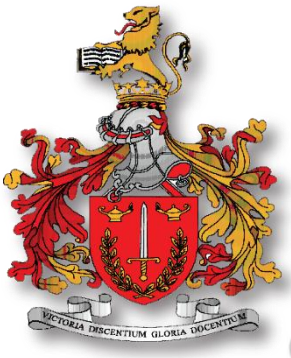
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA



A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

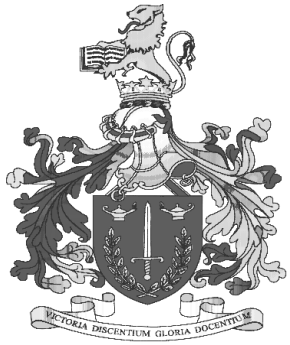
CONTRIBUTOS PARA O DESENVOLVIMENTO DE UM PLANO NACIONAL DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

Autor: João Franca da Fonseca Pestana

Orientador: Tito Eurico Miranda Fernandes (Subintendente)

Lisboa, 20 de junho de 2016

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA



SISTEMA DE SEGURANÇA INTERNA

A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

CONTRIBUTOS PARA O DESENVOLVIMENTO DE UM PLANO NACIONAL DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

Relatório Final do Curso de Comando e Direção Policial

Lisboa, 20 de junho de 2016

JOÃO FRANCA DA FONSECA PESTANA

Comissário

Secretariado Permanente do Gabinete Coordenador de Segurança

- Oficial de Ligação da Polícia de Segurança Pública -

ORIENTADOR

TITO EURICO MIRANDA FERNANDES

Subintendente

Sistema de Segurança Interna

- Adjunto do gabinete da Secretária-Geral do Sistema de Segurança Interna --

AGRADECIMENTOS

A elaboração deste Relatório Final não teria sido possível sem o apoio de várias pessoas, a quem me gostaria de dirigir neste momento em que termino o trabalho.

Em primeiro lugar a Teresa, minha mulher. O enorme esforço que fez para me libertar dos afazeres mundanos permitiu que eu mergulhasse em profundidade neste projeto, dando o melhor de mim.

Logo de seguida, o Subintendente Tito Fernandes, meu colega, meu amigo e, neste trabalho, meu orientador. Não tenho quaisquer dúvidas de que sem a sua total disponibilidade, não teria conseguido terminar um trabalho desta dimensão. Muito mais do que se poderia exigir de um orientador, o Subintendente Tito foi o meu "copiloto", não só dando apoio à navegação, mas também conferindo todos os aspetos do trabalho, cada curva, cada ressalto, cada obstáculo, desde o arranque até ao cruzar da meta. Por vezes questiono-me se a sua energia não será inesgotável! Não posso dizer que tenha surpreendido, porque o conheço bem, mas sinto, e quero referi-lo agora, que eu não poderia ter feito melhor escolha.

Ao meu pai, infatigável "caçador de gralhas", pelo paciente trabalho de revisão do texto.

Uma palavra de apreço, também, à Dr.ª Isabel Pais, da ANPC, que ao longo dos últimos dois anos, teve a paciência de me transmitir algum do seu vasto conhecimento sobre este tema.

A Engenheira Luísa Pestana, da EDP, pela minúcia da sua análise, a suas sugestões e encorajamento.

Finalmente a todos aqueles que, direta ou indiretamente, contribuíram e tornaram possível a concretização deste relatório, nomeadamente: aos Srs. Superintendente-Chefe Paulo Lucas; Intendente Luís Elias, Intendente Alexandre

Coimbra, Tenente-Coronel José Inglês, Capitão-de-fragata Pedro Vinhas, Subintendente Norberto Rodrigues, Dr. Ricardo Carrilho, Dr.ª Carla Pinto, Dr. Miguel Serrão, Bibiane Andujar (CNPIC-Espanha) e Samuel Donikian (SGDSN - França).

A todos, os meus agradecimentos.

RESUMO E PALAVRAS-CHAVE

As sociedades contemporâneas assentam em larga escala, no pleno e contínuo funcionamento de sistemas de infraestruturas críticas.

A proteção destas infraestruturas deve ser um desígnio quer do Estado quer das empresas que as detém e operam.

As medidas protetivas, no seu sentido mais lato, envolvem inúmeras entidades, e a sua implementação está, em grande medida, dependente da existência de uma política específica, materializada num plano, e corporizada por um organismo público incumbido de a desenvolver e aplicar.

O presente contributo pretende apontar um foco naquele que deve ser o papel de um Estado responsável e previdente, e chamar a atenção para as necessidades de melhorar a prestação e todos os atores, aos vários níveis, para aquele que deve ser um dos compromissos mais importantes da Administração, em matéria de segurança.

Palavras-chave: Proteção de infraestruturas criticas; políticas de segurança, Sistema de Segurança Interna.

ABSTRACT AND KEY WORDS

Modern societies are built, to a high degree, on the proper functioning and ininterrupted operation of critical infrastructures.

Critical infrastructures protection must be a collective aim both for the State and for the private owners operating in this field.

Protective measures, in its broadest sense, involve countless entities and its implementation depends largely on the existance of an overall specific policy, materialized in a plan and promoted by a public body responsible for its development and implementation.

This report aims not only to draw attention to the major role expected from a cautious and responsible State, but also to highlight the need to improve the performance of all the relevant players, at various levels, with a view to achieve one of the State´s most significant duties as regards security.

Key-words: Critical infrastructure protection, security policies, Portuguese Internal Security System.

ÍNDICE

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

ALS	Agente de Ligação de Segurança
ANAC	Autoridade Nacional da Aviação Civil
ANPC	Autoridade Nacional de Proteção Civil
ANS	Autoridade Nacional de Segurança
CCDP	Curso de Comando e Direção Policial
CEDN	Conceito Estratégico de Defesa Nacional
CFR	Conforme
CNCS	Centro Nacional de Cibersegurança
CNPCE	Conselho Nacional de Planeamento Civil de Emergência
DGRM	Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos
DL	Decreto-Lei
EM	Estados-membros
ENCT	Estratégia Nacional de Combate ao Terrorismo
ENSC	Estratégia Nacional de Segurança do Ciberespaço
FA	Forças Armadas
FS	Força(s) de Segurança
FSS	Forças e Serviços de Segurança
GCS	Gabinete Coordenador de Segurança
GNR	Guarda Nacional Republicana
GNS	Gabinete Nacional de Segurança
IC	Infraestruturas Críticas
ICE	Infraestruturas Críticas Europeias
ICN	Infraestruturas Críticas Nacionais
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
LSI	Lei de Segurança Interna
MAI	Ministério da Administração Interna

OE	Objetivos específicos
OTAN	Organização do Tratado do Atlântico Norte (*North Atlantic Treaty Organization – NATO)*
PCCCOFSS	Plano de Coordenação e Cooperação das Forças e Serviços de Segurança
PD	Perguntas derivadas
PEIC	Proteção Europeia de Infraestruturas Críticas
PEPIC	Programa Europeu de Proteção de Infraestruturas Críticas
PIC	Proteção de Infraestruturas Críticas
PICE	Proteção de Infraestruturas Críticas Europeias
PM	Polícia Marítima
PNPIC	Plano/Programa Nacional de Proteção de Infraestruturas Críticas
PSO	Plano(s) de Segurança do Operador
PSP	Polícia de Segurança Pública
PSPE	Plano(s) de Segurança e Proteção Exterior
RAR	Resolução da Assembleia da República
RCM	Resolução do Conselho de Ministros
SGSSI	Secretário-Geral do Sistema de Segurança Interna
SIRP	Sistema de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
SSI	Sistema de Segurança Interna
UE	União Europeia

CAPÍTULO 1

INTRODUÇÃO

1.1. ENQUADRAMENTO DO TEMA

As sociedades contemporâneas são suportadas por sistemas de infraestruturas interdependentes, indispensáveis à sua sobrevivência e desenvolvimento.

A perturbação destas infraestruturas é passível de causar um impacto de tal dimensão que impossibilitaria a satisfação das necessidades mais elementares.

A estas infraestruturas designamos Infraestruturas Críticas (IC), e a sua proteção deverá constituir um desígnio do Estado e das entidades que as operam.

Na esteira das políticas europeias, e à semelhança de outros países, Portugal procurou organizar-se no sentido de melhorar as capacidades de segurança das IC, nos domínios *safety* e *security*.

Importa proceder a uma análise e avaliação do atual quadro de proteção de infraestruturas críticas (PIC) e, selecionando as melhores práticas e internacionais, lançar contributos para a edificação de um **Plano Nacional de Proteção de Infraestruturas Críticas (PNPIC)**, de resto na senda do Programa Europeu de Proteção de IC[1] (PEPIC).

1.2. JUSTIFICAÇÃO DO TEMA

Em 26 de fevereiro de 2012, por ocasião do primeiro (e até à data único) seminário subordinado ao tema “A proteção das infraestruturas críticas nacionais” (aspas do autor), o ex-ministro da Administração Interna, Dr. Figueiredo Lopes, alertava: “…as ameaças mais suscetíveis são fundamentalmente os riscos

[1] *Vide* COM(2005) 576 final da Comissão das Comunidades Europeias, de 17 de novembro. *Livro Verde relativo a um programa europeu de protecção das infraestruturas críticas*. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52005DC0576&from=EN [em linha] [consulta em 05 de junho de 2016].

ambientais, como os sismos, tecnológicos e ataques terroristas."[2]; e acrescentava: "…falta agora concretizar um programa nacional de proteção das infraestruturas críticas, definir melhor os sistemas de cooperação e os mecanismos que devem ser desenvolvidos para assegurar, quer na área do Estado, quer nas empresas, os domínios da prevenção em caso de ataques"[3].

Não obstante estes alertas, e as recomendações da Comissão Europeia para que fossem criados planos nacionais[4], quatro anos passaram e o panorama em Portugal quase não registou alterações.

Já o mesmo não se pode dizer do catálogo das ameaças que, sendo à data do seminário bastante significativas[5], se têm agravado substancialmente: as cidades europeias tornaram-se alvos de atentados sem precedentes desde a década de 70; milhares de cidadãos comunitários rumaram ao Médio Oriente para integrar grupos terroristas de matriz islâmica; os países europeus vêem-se a braços com uma pressão migratória de enorme melindre no que toca à infiltração de indivíduos de risco; e, finalmente, com implicações que ainda se desconhecem em toda a sua extensão, ocorre uma intervenção militar russa num país da Aliança Atlântica (OTAN) e com aspirações a integrar a União Europeia (UE).

São, portanto, diversos os desafios que justificam uma reflexão séria sobre esta matéria, mas também são múltiplas as oportunidades que o momento proporciona.

Desde logo o facto de existirem, nos Estados-membros (EM) da UE, modelos diferentes de proteção de IC – tendo a Comissão avaliado as suas vantagens e desvantagens - que podem servir de exemplo (a seguir ou a evitar).

---

[2] *Cfr.* artigo de imprensa online "Falta programa nacional de proteção de infraestruturas". Disponível em:http://www.dn.pt/portugal/interior/falta-programa-nacional-de-protecao-de-infraestruturas-2327004.html [em linha] [consulta em 05 de junho de 2016].

[3] *Idem*.

[4] *Vide* COM(2006) 786 final da Comissão das Comunidades Europeias, de 12 de dezembro. *Programa Europeu de Protecção das Infra-Estruturas Críticas*. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52006DC0786&from=PT [em linha] [consulta em 05 de junho de 2016].

[5] Em 2004, 191 pessoas perderam a vida num ataque terrorista perpetrado na estação ferroviária de Atocha, em Madrid. Disponível em: http://www.elmundo.es/documentos/2004/03/espana/atentados11m/hechos.html [em linha] [consulta em 05 de junho de 2016].

Portugal, sendo dos poucos países que ainda não desenvolveu um plano nacional, nem criou um organismo coordenador especializado, tem condições únicas para recolher as melhores práticas europeias, caso decida tomar este caminho.

Finalmente, o facto do processo de identificação e designação de IC nacionais ainda se encontrar numa fase inicial (apenas considerados dois dos doze setores revistos[6]) permite projetar, com enormes benefícios, quaisquer melhorias que nesta matéria venham a ser introduzidas.

São estes os motivos que no levam a escolher o tema da proteção de IC, na elaboração do Relatório Final do 2.º CCDP, enquadrado no tema 14 (Sistema de Segurança Interna).

