INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2016/2017

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

AS INFRAESTRUTURAS CRÍTICAS EM PORTUGAL: UM MODELO DE ABORDAGEM

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.

João Paulo dos Santos Martinho
Major CAV GNR

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

AS INFRAESTRUTURAS CRÍTICAS EM PORTUGAL: UM MODELO DE ABORDAGEM

MAJ CAV GNR João Paulo dos Santos Martinho

Trabalho de Investigação Individual do CEMC 2016/2017

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

AS INFRAESTRUTURAS CRÍTICAS EM PORTUGAL: UM MODELO DE ABORDAGEM

MAJ CAV GNR João Paulo dos Santos Martinho

Trabalho de Investigação Individual do CEMC 2016/2017

Orientador: TCOR ENG Leonel José Mendes Martins

Pedrouços 2017

Declaração de compromisso Antiplágio

Eu, **João Paulo dos Santos Martinho,** declaro por minha honra que o documento intitulado **"As Infraestruturas críticas em Portugal: um modelo de abordagem"** corresponde ao resultado de um Trabalho de Investigação Individual, desenvolvido enquanto auditor do **CEMC 2016/17** 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, **19** de **junho** de **2017**

João Paulo dos Santos Martinho

Agradecimentos

Um trabalho de investigação fruto da sua especificidade acaba por envolver vários contributos, quer pessoais, quer institucionais, os quais contribuem indubitavelmente para a sua elaboração. Este trabalho de investigação não foi exceção, daí que, deixo o meu "*bem hajam*":

Ao meu orientador, Tenente-coronel ENG Leonel José Mendes Martins, pelo seu interesse, disponibilidade e o grande envolvimento na concretização deste trabalho como seu orientador.

Aos Srs. Paulo Macedo e Sérgio Vieira da Silva, pela forma despegada, sincera e amiga como me apoiaram em momentos fulcrais deste trabalho, incentivando e oferecendo apoio em tudo o que dependia de si.

Ao Sr. Major-General da GNR Santos Correia, por me ter recebido e orientado de forma pragmática relativamente às particularidades que envolvem os desafios e as competências da GNR quanto à proteção das IC.

Ao Sr. Eng.º da ANPC Carlos Mendes, que me guiou de forma assertiva relativamente aos conteúdos relativos à temática das IC.

A todos os entrevistados, Sr.ª Dr.ª Helena Fazenda, atual Secretária-Geral do Sistema de Segurança Interna, Sr. Coronel da GNR Soares da Costa e o Sr. Major da GNR Paulo Delgado, por terem acedido à minha solicitação e contribuído com importantes conteúdos.

Ao Jorge Barbosa, um agradecimento muito especial pela sua amizade e permanente disponibilidade a qual permitiu desbloquear alguns constrangimentos relativamente a este trabalho.

Ao Manuel Lage e Mário Martins, pela sua permanente disponibilidade e camaradagem.

Por fim, à minha mulher e à minha filha, pela sua compreensão, abdicação e paciência ao longo destes últimos nove meses.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

O objetivo deste trabalho de investigação versa avaliar o papel e o peso que o atual modelo de abordagem atribuiu às Forças Armadas e Forças e Serviços de Segurança no esforço interoperável para garantir a proteção das infraestruturas críticas.

Através de uma metodologia de investigação qualitativa, privilegiando-se uma abordagem indutiva e descritiva, colocámos o enfoque do nosso estudo no atual modelo de abordagem às infraestruturas críticas, procurando compreender o papel e o peso que o mesmo atribui às Forças Armadas e Forças e Serviços de Segurança. Para tal, ancorámos a recolha de dados essencialmente na análise documental e em entrevistas semiestruturadas a um conjunto heterogéneo de *experts*.

Concluímos que, o modelo de abordagem às infraestruturas críticas apenas versa a identificação e designação de infraestrutura crítica, não contemplado nenhum modelo específico quanto à sua proteção. No entanto, verificámos que existe uma coordenação e controlo por parte do Secretário-Geral do Sistema de Segurança Interna, em particular, com as Forças de Segurança e a Autoridade Nacional de Proteção Civil. Outrossim constatámos que, as Forças e Serviços de Segurança têm uma intervenção direta na proteção das infraestruturas críticas, enquanto que, as Forças Armadas se encontram condicionadas à declaração dos estados de exceção.

Palavras-chave: Segurança Nacional; Infraestruturas Críticas; Modelo de Abordagem.

Abstract

The objective of this research is to evaluate the role and weight that the current model of approach has assigned to the Armed Forces and Forces and Security Services in the interoperable effort to ensure the protection of critical infrastructures.

Through a qualitative research methodology, with an emphasis on an inductive and descriptive approach, we have focused our study on the current model of critical infrastructures approach, seeking to understand the role and weight it attributes to the Armed Forces and Forces and Security Services. To this end, we have anchored data collection essentially in document analysis and in semi-structured interviews with a heterogeneous group of experts.

We conclude that the model of approach to existing critical infrastructures only addresses the procedure of identification and designation of critical infrastructure, not contemplating any specific procedure or model regarding its protection. However, we have verified that there is coordination and control by the Secretary General of the Internal Security System, in particular, with the Security Forces and the National Authority for Civil Protection. We have also observed that the Forces and Security Services have a direct intervention in the protection of critical infrastructures, whereas the Armed Forces are conditioned to the declaration of states of exception.

Keywords: *National Security; Critical Infrastructures; Approach Model.*

Lista de abreviaturas, siglas e acrónimos

A

ADPA	*Analysis of Dependency and Propagation Algorithm*
AdR	Análise de Risco
ANPC	Autoridade Nacional de Proteção Civil
ALS	Agente de Ligação de Segurança

C

CE	Comissão Europeia
CNPCE	Conselho Nacional de Planeamento Civil de Emergência
CEDN	Conceito Estratégico de Defesa Nacional
CNPS	Carta Nacional de Pontos Sensíveis
CNCSeg	Centro Nacional de Cibersegurança
CRP	Constituição da República Portuguesa

E

EUA	Estados Unidos da América

I

IC	Infraestrutura Crítica
ICE	Infraestrutura Crítica Europeia
ICN	Infraestrutura Crítica Nacional
IESM	Instituto de Estudos Superiores Militares

M

MACBETH	*Measuring Attractiveness by a Categorical Based Evaluation Technique*

N

NBQR	Nuclear, Biológico, Químico e Radiológico

O

OE	Objetivos Específicos
OCDE	Organização para a Cooperação e Desenvolvimento Económico

P

PCICE	Ponto de Contacto das Infraestruturas Críticas Europeias
PEPIC	Programa Europeu de Proteção de Infraestruturas Críticas
PNPIC	Programa Nacional de Proteção de Infraestruturas Críticas
PPIC	Projeto de Proteção de Infraestruturas Críticas
PrIDIC	Procedimento de Identificação e Designação de Infraestrutura Crítica
PrPIC	Procedimento de Proteção de Infraestrutura Crítica
PSO	Plano de Segurança do Operador
PSPE	Plano de Segurança e Proteção Exterior

F

FA	Forças Armadas
FdS	Força de Segurança
FSS	Forças e Serviços de Segurança

G

GCS	Gabinete Coordenador de Segurança
GNS	Gabinete Nacional de Segurança

Q

QC	Questão Central
QD	Questão Derivada

R

RAMCAP	*Risk Analysis and Management for Critical Assets Protection*
RU	Reino Unido

S

SIS	Serviço de Informações de Segurança
SG-SSI	Secretário-Geral do Sistema de Segurança Interna

V

Vv	Indicador de Criticidade

Introdução

O Conceito Estratégico de Defesa Nacional (CEDN) 2013 destaca a necessidade de implementação de um Programa Nacional de Proteção de Infraestruturas Críticas (PNPIC). Esta medida estratégica surge integrada num conjunto alargado de outras medidas diplomáticas, financeiras, judiciais, de informação pública e de *intelligence*[1], destinadas a responder eficazmente à ameaça das redes terroristas.

A pertinência deste tema faz-nos recuar a 2004, quando o Conselho Europeu solicitou à Comissão Europeia (CE) uma estratégia global para a proteção de infraestruturas críticas. A CE, através de uma comunicação interna, definiu quais os produtos necessários para a concretização de um Programa Europeu de Proteção de Infraestruturas Críticas (PEPIC), à data focado no reforço da prevenção, preparação e capacidade da Europa relativamente a atentados terroristas que envolvessem Infraestruturas Críticas (IC) (União Europeia, 2008). Concomitantemente, em Portugal, o Conselho Nacional de Planeamento Civil de Emergência (CNPCE) encetou o início do Projeto de Proteção de Infraestruturas Críticas (PPIC), materializado fundamentalmente através da identificação das infraestruturas que, pelas suas características, poderiam vir a ser consideradas críticas.

Atinente aos conteúdos produzidos no âmbito da proteção das IC ao nível europeu, foi publicada a Diretiva n.º 2008/114/CE, de 8 de dezembro (União Europeia, 2008, p.77), que "estabelece um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, de modo a contribuir para a proteção das pessoas", sendo a energia e os transportes os principais setores a ter em consideração. Esta Diretiva viria a ser transposta para o enquadramento legal nacional através da publicação do Decreto-Lei (DL) n.º 62/2011, de 9 de maio, vinculando as entidades nacionais à implementação de um conjunto de procedimentos reguladores desta matéria. Passado pouco menos de um ano da sua publicação, dá-se a extinção do CNPCE[2], passando todas as suas atribuições a serem assumidas pela Autoridade Nacional de Proteção Civil (ANPC) (MAI, 2012). Mais de quatro anos volvidos desde a publicação do CEDN 2013, a elaboração do referido PNPIC continua numa fase de discussão política e estratégica.

[1] "O produto resultante da recolha, processamento, integração, avaliação e interpretação de informações disponíveis sobre nações estrangeiras, forças ou elementos hostis ou potencialmente hostis, ou áreas de operações reais ou potenciais" (USDoD, 2017, p.118).
[2] Decreto-Lei n.º 73/2012, de 26 de março (MAI, 2012).

Face ao exposto, consideramos pertinente orientar o foco da investigação tendo por objeto de estudo os procedimentos de identificação e de proteção das IC, considerando a sua delimitação, no domínio do espaço, às infraestruturas designadas como Infraestruturas Críticas Nacionais (ICN), no domínio do tempo, ao período temporal entre 31 de dezembro de 2011 e 31 de maio de 2017, e, no domínio do conteúdo, à análise da forma como as Forças Armadas (FA) e as Forças e Serviços de Segurança (FSS) poderão contribuir para os procedimentos relativos à proteção das infraestruturas críticas no âmbito das ameaças à segurança nacional.

Reconhecendo como axioma que as FA e FSS têm uma inquestionável função a desempenhar em todo o processo de proteção das IC, é objetivo geral desta investigação avaliar o papel e o peso que o atual modelo de abordagem atribuiu às FA e FSS no esforço interoperável[3] para garantir a proteção das IC. Na prossecução do objetivo geral, propomo-nos atingir os seguintes objetivos específicos (OE):

- OE1: Conceptualizar IC num contexto securitário para o Estado Português;

- OE2: Apresentar o modelo de abordagem às IC;

- OE3: Avaliar as consequências do atual modelo para as FA e FSS.

Nesta senda, inferimos a nossa questão central (QC): "De que forma poderão as FA e FSS contribuir para a proteção das Infraestruturas Críticas Nacionais no âmbito do atual modelo de abordagem?", definindo as seguintes questões derivadas (QD):

- QD1: Qual o quadro conceptual de referência das IC ao nível da segurança nacional?

- QD2: O modelo de abordagem das IC é ajustado ao tipo de infraestruturas nacionais?

- QD3: As FA e as FSS têm a sua intervenção no domínio da proteção das IC ajustada à realidade nacional?

A materialização da presente investigação foi ancorada fundamentalmente através da sua QC e QD associadas, as quais, em cômputo, serviram de linha orientadora de toda a investigação e, aliadas a uma estratégia de investigação qualitativa, permitiram um entendimento mais alargado através de dados com origem em diversas fontes.

[3] "Capacidade de sistemas, pessoal e equipamento para fornecer e receber funcionalidades, dados, informações e/ou serviços para, e de, outros sistemas, pessoal e equipamento, entre agências públicas e privadas, departamentos e outras organizações, de tal maneira que lhes permite operar em conjunto de forma eficaz" (FEMA, 2017).

As técnicas de recolha de dados utilizadas focaram-se essencialmente no levantamento documental de diplomas legais e autores internacionais e nacionais, tendo-se também optado por realizar entrevistas semiestruturadas, versando uma amostra intencional, permitindo dessa forma uma transversalidade de intervenientes e conhecimento da temática.

Relativamente à estrutura do nosso trabalho, e no intuito de respondermos à nossa QC e às QD, decidimos dividi-lo em quatro capítulos. O primeiro foi dedicado sobretudo à apresentação dos aspetos principais da investigação, em particular a vertente metodológica seguida para atingir os objetivos propostos. No segundo capítulo expomos os conceitos que, pela sua relevância, permitem ancorar a conceptualização de segurança nacional e de IC. Nesta fase identificamos ainda as limitações relativas à ausência de uma definição de setor estratégico nacional, assim como, os constrangimentos associados à propriedade das IC. No terceiro capítulo apresentam-se os principais elementos que caracterizam as IC. Identificamos o enquadramento legal nacional e apresentamos o modelo de identificação e designação de IC e o PPIC. O quarto capítulo versa essencialmente a proteção das IC. São descritas as características da proteção e os possíveis impactos resultantes da degradação ou destruição das IC. Outrossim é feita a apresentação de um modelo de abordagem ao procedimento de proteção das IC no âmbito do DL n.º 62/2011, de 9 de maio, o qual se encontra estruturado essencialmente em quatro fases: (i) análise do risco do operador da IC; (ii) elaboração do PSO; (iii) planeamento de exercícios; e (iv) elaboração do PNPIC. Por fim, apresentamos as conclusões e recomendações consideradas relevantes para futuras investigações.

1. Abordagem metodológica

Relativamente à vertente metodológica do trabalho de investigação, irá cumprir-se o preconizado nas NEP/ACA-010 e NEP/ACA-018, de setembro 2015, do Instituto de Estudos Superiores Militares (IESM), e na obra coordenada por Lúcio Agostinho Barreiros dos Santos e Joaquim Manuel Martins do Vale Lima, intitulada "Orientações Metodológicas para a Elaboração de Trabalhos de Investigação" (IESM, 2016).

Neste trabalho será utilizada uma estratégia de investigação qualitativa, de natureza essencialmente indutiva e descritiva, sendo "o seu objectivo alcançar um entendimento mais profundo e subjetivo do objecto de estudo, sem se preocupar com medições e análises estatísticas" (Vilelas, 2009 cit. por IESM, 2016, p.29). No fundo, trata-se de, a partir dos dados, construir uma teoria explicativa que responda à QC.

Almejando identificar de forma assertiva o conhecimento envolto à temática, incidimos a nossa recolha de dados na análise documental, um dos métodos imputados às estratégias qualitativas, a qual se centra na recolha de fontes documentais que encerram princípios, objectivos e metas (IESM, 2016, p.31).

Pese embora os estudos efetuados relativamente às IC, como é o caso das investigações de Oliveira (2015) versando o enquadramento jurídico e a realidade em que os operadores das IC e a Autoridade Nacional de Proteção Civil (ANPC) operam e de Ferreira (2016) focando a identificação de áreas de melhoria na metodologia adotada pela ANPC para a identificação e caraterização das IC em Portugal, a verdade é que nenhum deles aborda a forma como as FA e FSS poderão contribuir para a proteção das IC no âmbito das ameaças à segurança nacional, deixando em aberto uma nova linha de investigação relativamente à temática.

1.1. Fases do percurso metodológico

A fase exploratória consubstanciou-se em leituras preliminares, entrevistas informais e opiniões de especialistas, e.g. ANPC, na matéria em apreço. Foi efetuada a revisão do estado da arte através de um exame prévio da literatura que, depois de consolidada e aprofundada, serviu de fundamento para as exposições que são apresentadas ao longo do trabalho, constituindo-se, portanto, como uma base fundamental para esta investigação.

No que respeita à fase analítica, e em complemento da análise documental, recorreu-se à entrevista, "um fortíssimo instrumento de recolha de informação" (IESM, 2016, p.84), através da qual "o pesquisador pode chegar a áreas de realidade que, de outra forma, permaneceriam inacessíveis, como as experiências e atitudes subjetivas das pessoas"

(Peräkylä, 2005), permitindo-lhe obter dados não disponíveis noutras fontes, fruto da sua especificidade (ibidem). A realização das entrevistas teve como amostra um conjunto de individualidades que detêm funções no âmbito dos procedimentos de identificação e proteção das IC, embora com responsabilidades distintas no que concerne à segurança nas vertentes *safety* e *security*.

A heterogeneidade dos entrevistados, das suas funções e das respetivas áreas de ação, implicou a opção por entrevistas semiestruturadas (IESM, 2016, p.86) que foram posteriormente submetidas a análise, a qual, por via da sua natureza, percorreu vários estádios, designadamente leitura, análise descritiva e análise interpretativa.

Por fim, na fase conclusiva, foi feita uma avaliação e ponderação dos resultados obtidos e plasmadas as conclusões e recomendações por nós consideradas como pertinentes para futuro.

2. A segurança nacional e as infraestruturas críticas

A publicação do DL n.º 62/2011, de 9 de maio[4], veio formalmente vincular Portugal à temática relativa à proteção das IC, nomeadamente no que concerne aos procedimentos de identificação e proteção das IC, os quais versam fundamentalmente duas dimensões: (i) *safety* e (ii) *security*. Seja em simultâneo ou individualmente, qualquer uma destas dimensões é fulcral para obter, em matéria de IC, quer uma identificação assertiva, quer medidas efetivas de proteção contra as ameaças e riscos.

Ao abordarmos hoje a temática relativa às IC, não podemos dissociá-la da importância estratégica que representa para a segurança nacional, fruto dos seus setores garantirem funções fulcrais que, em caso de disrupção ou destruição, podem comprometer o funcionamento do País. Assim, importa que sejam apresentados um conjunto de conceitos que permitam corporizar tanto a segurança nacional, como as IC.

2.1. A segurança nacional

2.1.1. Doutrina portuguesa

Atendendo a que não existe uma definição "oficial" do conceito de segurança nacional, neste trabalho será considerado o conceito definido por Cardoso (1981, p.23) enquanto "condição da Nação que se traduz pela permanente garantia da sua sobrevivência em Paz e Liberdade, assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda colectiva de pessoas e bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de acção política dos órgãos de soberania e o pleno funcionamento das instituições democráticas".

2.1.2. Tratado de Lisboa

Com a entrada em vigor, a 01 de dezembro de 2009, do Tratado de Lisboa, é reforçada a ideia de que, "em conformidade com a jurisprudência constante do Tribunal de Justiça da União Europeia, os Tratados e o direito adoptado pela União com base nos Tratados primam sobre o direito dos Estados-Membros, nas condições estabelecidas pela referida jurisprudência" (AR, 2008b, p.444). Sendo este um dos princípios do que significa a integração europeia, a exceção ocorre ao abrigo do n.º 1 do artigo 4.º do Tratado, em que "as competências que não sejam atribuídas à União nos Tratados pertencem aos Estados-Membros" (ibidem, p.19). E, como estabelece o n.º 2 do artigo 4.º do mesmo Tratado, "a União respeita a igualdade dos Estados-Membros perante os Tratados, bem como a respectiva identidade nacional, reflectida nas estruturas políticas e constitucionais [...], as

[4] Ver anexo B.

funções essenciais do Estado, nomeadamente as que se destinam a garantir a integridade territorial, a manter a ordem pública e a salvaguardar a segurança nacional. Em especial, a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro" (AR, 2008b, p.19). Desta feita, e no que à segurança nacional concerne, cabe fundamentalmente às entidades nacionais garantir a segurança e defesa do seu território nacional.

2.1.3. Conceito estratégico de defesa nacional

A introdução do CEDN 2013 (MDN, 2013, p.33) "pressupõe uma estratégia nacional, [...] que para a realização dos objetivos da segurança e da defesa nacional concorrem todas as instâncias do Estado e da sociedade". Outrossim, enfatiza que é o CEDN que "define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional" (ibidem, p.6).

Destarte, na prossecução do garante dos objetivos da política de segurança e defesa nacional, o CEDN 2013 estabelece, entre outros aspetos, os principais riscos e ameaças à segurança nacional, definindo-os como ameaças de natureza global e riscos de natureza ambiental. Relativamente às primeiras, destacam-se: (i) o terrorismo; (ii) a proliferação de armas de destruição massiva; (iii) a criminalidade transnacional organizada; (iv) a cibercriminalidade; e (v) a pirataria (MDN, 2013, p.16). Quanto aos segundos, podemos identificar: (i) alterações climáticas, riscos ambientais e sísmicos; (ii) ocorrência de ondas de calor e de frio; (iii) atentados ao ecossistema, terrestre e marítimo; e (iv) pandemias e outros riscos sanitários (ibidem, p.17).

Cientes das ameaças e riscos com que a segurança nacional se poderá defrontar, o CEDN 2013 materializa um conjunto de respostas a essas ameaças, entre elas: (i) a operacionalização de um efetivo sistema nacional de gestão de crises; (ii) a interoperabilidade na prevenção e resposta operacional, maximizando a capacidade e eficiência no emprego de meios; (iii) contribuir, nas instâncias internacionais, para o reforço da prevenção e combate ao terrorismo e criminalidade organizada; (iv) interoperabilidade entre as FA e as FSS em missões no combate a agressões e às ameaças transnacionais; (v) promover uma abordagem integrada da segurança interna, incluindo uma intervenção articulada e coordenada entre as forças e serviços de segurança; (vi) promover a integração operativa da segurança interna, através da adoção de medidas operacionais que reduzam redundâncias e aumentem a integração operacional e a resiliência do sistema; e (vii) desenvolver as capacidades militares necessárias à mitigação

das consequências de ataques terroristas, cibernéticos[5], NBQR[6] e de catástrofes e calamidades (MDN, 2013, p.33).

O contributo do CEDN 2013 é revelador da intenção nacional em cada vez mais conjugar políticas, esforços e meios, na prossecução de uma resposta conjunta e interoperável aos desafios impostos à segurança e defesa nacional.

2.2. **As infraestruturas críticas**

2.2.1. Infraestrutura crítica

O DL n.º 62/2011 (MDN, 2011, p.2624) define IC como "a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais[7] para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções". Quanto ao conceito de ICN deverá considerar-se o referido no artigo 17.º do mesmo diploma (MDN, 2011, p.2627), que salienta que "o disposto no presente decreto-lei é aplicável, com exceção das fases correspondentes à componente transfronteiriça, às restantes infraestruturas críticas nacionais". Poderá, assim, assumir-se que a definição de IC é também atribuída a ICN.

O Reino Unido (RU), por sua vez, define IC como os ativos da infraestrutura (físicos ou eletrónicos) que são vitais para o contínuo funcionamento e integridade de serviços essenciais sobre os quais o RU se apoia, sendo que a sua perda ou compromisso levaria a graves consequências económicas, sociais ou perdas de vida (UK Government, 2010). Se os britânicos, por um lado, são objetivos na definição, não considerando o "modo de vida", por outro lado, deixam em aberto o que consideram serviços essenciais, o que também nos levaria numa interpretação restritiva.

Para a Alemanha, as IC são caracterizadas como estruturas físicas e organizacionais e instalações de importância vital para a sociedade e economia nacional cuja falha ou degradação resultaria em faltas de abastecimento sustentadas, disrupção significativa da segurança pública ou outras consequências dramáticas (GFMI, 2009). Observa-se que neste caso são mais focados nas possíveis consequências no âmbito da segurança pública, do que numa segurança em geral.

[5] Entendido como o "uso premeditado de atividades disruptivas, ou a ameaça delas, contra computadores e/ou redes, com a intenção de causar danos ou outros objetivos sociais, ideológicos, religiosos, políticos ou similares. Ou para intimidar qualquer pessoa em prol de tais objetivos" (USATDC, 2006).
[6] Nuclear, Biológico, Químico e Radiológico.
[7] "Termo para as atividades que mantêm uma determinada funcionalidade. Cada uma dessas funções está incluída em um dos setores da sociedade e é mantida por uma ou mais infraestruturas críticas" (MSB, 2014).

A União Europeia segue uma linha intermédia definindo ICE como um ativo, sistema ou parte deste, localizado nos Estados membros, que é essencial para a manutenção das funções societárias vitais, saúde, segurança, bem-estar económico ou social das pessoas e cuja disrupção ou destruição teriam um impacto significativo no Estado membro como resultado da incapacidade em manter aquelas funções (União Europeia, 2008). Reaparece aqui o bem-estar como parâmetro a ter em atenção na classificação da criticalidade da infraestrutura.

Outro caso particularmente curioso é o Japão, que define IC e também serviços de IC. As primeiras são consideradas como a base da vida social do povo e as atividades económicas formadas por negócios que providenciam serviços que são extremamente difíceis de serem substituídos por outros e que, se suspensos, deteriorados ou tornados indisponíveis, poderiam ter impacto significativo na vida social das pessoas e nas atividades económicas; os segundos serão os serviços providenciados por infraestruturas críticas fornecedoras e toda uma série de serviços que precisam de ser especialmente protegidos tomando em atenção o grau de impacto na vida social das pessoas e nas atividades económicas (ISPC, 2009). Neste caso, a importância é principalmente canalizada para os possíveis impactos na vida social e nas atividades económicas, não sendo feita menção à componente da segurança.

O Brasil define IC como o conjunto de instalações, serviços ou bens que, se destruídos, interrompidos ou tiverem o seu desempenho sensivelmente degradado por um período de tempo, poderão provocar sérios impactos sociais, económicos e/ou políticos (Nakamura et al., 2011). Além das especificidades das definições já apresentadas, o Brasil destaca ainda os possíveis impactos políticos inerentes à disrupção das IC. Outras definições poderiam ser dadas mas, para efeito de ilustração, estas são suficientes.

2.2.2. Interdependência

Segundo Zimmerman (2005, p.69), a interdependência "refere-se a um relacionamento no qual dois sistemas não só estão ligados, mas dependem um do outro de alguma forma". Em geral, podemos classificar a interdependência em termos geográficos, espaciais ou físicos, em termos funcionais e em termos económicos e financeiros; podem ainda ser interdependências sequenciais, paralelas ou ambas, bem como unidirecionais, bidirecionais ou multidirecionais (Zimmerman, 2005, p.69). A interdependência vai também definir o tipo de falha que pode existir: se em cascata – causando a disrupção

noutras IC – ou se escalável, onde o impacto na próxima IC terá maior severidade e/ou o tempo de recuperação será maior.

Para Rinaldi, Peerenboom e Kelly (2001, p.14), uma interdependência é "uma relação bidirecional entre duas infraestruturas através das quais o estado de cada infraestrutura influencia ou está correlacionado com o estado da outra. Por norma, duas infraestruturas são interdependentes quando cada uma é dependente da outra". Na prática, quanto maior for o número de ligações entre infraestruturas, i.e. interdependências, maior será a complexidade global do "sistema de sistemas" (ibidem).

