aplicação de medidas mitigadoras de riscos de pendor *security*, *safety* e *cyber*, tendencialmente de forma agregada e colaborativa, como reflexo da maturidade do sistema.

Face aos desígnios de melhorar a governação e potenciar a resiliência sistémica, destaca-se da Diretiva REC, conforme estipulado no seu artigo 4.º, a imperativa adoção de estratégias nacionais pelos EM, até 17 de janeiro de 2026, contemplando, nomeadamente, os objetivos e prioridades estratégicas, as medidas políticas, o quadro de responsabilidades, a avaliação nacional de riscos, entre outros aspetos estruturantes.

Em Portugal, a inexistência de uma estratégia nacional para a securitização de IC já havia sido apontada como vulnerabilidade, agravada pela dispersão normativa e fracionamento de responsabilidades, com repercussão na segmentação de perspetivas, entropia de processos e, em última análise, na fragilidade do sistema.

Perante a abundância de ameaças ciber-físicas e crescente interconectividade, a conjuntura de transformação em que surge a imperatividade de edificar a estratégia nacional constitui-se como oportunidade para reformular o quadro normativo e institucional, em prol de um arquétipo mais eficiente, que permita alavancar a resiliência do país.

No desiderato de contribuir para formulação da estratégia nacional para a REC, a presente investigação centrou-se na clarificação das prioridades estratégicas a considerar.

Seguindo o raciocínio indutivo e uma estratégia de investigação qualitativa, desenvolveu-se um estudo de caso focado nas idiossincrasias nacionais, contemplando, ainda, as boas práticas e axiomas internacionais hodiernos.

O percurso metodológico integrou duas fases. Na primeira efetuou-se a revisão literária inicial, estabelecendo-se a base conceptual, os objetivos e questões a responder, tendo por base os dados advenientes da análise documental e das entrevistas exploratórias e abertas realizadas. Na segunda consolidou-se o estado da arte, essencialmente sustentado na criteriosa análise documental, e desenvolveu-se o estudo empírico, para responder à **QC** "*Quais as prioridades estratégicas a considerar na formulação da Estratégia Nacional para a Resiliência de Entidades Críticas em Portugal*?", partindo da resposta às quatro QD enunciadas.

Considerando a **QD1**, elencaram-se os principais instrumentos políticos disponíveis e analisaram-se os documentos estratégicos de países anglo-saxónicos e europeus, tidos como referência na securitização de IC (Austrália, Canadá, Reino Unido, EUA, Espanha e Suécia), sistematizando as suas prioridades estratégicas no Quadro 2, constante da secção 2.2.2.

Em resposta à **QD2**, foram examinados os quadros normativos e institucionais subjacentes à temática, nos planos europeu e nacional, permitindo compreender a evolução e tendências, bem como as fragilidades nacionais, destacando-se a parca governança e as ineficiências resultantes da complexa articulação e segmentação de responsabilidades.

Para cabalmente responder à QD3 e à QD4, realizaram-se dez entrevistas semiestruturadas, visando colher as perspetivas de peritos e dirigentes de instituições envolvidas na temática, indagados de acordo com o quesito da representatividade, no fito de extrair resultados sustentados na convergência de prismas e *expertise* diferenciada.

Face à **QD3**, a análise do ambiente estratégico, exógeno e endógeno, foi consolidada com os contributos prestados pelos entrevistados, permitindo que fossem enfatizados os fatores estratégicos que mais influem na formulação de uma estratégia para a REC em Portugal.

Na senda, para responder à **QD4**, apelou-se à correlação de fatores estratégicos e partilha das respetivas perceções sobre os problemas críticos, potenciais promissores, medidas prioritárias, bem como objetivos e vetores estratégicos.

O procedimento visou a consolidação de dados, possibilitando a sua subsequentemente sistematização na matriz SWOT dinâmica constante do subcapítulo 4.3, da qual se extraem as estratégias emergentes para a REC em Portugal.

Finalmente, da congregação de respostas às quatro QD, no capítulo 5, respondeu-se à **QC**, sendo apontadas prioridades estratégicas, nos prismas operacional, estrutural e genético, cuja articulação se apresentou através do esboço parcial de um mapa da estratégia, evidenciando objetivos alinhados em três áreas/vetores: (i) inovar e potenciar recursos; (ii) maximizar sinergias; e (iii) otimizar governança.

Dos resultados obtidos, confirmou-se um panorama nacional com significativas fragilidades, marcado pela parca cultura de segurança e disfunções na governança, com escassa colaboração e partilha de informação intersetorial, em que se desconhecem as interdependências, subsistem visões segmentadas e se questiona a capacidade de assegurar a aplicação de medidas determinadas às IC ou de apoiar tempestivamente a resposta a incidentes, particularmente no âmbito cibernético, que ora suscita maior preocupação. Sublinha-se, também, a ausência de testes que permitam evidenciar e, subsequentemente, mitigar vulnerabilidades, bem como a falta de formação e exercícios conjuntos, a inexistência de sistemas de alerta precoce e a dependência de cadeias de abastecimento.

Perante o atual contexto de convergência europeia, surge, de facto, a oportunidade de transformar o paradigma, visando o aumento da resiliência sistémica do país.

Para o efeito, concomitantemente nos planos genético e estrutural da estratégia, advoga-se, como ponto de partida, suscitar a consciencialização política e a sensibilização geral, bem como criar um organismo agregador dedicado à securitização de IC, num plano supra/interministerial, estabelecendo, assim, a plataforma colaborativa permanente que permite a gradual mitigação das disfunções verificadas, bem como a cabal implementação e monitorização da estratégia. Este organismo deve congregar recursos especializados de diversas entidades e constituir-se como ponto central do sistema, garantindo a supervisão e coordenação de todas as atividades, a partilha de informação, o planeamento multisetorial integrado, bem como a gestão das inspeções ou auditorias às EC/IC, além da contínua exploração de mecanismos de cooperação em prol da resiliência, desde a prevenção e preparação, à resposta, recuperação e adaptação face a incidentes.

Destaca-se, no plano da estratégia genética, a criação de doutrina conjunta e a formação de peritos na securitização de IC e gestão de risco, bem como a capacitação de pessoas, sobretudo no domínio cibernético, a par da constituição de uma CSIRT nacional, exclusivamente dedicada à resiliência cibernética de EC.

No âmbito da estratégia estrutural, realça-se a aposta na prevenção e o emprego de soluções tecnológicas robustas, que permitam estabelecer sistemas de alerta precoce, promover a consciência situacional e agilizar a oportuna tomada de decisão, através de ISACs, bem como a exploração e implementação de recursos disponibilizados pela UE, além da promoção de parcerias com o meio académico e órgãos de I&D. Importa, igualmente, reformular o quadro normativo e institucional, otimizar a tomada de decisão, promover a análise de (inter)dependências, os exercícios e formação conjunta, reforçar a supervisão de ativos críticos, promover a segurança em projeto e facilitar o acesso a dados, por parte de atores nevrálgicos.

No prisma da estratégia operacional, enfatiza-se o reforço das capacidades de resiliência, potenciado pela monitorização dos seus níveis e a sua integração em *ratings*, a par da otimização de interdependências, partindo do fortalecimento de sinergias e confiança entre atores, da cooperação e partilha de informações, da testagem sistemática de vulnerabilidades e melhoria contínua, bem como da gestão holística do risco, com a visão agregada das dimensões *security*, *safety* e *cyber*.

Considera-se que a investigação reúne contributos pertinentes para a formulação da estratégia nacional para a REC, percecionada como premente face ao quadro atual. Além do contributo para o conhecimento sobre a temática no plano nacional, apresentam-se prioridades e propostas concretas, cuja adoção favorece a resiliência do país.

Não obstante, como limitações da investigação, aponta-se a sua natureza exploratória e a representatividade da amostra que, apesar do esforço para a maximização de prismas e distinção dos entrevistados, não inclui *stakeholders* de todos os setores críticos.

Em linha com as limitações, como proposta de estudos futuros, propõe-se consolidar as prioridades estratégicas apontadas por esta investigação, sugerindo-se um processo de comunicação e consulta junto de um conjunto mais alargado de entidades. Considera-se, também, importante desenvolver investigação sobre modelos de funcionamento de organismos dedicados à REC e de estruturas tipo ISACs, no intuito de contribuir para a articulação do organismo nacional, cuja edificação constitui indubitável prioridade.

Por fim, recomenda-se a célere criação de um núcleo permanente dedicado à temática, na dependência do SG-SSI, que se constitua como embrião do subsequente organismo agregador. Com o apoio do CNPCE e CNCS, sugere-se que este núcleo desenvolva a avaliação nacional de risco (agregada) e, através de um procedimento de comunicação e consulta, conceba a estratégia nacional para a REC, ponderando as prioridades estratégicas apontadas nesta investigação, a serem traduzidas em medidas concretas, associadas a um quadro de responsabilidades e indicadores de desempenho, por forma a garantir a sua implementação e controlo.

Referências bibliográficas

Autoridade Nacional de Proteção Civil [ANPC]. (2019). *Avaliação Nacional de Risco - 1.ª atualização* [versão PDF]. Retirado de http://www.prociv.pt/bk/RISCOSPREV/AVALIACAONACIONALRISCO/PublishingImages/Paginas/default/ANR2019-vers%C3%A3ofinal.pdf

Australian Government, Department of Home Affairs, Cyber and Infrastructure Security Centre. (2023a). *Critical Infrastructure Resilience Strategy* [versão PDF]. Retirado de https://www.cisc.gov.au/resources-contact-information-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

Australian Government, Department of Home Affairs, Cyber and Infrastructure Security Centre. (2023b). *Critical Infrastructure Resilience Plan* [versão PDF]. Retirado de https://www.cisc.gov.au/resources-contact-information-subsite/Documents/critical-infrastructure-resilience-plan-2023.pdf

Bardin, L. (2020). *Análise de Conteúdo* (4.ª Ed.). Lisboa: Edições 70, Lda.

Barroso, L. (2008). Análise Conceptual do Conceito Estratégico de Defesa Nacional. *Revista Militar*, *4*(2475), pp. 399-422. Retirado de https://www.revistamilitar.pt/artigopdf/274

Bertocchi, G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A., … Traballesi, A. (2016). *Guidelines for Critical Infrastructures Resilience Evaluation* [versão PDF]. doi: 10.13140/RG.2.1.4814.6167

Boone, W. (2013). Risk Management. Em R. Radvanovsky & J. Brodsky (Eds.), *Handbook of SCADA/Control Systems Security.* (pp. 69-111). *Londres: CRC Press*.

Bryman, A. (2012). *Social research methods* (Fourth edi). Oxford: Oxford University Press.

Buss, H., Amann, P., Ares, P., Garção, H., Joly, S., Gomes, R., & Giannopoulos, G. (2021, março). *PPUE2021 Seminar "Security and Protection of Public Spaces and critical Infrastructures"*. Seminário online organizado pela Presidência Portuguesa da União Europeia, Lisboa.

Cambridge Dictionary (s.d.). English Dictionary, Translations & Thesaurus [Página online]. Retirado de https://dictionary.cambridge.org/

Centre for European Policy Studies. (2010). *Report of a CESP Task Force-Protecting Critical Infrastructure in the EU* [Versão PDF]. Bruxelas: Autor. Retirado de http://www.ssrn.com/abstract=1756710

Centro Nacional de Cibersegurança [CNCS]. (s.d.). Glossário [Página online]. Retirado de https://www.cncs.gov.pt/pt/glossario/

Centro Nacional de Cibersegurança [CNCS]. (2022). *Relatório Cibersegurança em Portugal* [Versão PDF]. Lisboa: Autor. Retirado de https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

Comissão das Comunidades Europeias. (2006). *Comunicação da Comissão relativa a um Programa Europeu de Proteção das Infra-Estruturas Críticas* [Versão PDF]. Bruxelas: Autor. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

Comissão das Comunidades Europeias. (2008). *Decisão do Conselho sobre uma Rede de Alerta para as Infra-Estruturas Críticas*. [Versão PDF] Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52008PC0676&from=PT

Comissão Europeia. (2019a). *Evaluation of the Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection (Commission Staff Working Document)* [Versão PDF]. Bruxelas: Autor. Retirado de https://home-affairs.ec.europa.eu/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf

Comissão Europeia. (2019b). *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Final report)* [Versão PDF]. Bruxelas: Publications Office of the European Union. doi: 10.2837/864404

Comissão Europeia. (2020a). *Comunicação da Comissão Europeia ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a Estratégia da UE para a União da Segurança* [Versão PDF]. Bruxelas: Autor. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

Comissão Europeia. (2020b). *Proposal for a Directive of the European Parliament and the Council on the Resilience of Critical Entities* [Versão PDF]. Brussels: Autor. Retirado de https://home-affairs.ec.europa.eu/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

Gobierno de España, Consejo de Seguridad Nacional. (2021). *Estrategia de Seguridad Nacional 2021* [Versão PDF]. Madrid: Ministerio de la presidencia. Retirado de https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

Conselho da União Europeia. (2022). *Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities*. Bruxelas: Autor. Retirado de https://data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Fifth Ed.). Los Angeles: SAGE Publications Ltd.