1.3. PROBLEMÁTICA DA INVESTIGAÇÃO

Decorridos dez anos desde a adoção de um Livro Verde relativo à proteção de IC europeias, e oito anos desde a publicação da Diretiva 2008/114/CE do Conselho[7], os EM desdobram-se em esforços no sentido de aumentar a proteção das suas IC.

Na Europa, mas não só, inúmeros governos implementaram planos de proteção de âmbito nacional, e reforçaram as capacidades de coordenação das suas administrações.

Em contraste, não há ainda registo em Portugal de desenvolvimentos satisfatórios.

Assim, na fase em que nos encontramos e tendo em conta a experiência colhida, impõe-se suscitar a seguinte pergunta de partida (PP):

Como pode ser melhorada a proteção de IC em Portugal?

---

[6] A saber: Energia, Transportes, Comunicações/TIC, Indústria, Comércio, Serviços Financeiros, Órgãos de Soberania, Governação, Segurança e Defesa, Água, Alimentação e Saúde.

[7] *Vide* Diretiva 2008/114/CE de 08 de dezembro. *Identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção*. Disponível em: http://www.umic.pt/images/stories/publicacoes5/Directiva%202008%20do%20Conselho%20sobre%20infra-estruturas%20criticas.pdf [em linha] [consulta em 05 de junho de 2016].

Uma vez que o tema é abrangente, optou-se por decompor a pergunta de partida em seis perguntas derivadas (PD):

- PD1 - Existe em Portugal um plano ou uma estratégia nacional para a proteção de IC?
- PD2 - Que necessidades são sentidas pelos diferentes atores no domínio da proteção de IC?
- PD3 - Que modelos de governação e boas práticas são seguidas em outros países europeus?
- PD4 - Há necessidade de um plano ou de uma estratégia para a proteção de IC em Portugal?
- PD5 – A implementação e condução de um plano ou de uma estratégia para a proteção de IC requerem a criação de um organismo dedicado e especializado?
- PD6 – Considerando a realidade nacional, que desenho e configuração deverá ter um plano nacional de proteção de IC?

Tendo em consideração as perguntas de partida e derivadas, o autor propõe-se atingir o seguinte **objetivo geral (OG)**:

Maximizar o atual modelo de proteção de IC, na tripla vertente jurídica, orgânica e funcional, por via da identificação das necessidades sentidas pelos principais intervenientes, com vista ao esboço de um plano nacional, eficiente e alinhado com as boas práticas internacionais.

Para atingir o objetivo geral, foram estabelecidos os seguintes **objetivos específicos** (OE):

- OE1 - Compreender se o atual quadro legal relativo à proteção de IC é inteligível, eficiente e articulado.
- OE2 – Diagnosticar as necessidades sentidas pelos atores relevantes (Estado, reguladores e operadores de IC);
- OE3 – Identificar tendências e boas práticas no contexto de alguns EM da

UE, quer no domínio do modelo organizativo, quer no domínio das atividades de proteção;

- OE4 – Aferir da necessidade de criação de um Plano Nacional de Proteção de IC;
- OE5 – Aferir da necessidade de reforço da capacitação do Estado, através da criação de um organismo dedicado à proteção de IC;
- OE6 – Identificar os pilares que devem estar na base da construção de um Plano Nacional de proteção de IC, designadamente o modelo de articulação público-privado, os atores relevantes, as atividades a prosseguir, e um organismo de coordenação e tutela.

1.4. HIPÓTESE

Em convergência com a problemática da investigação, assumimos a seguinte hipótese que, para facilitar a compreensão, é aqui repartida em cinco afirmações:

- Inexiste um plano nacional de proteção das IC;
- O quadro legal regulador desta matéria denota incoerências e lacunas;
- Constata-se um défice de compromisso político;
- A Administração carece de capacidade orgânica neste contexto;
- De tudo isto resultando o despreparo do Estado para satisfazer suficientemente as necessidades sentidas pelos atores relevantes.

1.5. METODOLOGIA

Tendo em vista não só a necessária compreensão da temática, mas sobretudo a obtenção de respostas para as questões de investigação, foram utilizados métodos de recolha de informação, distribuídos por três fases do trabalho:

Fase concetual – fez-se uma revisão da literatura, mediante exploração de fontes primárias, mas também por observação direta, fruto do trabalho que o autor desenvolve nesta área.

Fase metodológica – caraterizaram-se as ferramentas de investigação utilizadas nos inquéritos aplicados[8].

Fase empírica – apresentaram-se os resultados do trabalho de investigação, e extraíram-se as conclusões gerais da investigação.

1.6. SÍNTESE DOS CAPÍTULOS

O trabalho comporta uma divisão em quatro capítulos:

1 – **Introdução**: é composto por um breve enquadramento e apresentação dos parâmetros gerais do trabalho.

2 **– Revisão da literatura**: através da revisão do quadro legal, são abordados os conceitos doutrinários mais relevantes, procurando-se que o leitor os consiga situar na realidade do nosso país.

O capítulo encerra com uma seleção de instrumentos desenvolvidos em países da Europa, nos EUA e no Canadá, e que se afiguram como boas práticas a transpor para o plano nacional.

3 - **A perspetiva dos atores (análise dos resultados dos inquéritos)**: no terceiro capítulo são caraterizadas as metodologias de investigação dos inquéritos conduzidos junto dos operadores e de um painel de especialistas, e são analisados os seus resultados.

4 **- Conclusões e recomendações:** no último capítulo, sintetizam-se respostas às questões do estudo e propõem-se algumas reflexões e recomendações.

O Relatório Final termina com a bibliografia, legislação e sítios da internet consultados.

[8] *Vide* Apêndices C, D e F.

CAPÍTULO 2

REVISÃO DA LITERATURA

2.1. INTRODUÇÃO

Com o segundo capítulo deste estudo propomo-nos apresentar uma revisão da literatura que garanta ao leitor o domínio dos conceitos essenciais, a compreensão do caminho percorrido em Portugal e na Europa, a perceção do complexo quadro jurídico que envolve esta temática, o papel dos vários atores e, finalmente, o contacto com algumas das melhores práticas internacionais.

2.2. RETRATO DAS INFRAESTRUTURAS CRÍTICAS EM PORTUGAL

2.2.1. CONTEXTO HISTÓRICO

Tempos houve, não muito distantes, em que chegou a acreditar-se no "fim da história"[9] (aspas do autor), surgindo a ilusão, por muitos partilhada, de que a queda do muro de Berlim e o termo da "guerra fria", no ocaso dos anos 80, trariam finalmente por arrasto uma era de equilíbrio, o triunfo incontestado da democracia liberal, uma ordem mundial mais pacífica, inclusiva e solidária.

As décadas seguintes, e desde logo o tremendo abalo causado pelos atentados de 11 de setembro de 2001, encarregaram-se de desmontar essa quimera, e despertaram muitas consciências do imprevidente torpor em que pareciam ter caído.

Mas seria apenas quatro anos depois, na sequência do atentado terrorista de 11 de março de 2004, na estação ferroviária de Atocha, em Madrid, que na Europa surgiriam as primeiras iniciativas dirigidas à proteção de IC.

[9] Título de um artigo (1989) e posteriormente de um livro (1992) publicado por Francis Fukuyama.

Assim, "…o Conselho Europeu de Junho de 2004 solicitou à Comissão que elaborasse uma estratégia global de proteção de IC. Em resposta a Comissão adotou, a Comunicação intitulada "proteção de IC no âmbito da luta contra o terrorismo", na qual são apresentadas sugestões claras sobre como reforçar a prevenção, estado de preparação e capacidade de resposta europeia relativamente a ataques terroristas que afetem IC"[10].

No ano seguinte, a Comissão elabora um Livro Verde que estabelece as opções políticas do que viria a ser o Programa Europeu de proteção de IC cujas conclusões foram aprovadas pelo Conselho em abril de 2007.

No final de 2008 foi finalmente publicada a Diretiva 2008/114/CE, "…**relativa à identificação e designação das IC europeias e à avaliação da necessidade de melhorar a sua proteção**"[11]. Este documento, para além de definir procedimentos relativos à identificação e designação de IC europeias, vem estabelecer a obrigatoriedade de elaboração de planos de segurança, quer por parte dos operadores quer por parte dos organismos do Estado.

Portugal acompanhou desde cedo as preocupações europeias nesta matéria. Em 2004 foi criado um grupo de trabalho, coordenado pelo então Conselho Nacional de Planeamento Civil de Emergência (CNPCE), que se propôs iniciar um processo estruturado em três fases:

- Identificação e classificação das IC nacionais;
- Análise e avaliação do risco associado à disfunção de IC e estudo e difusão de medidas eficientes para reforço da sua proteção;
- Implementação de medidas e monitorização do risco.

[10] *Cf.* COM(2006) 786 final de 12 de dezembro de 2006. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52006DC0786&from=EN [em linha] [consulta em 13 de junho de 2016].

[11] *Vide* Diretiva 2008/114/CE de 08 de dezembro. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114&from=PT [em linha] [consulta em 06 de junho de 2016].

O CNPCE foi extinto em 2012[12], sendo que as suas competências de identificação e classificação de IC passaram para a ANPC, e destas três fases apenas a primeira foi desenvolvida em profundidade.

2.2.2. A DIMENSÃO JURÍDICA

A proteção de IC é uma temática abrangente, onde se cruzam saberes provenientes das mais diversas disciplinas, aliás um pouco à semelhança dos sistemas, complexos, que caraterizam essas mesmas infraestruturas e as redes que as interligam.

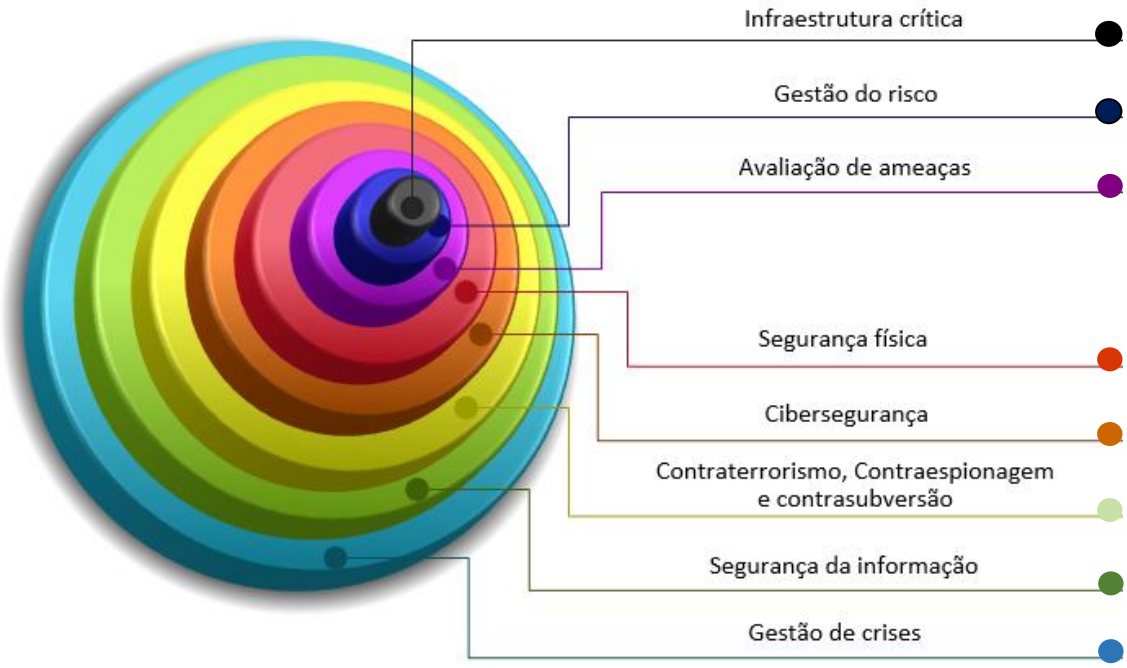


Figura 1: Disciplinas e saberes que concorrem para a proteção de infraestruturas críticas.

Fonte: Elaboração própria do autor.

Talvez isso ajude a compreender a falta de coerência do ordenamento jurídico que carateriza esta matéria em Portugal. Expressões como "protecção de infra-estruturas criticas"[13], "protecção de pontos sensíveis"[14], "instalações críticas"[15],

12 *Vide* DL n.º 73/2012 de 26 de março.

13 *Cfr.* DL n.º 62/2011 de 09 de maio (doravante DL n.º 62/2011).

14 *Cfr.* artigo 3º, n.º 1, alínea j), da Lei n.º 63/2007 de 06 de novembro (Lei orgânica da GNR).