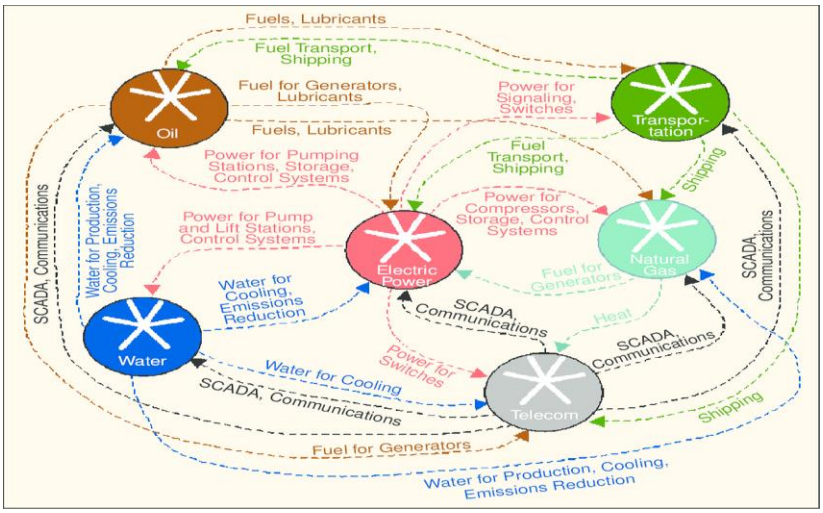

Figura 1 – Interdependências em infraestruturas

Fonte: (Rinaldi, Peerenboom e Kelly, 2001)

Para um melhor alinhamento relativamente ao estudo das interdependências de um sistema, Rinaldi, Peerenboom e Kelly (2001, p.14) identificam quatro formas de proceder à sua classificação: (i) interdependência física, quando duas infraestruturas que são fisicamente interdependentes e o estado de cada uma delas depender da saída material da outra; (ii) interdependência cibernética, quando o estado da infraestrutura depender da informação transmitida através de uma infraestrutura de informação; (iii) infraestruturas geograficamente interdependentes, quando um evento ambiental local possa criar mudanças de estado em todas as infraestruturas; e (iv) interdependência lógica, quando duas infraestruturas são logicamente interdependentes e o estado de cada uma depende do estado da outra através de um mecanismo que não é uma conexão física, cibernética ou geográfica (cf. Figura 1).

2.2.3. Ameaça

A definição do conceito de ameaça não é uma matéria de fácil tratamento tendo em conta a importação de conceitos de base norte-americana por força da sua sistematização e generalização. Os norte-americanos definem ameaça como "a probabilidade de um ativo, sistema ou rede em particular sofrer um ataque ou um incidente. No contexto do risco de um ataque terrorista, a estimativa é baseada na análise da intenção e da capacidade de um adversário; no contexto de desastres naturais ou acidentes, a probabilidade é baseada na probabilidade de ocorrência" (USDoHS, 2006, p.35). Daqui procede que a ameaça representa qualquer vetor de dano potencial quer este seja originado por um fenómeno natural, erro humano, acidente tecnológico ou vontade consciente de um adversário (e.g. ataque terrorista), incluindo, assim, as duas áreas tradicionais da segurança – *safety*[8] e *security*[9]. Nesta linha de pensamento, POA (2003) salienta que as ameaças podem assumir três formas distintas: (i) ameaças naturais, que incluem todas as emergências relacionadas com o clima, e.g. furacões, tornados, inundações, bem como eventos naturais não-climáticos (terramotos); (ii) ameaças humanas, enquanto ações e eventos adversos deliberados, incluindo atividades terroristas, incêndios criminosos, desordens civis, entre outros; e (iii) ameaças acidentais, abrangendo ações e eventos adversos não deliberados, que podem variar desde derramamentos de materiais perigosos até falhas de telecomunicações. Neste quadro, Boone (2013, p.89) categoriza as ameaças em quatro tipos – natural, deliberada, acidental e deterioração –, em função da sua natureza interna e externa (Tabela 1).

Daqui decorre que, quando a literatura norte-americana se refere à ameaça, tem sempre de a classificar em função da sua origem, sob pena de suscitar confusões conceptuais. Esta confusão é claramente demonstrada no *National Infrastructure Protection Plan* (USDoHS, 2006), onde a definição de ameaça apresentada supra não corresponde à constante no glossário do mesmo documento.

[8] *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, 1998).
[9] *Security*: a condição artificial de ausência de, ou liberdade do, perigo e preocupação, relativamente ao ativo. Isso resulta da implementação de medidas destinadas a evitar, prevenir, minimizar ou proteger, a ocorrência de danos que possam ser intencionalmente causados ao bem (ibidem).

Tabela 1 – Categorias de ameaça

Tipos de Ameaça	Externo	Interno
Natural	Terramoto, tornado, inundação, *tsunami*, tempestade tropical, furacão, tempestade, nevão/neve/tempestade de gelo, granizo, erupção vulcânica, deslizamento de terra, erosão, incêndio, vendaval, temperatura extrema, doença, seca, ataques de animais, meteorito, asteroide.	Não aplicável
Deliberada	Terrorismo, crime, sabotagem, subversão, hostilidade, ação militar, insurreição, espionagem estatal ou corporativa, ciberataques, ativismo político, embustes, envenenamento	Sabotagem por funcionários, roubo, greve, ações laborais (diminuição do ritmo de trabalho, paragens, atraso no acesso)
Acidental	Corte de cabo ou tubo de água, incêndio, derramamento de matérias perigosas, envenenamento	Erro, perda ou uso indevido de equipamentos, manutenção imprópria, deslizamentos e quedas, derramamentos, inundações, incêndio, intoxicação
Deterioração	Erosão, ferrugem/corrosão, fadiga pelo tempo	Desgaste, negligência, *stress*/fadiga estrutural, envelhecimento do equipamento ou material

Fonte: (Boone, 2013, p.89)

Assim, esta matéria seria objeto de extensa explanação não fora o GCS definir ameaça como "qualquer acontecimento ou ação, ainda não concretizados mas passiveis de o serem, protagonizados por um agente com intenção e capacidade para os executar, que contrarie a consecução de um ou mais objectivos de uma qualquer entidade (desde um Estado ou uma organização pública internacional até comunidades ou indivíduos) através de danos materiais ou morais" (GCS, 2011, p.9), deixando de lado os vetores de dano potencial de outra natureza que não os derivados da ação intencional e da capacidade de um agente. Esta perspetiva é demonstrada pelo facto do PSO estar dividido nas duas áreas clássicas (*safety* e *security*), sendo que a primeira é analisada pela ANPC e a segunda pelo GCS. Na realidade, e pelo facto do elemento diferenciador das duas áreas ser a existência de intencionalidade, as funções de prevenção, deteção e resposta na *security* são levadas a cabo por diferentes entidades com diferentes especialidades.

2.2.4. Risco

Neste enquadramento conceptual, dada a importância e influência que possui para a matéria em análise, importa definir o conceito de risco. São múltiplas as definições de risco, dependendo das diversas perspetivas, podendo ser agrupadas em duas grandes abordagens: a das ciências naturais e a das ciências sociais. No âmbito das primeiras, aceita-se que o risco é um dado objetivo, que pode ser medido, e que corresponde ao

produto da probabilidade de um dado evento ocorrer e da magnitude do efeito adverso (Lowrance, 1980) – consequência ou impacto – da sua ocorrência, utilizando para tal metodologias quantitativas. No quadro das ciências sociais, o risco é entendido como algo decorrente da perceção, portanto subjetivo, sendo "visto como um conceito que os seres humanos inventaram para os ajudar a entender e lidar com os perigos e incertezas da vida. Embora esses perigos sejam reais, não existe tal coisa como 'risco real' ou 'risco objetivo'" (Slovic e Weber, 2002, p.4).

Para Beck (2015, p.31), "risco significa antecipação da catástrofe. Os riscos dizem respeito à possibilidade de acontecimentos e desenvolvimentos futuros, tornam presente um estado do mundo que (ainda) não existe". Para a International Organization for Standardization, risco é o efeito da incerteza nos objetivos (ISO, 2009), enquanto, para Renn (2008), três elementos estão na essência do risco – independentemente da diferente conceptualização das várias perspetivas – um resultado que afecta algo que é valorizado pelos humanos, a possibilidade de ocorrência e uma fórmula que jogue com estes dois elementos. Na verdade, podemos traduzir o resultado que afecte algo que é valorizado pelos humanos como consequência ou o impacto, a possibilidade de ocorrência como a probabilidade ou frequência de um determinado evento e a fórmula como o produto destes dois factores anteriores (Risco = Probabilidade * Impacto). Também no caso da *security*, a consequência ou o impacto estão representados na fórmula, sendo que o produto da ameaça e da vulnerabilidade, se colocado entre parênteses, corresponde à probabilidade ou frequência [Risco = ameaça * vulnerabilidade * Impacto ou Risco = (ameaça * vulnerabilidade) * impacto]. Será este último entendimento que seguiremos ao longo deste trabalho porque é passível de ser aplicado independentemente da perspectiva a ser seguida (Renn, 2008).

A apreciação de risco, seguindo a ISO (2009), incorpora a identificação do risco, a análise de risco e a avaliação do risco, sendo que, no domínio da proteção, configura-se como uma ferramenta de apoio à decisão permitindo hierarquizar as prioridades a atribuir aos ativos que se querem protegidos, escolher e atribuir recursos para a proteção e validar o nível de risco aceitável.

No domínio das infraestruturas críticas, dir-se-ia que a perspectiva passível de ser utilizada seria a das ciências naturais, também designada perspectiva técnica (Bradbury, 1989), calculando, portanto, o risco com recurso a uma metodologia quantitativa, e.g. a avaliação probabilística de riscos. Tal ferramenta é frequentemente utilizada para o cálculo

do risco na área de *safety* (incluindo os fenómenos naturais, o erro humano[10] e os acidentes tecnológicos[11]). Mas que dizer da utilização desta ferramenta na área de *security*, onde raramente existem dados históricos e experiência acumulada para que os cálculos do analista possam ser validados? Bradbury (1989, p.383) é clara quando diz que, "embora a abordagem técnica do risco possa ser inteiramente apropriada para decisões puramente de engenharia, é inadequada quando utilizada como base para decisões societais"; ou, como referem Klima, Dorn e Beken (2011, p.17), "o cálculo do risco é sobre 'quantidades conhecidas' (frequências de eventos historicamente observadas, dados quantificáveis sobre perdas, criando um senso de gestão)".

Segundo Di Nicola e McCallister (2006, p.186), "as experiências anteriores quanto à avaliação de risco dizem-nos que uma avaliação abrangente de todos os riscos é uma impossibilidade", pelo que parece que haverá lugar à existência de duas metodologias de cálculo/estimativa do risco em função da área da segurança a que se dirigem, como parece ter sido o entendimento da ANPC quando, no que respeita ao Plano de Segurança do Operador (PSO) de IC, separou as áreas de *safety* e de *security*.

Outro entendimento está expresso no *National Infrastructure Protection Plan* dos EUA (USDoHS, 2006), o qual está fundamentado na aplicação da metodologia RAMCAP (*Risk Analysis and Management for Critical Assets Protection*) e conceptualiza o risco como função da ameaça, da vulnerabilidade e da consequência[12]. Seríamos levados a crer que estaríamos perante uma abordagem técnica pura não fora o conceito de ameaça utilizado pelo Department of Homeland Security incluir a probabilidade de todo e qualquer ataque ou incidente que possa ser sofrido por um activo, sistema ou rede, e onde se ressalva que, no contexto de um ataque terrorista, a estimativa da ameaça é realizada com base na análise da intenção e da capacidade de um adversário, enquanto que, no contexto de um desastre natural ou acidente, a ameaça é calculada em termos da sua probabilidade de ocorrência (USDoHS, 2006, p.35), mantendo-se a restante fórmula. Estamos, assim, na presença de uma fórmula quantitativa no caso da *safety* e perante uma fórmula semi-quantitativa, ou mesmo qualitativa, no caso da *security*, fórmula que utiliza os mesmos

[10] "Termo genérico para abranger todas as ocasiões nas quais uma sequência planeada de atividades mentais e físicas falham em atingir um resultado intencional, não podendo estas falhas serem atribuídas à intervenção de alguma agência de oportunidade" (Reason, 1990, p.9).
[11] Ameaças NBQR; Emergências radiológicas; Gasodutos e oleodutos; Substâncias perigosas em indústrias e armazenagens; e transporte de mercadorias perigosas (ANPC, 2017).
[12] R = f (C- Consequence,V- Vulnerability,T- Threat) (USDoHS, 2006).

factores, ainda que com um entendimento conceptual diferenciado no que se refere à ameaça conforme a área em análise.

2.2.5. Setor estratégico nacional

A abordagem do conceito de setor estratégico nacional encerra alguma dificuldade fruto da inexistência ao nível nacional de uma definição clara e perentória de quais os setores que assumem essa condição. Assim, neste quadro de vazio conceptual, destaca-se Fernandes (2004, p.49), que considera "o sector alimentar, o sector da educação e cultura, o sector da política externa, o sector das telecomunicações, o sector dos transportes, o sector energético e o sector de Informações da República", como setores fulcrais para a segurança nacional. Esta conceção não contempla, todavia, o contributo dos setores estratégicos para a garantia da autoridade do Estado de direito[13].

No caso particular de Espanha, o conceito de setor estratégico integra "cada uma das diferentes áreas dentro da atividade laboral, económica e produtiva que fornece um serviço essencial que garante o exercício da autoridade do Estado ou de segurança" (Gobierno de España, 2011, p.3), sendo o conjunto dos setores estratégicos nacionais constituídos pela administração pública, espaço sideral, indústria nuclear, indústria química, instalações de investigação, água, energia, saúde, tecnologias da informação e comunicações, transportes, alimentação e sistema financeiro e tributário (ibidem). Perante este conteúdo tão assertivo, e na ausência de um conceito nacional, iremos adotar como referência o conceito espanhol de "setor estratégico".

[13] O trabalho de Fernandes (2004) visou identificar os Setores Estratégicos Nacionais e a possível contribuição para a consolidação do Potencial Estratégico Nacional.

3. As infraestruturas críticas em Portugal

3.1. Enquadramento legal

Com a entrada em vigor do DL n.º 62/2011, de 9 de maio, surge finalmente um enquadramento jurídico corporizador de procedimentos de identificação e proteção de IC, em particular das infraestruturas com funções essenciais para a sociedade cuja disrupção ou destruição teria um impacto significativo na capacidade de assegurar serviços essenciais à sociedade como a saúde, a segurança, o bem-estar económico e social da sociedade e setores da energia e transportes (MDN, 2011, p.2624).

Subjacente à identificação e designação de IC está a abrangência do seu âmbito, que, no caso nacional, apenas versa os setores da energia e dos transportes. No setor da energia, distinguem-se essencialmente três tipos de infraestruturas: (i) produção e transporte de eletricidade; (ii) produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos; e (iii) produção, refinação, tratamento, armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido. Relativamente ao setor dos transportes, podemos observar cinco tipos de infraestruturas: (i) rodoviário; (ii) ferroviário; (iii) aéreo; (iv) por vias navegáveis interiores; e (v) marítimo (MDN, 2011, pp.2624-2625) (Tabela 2).

Tabela 2 – Setores e subsetores das IC

Setor	Subsetor
Energia	Eletricidade
	Petróleo
	Gás
Transportes	Rodoviário
	Ferroviário
	Aéreo
	Vias navegáveis interiores
	Marítimo, incluindo curta distância e portos

Fonte: (Adaptado de MDN, 2011)

No que alude à identificação e designação de ICN, cabe à ANPC orientar o referido processo tendo em consideração três critérios transversais: (i) a possibilidade de ocorrência de acidentes, (ii) o impacto económico estimado e (iii) os efeitos previsíveis no domínio público (MDN, 2011, p.2625). Pré-definidos os critérios, os mesmos são integrados num procedimento composto por três fases: (i) aplicação dos critérios setoriais, para efetuar uma primeira seleção das infraestruturas críticas dentro de determinado setor, (ii) aplicação

da definição de infraestrutura crítica constante da alínea a) do artigo 2.º do DL n.º 62/2011, de 9 de maio, sendo a importância do impacto significativo determinada pela utilização de métodos nacionais de identificação das infraestruturas críticas e pelo recurso a critérios transversais, e (iii) aplicação dos critérios transversais às potenciais ICN que não tenham sido identificadas após as fases um e dois do procedimento (MDN, 2011, p.2625) (Figura 2).

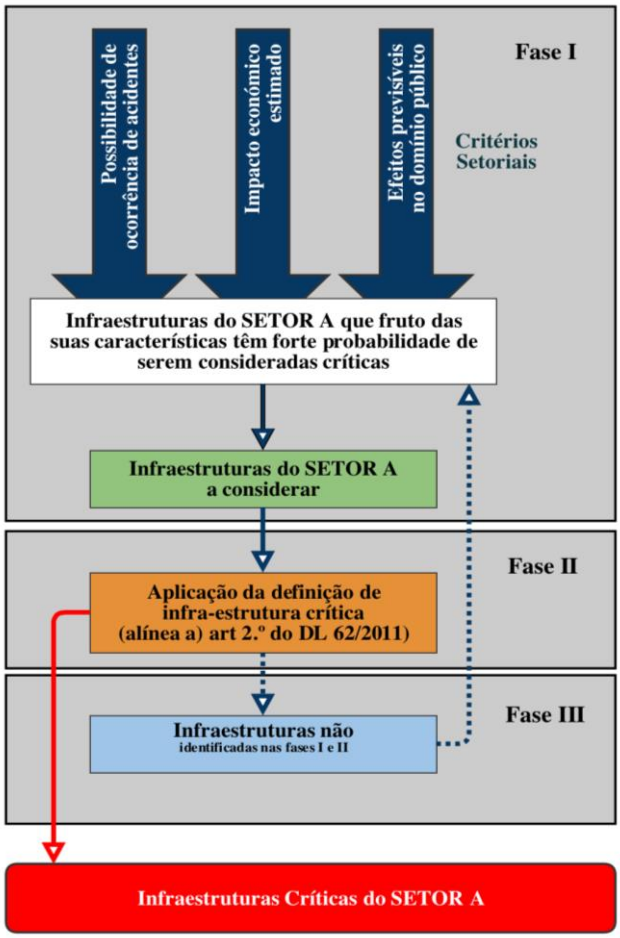

Figura 2 – Procedimento de identificação e designação de ICN (DL n.º 62/2011)

Fonte: (Adaptado de MDN, 2011)

Após a designação de uma infraestrutura como crítica, o seu operador fica obrigado a, no prazo de um ano, elaborar um Plano de Segurança do Operador (PSO), no qual deverá incluir obrigatoriamente os elementos da ICN e as soluções a executar para a sua proteção, designadamente: "(i) a identificação dos elementos importantes; (ii) análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada elemento e nos impactos potenciais; (iii) a identificação, seleção e prioridade de contramedidas e procedimentos de segurança permanentes; e (iv) a identificação, seleção e prioridade de

contramedidas e procedimentos de segurança progressivos a ativar consoante o grau de ameaça aplicável" (MDN, 2011, p. 2626). Decorrente das exigências relativas à forma e conteúdo do documento, os operadores deverão articular o seu PSO com o Plano de Segurança e Proteção Exterior (PSPE), da responsabilidade da Força de Segurança (FdS) territorialmente competente e da proteção civil. O DL n.º 62/2011, de 9 de maio, vai mais além, vinculando os operadores das ICN a procedimentos de segurança permanentes de identificação, seleção e prioridade de contramedidas, destacando-se: "(i) instalação de meios de detecção, controlo do acesso, proteção e prevenção; (ii) procedimentos de alerta e gestão de crises; (iii) medidas de controlo e verificação; (iv) comunicação, sensibilização e formação; (v) segurança dos sistemas de informação; e (vi) medidas de minimização dos danos e impactos e de reposição da normalidade" (ibidem).

Atendendo à sua especificidade, o PSO deverá ser elaborado e revisto anualmente pelos operadores e submetido a parecer prévio da FdS territorialmente competente e da ANPC, com vista à sua validação pelo Secretário-Geral do Sistema de Segurança Interna (SG-SSI) (MDN, 2011, p.2626). Este procedimento encontra-se desde logo vinculado às dimensões *security* e *safety*, na medida em que é com esse pressuposto que terão de ser elaborados dois capítulos distintos, embora constituindo um plano único (Mendes, 2017).

Considerando a complexidade de procedimentos envolvidos na gestão das ICN, em especial a ligação entre operadores e entidades legalmente competentes, surge o Agente de Ligação de Segurança (ALS), que se assume como ponto de contacto entre a ICN e o SG-SSI, assim como com a FdS territorialmente competente (MDN, 2011, p.2626). O ALS "deve cumprir todos os requisitos da categoria de diretor de segurança previstos no regime jurídico da atividade de segurança privada" (ibidem). Ciente da importância que o ALS desempenha em todo o processo relativo às IC, importa conhecer quais os requisitos para a admissão, permanência e exercício da profissão. Deste modo, em termos de requisitos de admisssão e permanência destaca-se a frequência de um curso específico a ser ministrado em estabelecimento de ensino superior oficialmente reconhecido. Por seu turno, o exercício da profissão implica: (i) ser cidadão português; (ii) possuir 12.º ano de escolaridade; (iii) possuir plena capacidade civil; (iv) não ter sido condenado judicialmente; (v) não ter exercido cargo ou função na segurança privada nos três anos precedentes; e (vi) não ter sofrido nenhuma pena de separação de serviço das forças ou serviços de segurança e forças armadas (MAI, 2013a, p.2928). Em termos das competências conferidas ao diretor de segurança, destacam-se: (i) planear, coordenar e

controlar a execução dos serviços de segurança privada; (ii) gerir os recursos relacionados com a segurança privada que lhe estejam atribuídos; (iii) organizar, dirigir e inspecionar o pessoal de segurança privada e promover a formação e atualização profissional do referido pessoal; (iv) assegurar o contacto com as forças e serviços de segurança; (v) zelar pelo cumprimento das normas aplicáveis ao exercício da atividade de segurança privada; e (vi) realizar análises de risco, auditorias, inspeções e planos de segurança, bem como assessorar os corpos gerentes das entidades de segurança privada" (MAI, 2013a, p.2927).

3.2. **Modelo de identificação e designação de IC**

O modelo adotado a nível nacional para a identificação e designação de IC consubstancia-se numa metodologia baseada em instrumentos como a teoria da decisão e a modelação matemática Força de Segurança (FdS). A primeira fase iniciou-se com a identificação do conjunto de "setores estratégicos" para o funcionamento do país, tendo sido identificados quatro setores-chave: (i) a segurança; (ii) a atividade governativa; (iii) a economia; e (iv) os valores e símbolos (Pais, Sá e Gomes, 2007, p.69). Definidos os "setores estratégicos" ao nível nacional, o CNPCE apresentou os resultados do levantamento das infraestruturas com fortes probabilidades de serem consideradas como críticas às comissões setoriais, i.e. entidades tutelares dos sectores, solicitando-lhes via questionários semi-abertos e entrevistas semiestruturadas que aferissem através da sua *expert opinion*[14] qual o grau de interdependência que poderia haver entre os vários sectores e, desse modo, proceder-se à análise de propagação de efeitos.

Após a compilação de toda a informação, foi desenvolvido o *Analysis of Dependency and Propagation Algorithm* (ADPA), que procura "medir o potencial de cada infraestrutura em propagar disfunções às que se situem a jusante dela devido a dependências funcionais, tendo-se recorrido à MACBETH[15] para o apoio à captação de probabilidades subjetivas dos múltiplos intervenientes" (Pais, Sá e Gomes, 2007, p.70). Ou seja, com o algoritmo ADPA pretende-se obter a probabilidade máxima de um setor "*i*" sofrer uma forte disrupção caso o setor "*j*" seja gravemente afetado, podendo ser apresentada através das seguintes equações matemáticas (Almeida, n.d., p.3):

[14] A opinião de um profissional "que tenha adquirido conhecimentos e competências através do estudo e da prática ao longo dos anos, num determinado domínio ou tema, na medida em que a sua opinião possa ser útil na descoberta de factos, na resolução de problemas ou na compreensão de uma situação" (Businessdictionary, 2017).
[15] Cfr. Costa, Corte e Vansnick (2010).

$$P_{i,j} = P\begin{pmatrix} Sector\ "i"\ be\ seriously\ affected \\ if\ Sector\ "j"\ was\ disrupted \end{pmatrix} \quad (1)$$

$$P_{i,j} = P("i" = Fail | "j" = Fail) \quad (2)$$

$$P_{i,j} = P("i" = Fail) \times P("j" = Fail) \quad (3)$$

$$P("i" = Fail) \quad (4)$$

$$Probability\ of\ Sector\ "i"\ be\ seriously\ damaged$$

$$P("j" = Fail) \quad (5)$$

$$Probability\ of\ Sector\ "j"\ be\ significantly\ disrupted$$

Pese embora, a formulação matemática seja determinante para medir a probabilidade de disrupção entre setores, a forma como se integram no sistema influencia de sobremaneira as suas dependências funcionais (Figura 3).

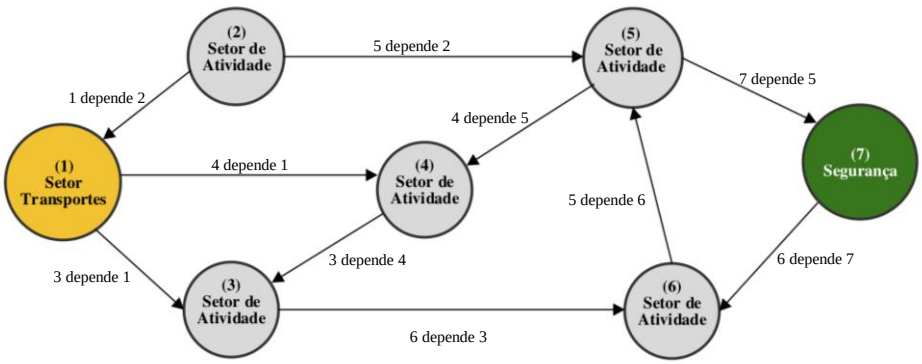

Figura 3 – Gráfico de dependências

Fonte: (Adaptado de Sá, 2005)

Para tal, são essenciais os contributos resultantes da *expert opinion* dos responsáveis dos setores e infraestruturas, destacando-se as ponderações[16] (Tabela 3) atribuídas às dependências relevantes.

Tabela 3 – Ponderações da *Expert Opinion*

	1	2	3	4	5	6	7
1		0,35					
2			0,20				
3	0,90			0,75			
4					0,89		
5		0,57				0,34	
6			0,25				0,15
7					0,45		

Fonte: (Adaptado de Sá, 2005)

[16] Os valores utilizados para este exemplo são fictícios, uma vez que os verdadeiros são alvo de classificação de segurança (n.º 2 do artigo 7.º do DL n.º 62/2011, de 9 de maio).