Critical Five. (2015). *Role of Critical Infrastructure in National Prosperity: Shared narrative* [Versão PDF]. Sem local: Critical Five. Retirado de https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-rl-crtclnfrstrctr-ntnlprsprty/2016-rl-crtclnfrstrctr-ntnlprsprty-en.pdf

Curt, C., & Tacnet, J.-M. (2018). Resilience of Critical Infrastructures: Review and Analysis of Current Approaches: Resilience of Critical Infrastructures. *Risk Analysis*, *38*(11), pp. 2441-2458. doi: 10.1111/risa.13166

Cybersecurity and Infrastructure Security Agency [CISA]. (2019). *A Guide to Critical Infrastructure Security and Resilience*. Washington: U.S. Department of Homeland Security. Retirado de https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Cybersecurity and Infrastructure Security Agency [CISA]. (2021, junho). *Methodology for Assessing Regional Infrastructure Resilience: Lessons Learned from the Regional Resiliency Assessment Program*. Washington: U.S. Department of Homeland Security. Retirado de https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%20EAD%20Signed_with%20alt-text_0.pdf

David, F. R. (2011). *Strategic management: Concepts and cases* (13th Ed). Florence: Prentice Hall.

Decreto-Lei n.º 3/2012, de 16 de janeiro. (2012). *Aprova a orgânica do Gabinete Nacional de Segurança*. Diário da República 1.ª Série, 11, 174-177, Lisboa: Presidência do Conselho de Ministros.

Decreto-Lei n.º 20/2022, de 28 de janeiro. (2022). *Estabelece os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas*

críticas nacionais e europeias, procedendo à consolidação no direito nacional da transposição da Diretiva 2008/114/CE, do Conselho, de 8 de dezembro de 2008 [revoga o Decreto -Lei n.º 62/2011, de 9 de maio]. Diário da República, 1.ª série, 20, 2-14 Lisboa: Presidência do Conselho de Ministros.

Decreto-Lei n.º 43/2020, de 21 de julho. (2020). *Sistema Nacional de Planeamento Civil de Emergência*. Diário da República, 1.ª série, 140, 17-24. Lisboa: Presidência do Conselho de Ministros.

Decreto-Lei n.º 62/2011, de 09 de maio. (2011). *Estabelece os procedimentos de identificação e de protecção das infra-estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes e transpõe a Directiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro*. Diário da República, 1.ª série, 89, 2624-2627. Lisboa: Ministério da Defesa Nacional.

Decreto-Lei n.º 249/2015, de 28 de outubro. (2015). *Aprova a orgânica do ensino superior militar e consagra as suas especificidades no contexto do ensino superior e aprova o Estatuto do Instituto Universitário Militar*. Diário da República 1.ª Série, 211, 9298-9311, Lisboa: Ministério da Defesa Nacional.

Diretiva 2008/114/CE, de 08 de dezembro. (2008). *Identificação e Designação das Infraestruturas Críticas Europeias e à Avaliação aa Necessidade de Melhorar a sua Proteção*. Jornal Oficial da União Europeia, L 345, 75-82. Bruxelas: Conselho Europeu.

Diretiva 2022/2555, de 14 de dezembro de 2022. (2022). *Diretiva da União Europeia relativa 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 SRI 2)*. Jornal Oficial da União Europeia, L 333, 80-152. Bruxelas: Parlamento Europeu e o Conselho da União Europeia.

Diretiva 2022/2557, de 14 de dezembro de 2022. (2022). *Diretiva da União Europeia relativa à resiliência de entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho*. Jornal Oficial da União Europeia, L 333, 164-198. Bruxelas: Parlamento Europeu e o Conselho da União Europeia.

European Risk & Resilience Assessment and Rating Initiative [ERRA]. (s.d.) ERRA Homepage [Página online]. Retirado de http://erra.eu-vri.eu/

European Union Agency for Cybersecurity [ENISA] (2017). *Information sharing and analysis centres (ISACs): Cooperative models* [versão PDF]. doi: 10.2824/549292

European Union Agency for Cybersecurity [ENISA]. (2023). *A governance framework for national cybersecurity strategies* [versão PDF]. doi: 10.2824/211856

Fachada, C. P. A., Ranhola, N. M. B., Marreiros, J. P. R., & Santos, L. A. B. (2020). *Normas de Autor no IUM* (3.ª Ed., revista e atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.

Gheorghe, A. V., Vamanu, D. V., Katina, P. F., & Pulfer, R. (2018). *Critical Infrastructures, Key Resources, Key Assets*. *Risk, Vulnerability, Resilience, Fragility, and Perception Governance*. Cham: Springer International Publishing.

Google Trends. (2022). Explore search interest for resilience, Infrastructures by time, location and popularity on Google Trends [Página online]. Retirado de https://trends.google.com/trends/explore?date=all&q=resilience,Infrastructures

Government of Canada. (2009). *National Strategy for Critical Infrastructure* [Versão PDF]. Ottawa: Her Majesty the Queen in Right of Canada. Retirado de https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

Government of Canada. (2021). *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure* [Versão PDF]. Ottawa:Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness. Retirado de https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf

Geospatial Risk and Resilience Assessment Platform [GRRASP]. (s.d.). Welcome page [Página online]. Retirado de https://grraspresiliencetool.eu-vri.eu/home.aspx?lan=230&tab=3170&itm=3170&pag=3146

Guarda Nacional Republicana. (2020). *Relatório do 1.º Curso de Segurança e Proteção de Infraestruturas da GNR, 02 a 13 de março e 15 de junho a 03 de julho* [Documento reservado] Lisboa: Unidade de Segurança e Honras de Estado da Guarda Nacional Republicana.

Her Majesty Government [Reino Unido]. (2015). *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* [Versão PDF]. Londres: Crown. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

ISO 31000. (2018). *Risk management - Principles and guidelines*. Geneva: International Organization for Standartization.

ISO 22300. (2021). *Security and resilience - Vocabulary*. Geneva: International Organization for Standartization.

ISO 27001. (2022a). *Information security management systems*. Geneva: International Organization for Standartization.

ISO 31073. (2022b). *Risk management—Vocabulary.* Geneva: International Organization for Standartization.

IUM. (2020a). *NEP/INV - 01—Procedimentos Relativos à Elaboração de Trabalhos de Investigação no Âmbito de Cursos que não Atribuem Grau Académico*. Lisboa: Instituto Universitário Militar.

IUM. (2020b). *NEP/INV - 03—Estrutura e Regras de Citação e Referenciação de Trabalhos Escritos a Realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.

Jovanović, A., Klimek, P., Choudhary, A., Schmid, N., Linkov, Øien I., … Lieberz, D. (2016). *Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infastructure resilience* [Projeto Smart Resilience - EU-VRi: European Risk & Resilience Institute]. Estugarda: ReseachGate. doi: 10.13140/RG.2.2.32597.93927

Kaplan, R. S. (2010). Conceptual Foundations of the Balanced Scorecard. *Harvard Business School (working paper 10-074)*, 37, Retirado de https://www.hbs.edu/ris/Publication%20Files/10-074_0bf3c151-f82b-4592-b885-cdde7f5d97a6.pdf

Kaplan, R. S., & Norton, D. P. (1992). The Balanced Scorecard - Measures that Drive Performance. *Harvard Business Review* [Página online]. Retirado de https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2

Kaplan, R. S., & Norton, D. P. (2008). Integrating Strategy Planning and Operational Execution: A Six-Stage System. *Balanced Scoredcard Report*, 8. Harvard: Harvard Business School Publishing. Retirado de https://www.bki-se-institute.dk/wp-content/uploads/2020/01/Integrating-Strategy-Planning-and-Operational-Execution-BSCR-May-Jun-2008.pdf

Lei n.º 24-C/2022, de 30 de dezembro. (2022). *Lei das Grandes Opções para 2022-2026*. Diário da República 1.ª Série, 251, 74-(2)-74-(89), Lisboa: Assembleia da República.

Lei n.º 46/2018, de 13 de agosto. (2018). *Regime Jurídico Da Segurança Do Ciberespaço*. Diário da República, 1.ª série, 155, 4031-4037. Lisboa: Assembleia da República.

Lei n.º 50/2014, de 13 de agosto. (2014). *Lei Orgânica do Secretário-Geral Do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS)*. Diário da República, 1.ª Série, 155, 4206-4221. Lisboa: Assembleia da República.

Lei n.º 59/2015, de 24 de junho. (2015). *Primeira alteração à Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, modificando a composição do Conselho Superior de Segurança Interna e a organização e o funcionamento da Unidade de Coordenação Antiterrorismo*. Diário da República, 1.ª série, 121, 4411 - 4411. Lisboa: Assembleia da República.

Letras, R. (2022). *Estratégia de Segurança Interna: Um Modelo de Elaboração Estratégica para Portugal* (Trabalho de Investigação Individual do Curso de Promoção a Oficial General). Instituto Universitário Militar, Lisboa.

Lewis, L. P. (2019). *Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies. Contributing Paper to Global Assessment Report on Disaster Risk Reduction (GAR 2019)* [Versão PDF]. Argone: Argone National Laboratory. Retirado de https://www.undrr.org/publication/critical-infrastructure-interdependency-analysis-operationalising-resilience-strategies

Litting, B. (2009). Interviewing the Elite - Interviewing Experts: Is There a Difference? Em Bogner, A., Littig, B., Menz, W. (eds) *Interviewing Experts. Research Methods Series* (pp. 98-113). Londres: Palgrave Macmillan. doi: 10.1057/9780230244276_5

Manunta, G. (1999, julho). What Is Security? *Security Journal*, 57-66. doi: 10.1201/9781420031461.ch2

Martinho, J. (2017). *As Infraestruturas críticas em Portugal: Um modelo de abordagem* (Trabalho de Investigação Individual do Curso de Estado-maior Conjunto 2016/2017). Instituto Universitário Militar, Lisboa.

Mentges, A., Halekotte, L., Schneider, M., & Demmer, T. (2023). *A resilience glossary shaped by context: Reviewing resilience- related terms for critical infrastructures.* Sankt Augustin: German Aerospace Center - Institute for the Protection of Terrestrial Infrastructures. Retirado de: https://arxiv.org/ftp/arxiv/papers/2302/2302.04524.pdf

Ninković, V. M. (2021). *Critical Infrastructure Resilience - National apporaches in the United States of America, the United Kingdom and Australia*. Belgrado: University of Belgrade, Faculty of Security Studies, 1205–1225. doi: 10.5937/zrpfns55-30333

Organização para a Cooperação e Desenvolvimento [OCDE]. (2019). *Good Governance for Critical Infrastructure Resilience* [Versão PDF]. Paris: OECD Publishing. doi: 10.1787/02f0e5a0-en

Oliveira, J. (Coord), Gonçalves, J., Pais, I., Mendes, F., Messias, R., Silva, … Afonso, A. (2017). *Boas Práticas de Resiliência de Infraestruturas Críticas - Setor privado e setor empresarial do Estado* [Versão PDF]. Lisboa: Autoridade Nacional de Proteção Civil. Retirado de http://www.prociv.pt/bk/EDICOES/OUTRASEDICOES/Documents/Boas_Praticas_Resiliencia_Infraestruturas_Criticas-Setor_Privado_e_Empresarial_Estado_2017.pdf

Organização do Tratado do Atlântico Norte [OTAN]. (2023, 10 de fevereiro). NATO's response to hybrid threats [Página online]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm

O'Sullivan, E., Rassel, G. R., Berner, M., & Taliaferro, J. D. (2017). *Research methods for public administrators* (Sixth edition). New York: Routledge.