"serviços vitais nacionais"[16], "infraestruturas de informação críticas"[17], "ativos estratégicos essenciais"[18] ou "infraestruturas essenciais"[19] encontram-se pulverizadas por mais de uma dúzia de diplomas legais, e quase todos produzidos nos últimos cinco anos[20].

À primeira vista, esta insistência sugere uma cuidadosa atenção do legislador para a matéria de proteção de IC. Todavia, uma análise mais profunda evidencia outra realidade, que nos parece preocupante:

- Utilização de conceitos e definições vagas, não uniformes, e sem sustentação doutrinária[21] [22];
- Inexistência de referências que estabeleçam pontes jurídicas entre os diplomas.
- Diluição das responsabilidades dos vários atores, já que uma análise transversal não permite discernir, para além da dúvida razoável, quem faz o quê.

Em suma, é patente a ausência de uma visão estratégica suficientemente coerente e consolidada, e parece até haver alguma desatenção na produção legislativa. Corre-se o risco de que um conceito "crítico" como é este, seja utilizado de forma leviana, por inúmeros organismos, ficando refém de interesses corporativos, que em nada beneficiam os desígnios nacionais.

---

15 *Cfr.* artigo 3º, n.º 2, alínea j), da Lei n.º 53/2007 de 31 de agosto (Lei orgânica da PSP).

16 *Cfr.* RCM n.º 36/2015 de 12 junho (ENSC).

17 *Cfr.* RCM n.º 19/2013 de 05 de abril (CEDN).

18 *Cfr.* artigo 1º do DL n.º 138/2014 de 15 de setembro (Regime de Salvaguarda dos Ativos Estratégicos Essenciais).

19 *Cfr.* RCM n.º 7-A/2015 de 20 de fevereiro (ENCT).

20 *Vide* Apêndice G.

21 *Vide* subcapítulo 2.2.3.2 – Classificação de infraestrutura crítica – O que proteger.

22 Nota do Autor: Com que critérios e metodologias são classificadas as «infraestruturas essenciais» da Estratégia Nacional de Combate ao Terrorismo? Será com as mesmas metodologias do DL n.º 62/2011 de 09 de maio? Ou as infraestruturas críticas do primeiro diploma são diferentes das mencionadas no segundo? Se são diferentes, quais deverão constar no Plano Nacional de Proteção de infraestruturas críticas a que alude o Conceito Estratégico de Defesa Nacional? E este plano nacional, como se articula com o Plano de Ação para a Proteção de Aumento da Resiliência das IC, previsto na Estratégia Nacional de Combate ao Terrorismo?

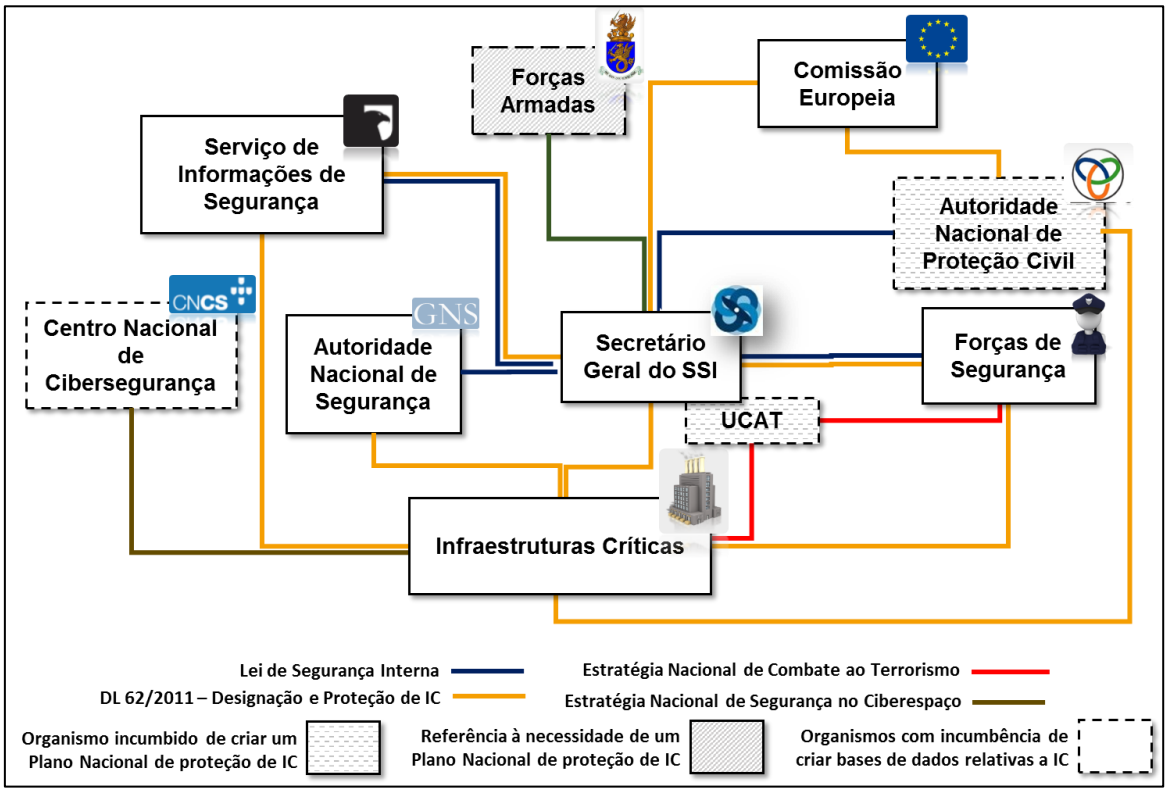


Figura 2: Proteção de IC - relações entre atores, de acordo com o quadro jurídico vigente.
Fonte: Elaboração própria do autor

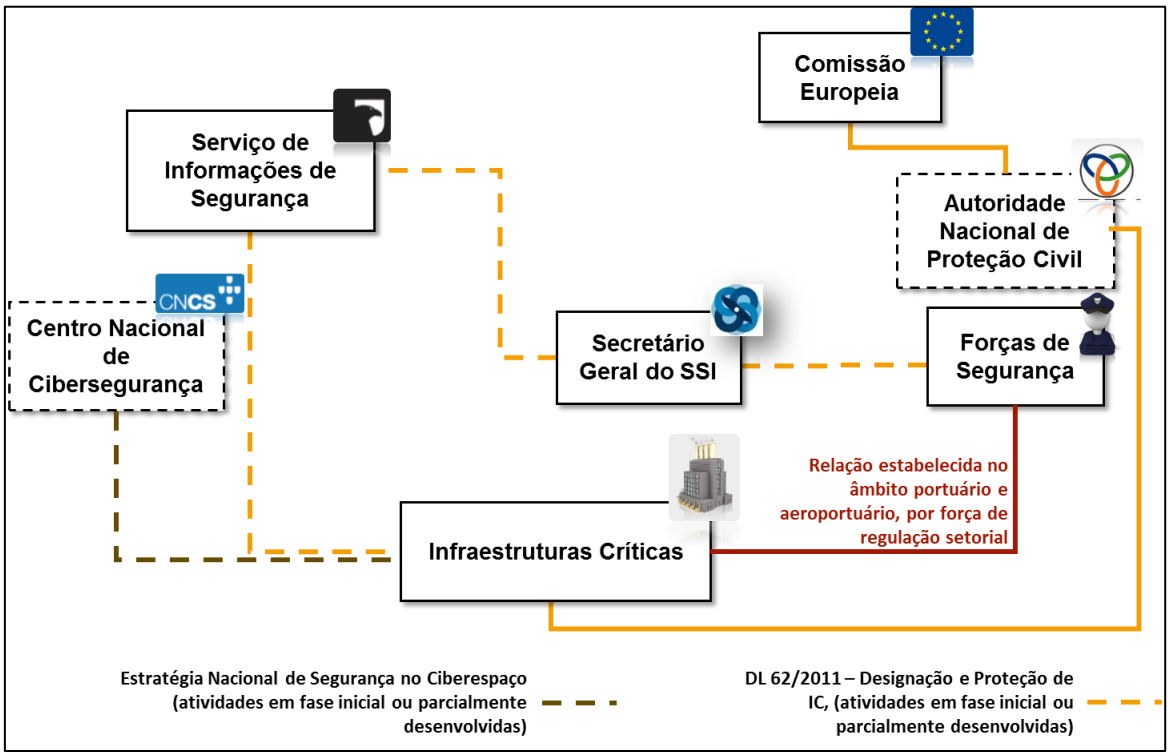


Figura 3: Proteção de IC – relações entre atores, de acordo com o quadro jurídico e com competências efetivamente exercidas.
Fonte: Elaboração própria do autor

2.2.2.1. O DL n.º 62/2011 de 9 de maio

Pese embora o trabalho previamente elaborado pela CNPCE, conforme já referido no subcapítulo anterior, "…a proteção de IC ganhou sustento legal em Portugal quando, em 9 de maio de 2011, foi publicado o DL n.º 62/2011, transpondo para o quadro jurídico nacional a Diretiva 2008/114/CE, publicada no final de 2008"[23].

Refira-se que esta transposição, embora tenha sido operada em tempo útil (o que não aconteceu em todos os EM), pouco mais é do que a tradução da Diretiva, com um nível mínimo de adaptação ao contexto nacional.

Para além da estabilização, tão necessária, do conceito de IC, relevam neste diploma os seguintes aspetos:

- A definição de procedimentos de identificação e designação de IC, ambos a cargo da ANPC (por extinção do CNPCE)[24];
- A elaboração de planos de segurança, referentes a cada IC. Estes planos, da responsabilidade do operador, descrevem os elementos críticos da infraestrutura, as potenciais ameaças e as medidas de segurança a adotar[25];
- A elaboração de Planos de Segurança e Proteção Exterior (PSPE) da responsabilidade da força de segurança territorialmente competente[26];
- A criação da figura do Agente de Ligação de Segurança (ALS) como ponto de contacto entre o proprietário e/ou operador da IC e o Secretário-Geral do SSI[27];
- A incumbência por parte do Estado de avaliar a ameaça em relação aos vários subsetores[28] [29] de IC[30];

---

[23] *Vide* Diretiva 2008/114/CE de 08 de dezembro. *Identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção*. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114&from=PT [em linha] [consulta em 06 de junho de 2016].

[24] *Vide.* artigos 4º, 5º e 6º do DL n.º 62/2011.

[25] *Vide.* artigo 10º, n.º 1 do DL n.º 62/2011.

[26] *Vide.* artigo 10º, n.º 5 do DL n.º 62/2011.

[27] *Vide.* artigo 11º do DL n.º 62/2011.

- A proteção de informação sensível[31].

Apesar destas inovações, é no seu artigo 13º, n.º 1 (Apoio às IC europeias)[32], que reside, a nosso ver, o ponto mais importante do articulado, mas também aquele que, como o estudo de campo se encarregará de demonstrar, menos tem sido concretizado:

> "…As entidades competentes devem apoiar os proprietários ou os operadores das IC europeias 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 de IC".

2.2.3. AS INFRAESTRUTURAS CRÍTICAS NACIONAIS

2.2.3.1. Definição de infraestrutura crítica

Não obstante se encontrar generalizado o termo "infraestrutura crítica" (aspas do autor), inexiste uma definição doutrinária única e mundialmente aceite. Em Portugal, em linha com o critério de funcionalidade[33] adotado quer pela OTAN quer pela UE, estabilizou-se no já citado DL n.º 62/2011 a seguinte definição de 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

[28] São subsetores da Energia: infraestruturas e instalações de produção e de transporte de eletricidade; infraestruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos; infraestruturas de produção, refinação, tratamento, armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido (GPL).

[29] São subsetores dos Transportes: transportes rodoviários; transportes ferroviários; transportes aéreos; transportes por vias navegáveis interiores; transportes marítimos, incluindo de curta distância, e portos.

[30] *Vide* artigo 12º do DL n.º 62/2011.

[31] *Vide* artigo 14º do DL n.º 62/2011.

[32] Por força do artigo 17º, e conforme já constatado, aplica-se também às IC nacionais.

[33] Em contraposição com critérios pontualmente utilizados noutros países como os *Crowded Places*, ou impactos psicológicos.

perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções"[34].

2.2.3.2. Classificação de infraestrutura crítica – O que proteger

Tendo por base a definição nacional de «infraestrutura crítica», o CNPCE, em colaboração com o Instituto Superior Técnico, desenvolveu o algoritmo *Adpa*, destinado a construir um indicador de criticidade para cada IC, que apoia a classificação da sua importância relativa para o País. Este algoritmo adequa-se a cenários de informação deficitária e, se aplicado "…em complemento com Macbeth, permite extrair a máxima utilidade da disponibilidade de "*Expert Opinion*"" (Pais & Gomes *apud* Soares & Antão, 2007, p. 71).