Nesta etapa, cientes do sistema e das probabilidades condicionadas entre setor e infraestrutura, poderemos calcular a probabilidade máxima do "setor estratégico" da segurança (7) sofrer uma forte disrupção caso o setor dos transportes (1) seja gravemente afetado (Figura 4).

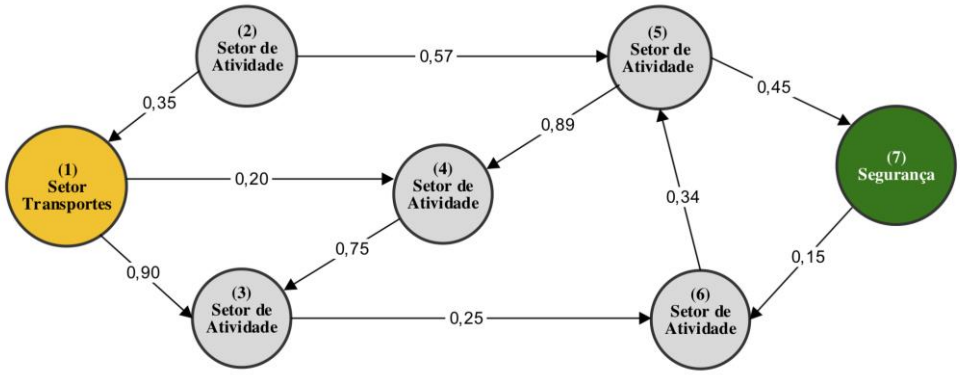

Figura 4 – Gráfico de dependências (probabilidades condicionadas)

Fonte: (Adaptado de Sá, 2005)

Assim, podemos desde logo verificar que existem dois caminhos possíveis para que o "setor estratégico" da segurança (7) seja gravemente afetado pelo setor dos transportes (1), ou seja: (i) caminho 1 inicia-se em (1) e passa pelos pontos (3), (6), (5), terminando no (7), respetivamente com as probabilidades condicionadas 0,90 (1 a 3), 0,25 (3 a 6), 0,34 (6 a 5) e 0,45 (5 a 7); (i) caminho 2 inicia-se em (1) e passa pelos pontos (4), (3), (6), (5), terminando no (7), respetivamente com as probabilidades condicionadas 0,20 (1 a 4), 0,75 (4 a 3), 0,25 (3 a 6), 0,34 (6 a 5) e 0,45 (5 a 7). Deste modo, ao aplicarmos os dados à equação matemática (1), obtemos:

$P_{(7,1)}$ = P("7" = Falhar| "1" = Falhar) = Máx. (Caminho 1;Caminho 2) *(6)*

$P_{(7,1)}$ = P("7" = Falhar| "1" = Falhar) = Máx. ($P_{(3,1)}$ x $P_{(6,3)}$ x $P_{(5,6)}$ x $P_{(7,5)}$; $P_{(4,1)}$ x $P_{(3,4)}$ x $P_{(6,3)}$ x $P_{(5,6)}$ x $P_{(7,5)}$) *(7)*

$P_{(7,1)}$ = P("7" = Falhar| "1" = Falhar) = Máx. (0,90 x 0,25 x 0,34 x 0,45 ; 0,20 x 0,75 x 0,25 x 0,34 x 0,45) *(8)*

$P_{(7,1)}$ = P("7" = Falhar| "1" = Falhar) = Máx. (0,034 ; 0,005), *(9)*

Ou seja, sendo que o maior resultado do produto das probabilidades condicionadas resulta do caminho 1, a probabilidade máxima do "setor estratégico" da segurança (7) sofrer uma forte disrupção caso o setor dos transportes (1) seja gravemente afetado é de 3,4%.

A etapa seguinte materializa a criação de uma Matriz de Dependência, a qual representa a probabilidade de cada nó, i.e. setor/infraestrutura, num sistema complexo de subsistemas interconectados ou interdependentes, ser seriamente interrompido, direta ou indiretamente devido a efeitos de propagação de outro nó (Sá, 2005).

Numa segunda fase, as principais infraestruturas de cada setor e subsetor foram enumeradas e classificadas, seguindo uma lógica análoga, tendo a sua relevância sido mensurada pelo seu impacto funcional.

Com a conclusão das duas fases, a informação recolhida permitiu a materialização de um indicador numérico e objetivo de criticidade, i.e. indicador de criticidade, significando a quantificação que uma grave disfunção de uma infraestrutura pode causar ao País. O indicador de criticidade é essencialmente um valor numérico compreendido numa escala de 0 a 1, representado através da seguinte equação matemática (Pais, Sá e Gomes, 2007; Mendes, 2017; Pais, n.d.):

$$\text{Indicador de Criticidade (Vv)} = V.ADPA \times V.infra \qquad (10)$$

A equação de cálculo do indicador de criticidade (Vv) encontra-se por sua vez condicionada a duas variáveis: (i) a *V.ADPA*, representando a probabilidade de uma grave disfunção do setor a que pertence a infraestrutura se propagar aos restantes setores de atividade nacionais, afetando de forma crítica o funcionamento do País e o bem-estar da população, essencialmente devido a perturbar um ou mais "setores estratégicos" nacionais;

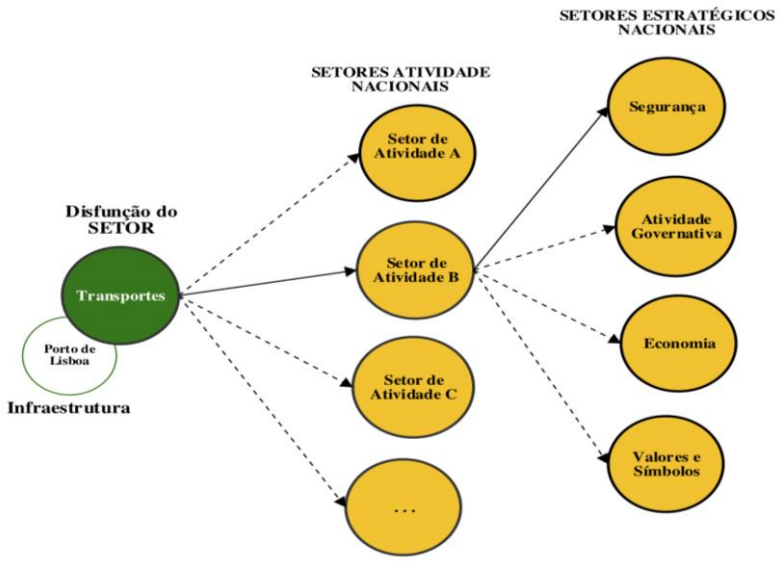

Figura 5 – Modelo da variável *V.ADPA*

Fonte: (Adaptado de Pais, Sá e Gomes, 2007; Mendes, 2017; Pais, n.d.)

e (ii) a *V.infra*, versando a probabilidade de uma grave disfunção de uma infraestrutura afetar gravemente o funcionamento do setor/subsetor em que se insere. Esta variável é obtida por tratamento de escalas de impacto[17], as quais foram desenvolvidas pelas entidades envolvidas no processo de identificação e avaliação de IC (Mendes, 2017; Pais, n.d.).

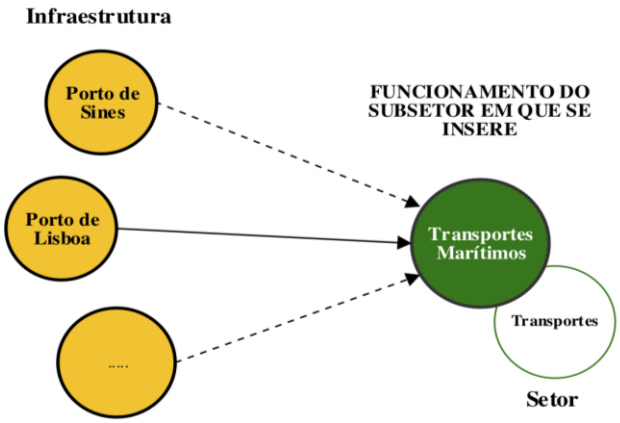

Figura 6 – Modelo da variável *V.infra*

Fonte: (Adaptado de Pais, Sá e Gomes, 2007; Mendes, 2017; Pais, n.d.)

Cientes das infraestruturas consideradas críticas, fundamentalmente resultante do grau de impacto funcional que a disfunção de um setor/subsetor pode provocar no normal funcionamento do País, sendo para tal hierarquizadas através do indicador de criticidade, torna-se necessário classificar quais destas IC poderão ou não ser consideradas ICN (Figura 7). Assim, através de uma metodologia de análise de *clusters*[18], foi possível definir cinco classes de criticidade, tendo o procedimento sido elaborado por forma a que dentro de cada *cluster* os valores de criticidade apresentassem um desvio padrão mínimo e os valores médios de cada classe fossem o mais distantes possível entre classes. Por fim, das IC identificadas, foi possível classificar de ICN apenas as IC que, cumulativamente,

[17] Os valores utilizados nas escalas de impacto não são apresentados fruto da sua classificação de segurança (n.º 2 do artigo 7.º do DL n.º 62/2011, de 9 de maio). No entanto, poderemos apresentar a escala qualitativa correspondente: Extremo ou total; Muito forte; Forte; Média; Fraca; Muito Fraca.

[18] "É um nome genérico para uma variedade de métodos matemáticos, numerados à centena, que pode ser usado para descobrir num conjunto de objetos quais os que são semelhantes. Por exemplo, se reuníssemos um conjunto de pedras de um riacho e observássemos as suas características em termos de tamanho, forma e cor e organizássemos as pedras semelhantes nas mesmas pilhas, estaríamos a realizar uma análise de *cluster* física. Cada pilha de pedras semelhantes seria um *cluster*. Os métodos matemáticos de análise de *cluster* realizam isso matematicamente. Em vez de classificar objetos reais, estes métodos classificam objetos descritos como dados. Objetos com descrições semelhantes são matematicamente reunidos no mesmo *cluster*. De facto, se fizéssemos uma análise de *cluster* física a um conjunto de pedras e, novamente, usando um método matemático de análise de *cluster*, deveríamos obter essencialmente o mesmo conjunto de *clusters*" (Romesburg, 2004, p.2).

estavam situadas no *cluster* máximo (5) e tivessem um nível de impacto nacional ou internacional (Mendes, 2017; Pais, n.d.).

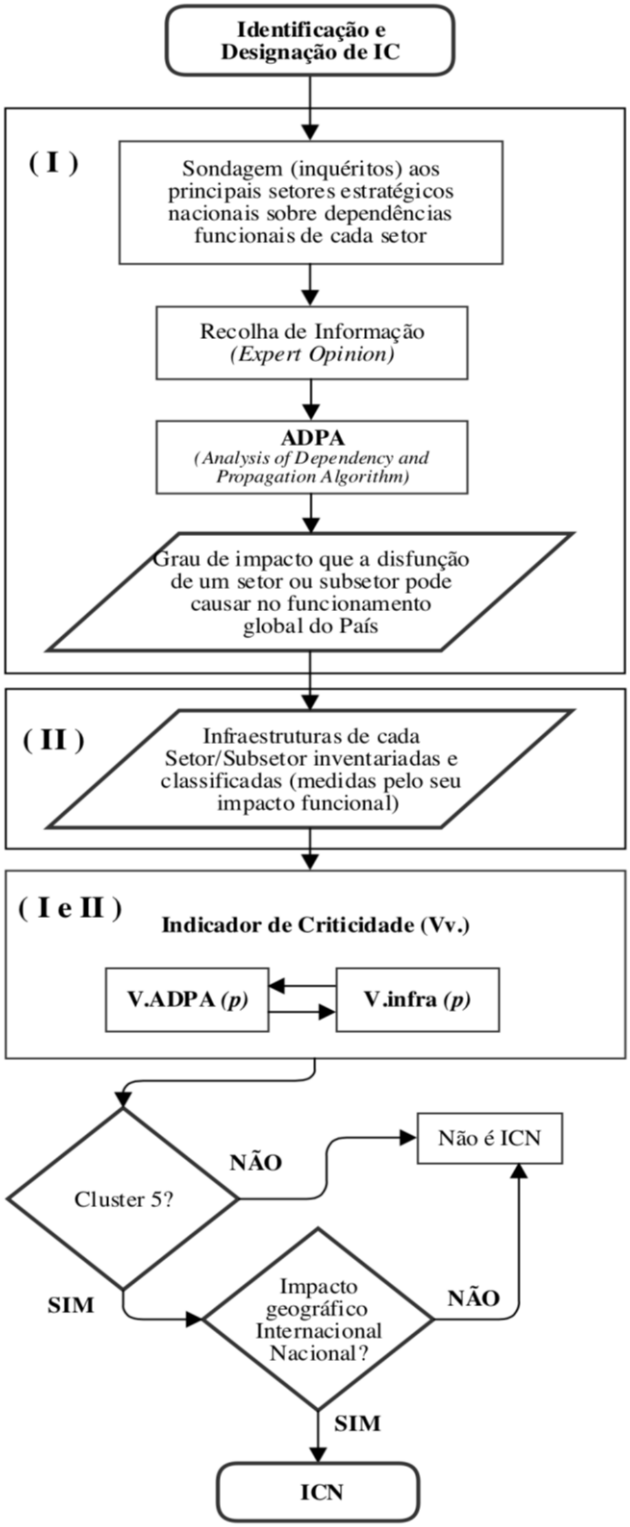

Figura 7 – Modelo de identificação e designação de IC/ICN

Fonte: (Adaptado de Pais, Sá e Gomes, 2007; Mendes, 2017; Pais, n.d.)

Plasmada a estrutura e articulação do procedimento relativo ao reconhecimento de uma infraestrutura como crítica pelo CNPCE, e atualmente utilizado pela ANPC, constata-se que a corporização do modelo de referência para a identificação e designação das IC se encontra sustentado numa metodologia (teoria da decisão, modelação matemática e *expert opinion*) de rigor e próxima dos "setores estratégicos" nacionais, salientando Mendes (2017) que "tem provado ser atualizada e adequada".

3.3. **Projeto de proteção de IC**

Na faculdade das suas atribuições de "definição e permanente atualização das políticas do planeamento civil de emergência, nomeadamente nas áreas dos transportes, da energia, da agricultura, pescas e alimentação, da indústria e das comunicações" (MDN, 1991, p.2284), o CNPCE constitui-se como a principal entidade em termos de competências relativamente ao desenvolvimento da Carta Nacional de Pontos Sensíveis (CNPS), atualmente designada por Proteção de Infraestruturas Críticas (Pais e Candeias, 2000).

Com a publicação da Deliberação do Conselho de Ministros n.º 51DB/2004, de 18 de março, o CNPCE assume a responsabilidade de coordenação e desenvolvimento do Projeto de Proteção de Infraestruturas Críticas (PPIC), constituindo um grupo de trabalho com os responsáveis dos setores e subsetores "estratégicos", com o objetivo de iniciar o PPIC nacional, tendo por base a CNPS (Pais, Sá e Gomes, 2007, p.68). Com a publicação da Diretiva n.º 2008/114/CE, de 8 de dezembro[19], a temática assume novo ímpeto e ao grupo de trabalho já constituído juntam-se também o SG-SSI, o Instituto Superior Técnico e a Fundação para a Computação Científica Nacional (Mendes, 2017).

Para Pais, Sá e Gomes (2007), a visão é uma estratégia nacional de proteção de infraestruturas fulcrais ao funcionamento do País, quer em situação de crise, quer do ponto de vista preventivo, sendo o PPIC materializado essencialmente em duas etapas: (i) identificação e classificação das infraestruturas estratégicas para o normal funcionamento do País e do bem-estar da sua população ou, em situação de crise, mantê-lo em níveis de funcionamento aceitáveis; e (ii) a elaboração do Programa Nacional para a Proteção de Infraestruturas Críticas (PNPIC), consubstanciando-se na "identificação e avaliação das vulnerabilidades das infraestruturas identificadas, face às principais ameaças passíveis de as atingir e no estudo e apoio à implementação de medidas de prevenção com vista a conter os riscos em níveis considerados aceitáveis" (ibidem, p.68).

[19] Ver anexo A.

Relativamente à revisão do estado da arte do PPIC, a primeira etapa, i.e. identificação e designação das IC, já foi concluída, constituindo-se como a base fundamental para a priorização das infraestruturas a serem integradas numa estratégia securitária a ser implementada a nível nacional, tendo em consideração a importância relativa para o País e catalogadas numa base de dados georreferenciada (ANPC, 2016). Para Pais, Sá e Gomes (2007, p.71) a metodologia implementada possibilitou atingir o seu grande objetivo, ou seja, "identificar quais as Infra-Estruturas Críticas Nacionais, classificá-las por critérios que objectivamente traduzem a sua importância relativa para o País, catalogá-las e reuni-las numa base de dados, onde a dimensão geográfica, estando também presente, lhe confere potencialidades que uma mera listagem (base de dados tradicional) não permite". Deste modo, foi então possivel vislumbrar a realidade nacional no que diz respeito às ICN, em particular: (i) mais de 65% podem ser gravemente afetadas por uma ocorrência sísmica, provável ou plausível; (ii) mais de 300 incutem uma significativa atratividade ou um elevado potencial para ações mal-intencionadas; (iii) parte delas localizam-se em zonas de elevado risco de incêndio florestal ou leitos de cheia; e (iv) urge a necessidade de implementar políticas e mecanismos focados na resiliência e manutenção da sua integridade (Pais, Sá e Gomes, 2007, p.71).

No que concerne à segunda etapa, a ANPC (2016, para.5) salienta que "constitui-se como a etapa central da proteção de infraestruturas críticas, na medida em que se identificam as vulnerabilidades face às ameaças que as poderão afetar, de modo a permitir implementar medidas eficientes para a redução daquelas. Esta fase está em curso". Ou seja, encontram-se por concretizar duas fases estruturantes e que materializam o PNPIC: "(i) análise e avaliação do risco associado à disfunção de infraestruturas críticas e estudo e difusão de medidas eficientes para reforço da sua proteção; e (ii) a implementação de medidas e monitorização do risco" (ibidem, para.3).

3.4. **A problemática da propriedade das IC**

3.4.1. Setor privado *versus* setor público

Quando hoje fazemos uma análise à propriedade de grande parte das IC em Portugal, não é com admiração que verificamos que na sua grande maioria são detidas pelo setor privado. Esta realidade não é apenas nacional; a nível europeu, "aproximadamente 90% das infraestruturas críticas nacionais estão efetivamente nas mãos do setor privado" (BSI, 2004, p.2), levando "as agências governamentais a adaptarem o seu estilo de interação com

esses operadores, passando de uma abordagem reguladora para uma mutuamente benéfica" (Comissão Europeia, 2009, p.15).

Neste âmbito, Pais, Sá e Gomes (2007, p.73) salientam que a cooperação entre setores público-privados é imprescindível, tornando-se um meio para que cada parte se vincule às suas responsabilidades, melhorando a forma como é garantida a segurança. Apesar da atribuição da gestão de um número significativo de IC ao setor privado, a responsabilidade atribuída ao Estado não foi substituída por ele, mas sim complementada (Schneider, 2014, p.4), na medida em que ninguém poderá estar melhor posicionado do que o setor privado para identificar e avaliar quais os sistemas/subsistemas dentro da sua própria empresa/setor que requerem proteção especial (BSI, 2004, p.2). Mantém-se a legitimidade e a obrigação de coordenação dentro da esfera pública, implicando uma interação entre públicos e privados (Schneider, 2014, p. 4).

Brunner e Suter (2008, p.47) referem que "em muitos países, a maioria dos elementos da infraestrutura crítica são propriedade ou operados como empresas comerciais", o que molda de facto a forma de encarar a gestão público-privada deste tipo de infraestrutura, assim como garante o cumprimento das responsabilidades a elas associadas. Em última análise, o Estado assegura a sua legitimidade na classificação das IC, mas, em contrapartida, apenas controla parte de um todo que é gerido por empresas privadas.

3.4.2. O domínio do capital estrangeiro sobre as IC

Ao abordarmos o investimento estrangeiro em Portugal, verifica-se desde logo que o princípio que norteia o quadro normativo é o da não discriminação do investimento em razão da nacionalidade (AICEP, 2017, para.1), à exceção das atividades onde as IC representem um ativo estratégico ao normal funcionamento do País e do bem-estar da sua população. Este facto é corroborado através do Instrumento de Tratamento Nacional da Organização para a Cooperação e Desenvolvimento Económico (OCDE), que, ao abrigo da "decisão processual do Conselho da OECD obriga os países aderentes a notificar as suas exceções ao tratamento nacional" (OECD, 2017, para.2), vincula Portugal a um conjunto de políticas de investimento discriminatórias.

Relativamente às exceções ao nível nacional, em particular ao investimento por empresas estrangeiras controladas, destaca-se desde logo o setor do transporte aéreo, sendo que o "estabelecimento no transporte aéreo regular nacional e internacional realizar-se-á através de empresas nacionais, empenhadas nesta atividade em exclusividade, com sede

em Portugal e onde a maior parte do capital e o controlo de gestão pertençam a entidades nacionais" (OECD, 2013, p.83). Outro exemplo versa o transporte marítimo, onde a "cabotagem marítima entre a parte continental portuguesa e os Açores, e entre os Açores, é reservada à bandeira nacional"[20] (OECD, 2014, p.82).

Comprova-se, assim, que a gestão destas políticas de investimento discriminatórias deve ser executada de forma assertiva, tendo em conta as várias formas que poderá assumir, designadamente: (i) restrições gerais, em que muitas restrições abrangentes afetam a infraestrutura e, em alguns casos, assumem a forma de uma proibição absoluta[21]; (ii) disposições de licenciamento específicas por setor; e (iii) medidas transetoriais, incluindo procedimentos de aprovação de investimentos, materialização de medidas transetoriais que podem ser aplicadas a investimentos em infraestruturas e, dessa forma, bloquear investimentos em infraestruturas (OECD, 2008). Pese embora as características apresentadas anteriormente, as mesmas políticas de investimento discriminatórias podem assumir-se também como complementares aos esforços para a proteção das IC, materializando-se essencialmente através de duas abordagens: "(i) a política de investimento pode servir como política de último recurso, i.e. se todos os outros mecanismos falharem, a política de investimento pode ser usada para evitar investimentos de entidades estrangeiras que se considere que representam riscos; [e] (ii) a política de investimento pode ser utilizada para abordar ou ajudar outras agências na identificação e avaliação das ameaças à segurança que possam ser colocadas pelos investidores internacionais" (OECD, 2008, p.8). Conforme podemos constatar, a forma como um País gere as suas políticas de investimento discriminatórias poderá influenciar sobremaneira a sua capacidade securitária e a forma como protege as suas IC.

[20] "Cabotagem Insular" para efeitos n.º 2 do DL n.º 7/2006, de 4 de janeiro, uma vez que versa "o transporte marítimo de passageiros e de mercadorias efectuado entre os portos do continente e os portos das Regiões Autónomas, e vice-versa, entre os portos das Regiões Autónomas e entre os portos das ilhas de cada uma das Regiões Autónomas" (MOPTC, 2006, p.71).

[21] "Na Coreia, a radiodifusão de rádio e televisão é totalmente fechada para investidores estrangeiros, embora a transmissão por cabo e por satélite seja permitida quando a taxa de controlo do investidor estrangeiro for 33% ou menos" (OECD, 2008, p.7).

4. A proteção das IC nacionais

4.1. As dimensões da proteção das IC

É perentório ao longo do nosso trabalho que a temática das IC tem uma abordagem relativamente à segurança sustentada em duas dimensões: o *safety* e o *security*. Embora na língua inglesa as duas palavras tenham significados diferentes, no caso português ambas significam "segurança". Apesar desta particularidade linguística, o *core business* de ambas complementa-se: a *safety* versa a prevenção ao perigo ou risco do acidente, enquanto a *security* integra a proteção contra as ameaças relativamente às pessoas, infraestruturas, organizações ou países. Desta forma, as definições relativas a ambas as dimensões são fulcrais na análise da especificidade própria de cada setor, devendo no caso nacional ser adequadas aos setores da energia e dos transportes.

Veja-se os exemplos internacionais, como é o caso do setor dos transportes aéreos espanhóis, onde a *safety* é definida como os processos orientados para mitigação do número de acidentes e incidentes aéreos, sustentando-se para tal em três pilares: (i) a definição de níveis de segurança aceitáveis, assim como de indicadores que permitam detetar um desvio que conduza à degradação ou perda de tais níveis; (ii) relatórios, investigações e análises de incidentes de segurança, assim como a posterior divulgação das *lessons learned*, e aplicação de medidas preventivas ou corretivas adequadas; e (iii) a deteção, avaliação e mitigação dos riscos, destinada à localização pró-ativa de possíveis perigos ao sistema de navegação aérea e a implementação de medidas de mitigação no sistema de modo a que o nível de risco seja tolerável (ENAIRE, 2017). Por seu turno, definem *security* como a proteção de passageiros, tripulações, pessoal de terra, público, aeronaves e instalações contra atos de interferência ilícita (ibidem). Poderíamos apresentar mais definições. Porém, o exemplo do setor dos transportes aéreos espanhóis é demonstrativo da forma como as dimensões *safety* e *security* poderão ser adaptadas, sem no entanto perderem o seu objetivo fundamental, i.e. proteção e segurança.

A realidade nacional de forma geral não difere daquelas que são as linhas orientadoras para a segurança das IC em termos internacionais, sendo no caso nacional feita uma integração de ambas as dimensões (*security* e *safety*) num único PSO[22] (Figura 8).

[22] Artigo 10.º do DL n.º 62/2011, de 9 de maio (MDN, 2011).