Pereira, R. (2022). *Metodologia de Segurança de Infraestruturas Críticas* [Trabalho de Investigação Individual do Curso de Estado-maior Conjunto 2021/2022]. Instituto Universitário Militar, Lisboa.

Pestana, J. (2016). *A Proteção de Infraestruturas Críticas – Contributos para o desenvolvimento de um Plano Nacional de Proteção de Infraestruturas Críticas*. (Relatório Final do Curso de Comando e Direção Policial) Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

Pinheiro, P. V. (2022, novembro). Qual o valor estratégico da segurança nas Infraestruturas Críticas em Portugal? Em: Culturgest, *O valor estratégico da segurança nas Infraestruturas Críticas em Portugal*. Conferência organizada pelo Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT), Lisboa.

Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure*, *8*(1), 85-101. doi: 10.1080/23789689.2022.2128562

Real Decreto 704/2011, de 20 de mayo. (2011). *Reglamento de protección de las infraestructuras críticas*. Boletín Oficial del Estado, Ref. BOE-A-2021-8849, núm. 12. Madrid: Ministerio del Interior. Retirado de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf

Recommended Elements of Critical Infrastructure Protection for policy makers in Europe [RECIPE]. (2011). *Good Practices Manual for CIP Policies*. European Commission - Directorate-General Home Affairs. Retirado de https://www.academia.edu/25202110/RECIPE_Good_Practices_Manual_for_CIP_Policies

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, pp. 125–138. doi: 10.1016/j.ijcip.2019.03.003

Resolução da Assembleia Geral das Nações Unidas 66/290, de 10 de setembro (2012). *Resolution 66/290 adopted by the General Assembly - Follow-up to paragraph 143 on human security of the 2005 World Summit Outcome*. Organização das Nações Unidas.. Nova Iorque: Assembleia Geral das Nações Unidas. Retirado de https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/476/22/PDF/N1147622.pdf?OpenElement

Resolução de Conselho de Ministros n.º 19/2013, de 05 de abril. (2013). *Conceito Estratégico de Defesa Nacional*. Diário da República, 1ª série, 67, 1981-1995. Lisboa: Ministério da Defesa.

Resolução de Conselho de Ministros n.º 112/2021, de 11 de agosto. (2021). *Estratégia Nacional para uma Proteção Civil Preventiva 2030*. Diário da República 1.ª Série, 155, 133-156, Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.o 7-A/2015, de 20 de fevereiro. (2015). *Aprova a Estratégia Nacional de Combate ao Terrorismo*. Diário da República 1.ª Série, 36, 2-4, Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 92/2019, de 05 de jumho. (2019). *Estratégia Nacional de Segurança do Ciberespaço*. Diário da República, 1.ª Série, 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.

Resolução legislativa P9_TA(2022)0394, de 22 de novembro. (2022). *Resolução legislativa do Parlamento Europeu sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa à resiliência das entidades críticas (COM(2020)0829 – C9-0421/2020 – 2020/0365(COD))*. Estrasburgo: Parlamento Europeu. Retirado de https://www.europarl.europa.eu/doceo/document/TA-9-2022-0394_PT.pdf

Ribeiro, A. S. (2008). *Processo de Formulação da Estratégia de Defesa Nacional* (Trabalho de Investigação Individual do Curso de Promoção a Oficial General). Instituto Universitário Militar, Lisboa.

Ribeiro, A. S. (2017a). *Teoria Geral da Estratégia - O essencial do processo estratégico*. Coimbra: Edições Almedina.

Ribeiro, A. S. (2017b). *O Processo Estratégico na Marinha.* Cadernos navais, 46, Lisboa: Edições Culturais da Marinha. Retirado de https://www.marinha.pt/pt/a-marinha/estudos-e-reflexoes/cadernos-navais/Documents/CAD_NAVAL_46.pdf

Richards, D. (1996). Elite Interviewing: Approaches and Pitfalls. *Politics*, *16*(3), 199–204. doi: 10.1111/j.1467-9256.1996.tb00039.x

Rumelt, R., Schendel, D., & Teece, D. (1995). Fundamental Issues in Strategy: A Research Agenda. *Administrative Science Quarterly*, *41*. Retirado de https://www.researchgate.net/publication/40937724_Fundamental_Issues_in_Strategy_A_Research_Agenda

Santos, L. A. B., & Lima, J. M. M. (Coord.). (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação*. (2.ª Ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures*, *7*(5), 67. doi: 10.3390/infrastructures7050067

Schwab, K. (2018, 05 de novembro). Globalization 4.0 - What does it mean? World Economic Forum [Página online]. Retirado de https://www.weforum.org/agenda/2018/11/globalization-4-what-does-it-mean-how-it-will-benefit-everyone/

Sistema de Informações de Segurança [SIS] (s.d.). Programa KRITICA [Página online] Retirado de https://www.sis.pt/pagina/115/programa-kritica

Sistema de Segurança Interna. (2010). *Plano de Coordenação, Controlo e Comando das Forças e Serviços de Segurança (PCCCFSS)* [Documento Confidencial]. Lisboa: Sistema de Segurança Interna.

Sistema de Segurança Interna. (2021). *Relatório Anual de Segurança Interna 2021 (RASI2021)*. Lisboa: Gabinete do Secretário-Geral do Sistema de Segurança Interna. Retirado de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3d

Sistema de Segurança Interna (2022) *Relatório Anual de Segurança Interna 2022 (RASI2021).* Lisboa: Gabinete do Secretário-Geral do Sistema de Segurança Interna. Retirado de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3D&fbclid=IwAR0fpMrzjIZWQ7t_3um46K8Fuxt1F2AJ1ptCZJ4kWoBZwJE0PToxqoyt-u8

SmartResilience. (s. d.). About Project [Página online]. Retirado de http://www.smartresilience.eu-vri.eu/

Soldatos, J., Philpot, J., & Giunta, G. (Eds.). (2020). *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Now Publishers. https://doi.org/10.1561/9781680836875

Soldatos, J., Praça, I., & Jovanović, A. (Eds.). (2021). *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*. Boston-Delft: Now Publishers. doi: 10.1561/9781680838237

Stapenhurst, T. (2009). *The benchmarking book: A how-to-guide to best practice for managers and practitioners*. Amsterdam/London: Elsevier/Butterworth-Heinemann.

Swedish Civil Swedish Civil Contingencies Agency. (2014). *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure*. Swedish Civil Contingencies Agency. Retirado de https://www.msb.se/RibData/Filer/pdf/27412.pdf

The White House [EUA]. (2022). *National Security Strategy*. Washington: The White House. Retirado de https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

The White House [EUA]. (2013). *Presidential Policy Directive - Critical Infrastructure Security and Resilience (PPD-21)*. Washington: The White House. Retirado de https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The World Bank. (2017). *World Development Report 2017: Governance and the Law*. Washington: The World Bank Group. Retirado de https://www.worldbank.org/en/publication/wdr2017

UK Cabinet Office. (2010). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. Londres: Autor. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf

United Nations. (2015). *Sendai Framework for Disaster Risk Reduction 2015-2030* [Versão PDF]. United Nations International Strategy for Disaster Reduction [UNISDR]. Geneva: UNISDR Secretariat. Retirado de https://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf?_gl=1*dchbmx*_ga*NzY2MjAxODk2LjE2Njk0NzYzODA.*_ga_D8G5WXP6YM*MTY2OTQ3OTM1NS4yLjAuMTY2OTQ3OTM1NS4wLjAuMA..

United Nations. (2022). *Principles for Resilient Infrastructure* [Versão PDF]. United Nations Office for Disaster Risk Reduction [UNDRR]. Geneva: UNDRR. Retirado de https://www.undrr.org/quick/70250

UNOCT, CTED, & Interpol. (2018). *The Protection of Critical Infrastructures agains terrorist attacks: Compendium of good practices* [Versão PDF]. Retirado de https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

U.S. Department of Homeland Security. (2013). *National Infrastructures Protection Plan* [Versão PDF]. Washington: Autor. Retirado de https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

U.S. Department of Homeland Security (2015). *DHS Training Glossary - Version 2.1*. Washington: Autor. Retirado de https://training.fema.gov/devres/docs/508/dhs-training-glossary.pdf

U.S. Department of Homeland Security. (2016). *Critical Infrastructure Threat Information Sharing Framework - A Reference Guide for the Critical Infrastructure Community* [Versão PDF]. Washington: Autor. Retirado de https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

U.S. Department of Homeland Security. (2019). *A Guide to Critical Infrastructure Security and Resilience* [Versão PDF]. Washington: Autor. Retirado de https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Van Audenhove, L., & Donders, K. (2019). Talking to People III: Expert Interviews and Elite Interviews. Em H. Van den Bulck, M. Puppis, K. Donders, & L. Van Audenhove (Eds.), *The Palgrave Handbook of Methods for Media Policy Research* (pp. 179–197). Bruxelas: Springer International Publishing. doi: 10.1007/978-3-030-16065-4_10

Vilelas, J. (2009). *Investigação: O Processo de Construção do Conhecimento* (3.ª Ed). Lisboa: Edições Sílabo.

Voronova, S. (2022). *Resilience of critical entities*. Estrasburgo: European Parliamentary Research Service. Retirado de https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738212/EPRS_ATA(2022)738212_EN.pdf

Wheelen, T. L., Hunger, J. D., Hoffman, A. N., & Bamford, C. E. (2014). *Strategic management and business policy: Globalization, innovation, and sustainability* (Fourteenth edition). Harlow: Pearson.

XXIII Governo Constitucional. (2022). *Programa do XXIII Governo Constitucional | 2022-2026*. Retirado de https://www.portugal.gov.pt/gc23/programa-do-governo-xviii/programa-do-governo-xviii-pdf.aspx?v=%C2%ABmlkvi%C2%BB=54f1146c-05ee-4f3a-be5c-b10f524d8cec

Yarger, H. R. (2006). *Strategic theory for the 21st century: The little book on big strategy*. Strategic Studies Institute. Carlisle: U.S. Army War College Press. Retirado de https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1722&context=monographs

Yin, R. K. (2018). *Case study research and applications: design and methods* (Sixth Edit). Los Angeles: SAGE Publications Ltd.

Apêndice A – Conceitos instrumentais e definições

Além dos conceitos estruturantes[37] densificados, considera-se relevante para a análise a clarificação de um conjunto de conceitos instrumentais, conforme definidos na Tabela 1[38].