Desde 2006 até hoje, esta metodologia permitiu a identificação de 162 IC nacionais, que abrangem 22 operadores dos setores da Energia e dos Transportes.

2.2.4. A RELAÇÃO PÚBLICO-PRIVADO – A CHAVE DO SUCESSO

Com maior ou menor prevalência dependendo dos setores, o facto é que a maioria das IC é detida e operada por empresas do setor privado. Compreende-se que a responsabilidade de garantir a proteção de determinada IC caiba, em primeira linha, ao seu operador.

Porém é bom não esquecer que a lógica empresarial visa sobretudo a geração de lucros, não necessariamente o bem-estar social, e naturalmente esta lógica tem reflexos no processo de gestão do risco.

Assim, cabe ao Estado a "…responsabilidade social de proteger os seus cidadãos de riscos inaceitáveis" (Pais & Gomes *apud* Soares & Antão, 2007, p. 72), sendo irrelevante a natureza pública ou privada das fontes de perigo.

[34] *Cfr.* artigo 2º, alínea a), do DL n.º 62/2011.

Figura 4: Perspetivas sobre a gestão do risco em IC.
Fonte: Adaptado pelo autor: http://www.tno.nl/recipereport

O equilíbrio destes dois desígnios é a pedra angular das políticas de proteção de IC no contexto europeu e, provavelmente, o tema de discussão mais frequente entre especialistas.

A linha que gera mais consenso é a de que ambos os atores (Estado e operadores privados) devem empenhar-se na proteção de IC, embora com contributos de natureza distinta.

Aos operadores caberá a assunção de medidas de caráter setorial/local, de que são exemplos a implementação de medidas concretas de segurança, a preparação de planos operacionais que visem uma resposta específica para cada IC e a melhoria das condições de resiliência e continuidade de negócio, tendo em conta o serviço que prestam.

Ao Estado incumbirá a concretização de medidas que visem apoiar, coordenar, facilitar, regular e harmonizar[35] a proteção de IC, otimizando o investimento dos operadores, estas medidas podem ser de âmbito material como a

[35] É particularmente importante a função harmonizadora do Estado, tendo em conta a natureza sistémica e de "segurança interdependente" (aspas do autor) das IC, em que cada uma gera externalidades negativas que afetam as restantes. Não havendo uma intervenção harmonizadora do Estado os operadores tendem a adotar estratégias do tipo "MiniMax", bem descritas na Teoria de Jogos e, em especial, no "Dilema do Prisioneiro" (Disponível em: https://pt.wikipedia.org/wiki/Dilema_do_prisioneiro [em linha] [consulta em 08 de junho de 2016]).

disponibilização de equipamento para as forças de segurança, ou podem ser medidas de âmbito organizacional como a implementação de políticas, a produção de conhecimento especializado, ou o reforço de órgãos de coordenação, em especial no que concerne à sua massa crítica.

2.2.5. O PAPEL DO OPERADOR DE INFRAESTRUTURAS CRÍTICAS

O DL n.º 62/2011 determina aos operadores a adoção de determinadas medidas destinadas à proteção de IC. Destacamos a adoção de um plano de segurança, cuja elaboração obedece a critérios específicos, e a designação de um ALS, incumbido de fazer a ponte com o Estado, em particular com o SGSSI (através da FS territorialmente competente[36]).

No que respeita ao plano de segurança do operador que cada IC deve ter, importa referir que, previamente à entrada em vigor do DL n.º 62/2011, uma parte dos operadores já dispunha de planos de segurança, de contingência ou de emergência, desenvolvidos por iniciativa própria[37] ou por força da intervenção de reguladores e autoridades setoriais[38].

No entanto, é fundamental realçar que o plano de segurança do operador tem três caraterísticas que o distingue dos planos internos dos operadores:

- A sua estrutura única para todas as IC, independentemente do setor, possibilita a análise comparativa interpares, o que facilita a função harmonizadora do Estado;
- A informação de caráter mais genérico e orientada para o público externo (contatos de responsáveis de segurança ao nível local, cartas topográficas, entre outros) favorece o tratamento em plataformas tecnológicas[39], especialmente vocacionadas para salas de situação ou centros de crise;

[36] *Vide* artigo 10º, n.º 5, do DL n.º 62/2011.
[37] Alguns operadores de IC demonstram grande cultura de segurança.
[38] Os operadores dos subsetores Transportes aéreos – ANAC – e Transportes marítimos – DGRM.
[39] Esta hipótese, em Portugal, encontra-se numa fase de maturação, estando a ser estudada a viabilidade da sua operacionalização.

- Por fim, a distribuição destes planos abrange atores relevantes da administração pública (em especial as forças de segurança), ao contrário dos planos internos que, por definição, são do uso exclusivo da empresa.

Alguns dos operadores, em particular os de maior dimensão, contam com departamentos de segurança e qualidade, que executam metodologias de análise e gestão do risco. No entanto, e como já vimos, o seu trabalho foca-se essencialmente no contexto local, da proteção de determinada IC ou, na melhor das hipóteses, no sistema de IC do seu setor (abordagem setorial).

Estas metodologias, apesar de essenciais no contexto do operador, afiguram-se limitadas quando se colocam desafios de interdependência multissetorial, motivo que levou a Comissão Europeia a rever em 2013 a sua política, passando a encorajar uma abordagem através do "sistema de sistemas"[40].

Como nota final, é justo reconhecer que o grau de adesão e compromisso dos operadores portugueses se tem revelado muito satisfatório.

2.2.6. OS ORGANISMOS DO ESTADO E A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

2.2.6.1. O Secretário-Geral do Sistema de Segurança Interna

De entre os órgãos do Estado é ao SGSSI que estão acometidas as maiores responsabilidades na proteção de IC, o que faz sentido à luz da natureza interdisciplinar que está na sua génese: "…a decisão política de criação do SISI tem como objetivo otimizar e projetar, de forma planeada, as capacidades operacionais dos vários sistemas, entidades, órgãos e serviços cuja atividade seja relevante para garantir a ordem, segurança e tranquilidade públicas" (Fernandes, 2014, p. 58).

Ao contrário de outros órgãos e organismos que, como já referimos, focam a sua atividade num só patamar de atuação, o SSI "…é concebido segundo um modelo de geometria variável, visando garantir a segurança em níveis

[40] *Vide* Commission Staff Working Document – SWD 318 (2013), p. 7.

horizontalmente diferenciados, mas verticalmente articulados (o local, o nacional e o internacional).” (Fernandes, 2014, p. 58).

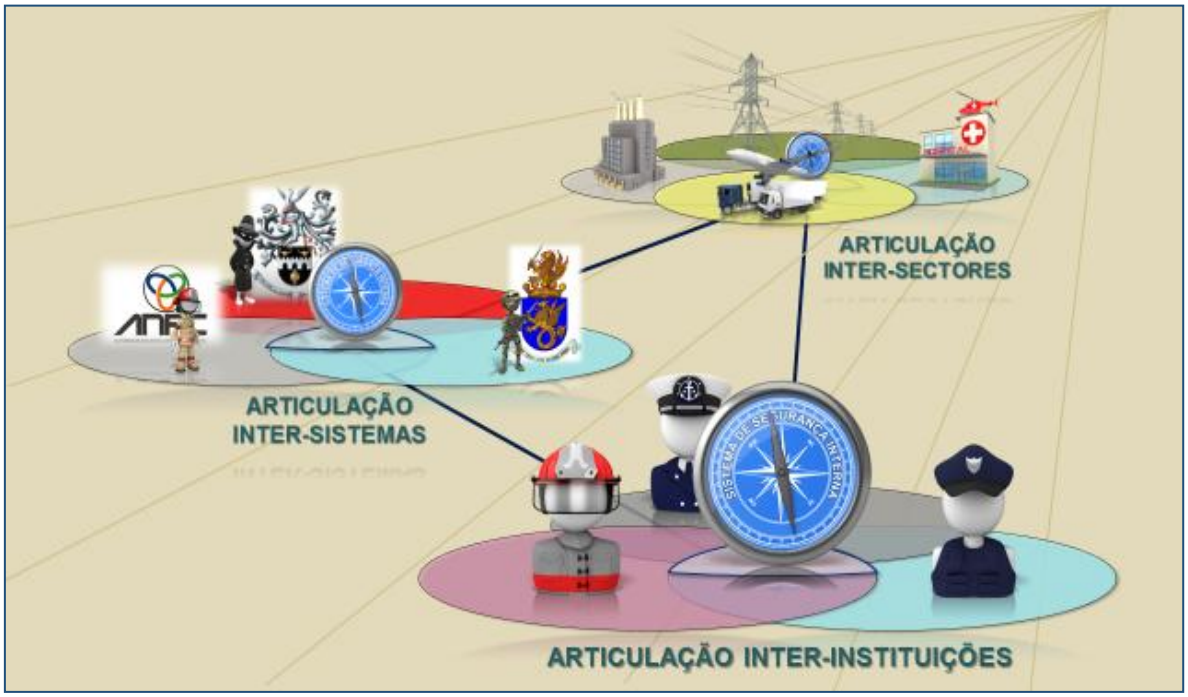


Figura 5: Representação da função de articulação do SGSSI em três patamares, no domínio da proteção de IC.
Fonte: Elaboração própria do autor.

É difícil selecionar as matérias específicas que conformam o mandato do SGSSI em matéria de proteção de IC, separando-as das suas competências de caráter genérico. Isto por ser justamente nos seus poderes alargados de coordenação, articulação e enquadramento que este órgão do SSI se diferencia dos restantes organismos, cujo mandato é geralmente mais operativo e setorial.

Nas figuras seguintes procuramos enumerar as competências mais relevantes que estão acometidas ao SGSSI em matéria de proteção de IC[41].

[41] Não é feita referência ao PCCCOFSS, por impedimento que decorre da sua classificação de segurança.

	DL 62/2011, de 09 de maio
Artigo 10º n.º 4	Validação do PSO
Artigo 11º n.º 1	Articulação entre ALS e SGSSI
Artigo 11º n.º 2	Troca de informações relativas a riscos e ameaças
Artigo 12º n.º 1	Avaliação de Ameaça aos subsectores
Artigo 12º n.º 2	Relatório bienal de dados para a Comissão Europeia
Artigo 13º n.º 1	Apoiar os operadores facultando acesso às melhores práticas e metodologias, formação
Artigo 15º n.º 2	Ponto de contacto CE no plano da segurança de ICE
	LSI (alterada pela Lei n.º 59/2015 de 24 de junho)
Artigo 16º n.º 2 b)	Coordenar ações conjuntas de formação, aperfeiçoamento e treino das forças e dos serviços de segurança;
Artigo 16º n.º 2 c)	Reforçar a colaboração entre todas as forças e os serviços de segurança, garantindo o seu acesso às informações necessárias
Artigo 16º n.º 2 d)	Garantir a coordenação entre as forças e os serviços de segurança e os serviços de emergência médica, segurança rodoviária e transporte de e segurança ambiental, no âmbito da definição e execução de planos de segurança e gestão de crises
Artigo 18º n.º 2 b)	Articulação das FSS necessários à gestão de incidentes tático policiais graves
Artigo 19º n.º 1	Em situações extraordinárias, determinadas pelo PM após comunicação fundamentada ao PR, de ataques terroristas ou de acidentes graves ou catástrofes que requeiram a intervenção conjunta e combinada de diferentes FSS e, eventualmente, do SIOP, estes são colocados na dependência operacional do SGSSI, através dos seus dirigentes máximos.
Artigo 35º	As FA colaboram em matéria de SI nos termos da Constituição e da lei, competindo ao SGSSI e ao CEMGFA assegurarem entre si a articulação operacional.
	Estratégia Nacional de Combate ao Terrorismo (RCM n.º 7-A/2015)
c)	Fortalecer a segurança dos alvos prioritários, reduzindo quer a sua vulnerabilidade, quer o impacto de potenciais ameaças terroristas. A proteção concretiza-se no aumento da segurança das…infraestruturas críticas, nacionais e ou europeias.
c) vi)	Desenvolver um registo central de identificação de infraestruturas criticas, em todos os setores de atividade económica e social, e prover à sua atualização;
c) vii)	Desenvolver o Plano de Ação para a Proteção de Aumento da Resiliência das Infraestruturas Críticas nacionais e europeias, com os respetivos PSO e planos de segurança externos da responsabilidade das FSS e da ANPC
c) x)	Avaliar periodicamente as vulnerabilidades resultantes de infraestruturas essenciais, nacionais e europeias, para transportes e energia,
c) xi)	avaliar as vulnerabilidades dos sistemas de informação críticos e manter e acompanhar a adoção das medidas de correção face a ciberataques;
6 A) i)	A cooperação entre as FA e as FSS é aprofundada em situações de intervenção perante agressões terroristas, de acordo com o Plano de Articulação e Operacional que contempla medidas de coordenação e a interoperabilidade de sistemas de equipamentos, serviços de proteção civil, emergência médica e FA
6 A) ii)	De acordo com o PNPIC, atribuindo ainda especial atenção à vigilância e ao controlo das acessibilidades marítima, aérea e terrestre ao território nacional.