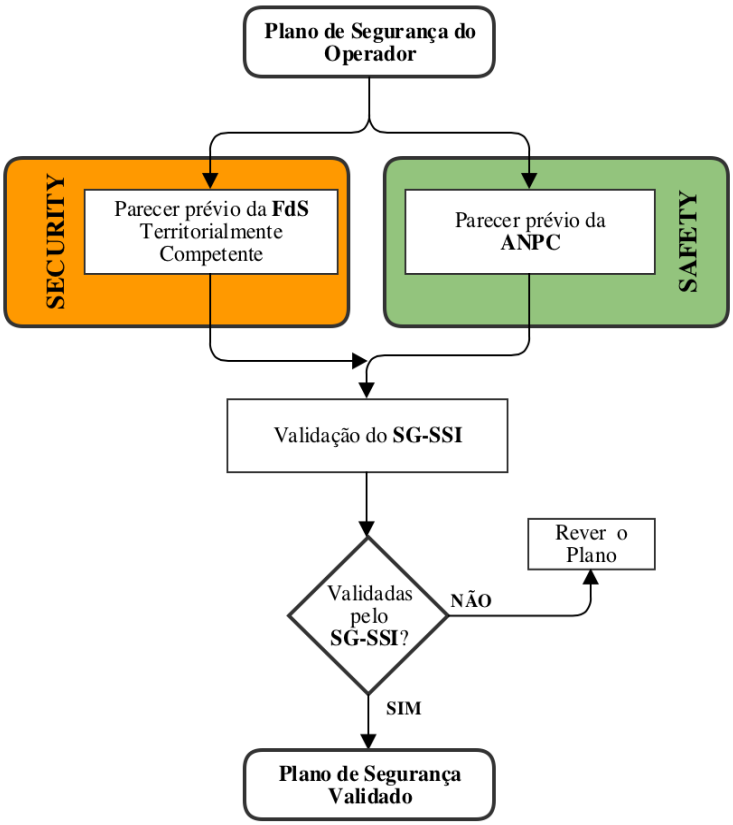

Figura 8 – Validação do PSO de ICN

Fonte: (Autor, 2017)

Assim, relativamente às IC na vertente *security*, o PSO deverá integrar obrigatoriamente no seu articulado os seguintes pontos: "(i) objetivos; (ii) legislação aplicável; (iii) identificação dos elementos importantes (críticos) da infraestrutura; (iv) análise de riscos; (v) contramedidas e procedimentos permanentes – seleção e prioridade; (vi) reação e resposta a incidentes de segurança identificados; (vii) contramedidas e procedimentos progressivos – seleção e prioridade; (viii) articulação com os planos externos à instalação; (ix) programa de formação do pessoal; e (x) programa de exercícios" (GCS, 2011, pp.3-9). Quanto às IC no âmbito *safety*, o PSO deverá integrar: "(i) objetivos; (ii) legislação aplicável; (iii) identificação dos elementos importantes (críticos) da infraestrutura; (iv) análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada componente e nos impactos potenciais; (v) identificação, seleção e prioridade de contramedidas e procedimentos permanentes e progressivos a aplicar consoante o grau de ameaça aplicável à IC ou o estado de segurança decretado; (vi) medidas de controlo e verificação; (vii) comunicação/sensibilização e formação; (viii)

segurança dos sistemas de informação e de comunicações; e (ix) articulação dos planos externos à instalação" (ANPC, 2013, pp.2-6).

Deste modo, e após o cumprimento dos imperativos legais sancionados quer pela FdS territorialmente competente, quer pela ANPC, o PSO integrando ambas as dimensões (*security* e *safety*) será entregue ao SG-SSI para análise e validação[23].

4.2. **Ameaças e riscos**

O enquadramento legal nacional relativo à identificação e proteção de IC é omisso quanto à abordagem a ter relativamente ao quadro das ameaças e dos riscos. Assim, dado que o preâmbulo do mesmo diploma especifica como objetivo a transposição para o enquadramento legal nacional da Diretiva n.º 2008/114/CE, de 8 de dezembro, somos levados a inferir que no caso nacional também seja aplicável a preocupação com as ameaças humanas, tecnológicas e catástrofes naturais, privilegiando as ameaças inerentes ao terrorismo (União Europeia, 2008, p.75).

Mendes (2017) salienta que, ao nível do risco, a ANPC versa a sua atuação tendo em consideração dois tipos de risco: (i) naturais, que envolvem acidentes geomorfológicos, cheias, ciclones, incêndios florestais, nevões, ondas de calor, precipitações intensas, secas, segurança de barragens, sismos, tornados, trovoadas e vagas de frio; e (ii) tecnológicos, que incluem ameaças NBQR, emergências radiológicas, gasodutos e oleodutos, substâncias perigosas em indústrias e armazenagem e transporte de mercadorias perigosas. No que às IC diz respeito, é dada especial atenção aos riscos naturais de cheias, incêndios florestais, segurança de barragens, sismos e tornados. Quanto aos riscos tecnológicos, é dada maior ênfase aos gasodutos, oleodutos, substâncias perigosas em indústrias e armazenagens (ibidem).

Relativamente à ameaça do terrorismo, e considerando que "muitos dos conflitos e disputas exploradas por organizações terroristas internacionais não mostram sinais de resolução rápida, até 2040, o terrorismo internacional persistirá" (UKMD, 2010, p.32) e criará ao nível nacional um maior desafio à segurança das IC.

4.3. **Agentes intervenientes na proteção das IC**

4.3.1. **ANPC**

A ANPC é a entidade nacionalmente responsável por "planear, coordenar e executar a política de proteção civil, [e] assegurar o planeamento e coordenação das necessidades nacionais na área do planeamento civil de emergência com vista a fazer face a situações de

[23] Artigo 10.º n.º 4 do DL n.º 62/2011, de 9 de maio (MDN, 2011).

crise ou de guerra" (MAI, 2014, p.5617). Neste âmbito, a ANPC assume um conjunto de atribuições específicas orientadas fundamentalmente para a componente da segurança na vertente *safety*, em particular: (i) previsão e gestão de risco e planeamento de emergência; (ii) ações de proteção e socorro; (iii) atividades no âmbito dos bombeiros; (iv) gestão de recursos de proteção civil; e (v) aplicação e fiscalização do cumprimento das leis, regulamentos, normas e requisitos técnicos aplicáveis no âmbito das suas atribuições (ibidem).

Com a publicação do DL n.º 73/2012, de 26 de março, a ANPC assumiu as atribuições relativas às IC, sucedendo ao CNPCE, sem contudo alterar o enquadramento jurídico plasmado no DL n.º 62/2011, de 9 de maio, relativamente às competências específicas no âmbito das ICN. Constituindo-se como a entidade nacionalmente responsável pela identificação e designação das IC, a intervenção da ANPC encontra-se fundamentalmente associada a quatro tarefas essenciais: (i) a identificação e designação de IC; (ii) emissão de pareceres prévios relativos aos planos de segurança de IC; (iii) coordenação com entidades estatais e operadores das IC; e (iv) representação nacional em fóruns internacionais (MDN, 2011, pp.2625-2627). Atendendo às exigências legais e técnicas, a Direção Nacional de Planeamento de Emergência[24] da ANPC assume grande parte das funções inerentes às ICN, nomeadamente: (i) a promoção da previsão, monitorização e avaliação dos riscos coletivos; (ii) avaliação das vulnerabilidades face ao risco; (iii) elaboração de orientações técnicas ajustadas à prevenção e socorro; e (iv) a apreciação e execução dos planos, e.g. PSO, que lhe sejam submetidos (MAI, 2014, p.5620).

Relativamente ao parecer do PSO pela ANPC (vertente *safety*), a sua avaliação é sustentada em três pontos principais: (i) análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada componente e nos impactos potenciais, subdividindo-se em identificação e caracterização dos riscos suscetíveis de afetar a instalação e tipos de emergências e cenários; (ii) identificação, seleção e prioridade de contramedidas e procedimentos permanentes e progressivos a aplicar consoante o grau de ameaça aplicável à IC ou o estado de segurança decretado, subdividindo-se em procedimentos de alerta e gestão de crises e medidas de minimização dos danos e impactos e de reposição da normalidade; e (iii) medidas de controlo e verificação, subdividindo-se em procedimentos de alerta de segurança e de gestão de crises (Delgado, 2017). Pretendendo tornar o

[24] Artigo 12.º do DL n.º 73/2013, de 31 de maio (MAI, 2013c).

processo de avaliação mais assertivo, foram criados ainda índices de ponderação para cada um dos três pontos.

Pese embora as ações e atividades executadas pela ANPC sejam orientadas principalmente para a vertente *safety*, a sua competência centralizadora no quadro do Sistema Integrado de Operações de Proteção e Socorro (SIOPS) permite-lhe um relacionamento direto com entidades da vertente *security*, e.g. FSS, sendo esta coordenação feita em função da localização da ICN, ou seja: (i) nível nacional, através do Comando Nacional de Operações de Socorro (CNOS); (ii) nível distrital, através do Comando Distrital de Operações de Socorro (CDOS); e (iii) nível municipal, através do Comandante Operacional Municipal (COM) (MAI, 2013b).

4.3.2. **Forças e serviços de segurança**

Considerando as especificidades de polícia (geral e especial) atribuídas às FSS, é sua função "defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos" (AR, 2005, p.142). Para Canotilho e Moreira (1993, p.272), "a distinção aqui feita entre defesa da legalidade democrática e garantia da segurança interna mostra que a primeira não coincide com a função tradicional de defesa da «ordem pública», que abrangia a defesa da tranquilidade (manutenção da ordem na rua, lugares públicos, etc.), da segurança (prevenção de acidentes, defesa contra catástrofes, prevenção de crimes) e da salubridade (águas, alimentos, etc.)". Por outro lado, a garantia da segurança interna concorre quer para a prevenção contra "o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem" (AR, 2008a), quer também para a "prevenção de acidentes" (Germano, 2001, p.61) graves ou catástrofes. No que concerne a garantia dos direitos dos cidadãos, esta apresenta-se como um limite à própria atividade de polícia, sendo os cidadãos "um dos próprios fins dessa função" (ibidem), principalmente devido ao garante dos seus direitos, liberdades e garantias[25].

Destarte, a "atribuição da função de segurança interna à polícia visa justamente colocar as FA à margem dessa função. No âmbito da polícia, a função de segurança interna cabe às forças de segurança" (Germano, 2001, p.955), que estarão sempre na "primeira linha de intervenção, quer na tomada de medidas preventivas, quer na resposta a situações anómalas" (Rodrigues, 2008, p.18).

A cultura de exigência relativamente à segurança das IC encontra-se associada em grande parte a dois fatores principais: (i) especificidade da atividade e (ii) o

[25] Ver artigos 24.º a 57.º da Constituição da República Portuguesa (CRP) (AR, 2005).

enquadramento legal que regula o sector. Quanto à especificidade da atividade, a mesma é de extrema importância relativamente a uma intervenção por parte das FdS, atendendo a que as IC só serão seguras enquanto funcionarem para o fim a que se destinam e em conformidade com os procedimentos técnicos específicos. Deste modo, uma intervenção das FdS descontextualizada poderá causar impactos irreparáveis, quer na própria infraestrutura, quer noutras essenciais ao funcionamento do País.

É neste quadro, e almejando uma interoperabilidade entre os operadores das IC e as FdS, que o plano de segurança dos operadores deverá ser articulado com o PSPE, em parte, da responsabilidade da FdS territorialmente competente (MDN, 2011), e que em caso de necessidade materializa uma resposta efetiva a este tipo de incidente. As competências das FdS são ainda mais abrangentes, na medida em que após receção do PSO de cada IC deverão elaborar um parecer prévio quanto ao (não) cumprimento do estabelecido no artigo 10.º do DL n.º 62/2011, de 9 de maio. Para tal, as FdS (vertente *security*) sustentam a sua avaliação consubstanciada em quatro pontos principais: (i) análise de risco, subdividindo-se em análise baseada no risco e caracterização; (ii) contramedidas e procedimentos permanentes, subdividindo-se em instalação de meios de deteção, controlo do acesso, proteção e prevenção, medidas de minimização dos danos e impactos e de reposição da normalidade e procedimentos de auditoria e verificação; (iii) reação e resposta a incidentes de segurança identificados, subdividindo-se em procedimentos de alerta de segurança e de gestão de crises; e (iv) contramedidas e procedimentos progressivos (Delgado, 2017). Em termos avaliativos, foram criados para cada um dos quatro pontos índices de ponderação, os quais são aplicados aquando da verificação do PSO.

4.3.3. **Forças Armadas**

Ao focarmo-nos nas duas grandes etapas[26] do PPIC, constata-se que as referências relativamente à intervenção ou participação das FA no processo são residuais, pese embora no quadro de resposta às ameaças e riscos do CEDN 2013 seja referido que "adquire grande acuidade a implementação de um Programa Nacional de Proteção das Infraestruturas Críticas" (MDN, 2013, p.45). Esta situação é ainda mais acentuada no DL n.º 62/2011, de 9 de maio, onde as entidades vinculadas diretamente à temática das IC são a ANPC, o SG-SSI, as FdS territorialmente competentes e os operadores.

[26] Primeira Etapa: identificação e designação das infraestruturas estratégicas ao normal funcionamento do País; Segunda Etapa: PNPIC (Pais, Sá e Gomes, 2007).

Conforme salienta Mendes (2017), a proteção das IC tenderá cada vez mais para uma integração direta nos planos de segurança, quer das próprias FdS, quer das estruturas de proteção civil locais. Ou seja, considerando que os domínios *security* e *safety* já possuem os seus próprios planos, não fará sentido estar a criar mais entropias aos sistemas já implementados e que funcionam. Assim, a intervenção das FA será sempre enquadrada atendendo ao enquadramento legal em vigor atualmente.

Assim, podemos desde logo verificar que as FA continuarão a "colaborar em missões de proteção civil, em tarefas relacionadas com a satisfação de necessidades básicas e a melhoria da qualidade de vida das populações, [e] no âmbito da política nacional de cooperação" (AR, 2005, p.144), particularmente, no caso dos Estados de Sítio e de Emergência[27], sendo fulcral o enquadramento legal relativamente às "condições do emprego das Forças Armadas quando se verifiquem essas situações" (ibidem), até porque "a etimologia estado de exceção implica a observância do princípio da excepcionalidade e do princípio da indispensabilidade na sua decretação, sob pena da exceção se converter em regra" (Valente, 2013, p.19).

A forma como se integram as FA em caso dos Estados de Sítio e de Emergência encontra-se plasmada na Lei n.º 44/86[28], de 30 de setembro (AR, 2012), vislumbrando-se uma diferença significativa em ambas as situações. Enquanto que no Estado de Sítio as FA assumem uma preponderância nacional relativamente às FdS, uma vez que "ficarão colocadas, para efeitos operacionais, sob o comando do Chefe do Estado-Maior-General das Forças Armadas, por intermédio dos respectivos comandantes-gerais"[29] (AR, 2012, p.2467), no Estado Emergência as FA, se necessário, apoiam em "reforço dos poderes das autoridades administrativas civis"[30] (ibidem, p.2468). Assim, Valente (2013, p.22) destaca que a intervenção das FA na segurança interna assenta em quatro princípios fundamentais: "(i) cooperação; (ii) indispensabilidade da intervenção das Forças Armadas; (iii) proporcionalidade da intervenção e da cooperação das Forças Armadas; e (iv) a subsidiariedade da intervenção das Forças Armadas. Todos têm em comum que o ente cooperador é as Forças Armadas e o ente cooperado é as forças de segurança". Esta cooperação leva-nos a uma abordagem sustentada em dois pontos fundamentais: "(i) a

[27] Artigo 19.º da CRP (AR, 2005).
[28] Alterada, i.e. artigos 7.º, 12.º, 14.º, 15.º, 16.º, 20.º, 23.º, 25.º e 28.º, através da Lei Orgânica n.º 1/2012, de 11 de maio.
[29] Artigo 8.º n.º 3 da Lei n.º 44/86, de 30 de setembro (AR, 2012).
[30] Artigo 9.º n.º 2 da Lei n.º 44/86, de 30 de setembro (ibidem).

ideia de que a atribuição da segurança interna é originária da polícia[31] e esta assume a responsabilidade civil, jurídica e política de toda a ação; e (ii) o comando ou direção da ação, que é do cooperado e não do cooperador, ou seja, as Forças Armadas cooperam sob o comando ou direção do *dominus* originário da atribuição e da competência – PSP, GNR" (Valente, 2013, p.23).

Ficamos, pois, com uma noção clara de que, apesar das FA não estarem associadas (pelo menos diretamente) à construção do PNPIC, acabam por o estar quer enquanto operadores de algumas das suas infraestruturas, quer na posição que ocupam num conjunto de fóruns, i.e. nacionais, distritais, municipais, que a jusante do plano consubstanciarão um forte ativo na estrutura nacional de proteção de IC.

4.3.4. **Serviço de informações de segurança**

Para assegurar o bom funcionamento e segurança do País, torna-se fulcral que o Estado enquanto entidade máxima responsável pela segurança coletiva, seja detentor de informações adequadas aos vários tipos de ameaças que possam afetar a integridade das IC. Neste sentido, o Serviço de Informações de Segurança (SIS) apresenta-se como "o único organismo incumbido da produção de informações destinadas a garantir a segurança interna e necessárias a prevenir a sabotagem, o terrorismo, a espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido" (SIRP, 2014, p.4208). Tendo no SG-SSI o seu principal ponto de coordenação para as IC, o SIS contribui de sobremaneira para a "avaliação das ameaças em relação aos subsetores das infraestruturas críticas" (MDN, 2011, p.12), quer no que concerne à adequação de ações a implementar, quer em apoio direto junto dos operadores das IC.

O Relatório Anual de Segurança Interna 2016 (GCS, 2016, p.78) realça, no conjunto das ações de informações do SIS, "o papel desempenhado no domínio da proteção de infraestruturas críticas, pontos sensíveis e outras infraestruturas relevantes de setores estratégicos portugueses, designadamente através o Programa *Krítica*". Implementado enquanto estratégia para a melhoria da proteção das IC face a eventuais ameaças terroristas, o Programa *Krítica* foi desenvolvido em duas vertentes: "(i) produção de avaliações de ameaça terrorista setoriais ou relativas a infraestruturas específicas, tendo como destinatários as tutelas do SIS, as Forças e Serviços de Segurança e as demais entidades públicas com competências nos setores visados; e (ii) ações de sensibilização

[31] Artigo 272.º da CRP (AR, 2005).

junto dos principais operadores, entidades reguladoras e associações de cada setor, específicas para cada destinatário ou grupo de destinatários, nas quais é partilhada informação reservada e não classificada" (SIS, n.d., para.2-3).

Desde a sua criação, em 2012, o Programa *Krítica* evoluiu e adaptou-se aos novos desafios da ameaça, tornando o SIS mais próximo quer das FSS, quer principalmente dos operadores das IC. Neste último caso, o SIS tem desenvolvido ações de sensibilização com foco na natureza da ameaça terrorista por setor, assim como na melhoria de medidas de proteção de infraestruturas (SIS, n.d.).

4.3.5. **Centro nacional de cibersegurança**

O Gabinete Nacional de Segurança (GNS) tem por missão garantir a segurança da informação classificada (nacional e internacional) e exercer a função de autoridade de credenciação e manuseamento de informação classificada (PCM, 2014). Atendendo a esta especificidade, foi entendimento governamental que o GNS era o serviço mais adequado para integrar o Centro Nacional de Cibersegurança (CNCSeg) na fase inicial da sua materialização, sem que isto inviabilizasse uma futura autonomia (ibidem).

A criação do CNCSeg surge alinhada com uma das ameaças de natureza global identificadas no CEDN 2013 (MDN, 2013, p.22), particularmente os ciberataques enquanto "ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna". O Despacho n.º 13692/2013, do Ministério da Defesa Nacional, de 28 de outubro (CNCS, 2013, p.3197), reconhece "que essas ações representam uma ameaça crescente sobre infraestruturas críticas, cujos efeitos e impactos podem provocar o colapso da estrutura tecnológica da organização social e económica do País".

Almejando uma resposta efetiva à nova ameaça, foi atribuída ao CNCSeg a missão de "contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, [...] bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas" (PCM, 2014, p.2715). Para tal, o CNCSeg deverá, no âmbito das suas competências, "(i) exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente [...] aos operadores de infraestruturas críticas nacionais; e (ii) contribuir para

assegurar a segurança dos sistemas de informação e comunicação [...] das infraestruturas críticas nacionais" (ibidem).

O desafio da cibersegurança criou novos desafios à segurança dos Estados, tendo levado muitos países europeus a adotar "uma estratégia nacional de cibersegurança, ou a mencionarem a cibersegurança como um aspeto importante das suas estratégias de segurança nacional" (Cîrlig, 2014, p.6), sendo no caso nacional materializada no CNCSeg.

4.4. **Os impactos da destruição, ou degradação do nível de serviço, das ICN**

Chegados a este ponto, e após uma análise global do enquadramento legal nacional relativo às ICN, tornam-se facilmente identificáveis os principais intervenientes envolvidos na sua proteção, a saber: SG-SSI, ANPC, FdS territorialmente competentes e os operadores das IC. Desta forma, cientes da missão que cada um desempenha direta ou indiretamente na proteção das IC, apresentaremos alguns exemplos da forma como também eles poderão ser prejudicados no caso de alguma IC ser afetada gravemente.

Relativamente ao SG-SSI, as implicações inerentes à destruição ou degradação das ICN poderá decorrer essencialmente da privação de energia elétrica, que se refletirá na prática na quebra de comunicações fixas, e.g. telefones e internet, comprometendo ações de coordenação, direção, controlo e comando operacional[32] com outras entidades, e.g. FSS e ANPC. Intuitivamente, somos levados a contrapor esta limitação com a existência de equipamentos redundantes, i.e. gerador, permitindo a salvaguarda imediata num caso de necessidade, no entanto, até os próprios terão de ser mantidos.

No que concerne à proteção civil, verificamos que é uma estrutura que se encontra descentralizada por todo o território nacional, fundamentalmente através dos CDOS e do COM, estando o CNOS instalado na sede da ANPC. Esta tipologia organizacional *per se* permite à ANPC mitigar alguns constrangimentos à sua atividade e continuar a desempenhar a sua missão mesmo que afetada pela destruição ou degradação de algumas das ICN. Ou seja, sempre que uma estrutura for afetada, será assegurada por outra até ao restabelecimento total das suas capacidades. Segundo Mendes (2017), a estrutura da ANPC encontra-se devidamente preparada para reagir em caso de destruição ou degradação das ICN que possam afetar a sua atividade, tendo no caso do CNOS medidas redundantes, i.e. geradores, que asseguram a manutenção da energia elétrica caso exista uma falha no seu fornecimento. E mais, no caso particular do subsetor do petróleo, i.e. combustíveis, Mendes (2017) salienta que poderá ser imposta uma limitação de abastecimento à

[32] Artigo 15.º da Lei n.º 53/2008, de 29 de agosto (AR, 2008a).

população em geral enquanto factor mitigador dos constrangimentos às ações da ANPC. Verifica-se então que a ANPC está também ela sujeita às limitações impostas pela destruição ou degradação das ICN. Porém, fruto daquilo que é a sua própria missão[33], muniu-se de estruturas e mecanismos que versam o menor impacto possível na sua organização.

Ao abordarmos o caso particular das FdS territorialmente competentes, temos de mencionar que, em consequência da sua organização e consequente dispersão territorial[34], também os impactos poderão serão diferentes. Existem, contudo, dois fatores que são primordiais para o cumprimento das missões das FdS: comando e controlo. Assim, quando pensamos nas implicações em caso de destruição ou degradação das ICN, podemos desde logo associar ao setor da energia, em particular: (i) ao subsetor elétrico, o qual provocaria sérios constrangimentos na ligação entre estruturas dentro da FdS e com as restantes entidades envolvidas na proteção das IC, e.g. operadores das IC; e (ii) ao subsetor do petróleo, i.e. combustíveis, que afetaria de sobremaneira a capacidade de resposta das FdS caso fossem necessárias, como foi o caso ocorrido em 2008 aquando da greve dos camionistas no nosso país, e onde a Guarda Nacional Republicana executou a escolta a vários veículos pesados de combustível para abastecimento do aeroporto de Lisboa e bombas de combustível que se encontravam à beira da rutura.

Por fim, as implicações para os próprios operadores das IC. Tendo como foco essencialmente o lucro, os operadores são os primeiros a apostar na eliminação ou mitigação de qualquer probabilidade de quebra da prestação de serviço da sua IC. No entanto, as IC podem efetivamente ser alvos de destruição e degradação, provocando efeitos diretos naquilo que são não só os lucros perdidos, como também a despesa para o seu restabelecimento até estar novamente em condições de prestar o serviço.

4.5. **Um "modelo de abordagem"**

Os Estados operam, hoje em dia, numa conjuntura cada vez mais global. Neste âmbito, podemos constatar que a proteção das IC enquanto processo dinâmico sustenta-se significativamente na capacidade de resposta face aos novos desafios securitários, quer nacionais, quer transnacionais. Deste modo, e após a materialização do Procedimento de Identificação e Designação de IC (PrIDIC), impõe-se que apresentemos uma proposta de um modelo de abordagem relativamente à forma como deverá ser estruturado o

[33] Artigo 2.º do DL n.º 73/2013, de 31 de maio (MAI, 2014).
[34] DL n.º 44/2007, de 19 de março (PCM, 2007); Portaria n.º 340-A/2007, de 20 de março (MAI, 2007).

Procedimento de Proteção de IC (PrPIC)[35], enquanto instrumento de interoperabilidade e aprendizagem entre os intervenientes envolvidos, o que se afigura como um desafio extremamente importante para o sucesso da proteção das IC.

Tendo em conta o exposto, procedemos à elaboração de um modelo que se pretende prático na operacionalização da fase II do PPIC, i.e. PNPIC, o qual foi ancorado em quatro pressupostos essenciais: (i) a simplicidade; (ii) a sistematização; (iii) a abrangência; e (iv) a lógica. Com este arranjo estrutural, focámo-nos em apresentar um modelo visando os seguintes objetivos: (i) criar uma metodologia sistemática e estruturada; (ii) interligação lógica entre os intervenientes no procedimento; (iii) alargamento das áreas a serem consideradas para validação; e (iv) harmonização de procedimentos.

Relativamente ao modelo proposto, podemos distinguir, desde logo, quatro fases sequenciais, a saber: (i) análise do risco do operador da IC; (ii) elaboração do PSO; (iii) planeamento de exercícios; e (iv) elaboração do PNPIC.

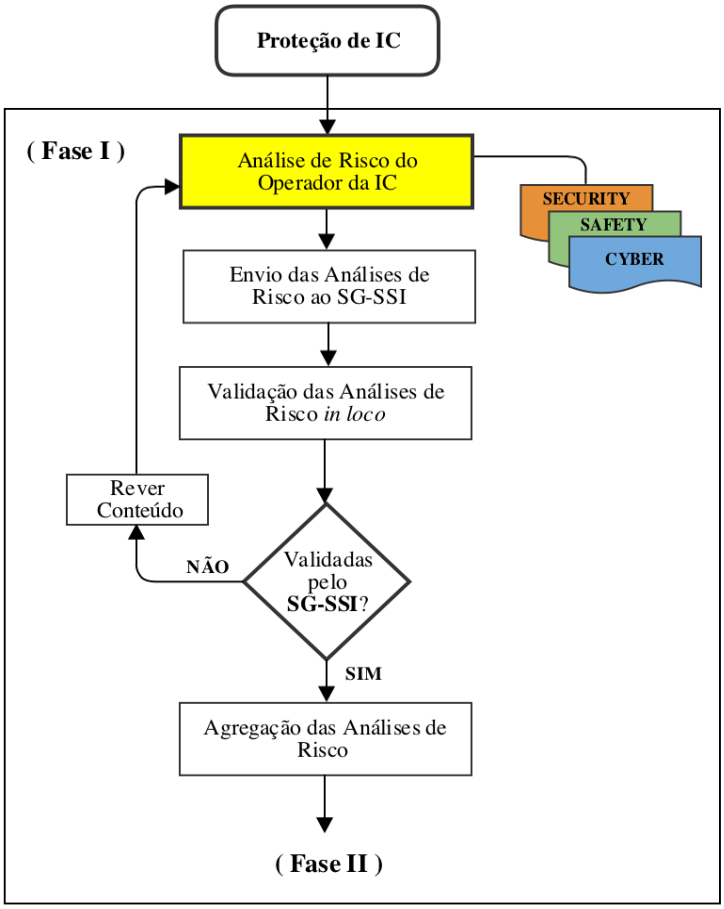

Figura 9 – Fase I do procedimento de proteção

Fonte: (Autor, 2017)

[35] Artigos 10.º a 15.º do DL n.º 62/2011, de 9 de maio (MDN, 2011).