Tabela 1 – Conceitos instrumentais e definições

CONCEITO E FONTE	DEFINIÇÃO
Agregação de riscos ISO 31000:2018 | ISO 31073:2022	Combinação de uma série de riscos em um único risco para desenvolver uma compreensão mais completa do risco global.
Alerta precoce (*Early warning*) ISO 22300:2021	Fornecimento de informações através de redes locais, permitindo às pessoas afetadas tomar medidas para evitar ou reduzir os riscos e preparar respostas.
All-hazards ISO 22300:2021	Eventos naturais, eventos antropogénicos (intencionais e não intencionais) e eventos tecnológicos com potencial impacto numa organização, comunidade ou sociedade e no ambiente de que depende.
Ameaça ISO 31000:2018 | ISO 31073:2022	Fonte potencial de perigo, dano ou outro resultado indesejável.
Ameaças híbridas Organização do Tratado do Atlântico Norte [OTAN] (2023)	Combinação ampla, complexa e adaptável, de meios convencionais e não-convencionais e de medidas militares, paramilitares e civis, encobertas e abertas […] visando destabilizar e minar as sociedades para alcançar os respetivos objetivos, utilizando várias ferramentas e táticas, incluindo, físicas, tecnológicas, humanas ou económicas.
Ameaça interna (*Insider threat*) CNCS - Glossário (s.d.)	Traduz-se no abuso de forma involuntária ou intencional, de qualquer atual colaborador ou ex-colaborador, sócio ou fornecedor, que tenha, ou tenha tido, acesso aos ativos digitais da organização. Os três tipos mais comuns de ameaças internas são: insider malicioso, que age intencionalmente; insider negligente, que é desleixado ou não está em conformidade com as políticas e instruções de segurança; e insider comprometido, que age involuntariamente como instrumento de um atacante real.
Análise da criticidade ISO 22300:2021	Processo concebido para identificar e avaliar sistematicamente os ativos de uma organização com base na importância da sua missão ou função, no grupo de pessoas em risco, ou no significado de um acontecimento indesejável ou de uma perturbação na sua capacidade de satisfazer as expectativas.
Análise de impactos (ou consequências) ISO 22300:2021	Processo de análise de todas as funções operacionais e do efeito que uma interrupção operacional pode ter sobre elas.
Avaliação dos riscos Diretiva REC (Diretiva 2022/2557, de 14 de dezembro)	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;
ISO 31000:2018 | ISO 31073:2022	Processo de comparação dos resultados da análise de riscos com os critérios de risco para determinar se o risco é aceitável ou tolerável.
Benchmarking Stapenhurst (2009, pp. 3-6)	Método que visa melhorar níveis de desempenho organizacional através da comparação com os melhores. Comparação dos níveis de desempenho para determinar que organizações estão a atingir níveis de desempenho superiores, seguido da identificação, adaptação/melhoria, e adoção das práticas que conduzem a estes níveis superiores de desempenho.

[37] Conceitos estruturantes definidos no subcapítulo 2.1: (i) Estratégia; (ii) Entidades e Infraestruturas Críticas; e (iii) Resiliência de Entidades e Infraestruturas Críticas.

[38] Lista não exaustiva. Sugere-se a consulta das referências elencadas, mormente das normas ISO, para clarificação de outros conceitos associados.

Boa prática U.S. DHS (2015)	Uma boa prática avalia o que já existe, que lições foram aprendidas, e o que deve ser alterado ou evitado para o fazer possível, visando atingir objetivos definidos. Assim, uma boa prática corresponde a um método ou técnica comprovadamente capaz de apresentar resultados bem-sucedidos.
Capacidade ISO 22300:2021	Combinação de todos os pontos fortes e recursos disponíveis dentro de uma organização, comunidade ou sociedade que podem reduzir o nível de risco ou os efeitos de uma crise. A capacidade pode incluir meios físicos, institucionais, sociais ou económicos, bem como pessoal qualificado ou atributos como liderança e gestão.
Ciber (*Cyber*) Gheorghe et al. (2018)	Conceito de ampla aplicabilidade, associado ao ciberespaço. No âmbito da securitização das IC, corresponde à prevenção, proteção e recuperação dos sistemas e tecnologias de informações, comunicações e de operações das IC.
Ciberataque CNCS - Glossário (s.d.)	Ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente. Ataque corresponde a qualquer tipo de atividade maliciosa que tenta coletar, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si.
Cibercrime ENSC 2019-2023 (RCM n.º 92/2019, de 05 de junho)	Os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa.
Ciberespaço ENSC 2019-2023 (RCM n.º 92/2019, de 05 de junho)	Ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.
Ciber-higiene CNCS - Glossário (s.d.)	Aplicar boas práticas do mundo digital. Por exemplo: não ler e-mails de origem desconhecida; manter sempre os sistemas autorizados; fazer cópias de segurança; proteger sistemas com password forte; e ter os devidos cuidados com a segurança física.
Cibersegurança ENSC 2019-2023 (RCM n.º 92/2019, de 05 de junho)	Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.
Comando e controlo ISO 22300:2021	Atividades de tomada de decisão orientadas para objetivos, incluindo a avaliação da situação, o planeamento, a execução das decisões e o controlo dos efeitos da execução.
Comunicação e consulta ISO 22300:2021	Processos contínuos e iterativos que uma organização conduz para fornecer, partilhar ou obter informações e para dialogar com as partes interessadas e outros relativamente à gestão do risco. A consulta é um processo bidirecional de comunicação informada entre uma organização e as suas partes interessadas ou outros sobre uma questão antes de tomar uma decisão ou determinar uma orientação sobre essa questão. A consulta é: (i) um processo que tem impacto numa decisão através da influência e não do poder; e (ii) um contributo para a tomada de decisões, e não uma tomada de decisões conjunta.
Cooperação ISO 22300:2021	Processo de trabalho ou atuação em conjunto visando interesses e valores comuns com base num acordo.
Coordenação ISO 22300:2021	Forma como diferentes organizações, públicas ou privadas, ou partes de uma mesma organização trabalham ou atuam em conjunto para atingir um objetivo comum.
Crise ISO 22300:2021	Condição instável que envolve uma mudança abrupta ou significativa iminente que requer atenção e ação urgentes para proteger a vida, os bens, a propriedade ou o ambiente.

Gestão de crises ISO 22300:2021	Processo de gestão holística que identifica potenciais impactos que ameaçam uma organização e estabelece um quadro para o desenvolvimento de resiliência, com capacidade para uma resposta eficaz que salvaguarde os interesses das principais partes interessadas da organização, a sua reputação, a sua marca e as suas atividades criadoras de valor, bem como o restabelecimento efetivo das suas capacidades operacionais. A gestão de crises também envolve a gestão da preparação, mitigação, resposta e continuidade ou recuperação no caso de um incidente, bem como a gestão do programa global através de formação, simulações e revisões para assegurar que os planos de preparação, resposta e continuidade se mantêm atuais e atualizados.
Entidade crítica Diretiva REC (Diretiva 2022/2557, de 14 de dezembro)	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 [da Diretiva REC].
Exercício ISO 22300:2021| ISO 22301:2019	Processo para formar, avaliar, praticar e melhorar o desempenho de uma organização. Os exercícios podem ser utilizados para validar políticas, planos, procedimentos, formação, equipamento e acordos interorganizacionais; elucidar e treinar o pessoal em funções e responsabilidades; melhorar a coordenação interorganizacional e as comunicações; identificar lacunas nos recursos; melhorar o desempenho individual e identificar oportunidades de melhoria; e uma oportunidade controlada para praticar o improviso.
Estratégia nacional de cibersegurança Diretiva SRI2 (Diretiva 2022/2555, de 14 de dezembro)	Quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos no domínio da cibersegurança e define a governação com vista à sua consecução no Estado-Membro em causa.
Gestão do risco ISO 31000:2018 | ISO 22301:2019 | ISO 31073:2022	Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. Método através da qual uma organização avalia e incorpora o impacto que determinado perigo ou ameaça representa para a sua atividade, tendo em conta as suas vulnerabilidades, a probabilidade de concretização do perigo ou ameaça e as suas consequências. É um processo sistematizado que integra o mapeamento de riscos; a avaliação de impactos e probabilidades dos riscos; a priorização dos riscos com maior gravidade; o tratamento dos riscos priorizados; e a monitorização constante de todos os riscos.
Governança The World Bank (2017)	Processo através do qual os atores estatais e não estatais interagem para conceber e implementar políticas dentro de um determinado conjunto de regras formais e informais que moldam ou são moldadas pelo poder.
Grau de Risco Apêndice 7 do Anexo B ao Plano de Coordenação, Controlo e Comando Operacional das Forças e dos Serviços de Segurança (SSI, 2010)	Definido em função da probabilidade de materialização da(s) ameaça(s) sobre um determinado alvo, das vulnerabilidades do alvo e das consequências expectáveis caso a ameaça se concretize. Pode ser representado por: Grau de risco = *f* (Probabilidade (Ameaça), Vulnerabilidades + Consequências)
Hacktivistas CNCS - Glossário, s.d.	Atores de ameaças orientados a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais.
Identificação de riscos ISO 31000:2018 | ISO 31073:2022	Processo de busca, reconhecimento e descrição de riscos. A identificação de riscos envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

Incerteza ISO 31000:2018 | ISO 31073:2022	Estado, ainda que parcial, de deficiência de informação relacionada à compreensão ou conhecimento.
Incidente Diretiva REC (Diretiva 2022/2557, de 14 de dezembro)	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.
ISO 22300:2021	Acontecimento que pode ser, ou pode levar a uma perturbação, perda, emergência ou crise.
Incidente de cibersegurança Diretiva SRI2 (Diretiva 2022/2555, de 14 de dezembro)	Evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes.
Informações CNCS - Glossário (s.d.)	Conhecimento que pode ser comunicado sob qualquer forma. Dados que foram interpretados ou organizados de forma coerente e posteriormente comunicados sendo então possível tirar conclusões do seu significado.
Informações sensíveis Decreto-Lei n.º 20/2022, de 28 de janeiro	Factos, dados e informação relacionados com a segurança de uma infraestrutura crítica, que são considerados informação classificada (…), nomeadamente a sua designação, os respetivos planos de segurança, assim como outros elementos que, se divulgados, podem ser utilizados para planear e agir com o objetivo de provocar a perturbação do funcionamento ou a destruição da infraestrutura crítica
Infraestrutura ISO 22300:2021	Sistema de instalações, de equipamentos e de serviços necessários ao funcionamento de uma organização.
Infraestrutura crítica Decreto-Lei n.º 20/2022, de 28 de janeiro	Componente, sistema ou parte deste que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o 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.
Infraestrutura crítica de informação CNCS - Glossário (s.d.)	Qualquer sistema de tecnologias da informação que suportem ativos fundamentais e serviços das infraestruturas nacionais.
Interoperabilidade ISO 22300:2021	capacidade de diversos sistemas e organizações trabalharem em conjunto.
Monitorização ISO 31073:2022	Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.
Nível de Risco ISO 31000:2018 | ISO 31073:2022	Magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades.
Operador Decreto-Lei n.º 20/2022, de 28 de janeiro	Proprietário ou a entidade responsável pelo funcionamento de uma infraestrutura crítica, nacional ou europeia.
Objetivo ISO 31073:2022	Resultado a ser alcançado. Um objetivo pode ser estratégico, operacional ou tático. Pode ser expresso como um resultado pretendido, um propósito, um critério operacional, como objetivo de um sistema de gestão, ou pelo uso de outras palavras com significado similar (*e.g.* finalidade, meta, alvo).
Organização ISO 22300:2021	Pessoa ou grupo de pessoas que tem as suas próprias funções com responsabilidades, autoridades e relações para atingir os seus objetivos.
Parceria ISO 22300:2021	Relação organizada entre dois organismos (público-público, privado-público, privado-privado) que estabelece o âmbito, as funções, os procedimentos e os instrumentos para prevenir e gerir qualquer incidente com impacto na segurança e na resiliência.