Figuras 6: Competências (diretas e indiretas) do SGSSI na proteção de IC.
Fonte: Elaboração própria do autor.

Um bom exemplo da articulação que poderá ser implementada ao nível do SGSSI é a disponibilização de informação sobre os níveis de ameaça aos operadores de IC, tendo em vista o acionamento das medidas protetivas inscritas nos seus planos de segurança.

Esta prática é adotada em Espanha pelo CNPCI, que divulga o nível de ameaça em vigor a cada momento[42].

Figura 7: Informação sobre o nível de ameaça.
Fonte: Sítio do CNPIC.

Não obstante todo o suporte legal, o trabalho desenvolvido pelo SGSSI encontra-se ainda numa fase incipiente:

- Desde 2012 foram elaborados (em colaboração com a ANPC) conteúdos de referência, para apoio aos operadores na construção dos seus planos de segurança.

[42] Disponível em: http://www.cnpic.es/ [em linha] [consulta em 13 de junho de 2016].

- Muito recentemente, foi criado no âmbito do SGSSI um grupo de trabalho com representantes das forças e serviços de segurança, no sentido de ser coordenada a avaliação dos planos já enviados pelos operadores, e a harmonização da emissão de pareceres.
- Adicionalmente, tem sido desenvolvido um esforço para a criação de uma base de dados para registo de alguma informação contida nesses planos.

O facto de não haver profissionais que se dediquem em exclusivo a esta matéria constitui um compreensível obstáculo ao desejável desenvolvimento destes projetos, ou de outros que pudessem ser desencadeados.

2.2.6.2. A Autoridade Nacional de Proteção Civil

A ANPC tem um papel de enorme importância, desde logo porque é a única entidade responsável pela identificação e designação de IC[43].

Adicionalmente, cabe-lhe toda a componente de *safety*, designadamente a emissão de pareceres sobre os planos de segurança do operador[44].

Finalmente, importa fazer uma referência ao trabalho do ponto de contacto europeu para a proteção de IC no plano da designação das IC europeias[45], e ao seu notável papel na produção de doutrina. O trabalho que o Estado desenvolveu até ao momento, ainda que limitado contou sempre com a experiência e, em muitos casos, a orientação, deste ponto de contacto[46].

2.2.6.3. As forças de segurança

A ideia de ordem pública é indissociável da disponibilização de serviços vitais à população, por isso "…as forças e serviços de segurança estarão sempre na primeira linha de intervenção, quer na tomada de medidas preventivas quer na resposta a situações anómalas" (Rodrigues, 2008 p. 18).

[43] *Vide* artigos 4º, 5º e 6º do DL n.º 62/2011.
[44] *Vide* artigo 10º, n.º 4, do DL n.º 62/2011.
[45] *Vide* artigo 14º, do DL n.º 62/2011.
[46] A Dra. Isabel Pais, responsável pela área da proteção de IC da ANPC, é o ponto de contacto junto da Comissão Europeia.

Esta é aliás uma missão que decorre das respetivas leis orgânicas[47] [48].

Importa, no entanto, sinalizar que a intervenção das Polícias em determinados ambientes tem especificidades que, não sendo respeitadas, podem comprometer o objetivo da intervenção e a própria segurança dos intervenientes. Dito de outra forma, os procedimentos e a doutrina geral de empenhamento policial não se pode aplicar, sem a necessária adaptação, aos ambientes próprios (e geralmente perigosos) que caraterizam as IC.

Neste pressuposto, faz sentido a exigência que é feita às Polícias, de elaboração de um "Plano de Segurança e Proteção Exterior", que se articule com os planos do próprio operador[49], e que garantem um nível mínimo de preparação e conhecimento, em caso destas serem chamadas a intervir.

Como referência final à importância deste "princípio da especialidade" regista-se a criação da *Airpol* e da *Railpol* - redes europeias de partilha de informação e doutrina, que agrupam corpos de polícia especializada em segurança aeroportuária e de transportes ferroviários, respetivamente[50].

Já noutro domínio, o da inteligência, as forças de segurança têm como missão contribuir (juntamente com o SIS) para a avaliação das ameaças que se colocam aos subsetores das IC[51].

Igualmente importante é o papel das forças de segurança na emissão dos pareceres para a componente *security* dos planos de segurança do operador[52], bem como a fiscalização das atividades de segurança privada (muitas vezes exercida em IC).

Finalmente, cabe-lhes representar o SGSSI junto do agente de ligação de segurança de cada IC, o que acentua o caráter local da sua atuação ou, se preferirmos, de descentralização das políticas de proteção superiormente definidas.

---

47 *Vide* artigo 3º, n.º 2, alínea j), da Lei orgânica da PSP.

48 *Cfr.* artigo 3º, n.º 1, alínea j), da Lei orgânica da GNR.

49 *Vide* artigo 10º, n,º 4, do DL n.º 62/2011.

50 A PSP é membro da *Airpol*, através das suas cinco Divisões de Segurança Aeroportuária (Açores, Madeira, Lisboa Porto e Faro), sendo que a GNR está representada na *Railpol*.

51 *Vide* artigo 12º do DL n.º 62/2011.

52 *Vide* artigo 10º, n.º 4, do DL n.º 62/2011.

A realidade, no entanto, não acompanha a previsão legal. Com exceção do transporte marítimo e aéreo (setores que tradicionalmente são altamente regulados do ponto de vista do *security*) nem todos os comandantes locais conhecem as IC existentes na sua área de responsabilidade, e são poucos os que já as visitaram ou tiveram contactos com o respetivo agente de ligação. Como se depreende, também não foram preparados quaisquer planos de segurança externos que enquadrem as ações da polícia na prevenção ou de resposta a incidentes.

2.2.6.4. O Serviço de Informações de Segurança

Ao SIS cabem dois papéis relacionados com a proteção de IC: o primeiro, mais genérico, prende-se com a "…produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo e da espionagem"[53].

O segundo, mais concreto, decorre diretamente do artigo 12º do DL n.º 62/2011, e passa pelo contributo que este organismo presta ao SGSSI na avaliação das ameaças em relação aos subsetores de IC e nas ações de formação setoriais que desencadeia junto dos seus operadores.

A este propósito, é pertinente a menção ao projeto *Kritica*, desenvolvido desde 2013, e cujo objetivo passa por produzir avaliações de ameaça setoriais e por sensibilizar os operadores, através de ações de formação.

2.2.6.5. A Autoridade Nacional de Segurança

No âmbito das suas atribuições incumbe à ANS "…credenciar entidades públicas e privadas para o exercício de atividades industriais, tecnológicas e de investigação, quando tal seja exigido por disposição legal ou regulamentar"[54]. Tal parece ser o caso, no que toca a alguma da informação relacionada com as IC e a sua proteção.

Efetivamente, o DL n.º 62/2011 dispõe: "…os factos respeitantes a uma IC que, se divulgados, poderiam ser utilizados para planear e agir com o objetivo de

[53] *Cfr.* artigo 21º da Lei Orgânica n.º 4/2014 de 13 de agosto (quinta alteração à Lei n.º 30/84 de 5 de setembro, que aprova a Lei Quadro do SIRP.

[54] *Cfr.* artigo 2º, n.º 2, alínea i), do DL n.º 3/2012 de 16 de janeiro (Lei orgânica do GNS).

provocar a perturbação ou destruição das IC"[55] são considerados "informações sensíveis"[56]. E acrescenta que qualquer pessoa incumbida de tratar de informação classificada relativa à proteção de IC "…é sujeita a um procedimento de habilitação de segurança a ser concedido pela ANS"[57].

2.2.6.6. O Centro Nacional de Cibersegurança

A cibersegurança, no contexto das IC, é uma matéria que tem ganho relevância. Prevê-se que esta tendência se acentue com a progressiva transição do atual modelo industrial, em que a intervenção humana ainda é indispensável, para modelos cada vez mais assentes na automatização (e.g. o desenvolvimento dos atuais protocolos *Scada* e com a implementação de *Smartgrids*).

Embora o CNCS seja um organismo recém-criado, a maioria[58] as atividades de proteção de IC que tenham por objetivo "…fortalecer e garantir a segurança do ciberespaço das IC e dos serviços vitais de informação"[59] serão conduzidas ou orientadas por este organismo, conforme estipula a recente Estratégia Nacional de Segurança do Ciberespaço, que dedica um vasto conjunto de artigos à componente de cibersegurança das IC[60].

No entanto é bom não esquecer que a segurança deve ser considerada no seu todo, de resto como recomenda a Comissão Europeia (abordagem holística ou *all hazards aproach*), motivo pelo qual a atuação no domínio *ciber*, deve ser integrada e articulada com os restantes domínios

55 *Cfr.* artigo 14º, n.º 1, do DL n.º 62/2011.
56 *Ibidem*.
57 *Cfr.* artigo 14º, n.º 2, do DL n.º 62/2011.
58 Diz-se "maioria" porque à UCAT também são atribuídas competências semelhantes, por via do artigo 4.º, alínea c), do ponto VIII, (entre outros), da RCM n.º 7-A/2015
59 *Cfr.* anexo n.º 3 c) da RCM n.º 36/2015.
60 *Vide* Apêndice G.

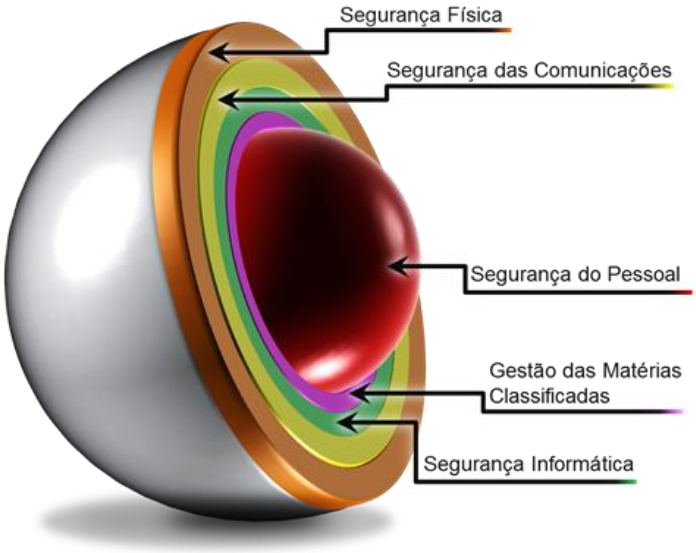


Figura 8: Domínios da segurança.
Fonte: Elaboração própria do autor.

2.2.6.7. As Forças Armadas

Conquanto não haja referências diretas a uma missão das FA no domínio da proteção de IC, o CEDN refere, no seu capítulo VI que "…reveste grande acuidade a implementação de um Plano Nacional de Proteção de IC"[61].

Sendo certo que concordamos com a construção de um plano, parece-nos que a sua origem deve estar no setor da segurança e não no da defesa. Isto não menorizando o papel que as FA podem ter, nas situações constitucionalmente consagradas dos estados de exceção.

Aliás, somos obrigados a reconhecer que a nossa pesquisa referenciou alguns países europeus, em especial na região do Báltico, que têm os seus planos de proteção de IC integrados em estratégias abrangentes, que incluem segurança, defesa e proteção civil[62].

[61] *Cfr.* ponto 1.4.2. (Responder às ameaças e riscos) – 1.4 Adequar as políticas de segurança e defesa nacional ao ambiente estratégico) – do capítulo VI (Conceito de ação estratégica nacional) da RCM n.º 19/2013 de 05 de abril (CEDN).
[62] *Vide* Apêndice H.