No que concerne a Fase I - Análise de risco do operador da IC (Figura 9), pretende-se que os operadores das IC procedam à Análise de Risco (AdR) das suas infraestruturas considerando as vertentes *security*, *safety* e *cyber*, dando uma visão global das suas vulnerabilidades quanto à probabilidade dos riscos e das ameaças. Reunida esta informação, o operador deverá enviar as AdR para o SG-SSI, o qual, deverá proceder à sua validação *in loco*. Caso a AdR não seja validada pelo SG-SSI, o operador terá de rever a AdR e tornar a iniciar o processo. Após a validação por parte do SG-SSI das AdR, será feita a sua agregação por setor e subsetor[36] de atividade num único documento, o qual, em cômputo, consubstanciará a realidade nacional quanto aos possíveis riscos das IC.

Neste arranjo, será possível um vislumbre do(s) risco(s) quer por tipo de dimensão, quer por setor/subsetor (Figura 10). Caso sejam identificadas IC onde o risco identificado não seja aceitável segundo os *standards* a serem definidos a nível nacional, competirá ao SG-SSI solicitar ao operador dessa IC que elimine ou mitigue o risco, tornando-o dessa forma aceitável e permitindo iniciar a elaboração do PSO (Fase II).

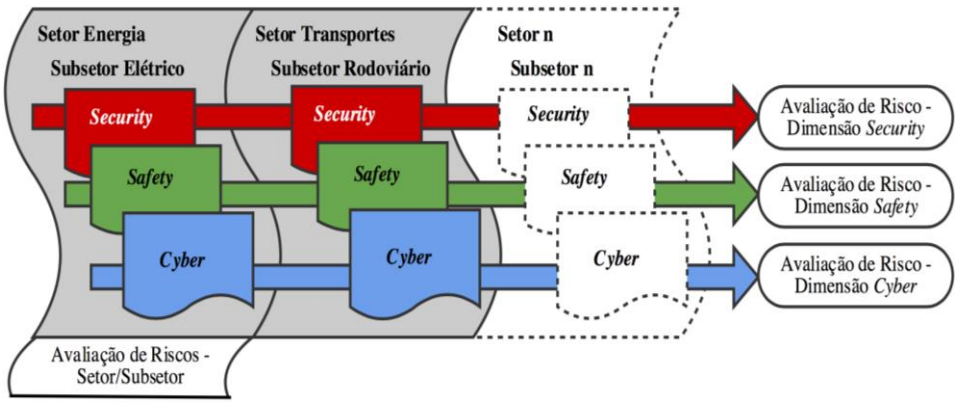

Figura 10 – Integração das avaliações de risco

Fonte: (Autor, 2017)

Na Fase II - Elaboração do PSO (Figura 11), o operador, após ter completado as suas obrigações inerentes à Fase I, inicia a elaboração do PSO da IC. Na posse do PSO, o operador deverá remeter três exemplares, respetivamente, para a FdS territorialmente competente, ANPC e CNCSeg, que emitirão pareceres prévios nas suas áreas de competência, i.e. *security*, *safety* e *cyber*. Depois de rececionar os três documentos com os pareceres prévios, o operador enviará os mesmos para o SG-SSI para validação. Caso o PSO não seja validado pelo SG-SSI, o operador terá de rever o mesmo e reiniciar o processo. Após a validação dos PSO pelo SG-SSI, será feita a sua integração num único

[36] Artigo 3.º do DL n.º 62/2011, de 9 de maio (MDN, 2011).

documento, versando o seu conteúdo a totalidade de PSO a nível nacional, por setor e subsetor de atividade das IC nacionais. Dada a sua relevância, o documento será enviado às FdS territorialmente competentes e à proteção civil, para em articulação procederem à sua integração no PSPE das IC instaladas na sua zona de ação.

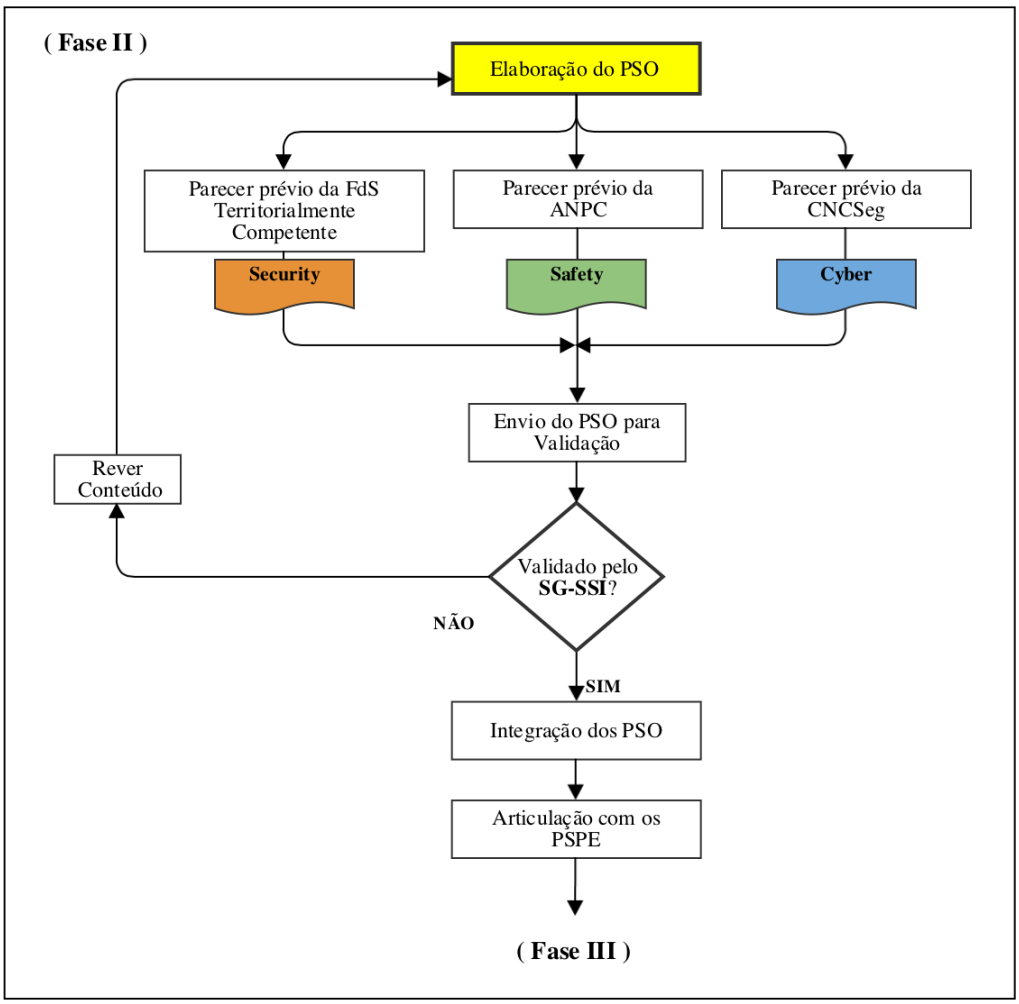

Figura 11 – Fase II do procedimento de proteção

Fonte: (Autor, 2017)

Cumpridas as fases I e II, e providos dos PSO por IC, iniciar-se-á a Fase III - Planeamento de exercícios (Figura 12), a qual deverá versar essencialmente três objetivos específicos: (i) operacionalizar as medidas vertidas no PSO; (ii) treinar via exercício(s) os procedimentos de resposta a incidentes ocorridos nas IC; e (iii) promover a interoperabilidade entre intervenientes com atribuições diretas e indiretas na área.

Para tal, entendemos ser pertinente dividir a Fase III em dois tipos de incidentes: (i) proteção civil (Fase III-A) e (ii) segurança interna (Fase III-B). Definidos os cenários base para o planeamento de exercícios, prosseguimos para a Fase III-A – Incidentes no âmbito

da proteção civil, a qual desde logo consubstancia uma reunião preparatória com as entidades a serem envolvidas no exercício, podendo essa coordenação ocorrer ao nível nacional, distrital ou municipal.

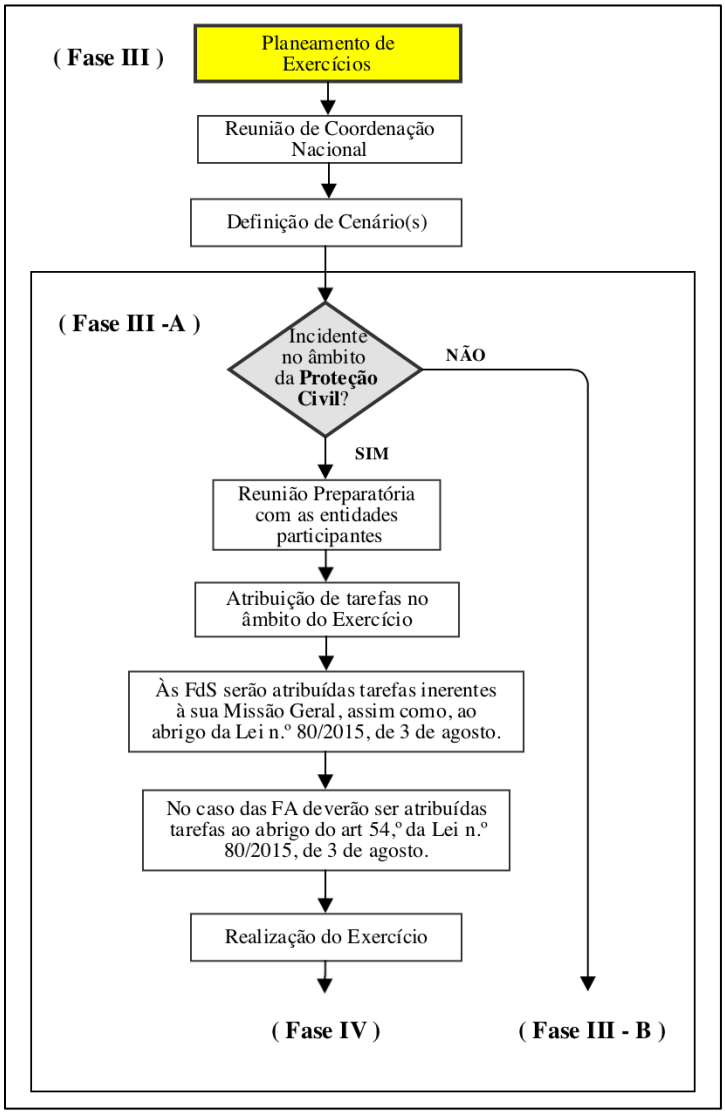

Figura 12 – Fases III e III-A do procedimento de proteção

Fonte: (Autor, 2017)

Pretende-se que o produto desta reunião seja essencialmente a atribuição de tarefas aos intervenientes envolvidos direta e indiretamente no cenário. Ou seja, pese embora as especificidades das FdS e das FA decorrentes da sua condição, a sua integração nesta fase poderá passar pela atribuição de tarefas enquanto agentes de proteção civil, enquadrada na Lei n.º 80/2015, de 03 de agosto. O final desta fase dá-se com a compilação de contributos para o PNPIC (Fase IV).

Em complemento à Fase III-A, apresentamos a Fase III-B – Incidentes no âmbito da segurança nacional (Figura 13), a qual reveste características muito próprias em termos de atribuições de tarefas para os exercícios, em particular no caso das FA. Em geral, podemos constatar que a diferença da Fase III-A para a Fase III-B reside fundamentalmente na forma como as FA poderão ser empenhadas, ou seja: (i) estado de sítio, com tarefas de comando operacional das FdS e a subordinação das autoridades civis ou (ii) estado de emergência, com a atribuição de tarefas essencialmente de apoio às autoridades administrativas.

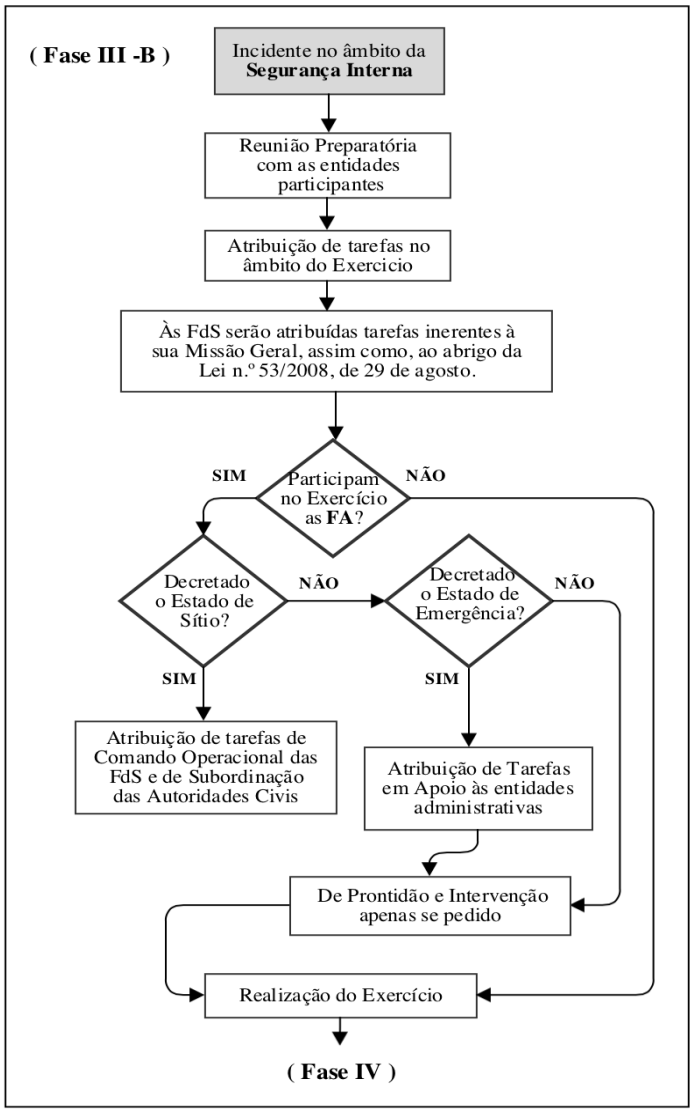

Figura 13 – Fase III-B do procedimento de proteção

Fonte: (Autor, 2017)

Por fim, mas não menos importante, alcançamos a Fase IV – Elaboração do PNPIC, o qual refletiria a estratégia nacional de proteção de IC, apresentando uma panorâmica

global dos fatores mais importantes nesse âmbito, contemplando de forma abrangente toda a informação necessária aos intervenientes no procedimento de proteção.

É evidente que, fruto da especificidade de cada setor e subsetor, o PNPIC teria de ter em conta um vasto conjunto de fatores que tornariam único. Acresce que, permitiria ser ajustado, caso a caso, sempre que houvesse quer alterações às ICN já consideradas, quer a novas infraestruturas.

Em suma, sustentados através de quatro fases estruturantes – análise do risco do operador da IC, elaboração do PSO, planeamento de exercícios e elaboração do PNPIC –, construímos um modelo de procedimento de proteção de IC que, embora possa parecer um objetivo ambicioso, poderá ser alcançado através da conjugação de esforços dos principais atores na área, sendo que a sua materialização efetiva dependerá sempre de um quadro político sensível à proteção das IC.

Conclusões e recomendações

Cientes de que a disrupção ou destruição de apenas uma IC poderá colocar em risco todo o País, e que relativamente ao PPIC iniciado em 2004 persiste ainda por finalizar o PNPIC, vislumbrámos uma oportunidade para realizar a presente investigação, tendo como objetivo principal avaliar o papel e o peso que o atual modelo de abordagem atribuiu às FA e FSS no esforço interoperável para garantir a proteção das IC.

A publicação do DL n.º 62/2011, de 9 de maio, resultante da transposição da Diretiva do Conselho n.º 2008/114/CE, de 8 de dezembro, materializou o surgimento formal dos procedimentos de identificação e proteção das ICE, sendo que, ao percorremos a norma, constatamos que a sua aplicabilidade é extensiva às ICN. Atendendo a que é condição *sine qua non* para uma infraestrutura ser designada de ICE ser a montante ICN, procedemos à delimitação da nossa investigação às infraestruturas designadas como ICN.

Destarte, deduzimos a nossa QC "De que forma poderão as FA e FSS contribuir para a proteção das Infraestruturas Críticas Nacionais no âmbito do atual modelo de abordagem?" à qual, aliamos três QD que permitiram guiar todo processo de investigação relativo à obtenção de uma resposta à nossa QC. Outrossim, conforme apresentado no primeiro capítulo, foram seguidas as principais fases do percurso metodológico definidos na publicação de referência do Instituto Universitário Militar (IESM, 2016).

O segundo capítulo da investigação foi dedicado à apresentação de conceitos que, por inerência da abordagem, permitiram conceptualizar um conjunto de matérias fundamentais à compreensão do efeito que as IC poderão ter na segurança nacional. Após a revisão da literatura, verificámos que o DL n.º 62/2011, de 9 de maio, é o único documento que apresenta uma definição vinculativa de IC. Assim, concluímos que, embora possam ser apresentadas outras definições de IC a nível nacional, o quadro conceptual prevalecente de IC é *unicus* e encontra-se plasmado no DL n.º 62/2011, de 9 de maio, considerando assim respondida a nossa QD1.

No terceiro capítulo focámo-nos inicialmente na análise do enquadramento legal nacional relativo às IC, tendo sido apresentadas as características mais relevantes no que toca à identificação e designação de IC, tipos de planos, i.e. PSO e PSPE, e entidades com responsabilidades na área. No seguimento, fizemos uma descrição detalhada do modelo de identificação e designação de IC em vigor que, fundamentalmente, se sustenta em instrumentos como a teoria da decisão e a modelação matemática. Para tal, explicitámos que o modelo assenta essencialmente em quatro "sectores estratégicos": (i) a segurança;

(ii) a atividade governativa; (iii) a economia; e (iv) os valores e símbolos. Ancorados na *expert opinion* dos operadores da cada setor, no algoritmo ADPA e na MACBETH, foi definido o grau de impacto que uma disfunção de um setor/subsetor poderia causar no funcionamento do País. Após a inventariação das infraestruturas e a atribuição de um Vv, a IC passará a ICN se e só se, cumulativamente, integrar o *cluster* 5 e tiver impacto geográfico nacional. Concluímos que o modelo versa única e simplesmente a identificação e designação de IC, não contemplando qualquer modelo relativo à sua proteção, o que inviabiliza uma abordagem global às ICN. Consideramos assim respondida a nossa QD2.

No quarto capítulo apresentámos uma visão transversal relativamente a importantes fatores e atores intervenientes na proteção das ICN. Verificámos as diferenças entre as dimensões *safety* e *security* e a forma como ambas são integradas nos PSO, tendo-se constatado que em ambas as circunstâncias a sua validação não é acompanhada por uma verificação *in loco*. Mais, após a validação do PSO, os atores intervenientes diretamente na proteção das IC não tomam conhecimento do plano aprovado.

Fizemos também um alinhamento das competências dos atores intervenientes diretamente na proteção das IC, i.e. SG-SSI, ANPC e FdS, com as das FA (ator indireto), e verificámos que, no caso das FA, a sua intervenção no âmbito da segurança interna só pode acontecer em duas condições: (i) no Estado de Sítio, em que assumem uma preponderância nacional relativamente às FdS; ou (ii) no Estado Emergência, onde, se necessário e a pedido, apoiam em reforço as autoridades administrativas civis.

Elaborámos um modelo de proteção de IC, o qual permite a integração da componente técnica com a componente de exercícios, possibilitando dessa forma "testar" não só a capacidade dos operadores, como também dos restantes atores intervenientes em caso de disrupção ou destruição da IC. Podemos concluir que, embora a norma limite a intervenção das FA no âmbito da proteção das IC, um planeamento de exercícios conjuntos revestir-se-á claramente como um excelente contributo para a adequabilidade da intervenção de todos os atores envolvidos, seja direta ou indiretamente, ao nível do contexto nacional. Consideramos assim respondida a nossa QD3.

Estamos, então, em condições de afirmar que conseguimos responder às nossas QD e, em conjunto, permite que reputemos a nossa QC respondida. Deste modo, foi atingido o objetivo principal de avaliar o papel e o peso que o atual modelo de abordagem atribuiu às FA e FSS no esforço interoperável para garantir a proteção das IC.

Como contributo essencial para o conhecimento, esta investigação permitiu uma identificação do atual modelo de identificação e designação das IC em Portugal, apresentando as principais fases para alcançar a designação de ICN. Contribuiu ainda, em resposta à QC da investigação, para expor o lugar reservado às FA e FSS na componente relativa à proteção das IC. De igual modo, aduz um modelo de proteção de IC corporizado essencialmente em quatro fases: (i) análise do risco do operador da IC; (ii) elaboração do PSO; (iii) planeamento de exercícios; e (iv) elaboração do PNPIC. Com o desenvolvimento do modelo de proteção de IC, almeja-se contribuir para um acréscimo de sustentação teórica que permita fechar o ciclo relativo ao PPIC.

Relativamente a recomendações que permitam um progresso da área em estudo, oferece-nos sugerir que seja feita uma alteração legislativa que permita adequar a norma à realidade atual que envolve as IC, destacando-se: (i) descentralização de competências nas FdS e da proteção civil a nível distrital, resultando num controlo próximo das IC por parte dos principais atores responsáveis pela sua validação e proteção; (ii) validação *in loco* da AdR do operador, permitindo uma perceção real não só do risco como também das especificidades das próprias infraestruturas; (iii) aumento temporal entre as revisões do PSO, aproximando assertivamente o enquadramento legal nacional da periodicidade das alterações das IC; e (iv) a inclusão no PNPIC de um planeamento de exercícios com todos os atores envolvidos (direta e indiretamente) na proteção de ICN, constituindo-se como um modelo nacional integrado e interoperável.

No que concerne às limitações para a elaboração desta investigação, destacamos o número reduzido da amostra relativamente à obtenção da *expert opinion*, essencialmente devido à especificidade da temática que não permite uma grande abrangência em termos de profissionais conhecedores da área. Todavia, conseguiu-se obter a transversalidade de atores envolvidos diretamente quer no procedimento de identificação e designação, quer no procedimento de proteção das ICN.

Para investigações futuras relativamente à temática, e atendendo a que neste caso delimitámos o estudo às ICN, seria pertinente avaliar a forma e o impacto resultante da operacionalização do modelo proposto na interoperabilidade entre as FA e os FSS; da mesma forma, seria útil aprofundar o estudo das responsabilidades e dos impactos financeiros decorrentes da legislação sobre a proteção de ICN de propriedade privada.

Bibliografia

Abrantes, P., 1993. Learning Activities Involving Mathematics in Real-Life Situations. In T. Breiteig, I. Huntley & G. Kaiser-Messmer, eds. *Teaching and Learning Mathematics in Context*. Chichester: Ellis Horwood, pp.103-114.

AICEP, 2017. *Investir em Portugal*. [Em linha] Disponível em: http://www.portugalglobal.pt/PT/InvestirPortugal/Criareinstalar/Paginas/OInvestimentoEstrangeiroPortugal.aspx [Acedido em 12 Jan. 2017].

Almeida, A., n.d. *A Multi-Criteria Methodology for the Identification & Ranking of Critical Infrastructures*. [Em linha] Disponível em: http://fenix.tecnico.ulisboa.pt/downloadFile/395142726454/Resumo.pdf [Acedido em 31 Mar. 2017].

ANPC [Autoridade Nacional de Proteção Civil], 2013. *Planos de Segurança do Operador (PSO) de Infraestruturas Críticas - Conteúdos dos PSO na Componente Safety*. Lisboa: Autoridade Nacional de Proteção Civil.

ANPC, 2016. *Infraestruturas Críticas*. [Em linha] Disponível em: http://www.prociv.pt/pt-pt/RISCOSPREV/INFRAESTRUTURASCRITICAS/Paginas/default.aspx [Acedido em 06 Nov. 2016].

ANPC, 2017. *Acidentes Tecnológicos*. [Em linha] Disponível em: http://www.prociv.pt/pt-pt/Paginas/default.aspx [Acedido em 28 Mar. 2017].

API [American Petroleum Institute], 2003. *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*. Washington: API.

AR [Assembleia da República], 2005. *Lei Constitucional n.º 1/2005, de 12 de agosto - Constituição da República Portuguesa - Sétima Revisão*. Lisboa: Assembleia da República.

AR, 2008a. *Lei n.º 53/2008 de 29 de agosto - Lei de Segurança Interna*. [Em linha] Lisboa Disponível em: http://www.legislacao.mai-gov.info/i/lei-de-seguranca-interna/ [Acedido em 01 Mar. 2017].

AR, 2008b. *Tratado de Lisboa*. [Em linha] Disponível em: http://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf [Acedido em 18 Fev. 2017].

AR, 2012. *Lei n.º 44/86, de 30 de setembro (2.ª alteração a coberto da Lei Orgânica n.º 1/2012, de 11 de maio) - Regime do Estado de Sítio e do Estado de Emergência*. [Em linha] Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626e526c654852766331396863484a76646d466

b62334d764d6a41784d69394d54313878587a49774d5449756347526d&fich=LO_1_2012.pdf&lnline=true [Acedido em 01 Fev. 2017].

ASME [American Society of Mechanical Engineers], 2009. *All-Hazards Risk and Resilience - Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach*. New York: ASME.

Australian Government, 2010. *Critical Infrastructure Resilience Strategy*. [Em linha] Disponível em: http://ccpic.mai.gov.ro/docs/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf [Acedido em 11 Fev. 2017].

Beck, U., 2015. *Sociedade de Risco Mundial: em busca da segurança perdida*. Lisboa: Edições 70.

Boone, W., 2013. Risk Management. In R. Radvanovsky & J. Brodsky, eds. *Handbook of SCADA/Control Systems Security*. London: CRC Press, pp.69-111.

Bradbury, J.A., 1989. The Policy Implications of Differing Concepts of Risk. *Science, Technology & Human Values*, 14(4), pp.380-399.

Brunner, E.M. & Suter, M., 2008. *International CIIP Handbook 2008/2009 - A Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*. Zurich: CSS - Swiss Federal Institute of Tecnology.

BSI [Bundesamt für Sicherheit in der Informationstechnik], 2004. *Critical Infrastructure Protection: Survey of World-Wide Activities*. [Em linha] Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile [Acedido em 12 Fev. 2017].