Parte interessada (*stakeholder*) ISO 31000:2018	Pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade. Pode ser um indivíduo ou um grupo que tem um interesse em qualquer decisão ou atividade de uma organização.
Perigo ISO 31000:2018	Fonte potencial de dano.
Planeamento ISO 22300:2021	Parte da gestão centrada na fixação de objetivos e na especificação dos processos operacionais necessários, bem como dos recursos intrínsecos, à prossecução dos objetivos.
Plano de continuidade do negócio/atividade ISO 22301:2019	Procedimentos documentados que orientam as organizações para responder, recuperar, retomar e restaurar um nível pré-definido de operacionalização, após disrupção.
Plano de segurança de infraestrutura crítica Decreto-Lei n.º 20/2022, de 28 de janeiro	Documento, elaborado pelo operador, destinado a identificar os elementos essenciais e as vulnerabilidades da infraestrutura crítica, bem como as medidas e ações a executar para assegurar a sua proteção e aumentar a sua resiliência.
Ponto ou instalação sensível Regulamento Geral de Serviço da GNR	Local ou instalação que importa preservar por ser considerado de interesse especial, de forma a evitar que sobre eles se exerçam ações que possam prejudicar o fim a que se destinam ou colocar em perigo a segurança das pessoas que os ocupam e dos bens que neles existam.
Prevenção ISO 22300:2021	Medidas que permitem a uma organização evitar, impedir ou limitar o impacto de um acontecimento indesejável ou de uma potencial perturbação.
Processo de avaliação de riscos (*risk assessment*) ISO 31073:2022	Processo global de identificação de riscos, análise de riscos e avaliação de riscos (*risk evaluation*).
Processo de gestão de riscos ISO 31000:2018 | ISO 31073:2022	Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitorização e análise crítica dos riscos.
Proteção ISO 22300:2021	Medidas que salvaguardam e permitem a uma organização reduzir o impacto de uma potencial perturbação.
Rede CNCS - Glossário (s.d.)	Conjunto formado por entidades e as suas interconexões. Em topologia de rede ou numa estrutura abstrata, as entidades interconectadas são pontos e as interconexões são linhas num esquema. Numa rede de computadores, as entidades interconectadas são computadores ou equipamentos de comunicação de dados e as interconexões são ligações de dados.
Redução do risco de catástrofe ISO 22300:2021	Política destinada a prevenir novos riscos de catástrofes e a reduzir os existentes, bem como a gerir os riscos residuais, contribuindo todos eles para o reforço da resiliência e, por conseguinte, para a consecução do desenvolvimento sustentável
Resiliência Diretiva REC (Diretiva 2022/2557, de 14 de dezembro)	Capacidade de uma entidade crítica para prevenir incidentes, se proteger deles, lhes dar resposta, lhes resistir, os atenuar, os absorver, se adaptar a eles e recuperar deles
Robustez ISO 22300:2021	Capacidade de um sistema para resistir a ataques virtuais ou físicos, internos ou externos.
Reskilling *Cambridge Dictionary* (s.d.)	Processo de aprendizagem de novas aptidões para que se possa fazer um trabalho diferente, ou de formação de pessoas para fazer um trabalho diferente.
Risco Diretiva REC (Diretiva 2022/2557, de 14 de dezembro)	Potencial de perda ou perturbação causada por um incidente, expresso como uma combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente.

ISO 31000:2018 | ISO 31073:2022	Efeito da incerteza sobre os objetivos. Resulta da combinação entre a probabilidade de um evento (ameaça) e as suas consequências na exploração de uma vulnerabilidade de um bem ou recurso. Expressa-se na probabilidade de materialização dos perigos ou ameaças sobre um determinado alvo num determinado período de tempo.
Risco residual	Risco remanescente após o tratamento do risco.
ISO 31073:2022	
CNCS - Glossário (s.d.)	Risco que permanece após terem sido aplicadas medidas de segurança, dado que não é possível neutralizar todas as ameaças nem eliminar todas as vulnerabilidades.
Safety	Condição artificial de ausência de perigo em relação ao ativo e ao seu ambiente. Resulta da implementação de medidas destinadas a evitar, prevenir, minimizar ou proteger, a ocorrência de danos que podem ser causados ao ativo por fontes não intencionais.
Manunta (1999)	
Security	Condição artificial de ausência de, ou liberdade do, perigo e preocupação, relativamente ao ativo. Resulta da implementação de medidas destinadas a evitar, prevenir, minimizar ou proteger, a ocorrência de danos que possam ser intencionalmente causados ao bem.
Manunta (1999)	
ISO 22300:2021	Estado de ausência de perigo ou de ameaça quando os procedimentos são respeitados ou após a adoção de medidas adequadas.
Sistema de gestão	Conjunto de elementos inter-relacionados ou interatuantes de uma organização, para o estabelecimento de políticas, objetivos e de processos para atingir esses objetivos.
ISO 22301:2019	
Segurança da informação	Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças.
CNCS - Glossário (s.d.)	
Serviço essencial	Serviço que é indispensável à manutenção de funções societais ou atividades económicas vitais, da saúde e segurança pública ou do ambiente
Diretiva REC (Diretiva 2022/2557, de 14 de dezembro)	
Tratamento de riscos	Processo para modificar o risco. O tratamento de risco pode envolver: (i) a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; (ii) assumir ou aumentar o risco, a fim de buscar uma oportunidade; (iii) a remoção da fonte de risco; (iv) a alteração da probabilidade (*likelihood*); (v) a alteração das consequências; (vi) a partilha do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e (vii) a retenção do risco por uma escolha consciente. O tratamento de riscos relativos a consequências negativas é frequentemente designado como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos".
ISO 31073:2022	
Upskilling	Processo de aprendizagem de novas competências ou de ensino de novas competências aos colaboradores.
Cambridge Dictionary (s.d.)	
Vulnerabilidade	Propriedades intrínsecas de algo, resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência
ISO 31000:2018 | ISO 31073:2022	
CNCS - Glossário (s.d.)	Insuficiência, seja de que natureza for, que possa ser explorada por uma ou mais ameaças. A vulnerabilidade pode consistir numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional;

Apêndice B – Fases, capacidades e dimensões da REC

No prisma de Sathurshan et al. (2022), comum a outros autores, a resiliência tem por finalidade a rápida recuperação (ou mesmo superação) do nível de desempenho face a um evento disruptivo, traduzido sobretudo na capacidade de adaptação, graficada na Figura 16.

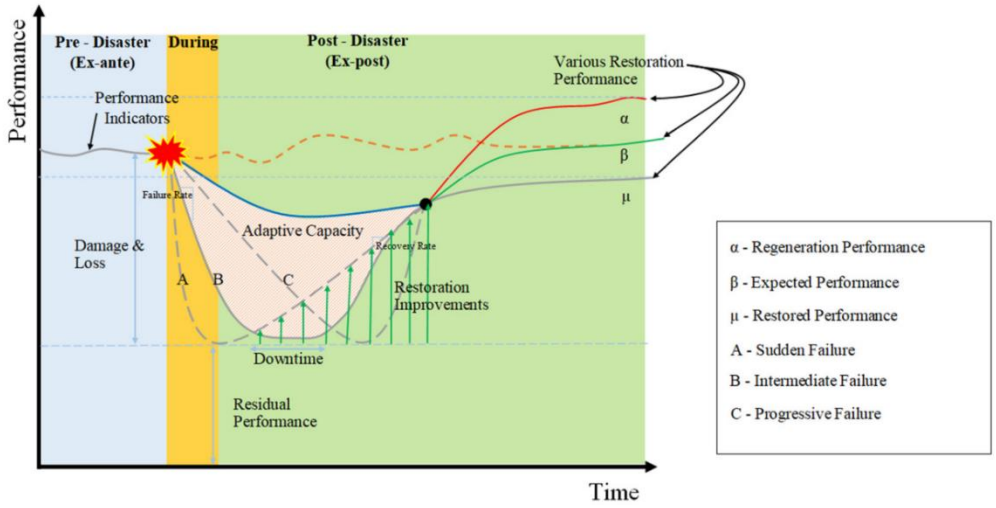

Figura 16 - Resiliência como capacidade de adaptação

Fonte: Sathurshan et al. (2022, p. 3).

Através de uma análise comparativa, Sathurshan et al. (*op. cit.*, p. 18) congrega os atributos-chave para inferir sobre a resiliência de uma infraestrutura antes, durante e após a ocorrência de uma disrupção, os quais se ilustram na Figura 17.

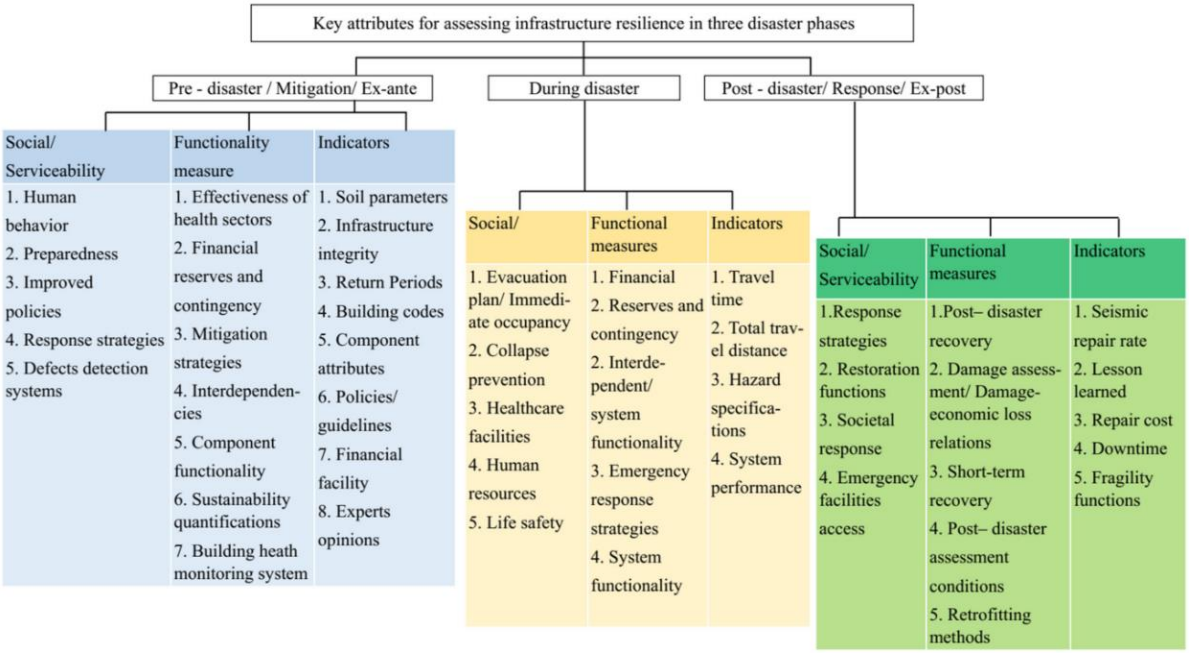

Figura 17 - Principais atributos para avaliar a resiliência de IC nas três fases da catástrofe

Fonte: Sathurshan et al. (2022, p. 18).

Conforme sintetizado por Bertocchi et al. (2016, p. 8-9), a REC alicerça-se numa abordagem multifacetada, que congrega múltiplas problemáticas, como: segurança; gestão do risco; continuidade da atividade (*business continuity*); e gestão de crises e emergências.

Segundo Rehak et al. (2019, p. 127), a resiliência de IC deve seguir uma lógica cíclica, propondo para o efeito um *framework* de avaliação, conforme se ilustra na Figura 18.

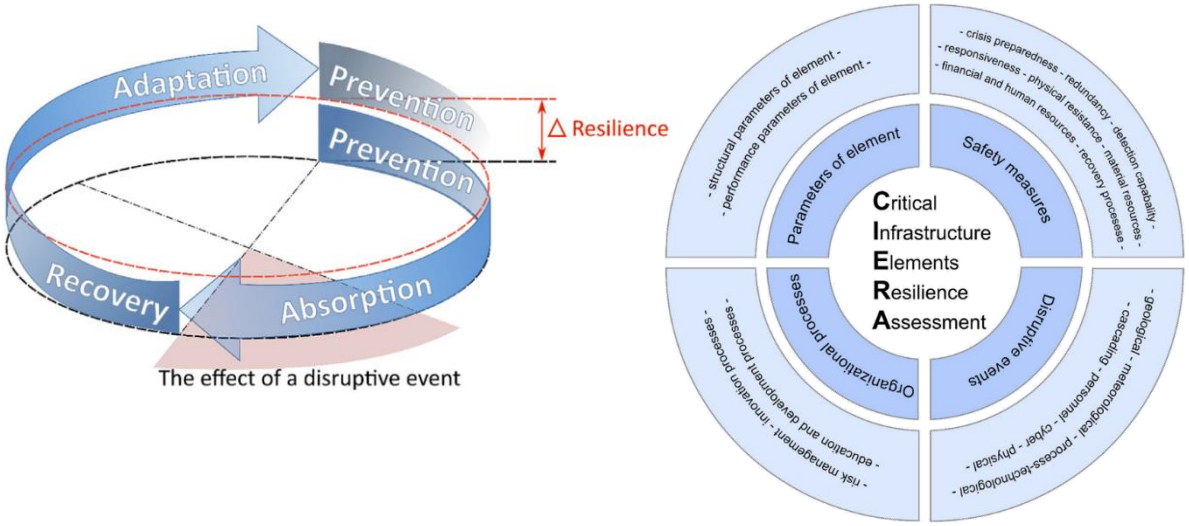

Figura 18 - Ciclo e *framework* de avaliação da REC

Fonte: Rehak et al., (2019, p. 127-128).