2.3. BOAS PRÁTICAS E RECOMENDAÇÕES INTERNACIONAIS

Tendo como ponto de partida os objetivos formulados no capítulo 1.3 (Problemática da Investigação), efetuámos uma revisão da literatura sobre as melhores práticas internacionais em dois patamares distintos:

- O das grandes opções estratégicas;
- O dos instrumentos e medidas de proteção.

As grandes opções para a fundação de um plano nacional devem ter em conta, essencialmente, três aspetos (todos em matéria de IC):

- O grau de relação que já exista entre o Estado e o setor privado;
- A natureza dessa relação (um papel do Estado mais ou menos intervencionista, um envolvimento do setor privado mais obrigatório ou mais voluntário);
- O estado de maturidade do país e de todos os atores, tendo em conta o trabalho previamente desenvolvido.

Com base no estudo de campo e na revisão da literatura, considerámos para Portugal os seguintes parâmetros:

- Apesar de pouco desenvolvido e testado, existe um **grau razoável** de potencial de **cooperação** entre o Estado e os operadores de IC. Este potencial resulta em parte das idiossincrasias culturais do nosso povo[63], designadamente a facilidade de estabelecer pontes e relações, e também da confiança generalizada que a sociedade deposita nos organismos da administração pública, em especial na área da segurança e proteção civil;
- No contexto da proteção de IC tem tido algum sucesso, no nosso país, uma **matriz** de relacionamento público-privado tendencialmente

[63] Refira-se, no entanto, que a aquisição de cotas importantes por parte de capitais estrangeiros (especialmente por grupos económicos oriundos de países terceiros) poderá prejudicar estas idiossincrasias. A este respeito recomenda-se a leitura do DL n.º 138/2014 de 15 de setembro).

voluntária/cooperativa embora com considerável enquadramento jurídico de referência (não sancionatório);

- Quanto à **maturidade** dos atores e do país, achamos que é **baixa.** Para além da identificação de IC, que obrigou a alguns contatos iniciais com os operadores, e da elaboração de planos de segurança, pouco trabalho específico foi desenvolvido.

Definidas as forças que moldam a relação público-privado, os restantes princípios essenciais de uma política de proteção de IC constam: uma visão e uma estratégia largamente partilhadas e difundidas, suportadas por um forte comprometimento político; e o desenvolvimento de doutrina, boas práticas, formação, investigação (I&D) e partilha de informação;

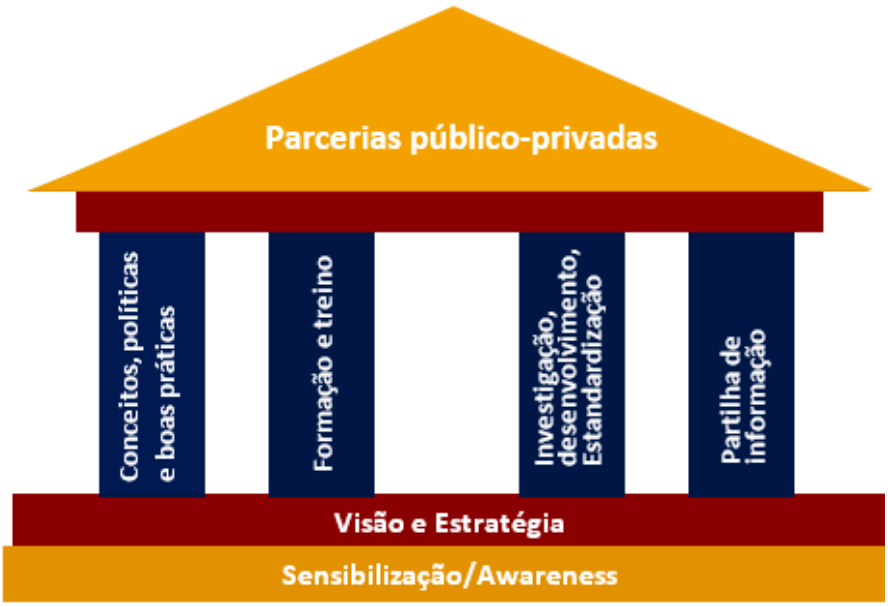


Figura 9: Pilares de uma estratégia de proteção de IC.
Fonte: Adaptado pelo autor: CESP *Task Force Report*, p. 75.

2.3.1. IMPLEMENTAÇÃO DE PLANOS NACIONAIS DE PROTEÇÃO DE IC

Na última década grande parte dos países do mundo ocidental envolveu-se na preparação e implementação de planos nacionais de proteção de IC[64].

De uma forma geral, os planos nacionais abordam os seguintes pontos:

64 *Vide* Apêndice H.

- Identificação de IC (inclui normas técnicas de identificação e procedimentos de notificação aos operadores);
- Identificação e estudo de interdependências;
- Definição de responsabilidades, deveres e obrigações dos operadores;
- Indicação das atividades do Estado (onde, para além da enumeração dos vários organismos chamados a participar no plano, por norma é mencionada a criação de organismos dedicados à proteção de IC;
- Previsão das modalidades de cooperação entre o Estado e os operadores de IC (e.g. procedimentos para a partilha de informação ou princípios gerais de colaboração);
- Políticas de gestão do risco (e.g. a decisão de incluir riscos naturais, ou ciberameaças[65] ou, pelo contrário, a segregação de matérias);
- Políticas de gestão de crises (por exemplo: normas e protocolos de atuação em caso de incidente que afete IC);
- Indicação sobre a articulação com outros planos ou estratégias de nível setorial ou nacional (estratégias de segurança, cibersegurança, defesa nacional ou de gestão de crises);
- Modalidades de financiamento (através do Orçamento Geral do Estado ou de taxas aplicáveis aos operadores ou, ainda, por comparticipação de ambos).

Em função da linha política escolhida, estes planos nacionais podem assumir uma matriz intervencionista, quando à Administração é atribuído maior grau de participação na implementação das medidas de proteção de IC, ou uma matriz pouco intervencionista, quando lhe estão apenas reservadas funções de *policy-making*.

O Reino Unido é um bom exemplo da linha intervencionista, onde a administração pública, através de vários organismos (em especial o *Center for*

[65] A já referida "abordagem holística" (aspas do autor).

the Protecion of National Infraestructure[66]), acautela uma forte presença em todos os domínios da proteção de IC, desde a identificação até ao desenho de medidas protetivas, passando pela formação prestada aos operadores.

Um exemplo da linha pouco intervencionista será a França, que tem um organismo de preparação de políticas de proteção (*policy-making*), cabendo quase exclusivamente aos operadores a operacionalização das medidas, e até a proposta de quais das suas infraestruturas devem ser consideradas críticas.

Outro aspeto a ter em conta na escolha de políticas de proteção é o caráter tendencialmente obrigatório ou tendencialmente voluntário dessas políticas.

Alguns países, como a Estónia ou a Suíça, optaram por legislar de forma intensa os aspetos de relação entre o Estado e os operadores. Nestes casos, os operadores são obrigados a cumprir com as disposições legais sob pena de sanções económicas ou limitações à sua atividade.

Em contrapartida, o Reino Unido optou por aprovar legislação que apela à participação voluntária dos atores do setor privado.

Não obstante, cumpre referir que, para o sucesso deste modelo cooperativo, é necessário que o Estado crie condições apelativas para os operadores, que facilmente aderem se percecionarem o seu envolvimento como uma mais-valia empresarial. A constituição de comités de aconselhamento estratégico, onde os operadores tenham assento (por exemplo, o SOVI[67] na Holanda), ou a criação de organismos do Estado altamente especializados (como é o caso, em Espanha, do CNPIC) funcionam como um magneto para o interesse do setor privado.

2.3.2. ORGANISMOS RESPONSÁVEIS PELA CONDUÇÃO DE POLÍTICAS DE PROTEÇÃO DE IC

Por força da complexidade, do vasto espetro de atividades, e do elevado número de atores que são chamados a participar na implementação de

[66] *Vide* sítio do CPNI. Disponível em: http://www.cpni.gov.uk/ [em linha] [consulta em 13 de junho de 2016]

[67] Criado em 2006, trata-se de um Grupo de aconselhamento estratégico junto do Governo holandês, que integra representantes do setor público e privado.

políticas de proteção de IC, a larga maioria dos países têm optado pela criação de organismos dedicados.

A dimensão destes organismos está diretamente relacionada com o grau de intervenção do Estado, bem como do universo de IC a proteger.

Tendo em conta a transversalidade de atores necessários à implementação de políticas de proteção de IC, estes organismos dependem, na maior parte dos casos, diretamente do Primeiro-Ministro[68] ou do Ministro do Interior[69].

A este propósito, a Comissão Europeia recomenda a criação de um organismo de proteção de IC, mandatado para lidar com as várias dimensões (proteção *security* [incluindo cibersegurança] e *safety*)[70].

2.3.3. AS ATIVIDADES QUE VISAM A PROTEÇÃO DE IC

As melhores políticas de proteção de IC incluem as atividades a desenvolver, quer pelo organismo de proteção de IC, quer por outras entidades. Neste trabalho, destacaremos apenas a organização de *workshops*, a estandardização, a partilha de informação e a implementação de plataformas de informação.

2.3.3.1. Organização de *workshops*

A organização de *workshops* é uma prática muito utilizada na Holanda.

As sessões podem envolver operadores, responsáveis setoriais e organismos do Estado, e apresentam, como principais vantagens, a facilidade de implementação, os baixos custos e a aproximação dos vários atores.

Muitos operadores não têm conhecimento suficiente sobre as interdependências das suas IC estabelecem com outras[71]. A realização de *workshops*, geralmente organizados e moderados pelo organismo nacional de

[68] França é um exemplo.
[69] Como é o caso de Espanha.
[70] *Vide* CEPS Task Force Report (2010, p. 48). *Protecting critical infrastructure in the EU*. Disponível em: https://www.ceps.eu/publications/protecting-critical-infrastructure-eu [em linha] [consulta em 13 de junho de 2016].
[71] *Idem*, p. 33.

proteção de IC, é apontada como uma das formas mais eficientes de preencher esse vazio, bem como de partilhar boas práticas no domínio da proteção.

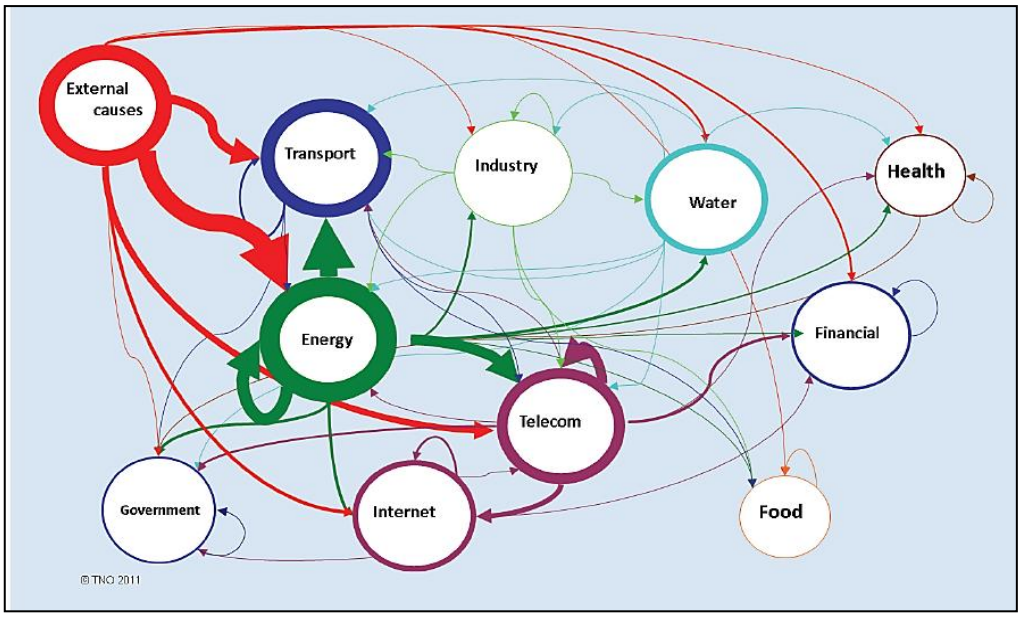


Figura 10: Perturbações em IC europeias entre 2003 e 2011.
Fonte: RECIPE[72], p. 31.
Nota: A espessura dos contornos demonstra o número de ocorrências e a expressão das externalidades negativas (interdependências)

2.3.3.2. Estandardização

A criação de taxonomia específica para a gestão do risco em IC (e particularmente em sistemas de IC), foi apontada como uma necessidade no relatório da *Task Force* do CEPS. Embora o relatório se debruce sobre o contexto europeu, temos de reconhecer que não existem em Portugal métricas próprias, ou sequer adaptadas, para fenómenos de impacto em sistemas de IC. Tão pouco conhecemos recomendações sobre que metodologias devem ser utilizadas pelos operadores.