Businessdictionary, 2017. *Definition of "Expert"*. [Em linha] Disponível em: http://www.businessdictionary.com/definition/expert.html [Acedido em 23 Abr. 2017].

Cambridge University Press, 2017. *Definition of "Safety"*. [Em linha] Disponível em: http://www.dictionary.cambridge.org/pt/dicionario/ingles/safety [Acedido em 03 Mar. 2017].

Cambridge University Press, 2017. *Definition of "Security"*. [Em linha] Disponível em: http://www.dictionary.cambridge.org/pt/dicionario/ingles/security [Acedido em 03 Mar. 2017].

Canotilho, G. & Moreira, V., 1993. *Constituição da República Portuguesa Anotada*. 3ª ed. Coimbra: Coimbra Editora.

Cardoso, L., 1981. Defesa Nacional - Segurança Nacional. *Nação e Defesa*, 17, pp.11-24.

Cîrlig, C.-C., 2014. *Cyber Defence in the EU - Preparing for Cyber Warfare*. [Em linha] Disponível em: http://europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf [Acedido em 14 Mar. 2017].

CNCS [Centro Nacional de Cibersegurança], 2013. *Enquadramento da Ciberdefesa no Conceito Estratégico de Defesa Nacional*. [Em linha] Disponível em: https://www.cncs.gov.pt/content/files/orientao_politica_para_ciberdefesa.pdf [Acedido em 03 Mar. 2017].

Comissão Europeia, 2009. *Stock-Taking of Existing Critical Infrastructure Protection Activities*. [Em linha] Disponível em: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/2009_cip_stock_taking_en.pdf [Acedido em 12 Fev. 2017].

Costa, C.B., Corte, J.-M. & Vansnick, J.-C., 2010. *Macbeth (measuring attractiveness by a categorical based evaluation technique)*. [Em linha] Disponível em: https://fenix.tecnico.ulisboa.pt/downloadFile/3779580061316/BanaeCostaEtAl2011.pdf [Acedido em 25 Abr. 2017].

Delgado, P., 2017. *As Infraestruturas Críticas Nacionais - Atuação da Guarda Nacional Republicana no âmbito do Decreto-lei 62/2011, de 9 de maio*. [Entrevista] Lisboa (10 abril 2017).

Di Nicola, A. & McCallister, A., 2006. Existing Experiences of Risk Assessment. *European Journal on Criminal Policy and Research*, 12(3), pp.179-187.

ENAIRE, 2017. *Seguridad: Safety o Security*. [Em linha] Disponível em: http://www.enaire.es/csee/Satellite/SeguridadOperacionalINA/es/Page/1228215516978/1228215409300/Monograficos.html [Acedido em 04 Mar. 2017].

FEMA [Federal Emergency Management Agency], 2017. *FEMA Glossary*. [Em linha] Disponível em: https://emilms.fema.gov/is700anew/glossary.htm#I [Acedido em 24 Fev. 2017].

Fernandes, L.M.S., 2004. *Quais os Sectores Estratégicos de Interesse para a Formulação de uma Actual Política de Defesa Nacional? Como Consubstanciar esse Interesse?* Trabalho Individual de Longa Duração. IAEM.

Ferreira, H.J.D., 2016. *Identificação e Caracterização de Infraestruturas Críticas - Uma Metodologia*. Trabalho de Investigação Individual do CEMC 2015/16. IUM.

Fonseca, J.N., 2010. *O Conceito de Segurança Nacional Perspetivado para 2030*. Trabalho de Investigação Individual CPOG 2009/10. IESM.

Freixo, M.J.V., 2011. *Metodologia Científica - Fundamentos, Métodos e Técnicas*. Lisboa: Instituto Piaget.

GCS [Gabinete Coordenador de Segurança], 2011. *Infraestruturas Críticas - Conteúdos dos Planos de Segurança do Operador (Componente Security)*. Lisboa: Gabinete Coordenador de Segurança.

GCS, 2016. *Relatório Anual de Segurança Interna 2016*. Lisboa: Gabinete Coordenador de Segurança.

Germano, S., 2001. *Ética Policial e Sociedade Democrática*. Lisboa: ISCPSI.

GFMI [German Federal Ministry of the Interior], 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. [Em linha] Disponível em: https://www.bbk.bund.de/ShareDocs/Downloads/BBK/EN/CIP-Strategy.pdf?_blod=publicationFile [Acedido em 11 Fev. 2017].

Gobierno de España, 2011. *Establecimiento de Medidas Para la Protección de las Infraestructuras Críticas*. [Em linha] Disponível em: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf [Acedido em 04 Dez. 2016].

Gobierno de España, 2013. *Estrategia de Seguridad Nacional - Un Proyecto Compartido*. [Em linha] Disponível em: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf [Acedido em 06 Dez. 2016].

Haimes, Y.Y. & Horowitz, M.B., 2004. Modeling Interdependent Infrastructures for Sustainable Counterterrorism. *Journal of Infrastructure Systems*, 10(2), pp.33-42.

Harmmerli, B. & Renda, A., 2010. *Protecting Critical Infrastructure in the EU*. Brussels: Centre for European Policy Studies.

IESM [Instituto de Estudos Superiores Militares], 2016. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação*. Porto: Fronteira do Caos.

ISO [International Organization for Standardization], 2009. *International Standard ISO 31000: Risk Management - Principles and Guidelines*. Geneve: ISO copyright office.

ISPC [The Information Security Policy Council], 2009. *The Second Action Plan on Information Security Measures for Critical Infrastructures*. [Em linha] Disponível em: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf [Acedido em 11 Fev. 2017].

Klima, N., Dorn, N. & Beken, T.V., 2011. Risk Calculation and Precautionary Uncertainty: Two Configurations Within Crime Assessment. *Crime, Law and Social Change*, 55(1), pp.15-31.

Lazari, A., 2014. *European Critical Infrastructure Protection*. London: Springer.

Lewis, T.G., 2015. *Critical Infrastructure Protection in Homeland Security - Defending a Networked Nation*. New Jersey: Wiley.

Lowrance, W.W., 1980. The Nature of Risk. In R.C. Schwing & W.A. Albers Jr., eds. *Societal Risk Assessment: How Safe is Safe Enough?* New York: Springer Science + Business Media, LLC, pp.5-17.

MAI [Ministério da Administração Interna], 2007. *Portaria n.º 340-A/2007, de 30 de março - Áreas de Responsabilidade da GNR e PSP*. [Em linha] Disponível em: http://reformassi.mai-gov.info/legislacao/portaria-n-340-a2007/ [Acedido em 03 Mar. 2017].

MAI, 2012. *Decreto-Lei n.º 73/2012, de 26 de março - Extinção da CNPCE e Atribuição de Competências à ANPC*. [Em linha] Disponível em: https://dre.pt/application/file/553859 [Acedido em 02 Dez. 2016].

MAI, 2013a. *Lei n.º 34/2013, de 16 de maio - Estabelece o Regime do Exercício da Atividade de Segurança Privada*. [Em linha] Disponível em: https://dre.pt/application/dir/pdf1sdip/2013/05/09400/0292102942.pdf [Acedido em 12 Jan. 2017].

MAI, 2013b. *Decreto-Lei n.º 72/2013, de 31 de maio - Sistema Integrado de Operações de Proteção e Socorro*. [Em linha] Disponível em: https://dre.pt/application/dir/pdf1sdip/2013/05/10500/0319003199.pdf [Acedido 01 Mar. 2017].

MAI, 2013c. *Decreto-Lei n.º 73/2013, de 31 de maio - Aprova a Orgânica da ANPC*. [Em linha] Disponível em: http://www.segurancaonline.com/fotos/gca/decreto-lei_73_2013_leiorganica_anpc_1370260481.pdf [Acedido em 01 Mar. 2017].

MAI, 2014. *Decreto-Lei n.º 163/2014, de 31 de outubro - Lei Orgânica da ANPC*. [Em linha] Disponível em: https://dre.pt/application/file/a/58660558 [Acedido em 12 Fev. 2017].

Manunta, G., 1998. *Security: An Introduction*. Cranfield: Cranfield University.

MDN [Ministério da Defesa Nacional], 1991. *Decreto-Lei n.º 153/91, de 23 de abril - Sistema Nacional de Planeamento Civil de Emergência*. [Em linha] Disponível em: http://dre.pt/application/dir/pdf1s/1991/04/094A00/22832289.pdf [Acedido em 02 Dez. 2016].

MDN, 2011. *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*. [Em linha] Disponível em: http://www.fd.unl.pt/docentes_docs/ma/aens_MA_20261.pdf [Acedido em 02 Dez. 2016].

MDN, 2013. *Conceito Estratégico de Defesa Nacional*. Lisboa: Ministério da Defesa Nacional.

Mendes, C., 2017. *As Infraestruturas Críticas Nacionais*. [Entrevista] Lisboa (07 abril 2017).

MOPTC [Ministério das Obras Públicas, Transportes e Comunicações], 2006. *Decreto-Lei n.º 7/2006, de 4 de janeiro - Regulação do Transporte de Passageiros e Mercadorias na Cabotagem Nacional*. [Em linha] Disponível em: http://dgpj.mj.pt/DGPJ/sections/leis-da-justica/livro-viii-leis/pdf-viii-2/dl-7-2006/downloadFile/file/DL_7_2006.pdf?nocache=1182361931.02 [Acedido em 22 Mar. 2017].

MSB [Swedish Civil Contingencies Agency], 2014. *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure*. [Em linha] Disponível em: https://www.msb.se/RibData/Filer/pdf/27412.pdf [Acedido em 04 Abr. 2017].

Nakamura, E.T., Silva, J.A., Rios, J.M.M., Lemos, L.M., Tavares, R. & Ribeiro, S.L., 2011. *Redes de Telecomunicações Móveis para a Copa de 2014*. [Em linha] Disponível em: http://www.gsma.com/latinamerica/wp-content/uploads/2011/02/CPQD-Copa2014-Port.pdf [Acedido em 11 Fev. 2017].

ODASA [Office of the Deputy Assistant Secretary of the Army], 2016. *Emerging Science and Technology Trends: 2016-2045 - A Synthesis of Leading Forecasts*. Washington: Office of the Deputy Assistant Secretary of the Army (Research & Technology).

OECD [Organisation for Economic Co-operation and Development], 2008. *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. [Em linha] Disponível em: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf [Acedido em 12 Jan. 2017].

OECD, 2013. *National Treatment for Foreign-Controlled Entreprises*. Paris: Organization for Economic Co-Operation and Development.

OECD, 2014. *National Treatment for Foreign-Controlled Enterprises*. Paris: Organisation for Economic Co-Operation and Development.

OECD, 2017. *National Treatment for Foreign-Controlled Enterprises*. [Em linha] Disponível em: http://www.oecd.org/daf/inv/investment-policy/nationaltreatmentinstrument.htm [Acedido em 12 Jan. 2017].

Oliveira, M.R.B., 2015. *A Segurança das Infraestruturas Críticas em Portugal*. Dissertação em Direito e Segurança. Universidade Nova de Lisboa.

Pais, I., n.d. *Classificação de Infra-estruturas Críticas*. Lisboa: Presidência do Conselho de Ministros.

Pais, I., & Candeias, J., 2000. O Significado da Transposição para Portugal da Diretiva Europeia. Para Proteção das Infra-estruturas Críticas. *Revista Planeamento Civil de Emergência*, 22, pp.20-22.

Pais, I., Sá, F.M. & Gomes, H., 2007. Proteção de Infraestruturas Críticas - A Cooperação Público-Privada. In C.G. Soares, A.P. Teixeira & P. Antão, eds. *Riscos, Públicos e Industriais*. Lisboa: IST Press, pp.65-83.

PCM [Presidência do Conselho de Ministros], 2007. *Resolução do Conselho de Ministros n.º 44/2007, de 19 de março - Aprova as Opções Fundamentais da Reforma da Guarda Nacional Republicana e da Polícia de Segurança Pública*. [Em linha] Disponível em: https://dre.pt/application/file/518675 [Acedido em 02 Mar. 2017].

PCM, 2014. *Decreto-Lei n.º 3/2012, de 16 de janeiro (2.ª alteração a coberto do Decreto-Lei n.º 69/2014, de 9 de maio) - Orgânica do Gabinete Nacional de Segurança - Criação do Centro Nacional de Cibersegurança*. [Em linha] Disponível em: https://dre.pt/application/file/a/25343853 [Acedido em 01 Mar. 2017].

Peräkylä, A., 2005. Analyzing Talk and Text. In N.K. Denzin & Y.S. Lincoln, eds. *The Sage Handbook of Qualitative Research*. 3rd ed. Thousand Oaks: Sage Publications, pp.869-886.

Pfeffer, J. & Salancik, G.R., 1978. *The External Control of Organizations*. [Em linha] Disponível em: http://web.unitn.it/files/download/12425/the_external_control_of_organizations_ch3_pfeffer.pdf [Acedido em 08 Dez. 2016].

POA, 2003. *Asset Protection and Security Management Handbook*. London: Auerbach.

Reason, J., 1990. *Human Error*. Cambridge: Cambridge University Press.

Renn, O., 2008. *Risk Governance: Coping With Uncertainty in a Complex World*. London: Earthscan.

Reveron, D.S., 2012. An Introduction to National Security and Cyberspace. In D.S. Reveron, ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington: Georgetown University Press. pp.3-19.

Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.K., 2001. *Critical Infrastructure Interdependencies*. [Em linha] Disponível em: http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf [Acedido em 10 Fev. 2017].

Rodrigues, N., 2008. *A Protecção e Segurança das Infra-estruturas Críticas*. Lisboa: ISCPSI.

Romesburg, C., 2004. *Cluster Analysis for Researchers*. Wadsworth: Lulu Press.

Sá, F.M., 2005. *Ranking Critical Infrastructures - The Portuguese Methodology*. Lisboa: Presidência do Conselho de Ministros ed. CNPCE.

Schneider, T., 2014. Responsability for Private Sector Adaptation to Climate Change. *Ecology and Society*, 19(2), p.8.

SIRP [Sistema de Informações da República Portuguesa], 2014. *Lei n.º 9/2007, de 19 de maio (1.ª alteração a coberto da Lei n.º 50/2014, de 13 de agosto) - Lei que Estabelece a Orgânica do SGSIRP, SIED e SIS*. [Em linha] Disponível em: https://www.sis.pt/legislacao [Acedido em 02 Mar. 2017].

SIS [Serviço de Informações de Segurança], n.d. *Programa Krítica*. [Em linha] Disponível em https://www.sis.pt/pagina/71/programa-kritica [Acedido em 02 Mar. 2017].

Slovic, P. & Weber, E.U., 2002. *Perception of Risk Posed by Extreme Events*. [Em linha] Disponível em: https://pdfs.semanticscholar.org/ef56/87859fc1b5d8c85997e4c142ad8a1c345451.pdf [Acedido em 16 Mar. 2017]

Swetz, F., 1992. Quando e como Podemos usar Modelação? *Educação Matemática*, pp.45-48.

UK Government, 2010. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. [Em linha] Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf [Acedido em 10 Fev. 2017].

UKMD [UK Ministry of Defence], 2010. *Strategic Trends Programme: Global Strategic Trends - Out to 2040*. 4th ed. London: UK Ministry of Defence.

União Europeia, 2008. *Diretiva do Conselho 2008/114/CE - Identificação e Designação das Infraestruturas Críticas Europeias e a Avaliação da Necessidade de Melhorar a sua Proteção*. [Em linha] Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114&from=PT [Acedido em 01 Dez. 2016].

URI [University of Rhode Island], 2012. *The Future of Information Technology and Implications for URI*. [Em linha] Disponível em: https://www.uri.edu/provost/files/The_Future_of_Information_Technology.pdf [Acedido em 16 Mar. 2017].

USATDC [US Army Training & Doctrine Command], 2006. *Critical Infrastructure Threats and Terrorism*. [Em linha] Disponível em: http://www.fas.org/irp/threat/terrorism [Acedido em 15 Abr. 2017].

USDoD [US Department of Defense], 2017. *DOD Dictionary of Military and Associated Terms*. [Em linha] Disponível em: http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf [Acedido em 31 Mai. 2017].

USDoHS [US Department of Homeland Security], 2006. *National Infrastructure Protection Plan*. US Department of Homeland Security.

USDoHS, 2007. *The National Strategy for Homeland Security*. [Em linha] Disponível em: https://www.dhs.gov/national-strategy-homeland-security-october-2007 [Acedido em 10 Fev. 2017].

USNIC [US National Intelligence Council], 2012. *Global Trends 2030: Alternative Worlds*. Washington: US National Intelligence Council.

Valente, M.M.G., 2013. *A Segurança (Interna) na Constituição da República Portuguesa de 1976*. [Em linha] Disponível em: http://www.iscpsi.pt/Inicio/Documents/desafiosSeguranca/Manuel%20Monteiro%20Guedes%20Valente.pdf. [Acedido em 01 Mar. 2017].

Yin, R.K. (1994), *Case Study Research: Design and Methods*. 2nd ed. Thousand Oaks: SAGE Publications.

Zimmerman, R., 2005. Social Implications of Infrastructure Network Interactions. In O. Coutard, R.E. Hanley & R. Zimmerman, eds. *Sustaining Urban Networks - The Social Diffusion of Large Technical Systems*. London: Routledge.

Anexo A – Diretiva n.º 2008/114/CE, de 8 de dezembro (Procedimento de identificação e designação das ICE e a avaliação da necessidade de melhorar a sua proteção)

Diretiva n.º 2008/114/CE, de 8 de dezembro

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia, nomeadamente o artigo 308.º,

Tendo em conta a proposta da Comissão,

Tendo em conta o parecer do Parlamento Europeu (1), Tendo em conta o parecer do Banco Central Europeu (2), Considerando o seguinte:

(1) Em Junho de 2004, o Conselho Europeu solicitou a elaboração de uma estratégia global de proteção das infraestruturas críticas. Em resposta a esse pedido, a Comissão adoptou, em 20 de Outubro de 2004, uma comunicação relativa à proteção das infraestruturas críticas no âmbito da luta contra o terrorismo, que apresenta sugestões sobre como reforçar a prevenção, o estado de preparação e a capacidade de resposta da Europa a atentados terroristas que envolvam infraestruturas críticas.

(2) Em 17 de Novembro de 2005, a Comissão adoptou um livro verde sobre um Programa Europeu de Proteção das Infraestruturas Críticas, com opções políticas relativas à elaboração deste programa e da Rede de Alerta para as Infraestruturas Críticas. As reações ao livro verde puseram em evidência o valor acrescentado de um enquadramento comunitário em matéria de proteção das infraestruturas críticas. Foi reconhecida a necessidade de aumentar a capacidade de proteção das infraestruturas críticas na Europa e de contribuir para diminuir a sua vulnerabilidade. Foi também sublinhada a importância de que se revestem os princípios fundamentais da subsidiariedade, da proporcionalidade e da complementaridade e o diálogo entre as partes interessadas.

(3) Em Dezembro de 2005, o Conselho (Justiça e Assuntos Internos) solicitou à Comissão que apresentasse uma proposta de Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC) e decidiu que este deveria assentar na abordagem de todos os riscos, com destaque para a luta contra as ameaças de terrorismo. Esta abordagem deveria atender às ameaças humanas e tecnológicas e às catástrofes naturais no processo de proteção das infraestruturas críticas, embora devesse privilegiar as ameaças de terrorismo.

(4) Em Abril de 2007, o Conselho aprovou conclusões sobre o PEPIC, em que reafirmava que cabe, em última instância, aos Estados-Membros assegurar a proteção das infraestruturas críticas nos respectivos territórios e se congratulava com os esforços desenvolvidos pela Comissão para desenvolver um procedimento europeu de identificação e designação de Infraestruturas Críticas Europeias (ICE) e avaliação da necessidade de melhorar a sua proteção.

(5) A presente diretiva constitui a primeira etapa de uma abordagem faseada para identificar e designar as ICE e avaliar a necessidade de melhorar a sua proteção. Concentra-se, enquanto tal, nos sectores da energia e dos transportes, e deverá ser revista com o objectivo de avaliar o seu impacto e a necessidade de incluir no seu âmbito de aplicação outros sectores, designadamente o das Tecnologias da Informação e Comunicação (TIC).

(6) A responsabilidade pela proteção das ICE cabe, em primeira e última instância, aos Estados-Membros e aos proprietários/operadores dessas infraestruturas.

(7) Existem na Comunidade diversas infraestruturas críticas cuja perturbação ou destruição teria um impacto transfronteiras significativo. Poderá tratar-se de efeitos intersectoriais transfronteiriços resultantes de interdependências entre infraestruturas interligadas. Essas ICE deverão ser identificadas e designadas por intermédio de um procedimento comum. A avaliação dos requisitos de segurança dessas infraestruturas deverá obedecer a orientações comuns mínimas. Os regimes bilaterais de cooperação entre os Estados-Membros no domínio da proteção das infraestruturas críticas constituem um meio já consagrado e eficaz de tratar das infraestruturas críticas transfronteiriças. O PEPIC deverá assentar nessa cooperação. As informações respeitantes à designação de uma infraestrutura como ICE deverão ser classificadas ao nível adequado, em conformidade com a legislação comunitária e nacional em vigor.

(8) Uma vez que vários sectores se caracterizam por experiências, competências e requisitos específicos em relação à proteção das infraestruturas críticas, deverá ser elaborada e aplicada neste domínio uma abordagem comunitária que atenda às especificidades sectoriais e às medidas já adoptadas nos diversos sectores, nomeadamente a nível comunitário, nacional ou regional, e, se for caso disso, a acordos de assistência mútua transfronteiras que tenham já sido celebrados entre os proprietários/operadores de infraestruturas críticas. Dada a participação muito significativa do sector privado no controlo e gestão dos riscos, nos planos de continuidade da exploração e na recuperação

pós-catástrofes, a abordagem comunitária deverá incentivar o pleno envolvimento deste sector.

(9) No que respeita ao sector da energia e, em particular, aos métodos de produção e transporte de eletricidade (em termos de abastecimento), entende-se que, se assim se considerar adequado, a produção de eletricidade poderá incluir elementos das centrais nucleares que sirvam para o transporte de eletricidade, excluindo contudo os elementos especificamente nucleares abrangidos pela legislação aplicável neste domínio, designadamente os tratados e o direito comunitário.

(10) A presente diretiva complementa as medidas sectoriais já adoptadas a nível comunitário e dos Estados-Membros. Quando já existam mecanismos comunitários, esses mecanismos deverão continuar a ser utilizados, contribuindo assim para a aplicação global da presente diretiva. Haverá que evitar duplicações ou contradições entre os diferentes atos e disposições.

(11) Todas as ICE designadas deverão dispor de Planos de Segurança dos Operadores (PSO) ou de medidas equivalentes que permitam identificar os elementos importantes, avaliar os riscos e definir, selecionar e conferir prioridade às contramedidas e procedimentos que se imponham. A fim de evitar duplicações desnecessárias, cada Estado-Membro deverá começar por verificar se os proprietários/operadores das ICE designadas dispõem de PSO adequados ou se adoptaram medidas equivalentes. Caso esses planos não existam, cada Estado-Membro deverá efectuar as diligências necessárias para garantir que sejam tomadas medidas adequadas. Competirá a cada Estado-Membro decidir do modo mais apropriado de assegurar a elaboração de PSO.

(12) As medidas, princípios ou orientações, incluindo medidas tomadas à escala comunitária, e os regimes de cooperação bilateral e/ou multilateral que prevejam a necessidade de dispor de um plano semelhante ou equivalente a um PSO, ou que prevejam a existência de um agente de ligação de segurança ou equivalente, deverão preencher os requisitos da presente diretiva no que respeita ao PSO ou ao agente de ligação de segurança, respectivamente.

(13) Deverão ser identificados, em todas as ICE designadas, agentes de ligação de segurança cuja função consistirá em facilitar a cooperação e a comunicação com as autoridades nacionais competentes em matéria de proteção das infraestruturas críticas. A fim de evitar duplicações desnecessárias, cada Estado-Membro deverá começar por verificar se os proprietários/operadores das ICE designadas dispõem já de um agente de ligação de segurança ou equivalente. Caso não exista agente de ligação de segurança, cada Estado-Membro deverá efectuar as diligências necessárias para garantir que sejam tomadas medidas adequadas nesse sentido. Competirá a cada Estado-Membro decidir do modo mais apropriado de assegurar a designação de agentes de ligação de segurança.

(14) A identificação eficaz dos riscos, ameaças e vulnerabilidades nos vários sectores exige que se estabeleçam formas de comunicação entre os proprietários/operadores de ICE e os Estados-Membros e entre estes últimos e a Comissão. Cada Estado-Membro deverá recolher informações sobre as ICE situadas no seu território. A Comissão deverá receber informações gerais sobre os riscos, ameaças e vulnerabilidades existentes nos sectores em que tenha sido identificada uma ICE, incluindo, se for caso disso, informações pertinentes sobre possíveis melhorias a introduzir nas ICE e dependências intersectoriais que possam servir de base à elaboração de propostas específicas da Comissão sobre a melhoria da proteção das ICE.

(15) Para facilitar a melhoria da proteção das ICE, poderão ser desenvolvidas metodologias comuns de identificação e classificação dos riscos, ameaças existentes no que respeita aos componentes das infraestruturas.

(16) Os proprietários/operadores de ICE deverão ter acesso às melhores práticas e metodologias em matéria de proteção das infraestruturas críticas, principalmente através das autoridades competentes dos Estados-Membros.

(17) A proteção eficaz das ICE requer comunicação, coordenação e cooperação a nível nacional e comunitário. O melhor meio para o conseguir é a nomeação de pontos de contacto para a proteção das infraestruturas críticas europeias («pontos de contacto PICE») em cada Estado-Membro, que deverão coordenar as questões relativas à proteção das infraestruturas críticas europeias quer a nível interno, quer com outros Estados-Membros e a Comissão.

(18) Para desenvolver atividades de proteção das ICE em domínios que requerem um certo grau de confidencialidade, convém assegurar um intercâmbio de informações coerente e seguro no quadro da presente diretiva. Importa que as regras de confidencialidade previstas na legislação nacional aplicável ou no Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (1) sejam observadas no que diz respeito a factos específicos, referentes a um componente de uma infraestrutura crítica, suscetíveis de serem utilizados para planear e agir com o objectivo de provocar efeitos inaceitáveis nas instalações de infraestruturas críticas. A informação classificada deverá ser protegida em conformidade

com a legislação comunitária e nacional aplicável. Os Estados-Membros e a Comissão deverão respeitar a classificação de segurança atribuída pela entidade de origem do documento.

(19) O intercâmbio de informações sobre ICE deverá decorrer num clima de confiança e segurança. A partilha de informações requer que entre as empresas e organizações se estabeleça numa relação de confiança em que os seus dados sensíveis e confidenciais deverão ser devidamente protegidos.

(20) Atendendo a que os objectivos da presente diretiva, a saber, a criação de um procedimento de identificação e designação das ICE e a concepção de uma abordagem comum relativamente à avaliação da necessidade de melhorar a proteção de tais infraestruturas, não podem ser suficientemente realizados pelos Estados-Membros, e podem, pois, devido à dimensão da ação prevista, ser melhor alcançados ao nível comunitário, a Comunidade pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5º do Tratado. Em conformidade com o princípio da proporcionalidade, consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir aqueles objectivos.