No que concerne às capacidades de resiliência, seguindo a doutrina anglo-saxónica, Bertocchi et al. (2016, p. 16) considera serem:

- *Preventiva*: capacidade de um sistema antecipar eventos perturbadores;
- *Absortiva*: grau em que um sistema pode absorver automaticamente o impacto das perturbações e minimizar as consequências;
- *Adaptativa*: grau em que o sistema é capaz de se auto-organizar para recuperar os níveis de desempenho;
- *Restaurativa*: a capacidade de um sistema ser rápida e facilmente reparado.

Analogamente, seguindo uma abordagem cíclica, a resiliência associa-se ao ciclo da catástrofe, tal como no manual de Boas Práticas de Resiliência de Infraestruturas Críticas[39], da Plataforma Nacional de Redução de Risco de Catástrofes (PNRRC), conforme Figura 19.

[39] Única referência de doutrina em Portugal sobre a resiliência de IC.

Figura 19 - Ciclo da catástrofe

Fonte: adaptado a partir de Oliveira, J. et al., (2017).

Em linha, Jovanović et al. (2016) apresentam indicadores de resiliência de dois níveis, conforme sistematizado na Figura 20.

Figura 20 - Indicadores de resiliência de 1.º e de 2.º nível

Fonte: adaptado a partir de Jovanović et al. (2016, p. 22)

Quanto às dimensões da resiliência de IC, Bertocchi et al. (2016, p. 15) consideram quatro:

- *Técnica / Lógica e Física*: emprego das mais atuais e eficientes tecnologias na proteção cibernética e física, considerando as aplicações específicas do sector;
- *Pessoal / Humana*: definição do perfil das pessoas responsáveis pela resiliência da IC, certificação das competências dos peritos e respetivo programa de formação, bem como a sensibilização e envolvimento de todas as pessoas no desafio global da segurança;
- *Organizacional*: definição e implementação de um sistema de gestão da Resiliência, atribuições e níveis de responsabilidade;
- *Cooperativa*: promoção da cooperação entre diferentes operadores de IC, tanto privados como públicos, bem como a definição de processos e a difusão de boas práticas.

Verifica-se outra corrente considerável de outros autores que incluem a dimensão cooperativa na organizacional, enquanto consideram também a dimensão económica. Numa revisão sistemática da literatura, Curt & Tacnet (2018) analisam a multiplicidade de abordagens às dimensões da resiliência, no intento de sistematizar os aspetos mais comummente considerados, o quais são graficamente resumidos na Figura 21.

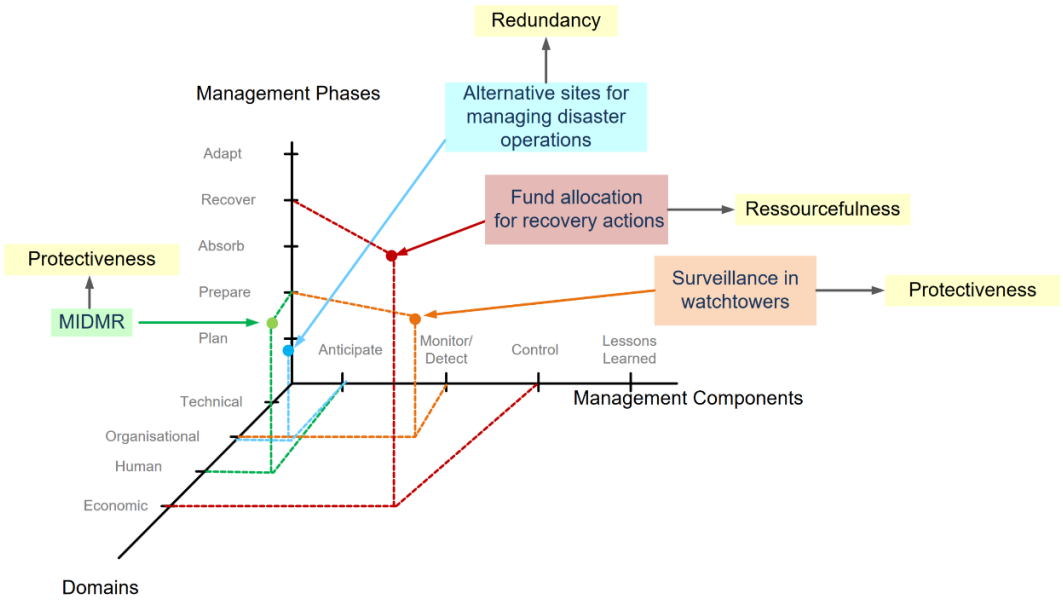

Figura 21 - Diferentes dimensões da REC

Fonte: Curt e Tacnet (2018, p. 14).

Na esteira dos trabalhos de Jovanović et al. (2016), a multiplicidade de categorizações atinentes às dimensões, indicadores e capacidades da resiliência constitui-se numa das atuais problemáticas, sendo que a indefinição de critérios transversais aos setores, subsetores e respetivas IC, resulta em complexidade adicional para a condução de uma avaliação de risco holística, dificultando a correspondente priorização das medidas de mitigação.

Da correlação entre as fases e as dimensões da resiliência, a equipa de investigadores do programa *SmartResilience* propõe uma síntese de medidas de resiliência conforme Quadro 12.

Quadro 11 - Medidas de resiliência, segundo fases e dimensões

	Percecionar Riscos	Antecipar / Preparar	Absorver / Resistir	Responder / Recuperar	Adaptar/ Aprender
Técnica Sistema / Física	– Revisão dos riscos para a IC física e rede de IC	– Estabelecer os recursos físicos de segurança e proteção	– Sistema de segurança física e componentes redundantes	– Flexibilidade na conceção do sistema, instalação temporária do sistema	– atualização das configurações do sistema com base nas lições aprendidas
Humana	– *Veetings* de segurança – Monitorar ameaças internas	– Formação e sensibilização de RH – Definição de responsabilidades	– Reservas de mantimentos – Apoio médico	– Salvaguarda da vida humana	– Formação sobre novos procedimentos
Organizacional	– Revisão organizacional periódica dos riscos relevantes, relatórios sobre eventos anteriores	– Orçamento e planos de preparação – Tratamento do risco – Políticas e guias	– Disponibilidade de um plano de ação e de pessoal competente para reação imediata a eventos	– Disponibilidade de orçamento e recursos de resposta de emergência suficientes	– *Debriefing* do evento e das operações de resposta ao pessoal diretamente envolvido
Informacional	– Consciência situacional (abordagem *All-Hazards*) – *Foresight* e Cenarização	– Informação de eventos anteriores (o que correu mal/bem) para aprender com erros e sucessos	– Monitorização em tempo real e automatismos	– Informação sobre instalações centralizadas e distribuição de fornecimentos e serviços essenciais	– Informação de sensores sobre eventos, operações de resposta e lições aprendidas
Cognitiva / Processo de Decisão	– Critérios de decisão (Perceção de risco, modelos mentais, indicadores)	– Capacidade de alerta sobre ameaças – Sistema de *Early warning*	– Capacidade de consciência situacional dos indivíduos para avaliar o desempenho durante o evento	– Transparência na resposta e na tomada de decisão e comunicação da recuperação	– Melhoria na tomada de decisões para lidar com eventos futuros
Cooperativa	– Esquematização e análise de interdependências – Partilha de informações – Parcerias e *Networking*	– Simulacros conjuntos	– Coordenação entre atores – Liderança	– Resposta a emergências – Coordenação e sinergias entre atores	– Partilha de boas práticas
Económica	– Estudo de impactos	– Investimento em segurança conjunto (economia de escala) – Reservas financeiras	– Distribuição de reservas	– Reparação, reconstrução e Recuperação	– Avaliação – *Security by design*
Política / Societal	– Troca de conhecimentos sobre riscos (incluindo perceções de risco na sociedade)	– Procura de informação das autoridades sobre avaliações de ameaças e preparação	– Alerta e comunicação externa	– Contacto/ligação com autoridades/ meios de comunicação social e comunicação regular	– Comunicação com as entidades envolvidas para transformar os procedimentos anteriores

Fonte: adaptado e ampliado a partir de Jovanović et al. (2016, p.41)

Apêndice C – Foco na análise de interdependências e Gestão do Risco para a REC

A perceção dos efeitos em cascada de múltipla ordem mediante a ocorrência de disrupções em IC, alavancou o desenvolvimento de análises de interdependências intra e intersectoriais (Comissão Europeia, 2020a; 2020b, pp. 6-7; 2020c), conforme se exemplifica na Figura 22.

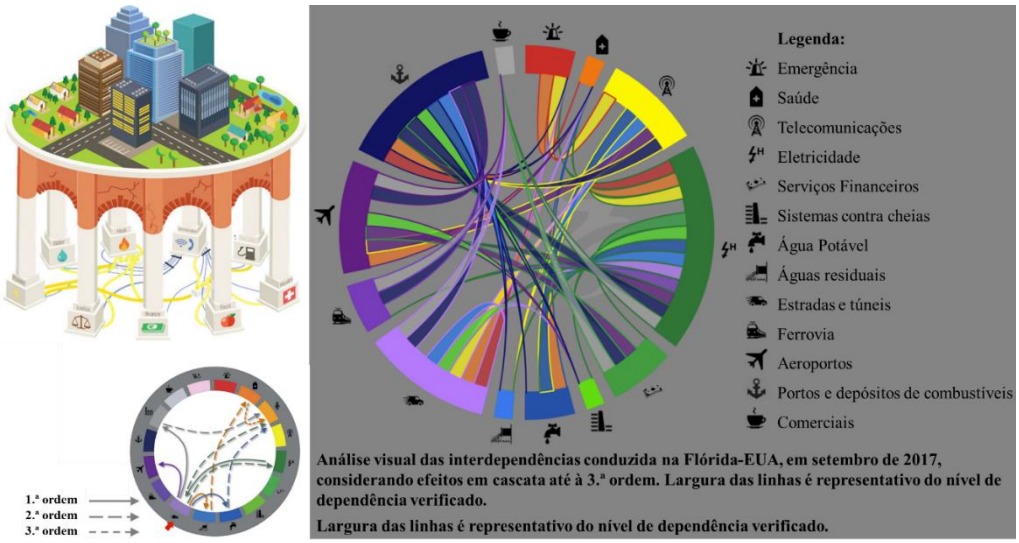

Figura 22 – Análise visual das interdependências de IC
Fonte: adaptado a partir de Jeuken et al. (2019).

Nos EUA, a Agência para a Cibersegurança e Segurança de Infraestruturas (CISA[40]), desenvolveu em 2021 a análise quanto às principais interdependências setoriais, sistematizadas através da matriz constante da Figura 23.

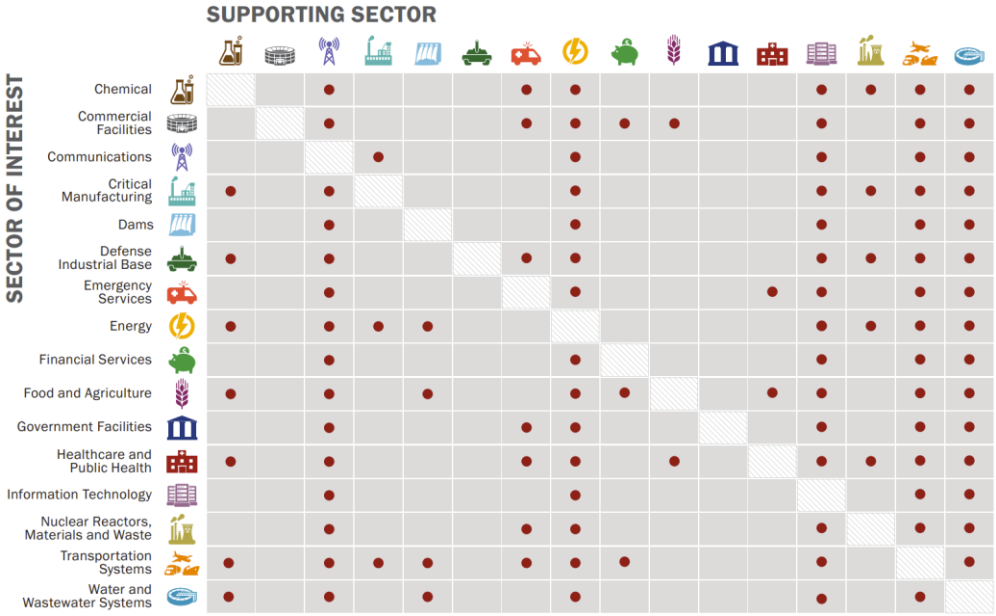

Figura 23 - Matriz de interdependências setoriais

Fonte: CISA (2021, p. 12).