As métricas utilizadas sectorialmente não satisfazem o "sistema de sistemas" (aspas do autor), sendo que a ferramenta mais aproximada de que dispomos (no sentido em que é customizada) é o algoritmo *Adpa*, que, todavia, foi desenvolvido com o propósito específico de identificação de IC, e não de avaliar a ameaça.

[72] Disponível em: http://repository.tudelft.nl/view/tno/uuid%3A29f15365-8885-4278-82fe-996567858ae9/ [em linha] [consulta em 13 de junho de 2016].

2.3.3.3. Partilha de informação sobre ameaças e vulnerabilidades

A informação sobre ameaças de natureza humana e deliberada é altamente valorizada no âmbito da proteção de IC, o que facilmente se entende à luz das teorias de gestão do risco: para aplicarmos medidas protetivas temos de saber do que nos estamos a proteger.

No Reino Unido o CPNI assume-se como verdadeiro facilitador para a partilha de informação entre organismos do setor público (FS, Serviços de inteligência, reguladores setoriais) e os operadores.

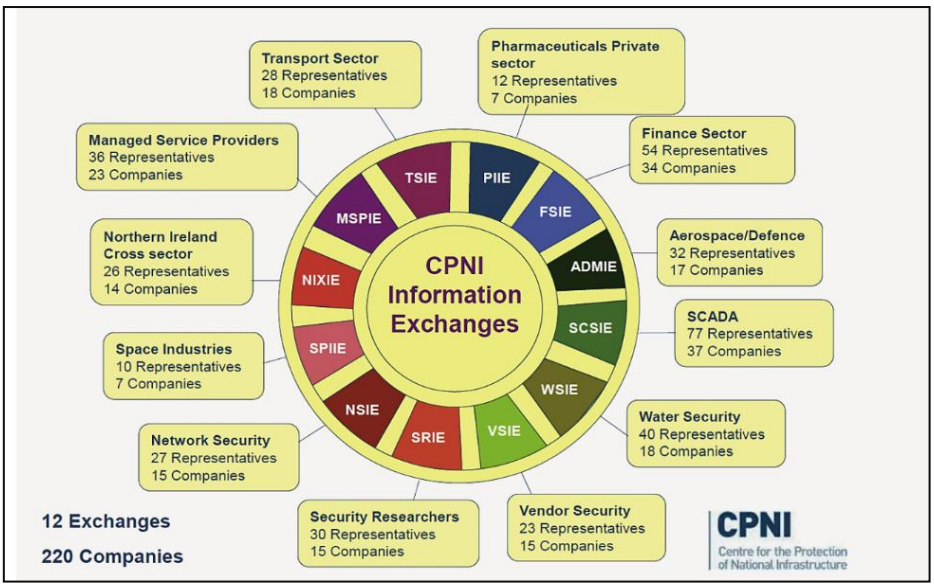


Figura 11: Modelo de partilha de informação do CPNI - Reino Unido.
Fonte: RECIPE p. 55

Esta prática oferece três vantagens: desde logo, os operadores aumentam o seu conhecimento sobre ameaças que se colocam às suas IC e ficam em melhores condições para aplicar medidas de segurança (gestão do risco); em segunda linha, o Estado obtém informação sobre as vulnerabilidades das IC e sobre o impacto que determinados eventos possam causar; e, por último, fortalece-se a confiança entre as partes envolvidas.

A partilha de informação que seja alvo de classificação de segurança obedece a regras e protocolos, por forma a criar confiança nos intervenientes.

O aspeto essencial, na construção de uma política de proteção de IC, no que respeita à partilha de informação, é criar consenso sobre o que partilhar, quem deve partilhar, quando e como. Nos EUA o plano nacional de proteção de IC

aborda estas quatro dimensões, vinculando todos os atores à necessidade de partilhar informação.

MODELO DE PARTILHA DE INFORMAÇÃO			
O quê	**Quem**	**Quando**	**Como**
Governo: • Informação sobre ameaças • Avisos • recomendações **Setor privado:** • Vulnerabilidades • Soluções • Avisos • Consultoria	• Serviços de informações • Forças de Segurança • Operadores de IC • Parcerias/ associações de coordenação (a todos os níveis)	**Antes do evento** • Consultoria • Avisos **Durante e depois do evento** • Passos para a mitigação e recuperação, • Coordenação de recursos	• Uso de PKI (public key infrastructure) • Politicas de segurança fortes (com penalizações por má utilização) • Tem de proteger operadores e administração

Figura 12: Modelo de partilha de informação dos EUA.
Fonte: Adaptado pelo autor: CESP *Task Force Report*, p. 77.

2.3.3.4. Criação de plataformas de centralização de informação

Os vários domínios de conhecimento convocados para a proteçao de IC geram um volume de informação que não se compadece com o tratamento analógico. Esta informação, quando tratada ao nível central de um órgão de coordenação, implica a utilização de bases de dados, sistemas de informação geográfica (SIG) e, idealmente, programas preditivos, com modulação de cenários e de análise de riscos.

A Comissão Europeia tem vindo a financiar projetos que visam o desenvolvimento de atividades deste tipo. Os EUA[73], a Suécia e a Finlândia[74] figuram entre os países que mais têm apostado estas ferramentas.

[73] *Vide* sítio da *Homeland Security*. *Infrastructure Information Collection Division*. Disponível em: https://www.dhs.gov/about-infrastructure-information-collection-division [em linha] [consulta em 13 de junho de 2016].
[74] *Vide* RECIPE (2011, p. 30). Disponível em: http://repository.tudelft.nl/view/tno/uuid%3A29f15365-8885-4278-82fe-996567858ae9/ [em linha] [consulta em 13 de junho de 2016].

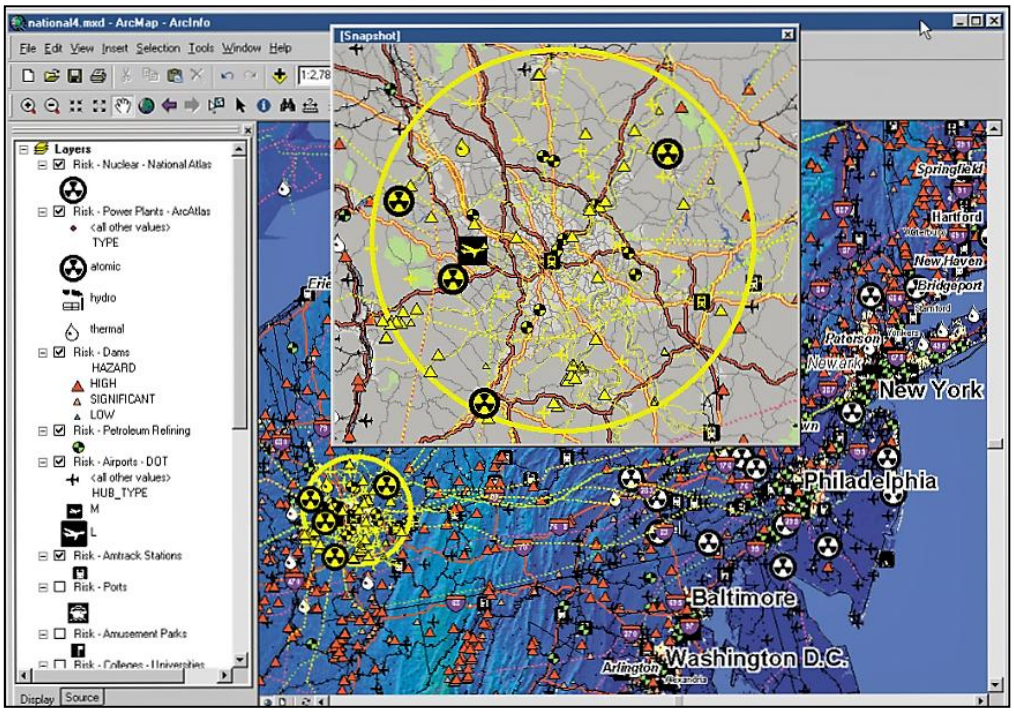


Figura 13: *Software* SIG[75] - de gestão da informação, com módulo de avaliação do risco (preditiva) e gestão de crises.
Fonte: http://www.esri.com/news/arcnews/winter0102articles/gis-homeland.html.

2.4. SÍNTESE

Em Portugal existem inúmeras referências à proteção de IC, disseminadas por diversa legislação. Porém, este quadro legal é ineficiente e carece de coerência.

O DL n.º 62/2011, sendo o único que se dedica exclusivamente à matéria de proteção de IC, não tem uma visão estratégica suficientemente coerente e consolidada, nem uma vocação aglutinadora, pelo que não se pode considerar que exista um verdadeiro e próprio Plano Nacional de Proteção de Infraestruturas Críticas.

O SGSSI detém a maior responsabilidade na condução das atividades de coordenação dos restantes atores. No entanto, esse mandato é diluído em vários diplomas, desarticulados, resultando pouco robusto. Seria pertinente que a elaboração de um plano clarificasse o papel deste órgão.

[75] Disponível em: http://www.esri.com/news/arcnews/winter0102articles/gis-homeland.html [em linha] [consulta em 13 de junho de 2016].

Por outro lado, a inexistência de recursos humanos dedicados a esta pasta levanta sérios obstáculos quer ao simples cumprimento da legislação, quer à condução de projetos que possam ser implementados no futuro.

A outros organismos do Estado, em particular aos do setor da segurança, também estão atribuídas competências em matéria de proteção de IC. Porém, na falta de um organismo facilitador, poucos são os que realmente desenvolvem atividades nesta matéria.

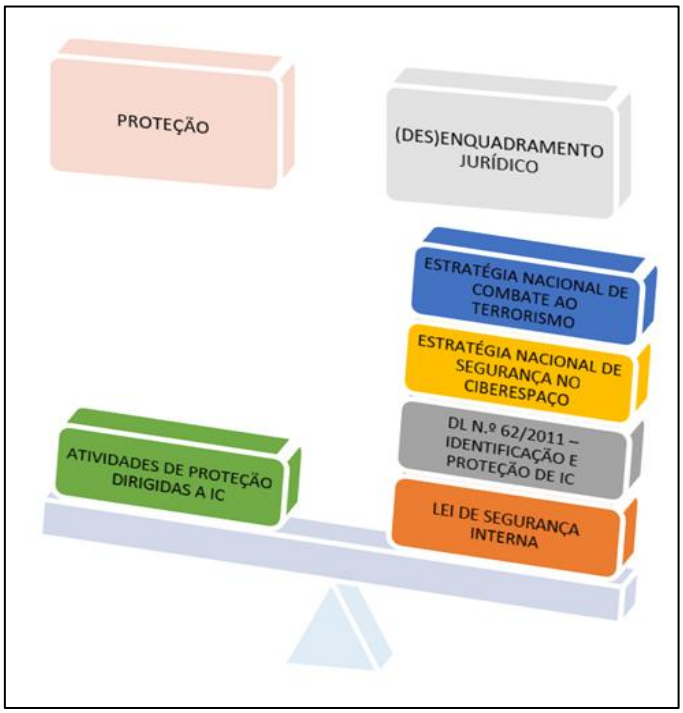


Figura 14: Representação da desproporção entre a densidade do quadro jurídico e as medidas concretas de proteção aplicadas pelo Estado em IC.
Fonte: Elaboração própria do autor.

Os operadores de IC têm um papel fundamental na sua proteção. Muitos já demonstram esta preocupação, embora focados no processo de continuidade do negócio, e na relação custo-benefício, para além de que a sua atenção é dirigida para o contexto local e organizacional.

As melhores práticas internacionais apontam para a necessidade de construção de uma política de proteção de IC, materializada através de um plano abrangente, integrador, que aborde todas as formas de ameaça (*safety* e *security*, incluindo cibersegurança). E que privilegie a relação entre o setor

público e o privado. Adicionalmente, é encorajada a criação de um organismo da administração, de caráter interministerial, incumbido de coordenar e tutelar a sua boa condução, através de um conjunto de medidas e atividades de proteção.

CAPÍTULO 3

A PERSPETIVA DOS ATORES (ANÁLISE DOS RESULTADOS DOS INQUÉRITOS)

3.1. INTRODUÇÃO

Neste capítulo apresentamos os resultados dos inquéritos realizados[76].