(21) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos, nomeadamente, na Carta dos Direitos Fundamentais da União Europeia,

Artigo 1.º

Objecto

A presente diretiva estabelece um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, de modo a contribuir para a proteção das pessoas.

Artigo 2.º

Definições

Para efeitos da presente diretiva, entende-se por:

a) «Infraestrutura crítica», o elemento, sistema ou parte deste situado nos Estados-Membros 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 ou destruição teria um impacto significativo num Estado-Membro, dada a impossibilidade de continuar a assegurar essas funções;

b) «Infraestrutura Crítica Europeia» ou «ICE», a infraestrutura crítica situada nos Estados-Membros cuja perturbação ou destruição teria um impacto significativo em pelo menos dois Estados-Membros. O significado do impacto deve ser avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas;

c) «Análise de risco», a ponderação dos cenários de ameaça relevantes, a fim de avaliar a vulnerabilidade e o potencial impacto da perturbação ou destruição de uma infraestrutura crítica;

d) «Informações sensíveis relacionadas com a proteção das infraestruturas críticas», os factos respeitantes a uma infraestrutura crítica que, se divulgados, poderiam ser utilizados para planear e agir com o objectivo de provocar a perturbação ou destruição das instalações de infraestruturas críticas;

e) «Proteção», todas as atividades destinadas a assegurar a funcionalidade, continuidade e integridade de uma infraestrutura crítica tendo em vista coarctar, atenuar e neutralizar uma ameaça, risco ou vulnerabilidade;

f) «Proprietários/operadores de uma ICE», as entidades responsáveis pelos investimentos num determinado elemento, sis- tema ou parte deste designado como ICE e/ou pelo respetivo funcionamento corrente nos termos da presente diretiva.

Artigo 3.º

Identificação das ICE

1. Nos termos do procedimento previsto no anexo III, cada Estado-Membro identifica as potenciais ICE que preencham simultaneamente critérios transversais e sectoriais e correspondam às definições consagradas nas alíneas a) e b) do artigo 2º.

A Comissão pode, a pedido dos Estados-Membros, ajudá-los a identificar as potenciais ICE.

A Comissão pode chamar a atenção dos Estados-Membros relevantes para a existência de potenciais ICE que se possa considerar satisfazerem os requisitos aplicáveis à designação de ICE.

Cada Estado-Membro e a Comissão prosseguem de forma permanente o processo de identificação de potenciais ICE.

2. Os critérios transversais a que se refere o n.º 1 incluem:

a) A ocorrência de acidentes (avaliada em termos de número potencial de feridos ou vítimas mortais);

b) O impacto económico (avaliado em termos de importância dos prejuízos económicos e/ou degradação de produtos ou serviços; incluindo também os potenciais efeitos ambientais);

c) Efeitos no domínio público (avaliados em termos de impacto na confiança das populações, sofrimento físico e perturbação da vida quotidiana, incluindo a perda de serviços essenciais).

Os limiares aplicáveis aos critérios transversais baseiam-se na gravidade do impacto causado pela perturbação ou destruição de uma dada infraestrutura. Os limiares aplicáveis aos critérios transversais são determinados caso a caso com exatidão pelos Estados-Membros aos quais uma determinada infraestrutura crítica diga respeito.

Cada Estado-Membro informa anualmente a Comissão do número de infraestruturas que, em cada sector, tenham suscitado debates sobre os limiares aplicáveis aos critérios transversais.
Os critérios sectoriais têm em conta as características dos diferentes sectores em que existam ICE.
A Comissão, juntamente com os Estados-Membros, elabora diretrizes para a aplicação dos critérios transversais e sectoriais e dos limiares aproximados a utilizar na identificação das ICE. Esses critérios constituem informação classificada. A utilização dessas orientações é facultativa para os Estados-Membros.
3. Os sectores que servem de base à execução da presente diretiva são os da energia e dos transportes. No anexo I enumeram-se os subsectores respectivos. Se se considerar oportuno, podem ser identificados, em simultâneo com a revisão da presente diretiva prevista no artigo 11.º, outros sectores para efeitos de execução da presente diretiva. Deve ser dada prioridade ao sector das Tecnologias da Informação e Comunicação (TIC).

Artigo 4.º
Designação das ICE

1. Cada Estado-Membro informa os demais Estados-Membros suscetíveis de serem afectados de forma significativa por uma potencial ICE acerca da sua identidade e das razões que presidem à sua designação como potencial ICE.
2. Cada Estado-Membro em cujo território esteja situada uma potencial ICE procede a debates bilaterais e/ou multilaterais com os outros Estados-Membros suscetíveis de serem afectados de forma significativa por essa infraestrutura. A Comissão pode participar nesses debates mas não tem acesso a informações pormenorizadas que permitam a identificação inequívoca da infraestrutura em concreto.
Um Estado-Membro que tenha motivos para crer que pode ser afectado de forma significativa por uma potencial ICE não identificada como tal pelo Estado-Membro em cujo território esteja situada pode informar a Comissão de que deseja encetar debates bilaterais e/ou multilaterais sobre a questão. A Comissão deve comunicar imediatamente essa pretensão ao Estado-Membro em cujo território esteja situada a potencial ICE e esforçar-se por facilitar a obtenção de acordo entre as partes.
3. O Estado-Membro em cujo território esteja situada uma potencial ICE deve designá-la enquanto ICE após a obtenção de um acordo entre esse Estado-Membro e os Estados-Membros que possam ser afectados de forma significativa.
O Estado-Membro em cujo território se situe a infraestrutura a designar como ICE deve dar o seu consentimento.
4. O Estado-Membro em cujo território se encontre situada uma ICE informa anualmente a Comissão do número de ICE designadas em cada sector e do número de Estados-Membros dependentes de cada ICE designada. A identidade de uma ICE deve apenas ser conhecida dos Estados-Membros que possam ser por ela afectados de forma significativa.
5. Os Estados-Membros em cujo território esteja situada a ICE informam o proprietário/operador da infraestrutura da sua designação como ICE. As informações respeitantes à designação de uma infraestrutura como ICE são classificadas ao nível adequado.
6. O processo de identificação e designação das ICE nos termos do artigo 3º e do presente artigo deve ser concluído até 12 de Janeiro de 2011 e revisto periodicamente.

Artigo 5.º
Planos de segurança dos operadores

1. O procedimento aplicável aos Planos de Segurança dos Operadores (PSO) deve identificar os elementos da ICE e as soluções de segurança que existam ou estejam a ser executadas para a sua proteção. No anexo II identifica-se o conteúdo mínimo que o procedimento aplicável ao PSO de uma ICE deve contemplar.
2. Cada Estado-Membro avalia se cada ICE designada situada no seu território dispõe de um PSO ou se foram adoptadas medidas equivalentes que contemplem as questões referidas no anexo II. Caso um Estado-Membro conclua pela existência de um PSO ou equivalente regularmente atualizado, não é necessário adoptar outras medidas de execução.
3. Caso conclua que não foi elaborado nenhum PSO ou equivalente, o Estado-Membro deve garantir, através das medidas que considere adequadas, que é elaborado um PSO ou equivalente que contemple as questões referidas no anexo II.
Cada Estado-Membro garante a execução e a revisão periódica dos PSO, ou de planos equivalentes, no prazo de um ano após a designação da infraestrutura crítica como ICE. Esse prazo pode ser prorrogado em circunstâncias excepcionais, mediante acordo com a autoridade competente do Estado-Membro e notificação da Comissão.
4. O presente artigo não prejudica as disposições existentes em matéria de supervisão ou controlo de uma ICE, desempenhando a autoridade competente do Estado-Membro a que se refere o presente artigo as funções de supervisor ao abrigo dessas disposições.
5. Considera-se que a observância das medidas, incluindo das que tenham sido adoptadas à escala comunitária, que, num determinado sector, requeiram ou prevejam a necessidade de se dispor de um plano similar ou equivalente a um PSO e respectivo controlo por parte da autoridade competente, satisfaz todos os requisitos impostos aos Estados-Membros pelo presente artigo ou adoptados ao abrigo do mesmo. As orientações de

execução a que se refere o n.º 2 do artigo 3.º devem incluir uma lista indicativa das medidas em causa.

Artigo 6.º

Agentes de ligação de segurança

1. O agente de ligação de segurança desempenha a função de ponto de contacto para questões de segurança entre o proprietário/operador da ICE e a autoridade competente do Estado-Membro.
2. Cabe a cada Estado-Membro certificar-se de que cada ICE designada que se situe no seu território dispõe de um agente de ligação de segurança ou equivalente. Se um Estado-Membro concluir pela existência de um agente de ligação de segurança ou equivalente, não é necessário adoptar outras medidas de execução.
3. Caso conclua que uma dada ICE designada não dispõe de agente de ligação de segurança ou equivalente, o Estado-Membro assegura, através das medidas que considere adequadas, a designação de um agente de ligação de segurança ou equivalente.
4. Cada Estado-Membro deve pôr em prática um mecanismo de comunicação adequado entre a autoridade competente do Estado-Membro e o agente de ligação de segurança ou equivalente, com o objectivo de trocar informações pertinentes relativas aos riscos e ameaças identificados em relação à ICE em causa. Esse mecanismo de comunicação não prejudica os requisitos nacionais em matéria de acesso a informação sensível e classificada.
5. Considera-se que a observância das medidas, incluindo das que tenham sido adoptadas à escala comunitária, que, num determinado sector, requeiram ou prevejam a necessidade de se dispor de um agente de ligação de segurança ou equivalente, satisfaz todos os requisitos impostos aos Estados-Membros pelo presente artigo ou adoptados ao abrigo do mesmo. As orientações de execução a que se refere o n.º 2 do artigo 3.º devem incluir uma lista indicativa das medidas em causa.

Artigo 7.º

Relatórios

1. Cada Estado-Membro procede a uma avaliação das ameaças em relação aos subsetores das ICE, no prazo de um ano a contar da designação da infraestrutura crítica situada no seu território como ICE dentro desses subsectores.
2. Cada Estado-Membro transmite, de dois em dois anos, à Comissão um resumo dos dados gerais sobre os tipos de riscos, ameaças e vulnerabilidades com que se depara cada um dos sectores das ICE identificadas como tal nos termos do o artigo 4. e que se situem no seu território.
A Comissão pode elaborar um modelo comum desses relatórios, em colaboração com os Estados-Membros.
Cada relatório é classificado a um nível adequado, se o Estado-Membro que o transmitiu o considerar necessário.
3. Com base nos relatórios referidos no n.º 2, a Comissão e os Estados-Membros devem avaliar, sector a sector, a adoção de medidas de proteção adicionais ao nível comunitário aplicáveis às ICE. Este processo é realizado em simultâneo com a revisão da presente diretiva prevista no artigo 11.º.
4. A Comissão, em colaboração com os Estados-Membros, pode elaborar orientações metodológicas comuns aplicáveis à realização de análises de risco relativas às ICE. A utilização dessas orientações é facultativa para os Estados-Membros.

Artigo 8.º

Apoio da Comissão às ICE

A Comissão deve apoiar, através da autoridade competente do Estado-Membro, os proprietários/operadores das ICE designadas, facultando-lhes o acesso às melhores práticas e metodologias disponíveis, bem como ações de formação e informações sobre os novos avanços técnicos relacionados com a proteção das infraestruturas críticas.

Artigo 9.º

Informações sensíveis relacionadas com a proteção das infraestruturas críticas europeias

1. Qualquer pessoa que, por força da presente diretiva, trate informação confidencial em nome de um Estado-Membro ou da Comissão é sujeita a um procedimento de habilitação de segurança adequado. Os Estados-Membros, a Comissão e os organismos de supervisão competentes asseguram que as informações sensíveis relacionadas com a proteção das infraestruturas críticas europeias, e que sejam transmitidas aos Estados-Membros ou à Comissão, não sejam utilizadas para fins distintos dos da proteção das infraestruturas críticas.
2. O disposto no presente artigo aplica-se igualmente às informações não escritas trocadas durante reuniões em que sejam debatidos assuntos sensíveis.

Artigo 10.º

Pontos de contacto para a proteção das infraestruturas críticas europeias

1. Cada Estado-Membro deve nomear um ponto de contacto para a proteção das infraestruturas críticas europeias («ponto de contacto PICE»).
2. O ponto de contacto PICE coordena as matérias relativas à proteção das infraestruturas críticas europeias a nível do Estado-Membro, bem como com outros Estados-Membros e a Comissão. A nomeação de um ponto de contacto PICE não impede a participação de outras autoridades de um Estado-Membro em assuntos relacionados com a proteção das infraestruturas críticas europeias.

Artigo 11.º

Revisão

A revisão da presente diretiva deve iniciar-se em 12 de Janeiro de 2012.

Artigo 12.º

Execução

Os Estados-Membros tomam as medidas necessárias para dar cumprimento à presente diretiva até 12 de janeiro de 2011 e informam imediatamente a Comissão desse facto.

Quando os Estados-Membros tomarem essas medidas, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. As modalidades dessa referência são aprovadas pelos Estados-Membros.

Artigo 13.º

Entrada em vigor

A presente diretiva entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.

Artigo 14.º

Destinatários

Os Estados-Membros são os destinatários da presente diretiva.

Feito em Bruxelas, em 8 de Dezembro de 2008.
Pelo Conselho O Presidente B. KOUCHNER

Anexo B – Decreto-Lei n.º 62/2011, de 9 de maio (Procedimentos de identificação e de proteção de IC)

Decreto-Lei n.º 62/2011, de 9 de Maio

O presente decreto-lei estabelece 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 sectores da energia e transportes, transpondo a Diretiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro.

Com o presente decreto-lei, estabelecem-se procedimentos para a identificação das diversas infraestruturas com funções essenciais para a sociedade, cuja perturbação ou destruição teria um impacto significativo, porque implicaria que essa infraestrutura deixasse de poder assegurar essas funções.

Assim, com o regime agora criado, Portugal adquire uma maior capacidade de intervenção ao nível da segurança e resiliência das infraestruturas que venham a ser sectorialmente consideradas críticas, no âmbito europeu, integrando o futuro Programa Europeu de Proteção de Infraestruturas Críticas (PEPIC) suportado numa abordagem transversal dos riscos a que essas infraestruturas possam estar expostas.

A proteção efetiva das infraestruturas críticas europeias (ICE) requer comunicação, coordenação e cooperação, aos níveis nacional e comunitário, processos mais adequadamente prosseguidos através da existência e intervenção efetiva, em cada país, de pontos de contacto para a proteção de infraestruturas críticas europeias («pontos de contacto PICE»). Os regimes bilaterais de cooperação entre os Estados membros da União Europeia neste domínio constituem um meio já consagrado de tratar as infraestruturas críticas transfronteiriças, devendo o PEPIC assentar nesta cooperação, bem como numa participação significativa do sector privado, dada a sua presença significativa na exploração das ICE.

Assim:

Nos termos da alínea a) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

Artigo 1.º

Objecto

O presente decreto-lei estabelece 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 sectores da energia e transportes, transpondo a Diretiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro.

Artigo 2.º

Infraestruturas críticas

Para efeitos do presente decreto-lei, entende-se por:

a) «Infraestrutura crítica» a componente, sistema ou parte deste situado em território nacional 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 ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções;

b) «Infraestrutura crítica europeia» ou «ICE» a infraestrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da União Europeia, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersetoriais em relação a outros tipos de infraestruturas.

Artigo 3.º

Âmbito

1- Os procedimentos de identificação e de designação de ICE previstos no presente decreto-lei aplicam-se ao sector da energia, designadamente:

a) Infraestruturas e instalações de produção e de transporte de eletricidade;

b) Infraestruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos; e

c) Infraestruturas de produção, refinação, tratamento, armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido (GNL).

2- Os procedimentos de identificação e de designação de ICE previstos no presente decreto-lei aplicam-se ainda ao sector dos transportes, designadamente:

a) Transportes rodoviários;

b) Transportes ferroviários;

c) Transportes aéreos;

d) Transportes por vias navegáveis interiores;

e) Transportes marítimos, incluindo de curta distância, e portos.

Artigo 4.º

Identificação das ICE

1- Nos termos do procedimento previsto nos números seguintes, compete ao Conselho Nacional de Planeamento Civil de Emergência (CNPCE) a identificação das potenciais ICE que preencham simultaneamente critérios transversais e sectoriais e que correspondam às definições previstas nas alíneas a) e b) do artigo 2.º

2- O processo de identificação de potenciais ICE é permanente e conduzido pelo CNPCE.

3- Os critérios transversais a que se refere o n.º 1 incluem:

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

b) O impacto económico estimado, avaliado em termos de importância dos prejuízos económicos e da degradação de produtos ou serviços, incluindo também os potenciais efeitos ambientais;

c) Os efeitos previsíveis no domínio público, avaliados em termos de impacto na confiança das populações, sofri- mento físico e perturbação da vida quotidiana, incluindo a perda de serviços essenciais.

4- Os critérios transversais são avaliados com base na gravidade do impacto causado pela perturbação ou destruição de uma dada infraestrutura, sendo os limiares de avaliação desses critérios determinados, caso a caso, pelo CNPCE.

5- O CNPCE informa anualmente a Comissão Europeia do número de infraestruturas que, em cada sector, tenham suscitado discussão sobre os limiares de avaliação dos critérios transversais.

6- Os critérios sectoriais devem considerar as características específicas dos diferentes sectores em que existam ICE.

Artigo 5.º

Procedimento de identificação das ICE

1- A identificação das potenciais ICE processa-se através da aplicação de um procedimento composto por quatro fases.

2- Na primeira fase do procedimento de identificação das potenciais ICE, são aplicados os critérios sectoriais, para efectuar uma primeira seleção das infraestruturas críticas dentro de determinado sector.

3- Na segunda fase do procedimento de identificação, após a seleção referida no número anterior, é aplicada a definição de infraestrutura crítica constante da alínea a) do artigo 2.º às potenciais ICE, sendo a importância do impacto significativo determinada pela utilização de métodos nacionais de identificação das infraestruturas críticas e pelo recurso a critérios transversais.

4- Na terceira fase do procedimento de identificação, é aplicado o elemento transfronteiriço constante da definição de ICE, nos termos da alínea b) do artigo 2.º, às potenciais ICE que tenham concluído as duas primeiras fases do procedimento.

5- Na quarta fase do procedimento de identificação, são aplicados os critérios transversais referidos no artigo anterior às potenciais ICE que não tenham sido identificadas nos termos dos números anteriores.

6- Sempre que estejam em causa infraestruturas que forneçam um serviço essencial, são tidas em conta as alternativas disponíveis no fornecimento desse serviço e a duração da perturbação e de recuperação da infraestrutura em causa.

7- As potenciais ICE que não preencham os requisitos de qualquer uma das fases do procedimento previsto no presente artigo não são consideradas ICE para os efeitos do presente decreto-lei.

Artigo 6.º

Designação das ICE

1- O CNPCE informa os Estados membros da União Europeia:

a) De quais as ICE identificadas nos termos dos artigos 4.º e 5.º que sejam suscetíveis de afectar esse Estados de forma significativa;

b) Das razões que presidem à sua designação como ICE.

2- As potenciais ICE devem ser designadas como tal pelo CNPCE, após obtenção de acordo com as entidades responsáveis dos Estados membros da União Europeia que por ela possam ser afectados de forma significativa.

Artigo 7.º

Classificação da informação

1- A identidade de uma ICE deve apenas ser conhecida dos Estados membros da União Europeia que possam ser por ela afectados de forma significativa.

2- As informações respeitantes à designação de uma infraestrutura como ICE são objecto de classificação de segurança adequada.

Artigo 8.º

Informação da designação de uma ICE

1- O CNPCE informa anualmente a Comissão Europeia do número de ICE designadas em cada sector e do número de Estados membros da União Europeia dependentes de cada ICE designada.

2- O CNPCE informa o proprietário ou operador da infraestrutura da sua designação como ICE.

Artigo 9.º

ICE não identificadas

As entidades competentes, caso considerem existir motivos para crer que o Estado Português pode ser afectado de forma significativa por uma potencial ICE não identificada como tal por outro Estado membro em cujo território esteja situada, podem desencadear o processo de comunicação à Comissão Europeia, para que se iniciem debates bilaterais ou multilaterais sobre a identificação e designação dessa infraestrutura como ICE.

Artigo 10.º

Planos de segurança dos operadores

1- Cada ICE dispõe de um plano de segurança da responsabilidade do seu operador, aprovado até um ano após a designação da infraestrutura crítica como ICE e revisto anualmente.

2- O plano de segurança referido no número anterior identifica os elementos da ICE e as soluções de segurança a executar para a sua proteção, incluindo:

a) A identificação dos elementos importantes;

b) Uma análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada elemento e nos impactos potenciais;

c) A identificação, seleção e prioridade de contramedidas e procedimentos de segurança permanentes; e

d) A identificação, seleção e prioridade de contramedidas e procedimentos de segurança progressivos a ativar consoante o grau de ameaça aplicável à ICE ou o estado de segurança decretado.

3- As contramedidas e procedimentos de segurança permanentes previstos na alínea c) do número anterior incluem:

a) A instalação de meios de deteção, controlo do acesso, proteção e prevenção;

b) Procedimentos de alerta e gestão de crises;

c) Medidas de controlo e verificação;

d) Comunicação, sensibilização e formação;

e) A segurança dos sistemas de informação; e

f) Medidas de minimização dos danos e impactos e de reposição da normalidade.

4- O plano de segurança de cada ICE é elaborado e revisto anualmente pelos operadores e submetido a parecer prévio da forca de segurança territorialmente competente e da Autoridade Nacional de Proteção Civil, com vista à sua validação pelo Secretário-Geral do Sistema de Segurança Interna.

5- O plano de segurança dos operadores é articulado com o plano de segurança e proteção exterior da ICE, da responsabilidade da força de segurança territorialmente competente e da proteção civil.

Artigo 11.º

Agentes de ligação de segurança

1- Cada ICE dispõe de um agente de ligação de segurança, designado pelo operador, que desempenha a função de ponto de contacto para questões de segurança entre o proprietário da ICE e o Secretário-Geral do Sistema de Segurança Interna, que se faz representar pela força de segurança territorialmente competente.

2- Compete às entidades referidas no número anterior trocar as informações pertinentes relativas aos riscos e ameaças identificados em relação à ICE em causa, sem prejuízo do regime do segredo de Estado.

3- O agente de ligação de segurança referido no n.º 1 deve cumprir todos os requisitos da categoria de diretor de segurança previstos no regime jurídico da atividade de segurança privada.

Artigo 12.º

Relatórios

1- Compete ao Secretário-Geral do Sistema de Segurança Interna, em articulação com as forças e serviços de segurança competentes, proceder a uma avaliação das ameaças em relação aos subsectores das infraestruturas críticas um ano após a sua designação como ICE.

2- Compete, ainda, ao Secretário-Geral do Sistema de Segurança Interna transmitir à Comissão Europeia um resumo bienal de dados gerais sobre os riscos, ameaças e vulnerabilidades de cada ICE identificada.

Artigo 13.º

Apoio às ICE

1- As entidades competentes devem apoiar os proprietários ou os operadores das ICE designadas, facultando-lhes o acesso às melhores práticas e metodologias disponíveis, bem como ações de formação e informações sobre os novos avanços técnicos relacionados com a proteção das infraestruturas críticas.

2- Para os efeitos do presente decreto-lei, consideram-se proprietários ou operadores de uma ICE as entidades responsáveis pelos investimentos num determinado ele- mento, sistema ou parte deste designado como ICE ou pelo respectivo funcionamento corrente.

Artigo 14.º

Informações sensíveis relacionadas com a proteção das ICE

1- Para os efeitos do presente decreto-lei, consideram-se informações sensíveis relacionadas com a proteção das infraestruturas críticas os factos respeitantes a uma infraestrutura crítica que, se divulgados, poderiam ser utilizados para planear e agir com o objectivo de provocar a perturbação ou destruição das infraestruturas críticas.

2- Qualquer pessoa que, por força do presente decreto-lei, trate informação classificada é sujeita a um procedimento de habilitação de segurança adequado, a ser concedido pela Autoridade Nacional de Segurança.

3- As entidades competentes asseguram que as informações sensíveis relacionadas com a proteção das ICE não sejam utilizadas para fins distintos dos da proteção das infraestruturas críticas.

4- O disposto no presente artigo aplica-se igualmente às informações não escritas trocadas durante reuniões em que sejam debatidos assuntos sensíveis.

Artigo 15.º

Pontos de contacto para a proteção das ICE

1- O CNPCE é o ponto de contacto junto da Comissão Europeia para a proteção das infraestruturas críticas europeias (PICE) e especificamente no plano da designação das ICE.

2- O Secretário-Geral do Sistema de Segurança Interna é o ponto de contacto para a proteção das infraestruturas críticas europeias (PICE), no plano da segurança das ICE.

Artigo 16.º

Taxa

Os procedimentos para identificação e designação de cada ICE, bem como para a validação e revisão

do plano de segurança, são objecto de uma taxa a fixar por portaria dos membros do Governo responsáveis pelas áreas das finanças, da defesa nacional e da administração interna.

Artigo 17.º

Infraestruturas críticas nacionais

O disposto no presente decreto-lei é aplicável, com exceção das fases correspondentes à componente transfronteiriça, às restantes infraestruturas críticas nacionais.

Artigo 18.º

Identificação e designação das ICE

O processo de identificação e designação das ICE nos termos do presente decreto-lei deve ser concluído até 31 de Dezembro de 2011, sendo objecto de revisão periódica.

Visto e aprovado em Conselho de Ministros de 24 de Março de 2011. — José Sócrates Carvalho Pinto de Sousa — Luís Filipe Marques Amado — Fernando Teixeira dos Santos — Marcos da Cunha e Lorena Perestrello de Vasconcellos — Rui Carlos Pereira — José António Fonseca Vieira da Silva — Paulo Jorge Oliveira Ribeiro de Campos.
Promulgado em 3 de Maio de 2011.
Publique-se.

Apêndice A – Modelo de análise

Objetivos	Questões	Enquadramento concetual	Análise de resultados
Geral: Avaliar o papel e o peso que o atual modelo de abordagem atribuiu às FA e FSS no esforço interoperável para garantir a proteção das IC.	**Central:** De que forma poderão as FA e FSS contribuir para a proteção das Infraestruturas Críticas Nacionais no âmbito do atual modelo de abordagem?		Leitura, análise descritiva e análise interpretativa das entrevistas semiestruturadas, realizadas a quatro entrevistados com funções no âmbito da identificação e proteção das IC.
OE1: Conceptualizar IC num contexto securitário para o Estado Português.	**QD1:** Qual o quadro conceptual de referência das IC ao nível da segurança nacional?	**Capítulo 2.** A segurança nacional e as infraestruturas críticas.	
OE2: Apresentar o modelo de abordagem às IC.	**QD2:** O modelo de abordagem das IC é ajustado ao tipo de infraestruturas nacionais?	**Capítulo 3.** As infraestruturas críticas em Portugal.	
OE3: Avaliar as consequências do atual modelo para as FA e FSS.	**QD3:** As FA e as FSS têm a sua intervenção no domínio da proteção das IC ajustada à realidade nacional?	**Capítulo 4.** A proteção das IC nacionais.	Avaliação e ponderação dos resultados obtidos através do enquadramento teórico.