[40] *Cybersecurity & Infrastructure Security Agency*, integrada no DHS.

Na mesma publicação (CISA, 2021, p. 14), enfatizam-se os efeitos que as interdependências suscitam no risco, exponenciando o seu grau, conforme sintetizado na Figura 24.

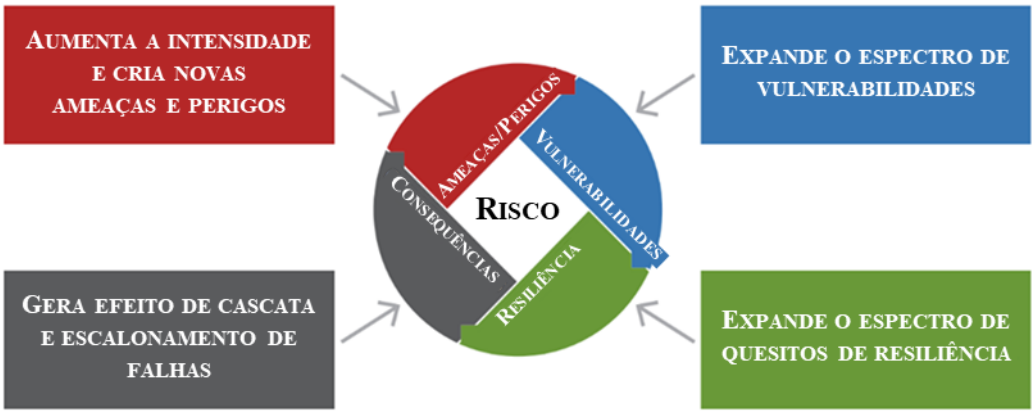

Figura 24 - Efeitos da (inter)dependência de IC no risco

Fonte: adaptado a partir de CISA (2021, p. 14).

Numa abordagem procedimental e focada no planeamento, a CISA vem promovendo a difusão de um *framework* para a gestão do risco de IC (CISA, 2019, p. 15), modelo este que foi adaptado em Portugal pela Guarda Nacional Republicana (GNR), e ministrado nos Cursos de Segurança e Proteção de Infraestruturas (CSPI), organizados em colaboração com 42 entidades parceiras, procurando promover a confiança e partilha de informação, bem como abordagens, métodos e técnicas comuns (GNR, 2020), conforme Figura 25.

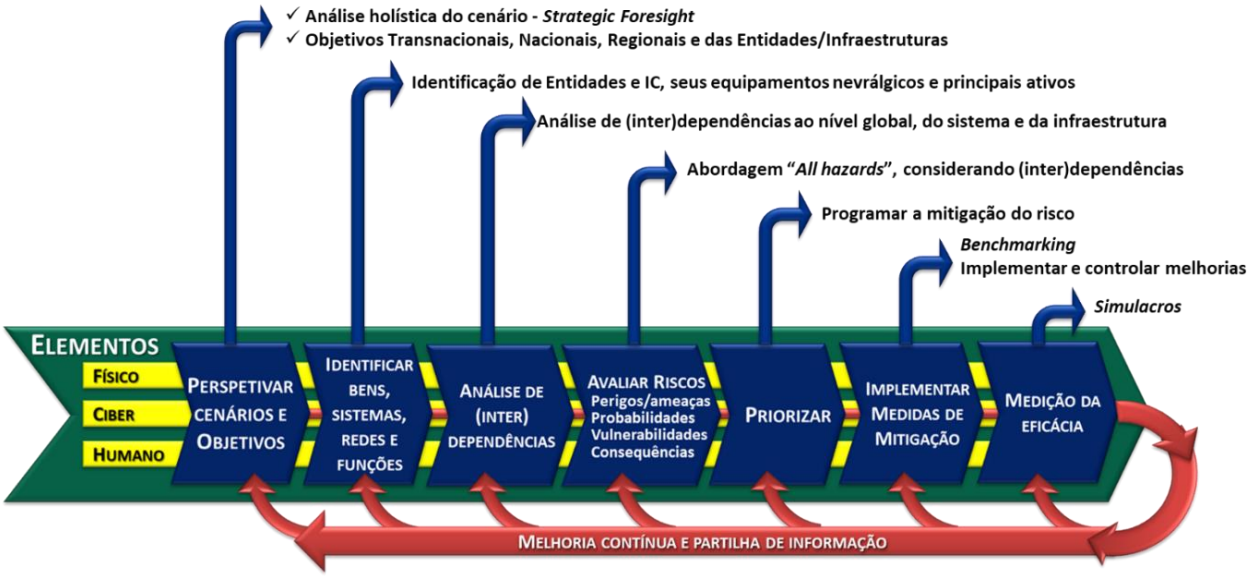

Figura 25 - *Framework* de Planeamento e Gestão de Risco para IC

Fonte: adaptado pela GNR (2020) de CISA (2019, p. 15).

Apêndice D – Sistematização de documentos estruturantes, europeus e nacionais, intrínsecos à temática da REC

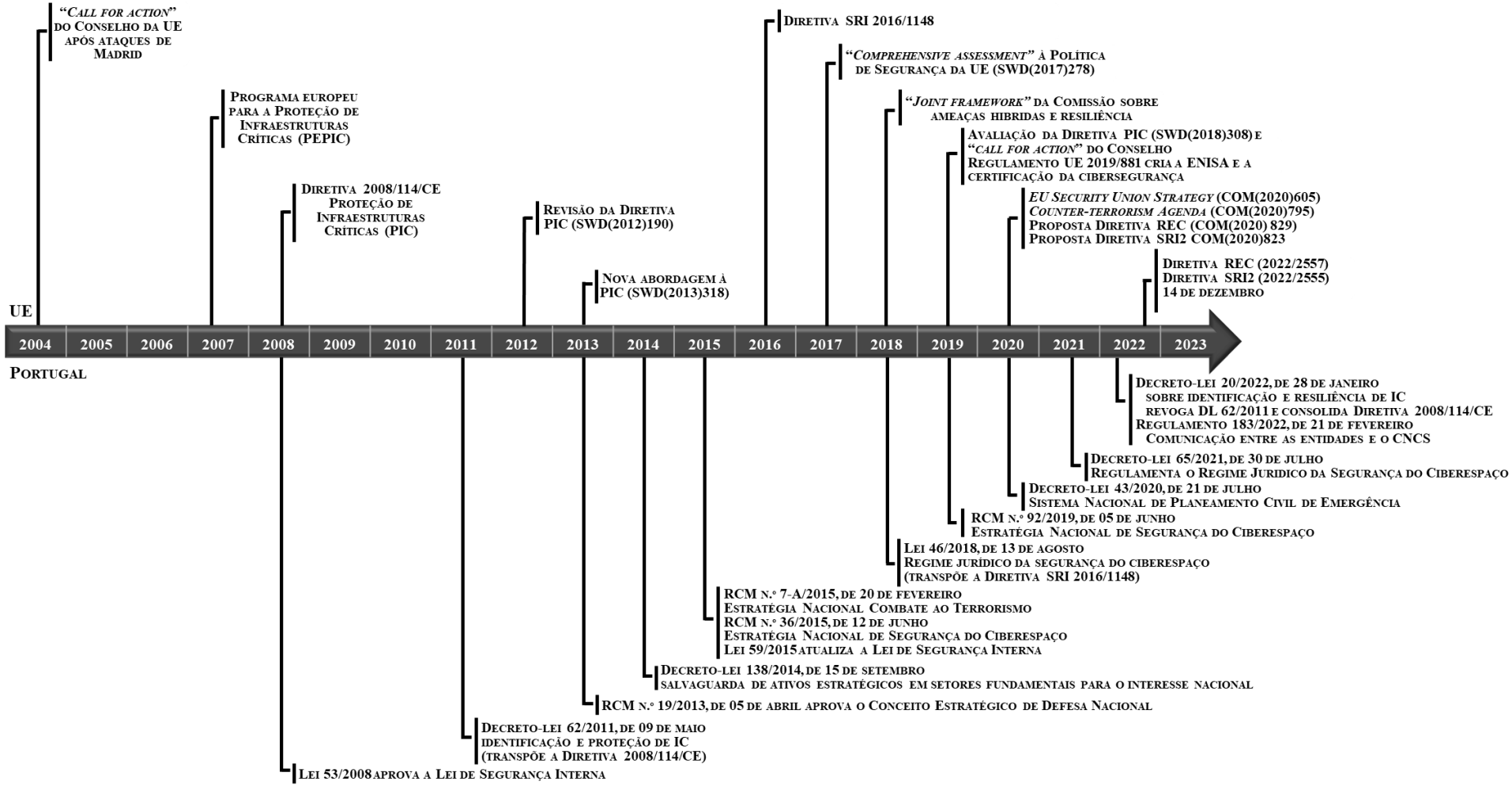

Figura 26 - Sistematização de documentos estruturantes, nacionais e europeus, intrínsecos à temática da REC

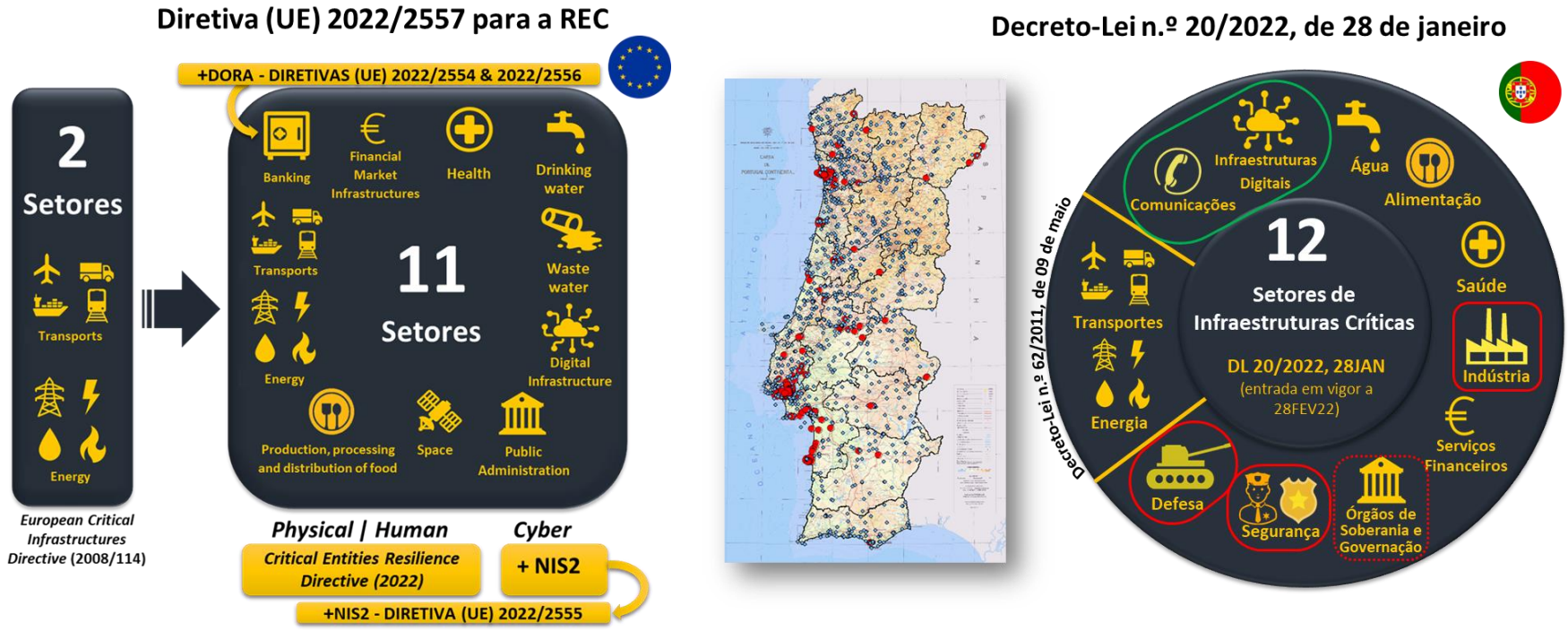

Figura 27 – Comparação dos setores críticos segundo Diretiva REC e o atual diploma nacional