Apêndice B – Guião da entrevista ao Sr. Eng.º Carlos Mendes

A presente entrevista foi efetuada ao Sr. Eng.º Carlos Mendes, Diretor de Serviços de Risco e Planeamento da ANPC, nas instalações da ANPC em Carnaxide, no dia 7 de abril de 2017. A entrevista versou a obtenção de conteúdos que permitam alcançar os **OE2** – Apresentar o modelo de abordagem às IC. Desta forma, procurar-se-á responder à **QD2** – O modelo de identificação e designação de IC é ajustado ao tipo de infraestruturas nacionais? Fruto da elevada experiência profissional e atual envolvimento na proposta de alteração ao enquadramento legal relativo às IC, o entrevistado reveste-se de extrema importância para o esclarecimento dos aspetos fulcrais desta temática.

Guião da Entrevista

Entrevistador (E)

Carlos Mendes (CM)

E:	**1. O PPIC foi materializado essencialmente em duas etapas: (i) identificação e designação das infraestruturas estratégicas ao normal funcionamento do País e do bem-estar da sua população, ou em situação de crise mantê-lo em níveis de funcionamento aceitáveis; e (ii) a elaboração do PNPIC, consubstanciando-se na "identificação e avaliação das vulnerabilidades das infraestruturas identificadas, face às principais ameaças passíveis de as atingir e no estudo e apoio à implementação de medidas de prevenção com vista a conter os riscos em níveis considerados aceitáveis". Qual o estado da arte?**
CM:	Não há um PNPIC no sentido em que haja varias fases. Não quer isto dizer que algumas das linhas de pensamento que estavam nas fases II e III, principalmente ao nível da resiliência e do trabalho dos operadores, não se fosse fazendo embora com outros enquadramentos, mas não consubstanciado num programa nacional. O CNPCE começou em 2004 por tentar fazer a CNPS, levantando um conjunto de pontos no país, de acordo com perspetivas diferentes consoante os utilizadores. Isto permitiu identificar cerca de 12000 infraestruturas, sendo ainda hoje considerado o maior inventário feito à escala nacional, na medida em que envolveu aproximadamente 12 setores. Durante este processo, o que se pretendia era aferir o grau de interdependência que havia entre setores para a partir desse grau de interdependência se puder fazer a análise de propagação de efeitos (aplicação do modelo de identificação e designação) e hierarquizar as infraestruturas. Desta forma, foi criado um indicador de criticidade que no fundo traduzia o peso relativo daquela infraestrutura para o país, o impacto nela e noutros setores. Neste momento ainda estamos a falar de um momento onde não haviam critérios sugeridos pela Comissão Europeia, i.e. 2005/2006. O que se convencionou na altura, neste caso o CNPCE e o IST, foi um patamar onde as duas/três classes de criticidade que corresponderiam a infraestruturas potencialmente críticas. Entretanto em 2008, surge a Diretiva Comunitária que coloca o foco nos transportes e na energia, sobretudo versando a identificação das infraestruturas europeias. Isto levou a que o CNPCE tivesse de orientar os esforços para os setores da energia e transportes, principalmente terrestre e marítimo, levando a um esforço junto dos operadores para tentar perceber qual era o grau de impacto, tanto numa perspetiva europeia, como também nacional. Em 2011, sai a transposição da Diretiva para o enquadramento legal nacional, dizendo que as características definidas para as ICE são também aplicáveis às ICN, tendo havido um ajustamento dessas infraestruturas sempre com o foco na energia e nos transportes. Em 2012, dá-se passagem do CNPCE para a ANPC, e finalmente em 2013, foram feitas as designações formais de cerca de centena e meia (150) de infraestruturas dos sectores da energia e dos transportes, como ICN. O que é que se entendeu como nacional, que o impacto é significativo à escala nacional. Aquilo que efetivamente consideramos como a primeira etapa do PPIC culminou com essa designação formal da centena e meia de ICN.
E:	**2. As principais dimensões da proteção das IC, focam-se essencialmente na *security* e na *safety*. Quais as principais ameaças e riscos que considera que Portugal corre no que concerne a proteção das IC?**
CM:	Não especificamente relativamente à Infraestruturas, mas no geral há uma Avaliação Nacional de Risco. No que diz respeito diretamente às IC, vão ter aqueles 4 a 5 riscos principais: (i) sismos; (ii) cheias; (iii) incêndios florestais; (iv) acidentes industriais, principalmente no sector da energia; e

	(v) tsunamis. A sua pertinência poderá ser abordada ou pela sua probabilidade (cheias) ou gravidade (sismos).
E:	**3. Quais as maiores dificuldades sentidas pela ANPC na implementação da PNPIC?**
CM:	Enquanto o CNPCE tinha um vinculo legal às comissões dos vários setores, portanto tinha capacidade real para trabalhar nesta temática, a ANPC não tem. Mais o próprio DL n.º 62/2011, de 9 de maio, também é omisso relativamente ao vínculo dos setores. Esta dificuldade tem sido superada através de uma base voluntária dos próprios setores dentro de um contexto em que eles não tenham obrigação legal. Esta situação leva a que, por exemplo a Direção Geral da Energia colabore com a ANPC nesta matéria tão específica. Existe uma relação muito próxima da ANPC, SG-SSI e FdS, com responsabilidades claras dos operadores, mas no entanto legalmente não se encontram referidas no DL n.º 62/2011, de 9 de maio, não existindo para todos os efeitos. Não existe um vinculo formal, funciona-se numa base de *Soft Approach*. Esta abordagem não se fazia sentir a aquando da CNPCE, uma vez que disponha de competência legais. No entanto em 2012, com a sua extinção e passagem das competências para a ANPC as mesmas não foram contempladas. Outra dificuldade, ou constrangimento, tem a ver com o levantamento das infraestruturas feito em 2004, ou seja, é um trabalho que se encontra datado no tempo e que avançando para outros setores terá de ser atualizado.
E:	**4. Atualmente apenas os setores da energia e dos transportes servem de base tanto à Diretiva 2008/114/CE do conselho de 8 de Dezembro de 2008 como ao Decreto-Lei n.º 62/2011, de 9 de Maio. Há algum trabalho que esteja a ser realizado para ampliação a outros setores ? De que forma poderão ser agrupados relativamente à realidade atual?**
CM:	Existe essa intenção, e na linha do que é a tendência europeia pretendemos avançar para comunicações, abastecimento de água e banca. Na parte das comunicações já existe algum trabalho, mas no entanto existe neste momento algum impasse que deriva da legalidade da ANPC para o fazer. Embora o DL n.º 62/2011, de 9 de maio, diga que se aplica a todas as ICN, também é verdade que no art.º 1.º do mesmo diploma diz que a sua aplicabilidade é apenas aos setores da energia e transportes.
E:	**5. Quais serão as consequências decorrentes da degradação do nível de serviço das ICN do "setor energético" nas ações da ANPC?**
CM:	Para acontecimentos graves como os que sucederam à dois/três anos no oeste, a solução passa por encontrar soluções de abastecimento alternativo, mediante solicitação da autoridade setorial ou do próprio operador, e dentro do que é a nossa competência de articulação enquanto proteção civil, compete-nos tentar encontrar soluções alternativas e potenciá-las mediante essa necessidade. Com base na informação que temos dos planos de emergência tentar perceber onde é que poderemos obter capacidades que possam mitigar essas necessidades, fundamentalmente, através de parceiros como as FA e outras entidades que possam ter o equipamento necessário. Em termos de impacto direto na ANPC, e embora as nossas instalações estejam guarnecidas com equipamentos de geração própria, também seriamos afetados, no entanto, haveria sempre margem para utilizadores prioritários.
E:	**6. Em termos práticos, considera a metodologia de identificação e designação das IC adotada pela ANPC ajustada à exigências atuais? Dado que a metodologia é de 2004, acha que se mantém atualmente ajustada às exigências atuais?**
CM:	A metodologia tem provado ser atualizada e adequada, tanto quer ao trabalho automático do modelo, quer à sua "calibração" que normalmente tem-se sempre que fazer, i.e. *expert opinion*. O que poderá não estar tão atualizado serão os dados de base de alguns setores, considerando que existe alguma discrepância entre o sector da energia relativamente aos restantes. Por seu turno, o DL n.º 62/2011, de 9 de maio, necessitava de ser mais abrangente e robusto, relativamente a um conjunto de ações que possam de fato potenciar a resiliência das IC.
E:	**7. Atendendo à importância atribuída aos "*clusters*" enquanto factor classificador das ICN, qual é o critério da definição dos 5 *clusters*?**
CM:	Nada a referir.

E:	**8. Atendendo à importância atribuída à "importância internacional ou nacional" enquanto factor classificador das ICN, qual o critério da definição?**
CM:	Atendendo a que em 2006 nós estávamos a utilizar esta metodologia com o CNPCE, fomos incorporando na nossa documentação o que já se discutia na Comissão, sendo difícil dizer o que foi de pensamento nosso e o que foi influência dos trabalhos desenvolvidos pela Comissão. Efetivamente a Diretiva tem isso, e o DL n.º 62/2011, de 9 de maio, também, mas no entanto o pensamento já cá estava. Eu diria que a dimensão internacional veio claramente da Diretiva.
E:	**9. A ANPC já possui uma metodologia específica para a análise e avaliação do risco associado à disfunção de infraestruturas críticas?**
CM:	A avaliação da ANPC contempla sempre aquilo que são os impactos na população, nos bens (incluindo IC), na economia e no ambiente. A metodologia que utilizámos para a Avaliação Nacional de Risco implicitamente lá dentro tem também a questão das infraestruturas, e dentro destas as ICN. No entanto, não foi pensada numa lógica de IC, nem existe um campo especifico em relação a essa matéria.

Apêndice C – Guião da entrevista à Sr.ª Dr.ª Helena Fazenda

A presente entrevista foi efetuada à Sr.ª Dr.ª Helena Fazenda, SG-SSI, por escrito, tendo sido respondida no dia 26 de maio de 2017. A entrevista versou a obtenção de conteúdos que permitam alcançar o **OE3** – Avaliar as consequências do atual modelo para as FA e FSS. Desta forma, procurar-se-á responder à **QD3** – As FA e as FSS têm a sua intervenção no domínio da proteção das IC ajustada realidade nacional? Fruto da elevada experiência profissional enquanto SG-SSI, aliada às suas competências específicas no que concerne a coordenação e cooperação entre as FSS, a entrevistada reveste-se de extrema importância para o esclarecimento dos aspetos fulcrais desta temática.

Guião da Entrevista

Entrevistador (E)

Helena Fazenda (EF)

E:	**1. As principais dimensões da proteção das IC, focam-se essencialmente na *security* e na *safety*. Quais as principais preocupações com a proteção das IC em Portugal?**
HF:	A proteção de IC é um tema abrangente, que engloba diversas perspectivas que se complementam. Por um lado, quando falamos de incidentes, temos logo de discernir vários tipos de causas, as de origem humana intencional, as de origem humana não intencional e as de origem natural. Em função do tipo de causa existem atividades específicas a dois níveis, o da prevenção e o da resposta. Assim a proteção de IC requer medidas concretas por exemplo no domínio da prevenção para o risco de incêndios, diferentes daquelas que devem ser adotadas para a prevenção de ataques de natureza humana hostil. Há que distinguir as atividades do domínio físico, e as atividades do domínio ciber. Há toda a fase de resposta, em que se assume que o risco estrutural existe (maior do que 0) e portanto importa preparar mecanismos de resiliência e modelos de continuidade de negócio. Ora tudo isto deve ser trabalhado tendo como pano de fundo o estudo de interdependências (entre IC), que é, em bom rigor, aquilo distingue as IC das restantes infraestruturas, e pelo menos três tipos de escala de impacto, a local, a nacional e a internacional. Como se verifica, trata-se de um trabalho que se subdivide em inúmeras atividades, que envolve muitas entidades, do setor público e do setor privado, e que obriga a elevados esforços de coordenação.
E:	**2. Em termos práticos, considera que o DL 62/2011, de 9 de maio, permanece ajustado às exigências atuais relativamente à intervenção das FdS no domínio da proteção das IC? Em caso negativo, que alterações veria como mais adequadas?**
HF:	A proteção de IC, como já foi dito, vai muito para além da atuação preventiva das FdS. Mas obviamente que as medidas e atividades desenvolvidas por estas, tendo em vista um melhor conhecimento da IC, das ameaças que se colocam e da forma de atuação - que, por força do próprio ambiente de uma IC, são necessariamente diferentes, das formas de atuação na via pública - são aspetos fundamentais para o aumento dos níveis de segurança. Nesta linha, defendemos que o DL está atual. Valoriza o papel das FdS. Contudo, naturalmente que existe espaço para que seja melhorado, designadamente indicando um conjunto de boas práticas que devem ser desenvolvidas, como sejam por exemplo a realização de simulacros periódicos, a troca de informação entre as FdS e os operadores, entre outras questões.
E:	**3. Quais as principais dificuldades sentidas na coordenação entre o PSPE e o PSO de IC?**
HF:	Neste momento não estão registadas dificuldades.
E:	**4. Em sua opinião, quais as IC cuja destruição, ou diminuição do nível de serviço, teriam maior impacto na segurança nacional? Justifique?**
HF:	Todas as IC até ao momento identificadas têm um enorme potencial disruptivo, precisamente porque são as interdependências que lhes estão associadas que lhe conferem a qualidade de IC. Por isso não é tecnicamente correto afirmar-se que umas são mais críticas do que outras. Em todo o caso, sabe-se que a intensidade com que estas interdependências se estabelecem variam de sector para setor. E também se sabe que os setores da energia (em particular o subsetor da energia eléctrica, nas suas componentes transporte e distribuição) e das comunicações, são os que geram

	maior número de interdependências com outros sectores (e consigo próprios).
E:	**5. Considera que as FdS poderiam ter um maior contributo em matérias fundamentais para a proteção das IC?**
HF:	O contributo que decorre do DL n.º 62/2011 é suficiente, embora possa ser melhorada, designadamente com o desenvolvimento de atividades que envolvam as FdS e os operadores (exercícios, visitas, workshops etc…).
E:	**6. A Espanha, à semelhança de outros países da UE, possui um organismo exclusivamente dedicado à proteção das IC nas sua várias vertentes. Na sua opinião faria sentido Portugal seguir o mesmo modelo?**
HF:	O modelo espanhol é considerado um dos mais robustos e completos ao nível europeu. Portugal poderia aprender com este modelo e, à escala da realidade nacional, implementar algumas das suas componentes. Desde logo importaria aumentar a capacitação da Administração Pública, no que respeita a esta pasta, em particular ao nível de recursos humanos que se especializem nesta área. Um organismo como o Centro Nacional de Proteção de IC de Espanha, com 50 funcionários exclusivamente dedicados é um exagero para a nossa realidade, mas é importante reconhecer que a situação atual, em que praticamente não há recursos vocacionados para trabalhar esta matéria, também está longe de ser a situação ideal.

Apêndice D – Guião da entrevista ao Sr. Major Paulo Delgado

A presente entrevista foi efetuada ao Sr. Major Paulo Delgado, Chefe da Repartição de Segurança, da Direção de Informações da GNR, nas instalações do Comando Geral da GNR em Lisboa, no dia 24 de abril de 2017. A entrevista versou a obtenção de conteúdos que permitam alcançar o **OE3** – Avaliar as consequências do atual modelo para as FA e FSS. Para tal, almeja-se responder à **QD3** – As FA e as FSS têm a sua intervenção no domínio da proteção das IC ajustada realidade nacional?

O Sr. Major Paulo Delgado, entre outras funções, é o oficial de ligação da GNR relativamente às IC junto do SG-SSI e da ANPC, sendo também o principal responsável pela emissão dos "pareceres prévios" dos PSO da responsabilidade da GNR.

Guião da Entrevista

Entrevistador (E)

Paulo Delgado (PD)

E:	**1. As principais dimensões da proteção das IC, focam-se essencialmente na *security* e na *safety*. Quais as principais ameaças e riscos que considera que Portugal corre no que concerne à proteção das IC?**
PD:	Felizmente em Portugal não têm sido detetadas ameaças diretas ou indiretas que indiciem o planeamento e/ou a preparação de ataques à segurança pese embora, a nível da Europa, ultimamente persistir um nível elevado da ameaça terrorista. Espelho dessa situação foram os recentes ataques dos quais se destacam a tentativa de atropelamento de vários transeuntes na cidade da Antuérpia, o envio de um envelope armadilhado endereçado à sede do Fundo Monetário Internacional, em Paris, que ao explodir acabou por ferir uma pessoa ou ainda o falecimento de um polícia em Londres depois de um indivíduo ter atropelado vários peões na Ponte de *Westminster* no Reino Unido. Se a estes acontecimentos juntarmos os ataques terroristas que ocorreram em março do ano passado no aeroporto de *Zaventem* e na estação de metro na Bélgica, que provocaram dezenas de mortos e feridos, ou recuarmos a junho de 2015 em que *hackers* efetuaram um ataque informático sobre o sistema responsável pelas operações nos sistemas da companhia aérea da polaca *Lot*, impedindo os computadores em solo de criar planos de voo, julgo que as ameaças terroristas e os ciberataques são as ameaças mais prováveis de acontecer em Portugal tendo em consideração outras ameaças tais como o crime organizado, armas de destruição massiva, entre outras.
E:	**2. Em termos práticos, considera que o DL 62/2011, de 9 de maio, permanece ajustado às exigências atuais relativamente à intervenção das FdS no domínio da proteção das IC?**
PD:	O DL n.º 62/2011, de 9 de maio, veio transpor a Diretiva 2008/114/CE do Conselho, de 08 de dezembro, e estabelecer os procedimentos de identificação e designação e proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico-social da sociedade nos setores dos transportes e energia, contudo além de terem de ser considerados outros normativos tais como a Lei de Segurança Interna, a Estratégia Nacional de Combate ao Terrorismo, a Estratégia Nacional de Segurança no Ciberespaço, entre outros, torna-se um documento pouco abrangente quando especificamente não prevê setores tais como a água, a indústria, comunicações entre outros.
E:	**3. Sendo imperativo legal que o operador de uma IC terá de proceder à elaboração de um PSO e submetê-lo a parecer prévio das entidades competentes, i.e. ANPC e FdS. Considera adequados os critérios de avaliação do PSO em vigor? Justifique?**
PD:	Sim. Julgo que sim, dados os critérios previstos na matiz serem abrangentes e permitirem uma avaliação criteriosa e rigorosa dos PSO´s. Evidentemente e tratando-se de documentos em constante atualização não significa que a matriz não possa ser atualizada até porque o objetivo é mesmo esse, fazer mais e melhor. No entanto, considero que os critérios atuais são os adequados, tanto no âmbito da *security*, como da *safety*. A GNR enquanto FdS territorialmente competente, tem em consideração na elaboração do seu parecer prévio (*security*) o preenchimento dos seguintes requisitos: (i) análise de risco, subdividindo-se em análise de risco baseada e caracterização; (ii)

	contramedidas e procedimentos permanentes, subdividindo-se em instalação de meios de detecção, controlo do acesso, proteção e prevenção, medidas de minimização dos danos e impactos e de reposição da normalidade e procedimentos de auditoria e verificação; (iii) reação e resposta a incidentes de segurança identificados, subdividindo-se em procedimentos de alerta de segurança e de gestão de crises; e (iv) contramedidas e procedimentos progressivos. Torna-se um pouco mais abrangente do que o parecer prévio da componente *safety*, ou seja: (i) análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada componente e nos impactos potenciais, subdividindo-se em identificação e caracterização dos riscos susceptíveis de afectar a instalação e tipos de emergências e cenários; (ii) identificação, seleção e prioridade de contramedidas e procedimentos permanentes e progressivos a aplicar consoante o grau de ameaça aplicável à IC ou o estado de segurança decretado, subdividindo-se em procedimentos de alerta e gestão de crises e medidas de minimização dos danos e impactos e de reposição da normalidade; e (iii) medidas de controlo e verificação, subdividindo-se em procedimentos de alerta de segurança e de gestão de crises.
E:	**4. Em sua opinião, quais as IC cuja destruição, ou diminuição do nível de serviço, teriam maior impacto para a missão da GNR?**
PD:	A GNR tendo na sua área de jurisdição 70% (162) das IC identificadas até ao momento, deve ter a mesma atenção, salvaguarda e condições de segurança por forma a evitar o máximo de perturbações económicas ou sociais. É isto, a meu ver, o mais importante deste processo, assegurar a resiliência das infraestruturas que se revelam indispensáveis à sobrevivência na sociedade global e que condicionam progresso e bem-estar.
E:	**5. Que contributos por parte das FdS considera fundamentais para a proteção das IC?**
PD:	As FdS são os órgãos responsáveis pela coordenação e supervisão de todas as atividades relacionadas com a proteção das IC. Desde a avaliação PSO ao nível da identificação das ameaças (prevenir), até à elaboração do plano de segurança exterior (proteger), bem como na deteção e neutralização das ameaças (perseguir) e na rápida reposição da normalidade (responder), as FdS são uma peça fundamental em qualquer um destes princípios.

Apêndice E – Guião da entrevista ao Sr. Coronel Soares da Costa

A presente entrevista foi efetuada ao Sr. Coronel Soares da Costa, Comandante do Comando Territorial dos Açores da GNR, por escrito, tendo sido respondida no dia 9 de junho de 2017. A entrevista versou a obtenção de conteúdos que permitam alcançar o **OE3** – Avaliar as consequências do atual modelo para as FA e FSS. Para tal, almeja-se responder à **QD3** – As FA e as FSS têm a sua intervenção no domínio da proteção das IC ajustada realidade nacional?

O Sr. Coronel Soares da Costa é detentor de um vastíssimo currículo, tendo a entrevista versado fundamentalmente a sua experiência na área das IC, em particular, nas funções de Adjunto do Gabinete da SG-SSI e de Diretor da Direção de Informações da GNR. Atualmente, vê a sua *expertise* relativamente à temática das IC ser complementada de sobremaneira enquanto Comandante do Comando Territorial dos Açores.

Guião da Entrevista

Entrevistador (E)

Soares da Costa (SC)

E:	**1. As principais dimensões da IC, focam-se essencialmente na *security* e na *safety*. Quais as principais ameaças e riscos que considera que Portugal corre no que concerne à proteção das IC?**
SC:	Dispensando a construção de uma matriz de risco e a elaboração de um *assessement* no que toca à avaliação da ameaça, documentos cujo valor terá de estar ligado a competência técnica de quem domina ferramentas, no que tange a esta matéria considero o que verdadeiramente faz falta, em primeiríssima instância, é a interiorização da capital importância desta matéria nos múltiplos *Stakeholders* que nela estão envolvidos, atenta a profusão, transversalidade e complexidade destas matérias. A mera identificação das ameaças (conceito associado à vulnerabilidade) e dos riscos (associado ideia de impacto no funcionamento) observados numa perspectiva individual e casuística é uma perigosa e minimalista abordagem deste dossier, que é imensamente mais complexo do que a elementar divisão entre domínios *safety* ou *security*.
E:	**2. Em termos práticos, considera que o DL n.º 62/2011, de 9 de maio, permanece ajustado às exigências atuais relativamente à intervenção das FdS no domínio da proteção das IC? Em caso negativo, que alterações veria como mais adequadas?**
SC:	Numa visão imediatista e pouco avisada creio que sim pois encerra os princípios e setores que prioritariamente devem ser acautelados. No entanto e face ao exponencial desenvolvimento da sociedade *"lato senso"* e à emergência de novos fenómenos, sejam de índoles social, económica, tecnológica ou securitária deverá este Diploma ser reformulado por forma a integrar uma ótica menos setorial e mais prospetiva, até para acompanhar a filosofia de majoração do valor de uma abordagem pluridimensional face à rede de implicações e consequências que frequentemente "o movimento de uma só peça" tem atualmente no puzzle da tomada de decisão.
E:	**3. Quais as principais dificuldades sentidas na coordenação entre o PSPE e o PSO de IC?**
SC:	Seriam muitas as possíveis dificuldades a elencar segundo a ótica que venho sustentando, o que desde logo compromete, quiçá de forma crítica, a articulação dos dois. Assim e desconstruindo esta aparente e matematizáveis dificuldades, identifico desde logo a gritante falta de cultura neste domínio, assim como a falta/fraca técnica e competências que deveriam ser pressupostos básicos e intrínseco a todo os que, por razões operam diversas neste domínio.
E:	**4. Em sua opinião, quais as IC cuja destruição, ou diminuição do nível de serviço, teriam maior impacto para a missão da GNR?**
SC:	A gradação do impacto da diminuição ou destruição de determinada IC na missão da GNR não pode ser tratada sozinha (como de gestão se tratasse), atenta a multiplicidade de implicações e o desconhecimento dos potenciais efeitos que em determinada estrutura tendo presente que a esmagadora maioria das IC se localizam na Zona de Ação da Guarda circunstância que desde logo deveria ser tomada como um fator de dificuldade e preocupação acrescida na atividade da Guarda.

E:	**5. Que contributos por parte das FdS considera fundamentais para a proteção das IC?**
SC:	Numa perspetiva meramente escolar poderíamos em sede de reflexão proceder ao levantamento dos *inputs* para este domínio. É no entanto meu convencimento que o contributo maior será mais do que um produto (*output*) deveria ser um resultado (*outcome*). A criação e adoção de uma mentalidade que faça com que tal relevante matéria passe a ser parte do acervo de preocupações e responsabilidades operacionais (*accountabillity*) à semelhança do que deveria ter passado com a assunção do papel da Guarda na Estratégia Nacional de Combate ao Terrorismo.
E:	**6. A Espanha, à semelhança de outros países da UE, possui um organismo exclusivamente dedicado à proteção das IC nas suas várias vertentes. Na sua opinião faria sentido Portugal seguir o mesmo modelo?**
SC:	Absolutamente no que toca à existência de um Organismo (de constituição multidisciplinar). Não necessariamente no que respeita ao seguir o modelo espanhol. Trata-se de uma bom exemplo como *benchmarking* o que não significa que outros modelos, sejam ao nível nacional, ao nível da instituição e até mesmo de modelos académicos (*predictive intelligence*) tal possibilidade apenas peca por tardia. Dito isto não se trata de não plagiar esta estrutura. Trata-se de pensar e conceber uma plataforma que não obstante as semelhanças culturais e demais afinidades, apenas deverá ser tomada como uma estrutura de referência que sirva de base à construção de um modelo que respeite as nossas especificidades cujo resultado final (neste tipo de assuntos) é sempre maior do que a soma das partes.