Apêndice E – Modelo de Análise

Quadro 12 - Modelo de análise

Tema	Resiliência de Entidades Críticas: contributos para uma Estratégia Nacional.			
Problema	Quais os vetores estruturantes para formular uma estratégia nacional para a resiliência de entidades críticas (REC) em Portugal?			
Objeto de estudo	Estratégia Nacional para a resiliência de entidades críticas em Portugal.			
Delimitação	**Temporal** 08DEC2008 (aprovação da Diretiva CIP) até 14ABR2023 (fim da investigação)	**Espacial** Portugal (com *benchmarking* de outros modelos de referência)	**Conteúdo** Prioridades a considerar na formulação estratégica para a REC em Portugal à luz da nova Diretiva UE 2022/2557	
Objetivo Geral	Formular contributos para uma Estratégia Nacional de Resiliência de Entidades Críticas em Portugal.			
Questão Central	Quais as prioridades estratégicas a considerar na formulação da Estratégia Nacional para a Resiliência de Entidades Críticas em Portugal?			
Metodologia	**Posição** Ontológico construtivista Epistemológica do interpretativista (Bryman, 2012; Santos & Lima, 2019, pp. 16-18)	**Raciocínio:** Indutivo (Creswell & Creswell, 2018, p.41; Santos & Lima, 2019, p. 36)	**Estratégia:** Qualitativa (Santos & Lima, 2019, p. 18)	**Desenho da pesquisa:** Estudo de caso único - português (Yin, 2018, p. 18)

	Objetivos Específicos	Questões derivadas	Conceitos estruturantes	Dimensões			Variáveis	Técnicas de recolha
Benchmarking	**OE1** Descrever as principais prioridades estratégias adotadas para a REC por países de referência na temática	**QD1** Quais as principais prioridades estratégicas adotadas para a REC por países de referência na temática?	Estratégia	Estratégia para a Resiliência de Infraestruturas Críticas			– Princípios – Orientações / Objetivos estratégicos – Vetores / áreas estratégicas – Medidas / atividades-chave	**1.ª Fase** - Entrevistas abertas (exploratórias); - Análise documental de normas, bibliografia e trabalhos académicos, com triangulação de dados, privilegiando fontes primárias; **2.ª Fase** - Entrevistas Semiestruturadas (*expert & elite interviewing*) - Análise documental de normas, bibliografia e trabalhos académicos, com triangulação de dados, privilegiando fontes primárias;
Diagnóstico Estratégico	**OE2** Examinar o quadro normativo e institucional	**QD2** Qual o enquadramento normativo e o papel dos atores para a REC?	Infraestruturas/ Entidades Críticas	Europeia			– Normas – Atores	
				Nacional				
	OE3 Avaliar o ambiente estratégico	**QD3** Que principais ameaças, oportunidades, potencialidades e vulnerabilidades influem na formulação de uma estratégia para a REC em Portugal?		Fatores estratégicos	Exógenos	– Político-Legais – Económicos Socioculturais – Tecnológicos	– Ameaças – Oportunidades	
					Endógenos	– Estrutura – Cultura – Recursos	– Potencialidades – Vulnerabilidades	
	OE4 Analisar as perceções dos atores quanto às prioridades estratégicas	**QD4** Quais são as perceções dos atores quanto às prioridades estratégicas para a REC?	Resiliência	Público		– Atores do SSI; – Entidades Setoriais; – Internacional e I&D	– Perceções – Prioridades	
				Privado		– Operadores de IC;		

Apêndice F – Guião de entrevista[41]

A. IDENTIFICAÇÃO DO ENTREVISTADO

Nome:

Cargo/Função:

Habilitações literárias:

Data e local:

B. ENTREVISTA

ENQUADRAMENTO

Na atual conjuntura da Globalização 4.0, marcada pela transformação digital, dinâmicas aceleradas e tecnologias disruptivas, todavia também pelo crescente espectro de ameaças híbridas e vulnerabilidades, resulta insofismável que as Entidades Críticas (EC), enquanto fornecedores de Serviços Essenciais (SE), desempenham um papel nevrálgico na manutenção das funções sociais e das atividades económicas vitais, num ambiente de crescente conectividade de sistemas. Em tal contexto, tornou-se prioridade para a União Europeia (UE) reforçar a sua resiliência face a toda a tipologia de perigos, de origem natural, humana, acidentais ou intencionais, procurando mitigar potenciais perturbações, geradoras de efeitos nefastos em cascata, resultantes das interdependências entre as Infraestruturas Críticas (IC).

A evolução do paradigma na UE ditou a substituição da Diretiva respeitante à *Proteção de Infraestruturas Críticas* (PIC) (Diretiva 2008/114/CE, de 08 de dezembro) pela nova Diretiva focada na *Resiliência de Entidades Críticas* (REC) (Diretiva 2022/2557, de 14 de dezembro). Procura-se fomentar uma abordagem mais holística e integrada, sustentada na contínua gestão do risco, na monitorização integrada de ameaças ciber-físicas, bem como na partilha de informação entre atores públicos e privados, além de uma profícua articulação entre setores, sistemas e instituições.

É neste enquadramento que, delimitando o tema da presente investigação ao imperativo do artigo 4.º da nova Diretiva REC (*CER Directive*), se pretende estudar e propor contributos para uma futura estratégia nacional para a resiliência de EC, centrando a análise nos objetivos e vetores estratégicos.

Assim, na expetativa da colaboração imprescindível para a análise da temática em questão, desenvolveu-se o **Guião de Entrevista** (semiestruturada) que se segue, rogando-se a V.Exa. o envio das respostas para o seguinte endereço eletrónico: garcao.hmg@ium.pt. Em alternativa, roga-se o agendamento da entrevista presencial ou por videoconferência, preferencialmente, até ao dia 17 de março de 2023.

Na eventualidade de qualquer esclarecimento, é favor contactar através do número: 963987587.

[41] O guião de entrevista ao Diretor do CNPIC de Espanha sofreu adaptações, *mutatis mutandis*, da perspetiva nacional para a ibérica.

As respostas apenas serão utilizadas no âmbito da investigação científica e a informação será processada de forma a garantir a integridade dos dados disponibilizados, partindo-se do pressuposto da autorização relativa à indicação da fonte na apresentação e discussão dos resultados.

No intuito de melhor enquadrar o contributo da entrevista, apresenta-se a estrutura da investigação que se encontra a ser desenvolvida:

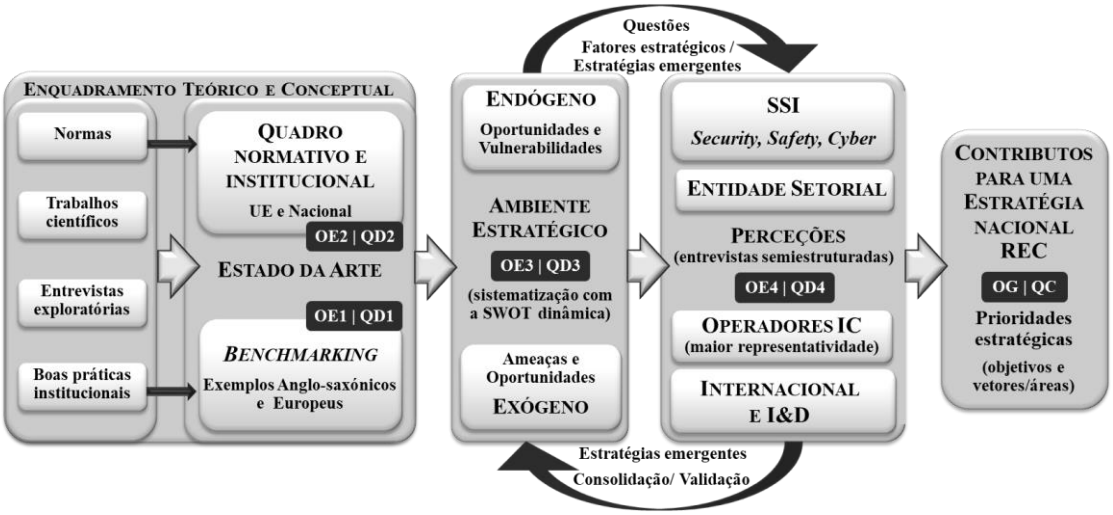

Figura 1 - Estrutura da Investigação

O guião de entrevista inclui **sete questões**, complementadas por notas a cinzento, que visam apoiar a estruturação das respostas de modo a agilizar a ulterior sistematização e análise dos dados, a transpor para o documento final da investigação.

GUIÃO

1. **Do seu ponto de vista, considerando a dimensão <u>externa</u> do ambiente estratégico de Portugal, quais as principais <u>ameaças</u> (1.1) e <u>oportunidades</u> (1.2) relativas à arquitetura de segurança nacional no âmbito da resiliência das entidades/infraestruturas críticas?**

   (Solicita-se que enuncie aproximadamente 6 a 8 aspetos, nomeadamente político-legais, económicos, socioculturais ou tecnológicos. Como mera referência: 3 a 4 principais ameaças e 3 a 4 principais oportunidades)

2. **Ainda sob o escopo do ambiente estratégico de Portugal, agora na sua dimensão <u>interna</u>, quais as principais <u>vulnerabilidades (2.1)</u> e <u>potencialidades</u> (2.2) da arquitetura de segurança nacional no âmbito da resiliência das entidades/infraestruturas críticas?**

   (Solicita-se que enuncie aproximadamente 6 a 8 aspetos, nomeadamente quanto à estrutura, cultura ou recursos. Como mera referência: 3 a 4 principais vulnerabilidades e 3 a 4 principais potencialidades)

3. **Correlacionando** as principais **ameaças** (externas) e as **vulnerabilidades** nacionais (internas) quais considera serem os **problemas críticos** de Portugal em matéria de segurança, proteção e resiliência de infraestruturas/entidades críticas?

   (Como referência, roga-se que enuncie aproximadamente 3 problemas, justificando muito sumariamente).

4. **Correlacionando** as principais **oportunidades** (externas) e as **potencialidades** nacionais (internas) quais considera serem as **vantagens promissoras** de Portugal em matéria de segurança, proteção e resiliência de infraestruturas/entidades críticas?

   (Como referência, roga-se que enuncie aproximadamente 3 vantagens, justificando muito sumariamente).

5. Para garantir maior resiliência das Entidades/Infraestruturas Críticas, Portugal deve prioritariamente **edificar ou reforçar recursos**? Melhorar que **aspetos organizativos**? **Empregar os recursos de forma mais eficiente**? Por favor, enuncie e justifique sumariamente 2 a 3 **medidas prioritárias**.

   (Por favor, concretize muito sinteticamente o «quem?», «o quê?», «como?», «quando?» e «porquê?»)

6. Atenta a perspetiva intrínseca ao cargo que desempenha e a experiência que detém, quais os **principais objetivos (6.1)** e **vetores estratégicos** (6.2) a definir na Estratégia Nacional (portuguesa) para a Resiliência de Entidades Críticas, por forma a atingir uma melhoria significativa e sustentável da arquitetura de segurança nacional.

   (Como referência, roga-se que enuncie aproximadamente 3 objetivos e 3 vetores estratégicos, justificando muito sumariamente).

7. Para finalizar a entrevista, deseja fazer alguma **sugestão ou comentário adicional** associado ao tema da investigação e **que ainda não tenha sido abordado**?

Grato pela oportuna colaboração!

Apêndice G – Ligação ao suplemento com os conteúdos das entrevistas

No suplemento acessível[42] através da ligação infra, encontra-se a transcrição dos excertos pertinentes das entrevistas realizadas, agrupadas por pergunta, a partir do qual se iniciou o processo de análise de conteúdo.

Ligação

Figura 28 - *QR Code* de acesso ao suplemento com os conteúdos das entrevistas

[42] Mediante solicitação.