Agrupámos a análise em cinco subcapítulos - em linha com os objetivos definidos no capítulo 1. Assim, e após o indispensável enquadramento metodológico, analisámos, desde logo, se é ou não sentida uma necessidade de melhorar o atual quadro de proteção de IC (OE1).

De seguida, focando um plano mais operativo, procurámos compreender quais são as atividades de proteção mais valorizadas pelos vários atores (OE2).

Passando para o patamar estratégico, observámos não só a perceção da necessidade de forjar um PNPIC (OE4), como a importância que os atores atribuem à criação de um organismo capaz de o implementar (OE5).

Pela sua transversalidade, o OE3 será explorado ao longo dos vários subcapítulos.

3.2. METODOLOGIA

Para a elaboração do presente capítulo, foram utilizadas as metodologias de investigação que de seguida se descrevem:

1 – "**Questionário aplicado aos operadores de IC**"[77] - Inquérito por questionário, anónimo, dirigido a operadores de IC, nos setores da Energia e

[76] Os questionários correspondentes aos três inquéritos foram precedidos de pedido de autorização dirigido ao Diretor do ISCPSI. *Vide* Apêndice A.

[77] *Vide* Apêndices E e F.

dos Transportes. Este inquérito abrangeu 21 dos 22 operadores de IC, tendo-se obtido resposta de 11 (50% dos existentes).

2 – "**Questionário aplicado aos especialistas e *policy-makers***"[78] - Inquérito por questionário, aberto, dirigido a 10 quadros superiores da administração pública que, têm ou tiveram (últimos cinco anos) responsabilidades em matéria de proteção de IC.

O painel de especialistas foi cuidadosamente preparado, selecionando-se um lote de pessoas com experiência em proteção de IC, mas com pontos de observação diferenciados[79].

Questionários semelhantes, mas traduzidos para inglês[80], foram enviados para o *Centro Nacional de Protección de Infraestruturas Críticas* (Espanha)[81] e para o organismo *Securité des Activités D´Importance Vitale*[82] - *Le Secrétariat Général de la Défense et de la Sécurité Nationale* (França).

Os inquéritos foram aplicados entre 24 de maio e 08 de junho de 2016.

Instrumento	Designação do questionário e ferramenta de aplicação	Qualidade dos destinatários	Número de questionários respondidos/ enviados	Método de análise de dados
Questionário de resposta fechada	*Questionário de operadores de IC* ---------- *Google forms*	Operadores de IC dos setores da energia e transportes	11/22	Estatística descritiva
Questionário de resposta fechada	*Questionário de especialistas* ---------- *Google forms*	Decisores políticos, Coordenadores de políticas de segurança, Forças de Segurança, Reguladores setoriais, Responsáveis estrangeiros de PIC	11/11	Estatística descritiva

Figura 15: Síntese metodológica do trabalho de investigação.
Fonte: Elaboração própria do autor.

Cada questionário integra perguntas autónomas e customizadas, que permitem explorar o conhecimento e experiências específicos do respetivo público-alvo.

78 *Vide* Apêndice B.
79 *Vide* Apêndice C.
80 *Vide* Apêndice D.
81 Tradução livre da responsabilidade do autor "… Centro Nacional de Proteção de Infraestruturas Críticas.
82 Tradução livre da responsabilidade do autor "… Segurança das Atividades de Importância Vital (SAIV) – Secretariado Geral da Defesa e Segurança Nacional.

Ao mesmo tempo, um bloco de questões transversais procura dar a conhecer a opinião que cada inquirido tem sobre o mesmo assunto[83].

3.3. COMO PROTEGER AS IC – AS ATIVIDADES

Conforme destacamos no segundo capítulo, o Estado pode desenvolver inúmeras atividades passiveis de contribuir para o aumento da proteção de IC, quer no domínio da gestão do risco (essencialmente preventivo) que no domínio da gestão de crises (essencialmente reativo). Estas iniciativas destinam-se ao aumento das capacitações de segurança dos operadores e à melhoria da resposta dos organismos do Estado.

No sentido de aferir quais as medidas mais valorizadas por estes dois atores (Estado e operadores), foi elaborada a seguinte questão base:

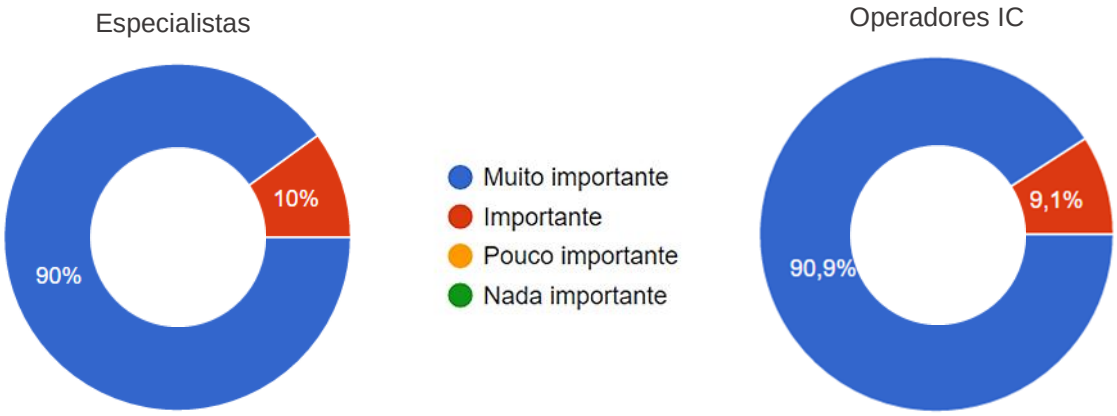
«De acordo com a sua experiência, indique o grau de intervenção que o Estado deverá ter na prossecução das seguintes medidas/atividades:»

Em seguida foram apresentadas treze atividades (selecionadas por constituírem boas práticas internacionais). Para cada atividade proposta o inquérito apresentou os seguintes resultados:

Proporcionar aos diferentes atores (operadores de IC, FSS, entidades reguladoras) informação sobre boas práticas de proteção de IC, do seu setor ou de outros, recolhidas tanto a nível nacional como internacional.

83 *Vide* Apêndice J.

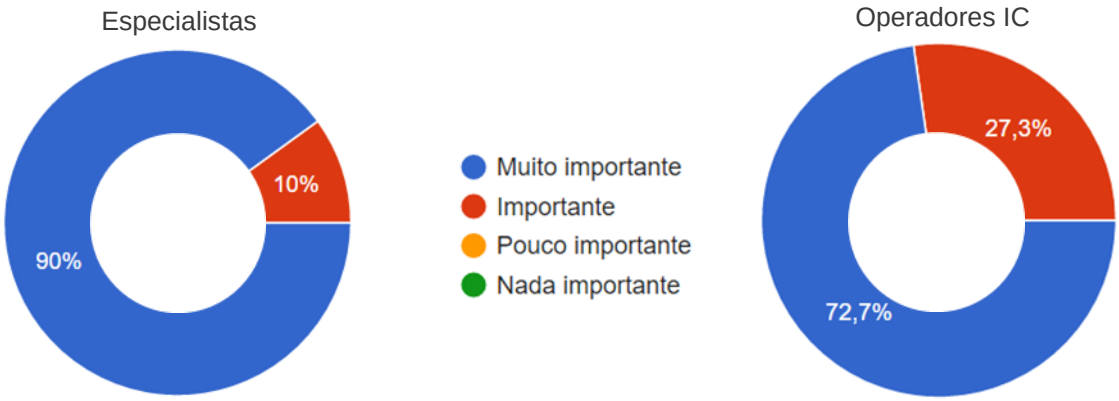
Proporcionar acesso a informação sobre potenciais ameaças a IC, que possam contribuir para um melhor nível de proteção.



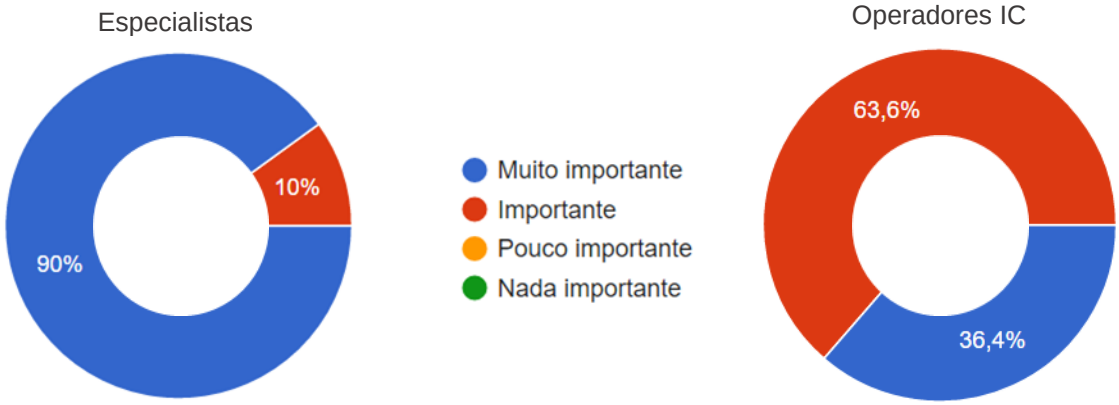
Organizar e proporcionar o acesso a *workshops* com vários operadores de IC, e com outros atores (FSS, entre outros), para discussão e partilha de boas práticas de proteção/resposta a incidentes, rentabilizando desta forma o *know-how* que se encontra disperso entre o setor público e o setor privado.

Proporcionar apoio técnico na deteção de vulnerabilidades em IC (quando, e na medida do solicitado pelo operador de IC) através de especialistas das FS e/ou de outros organismos de reconhecida competência (LNEC, universidades, etc).

Organizar (participar) exercícios de tomada de decisão, ou simulacros, abrangendo IC do mesmo setor e outros atores (FSS, entidades reguladoras).



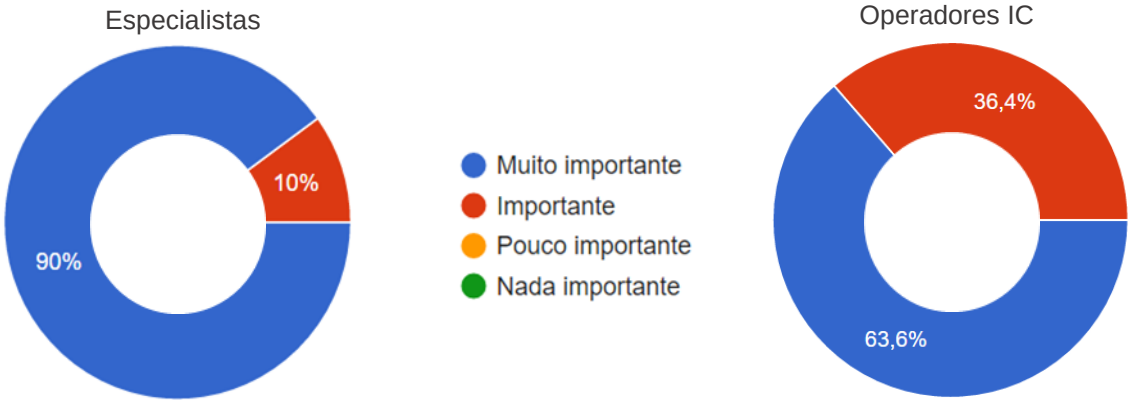
Organizar (participar em) exercícios de tomada de decisão, ou simulacros, abrangendo IC de diversos setores, com exploração de efeitos sistémicos como os "fenómenos de cascata".



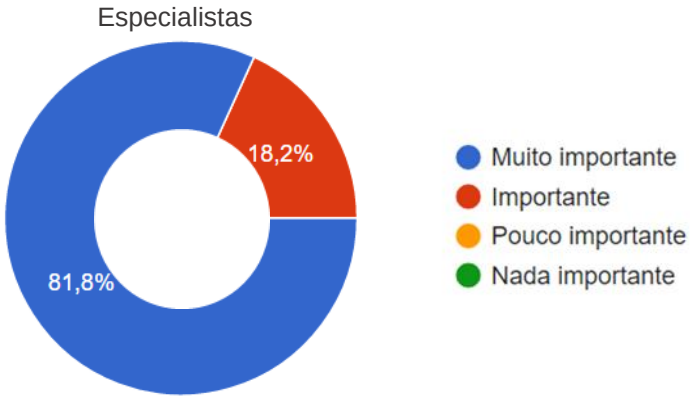
Disponibilizar (solicitar no caso dos operadores) equipas de peritos/observadores, provenientes de organismos com competência no âmbito *security*, para observação e avaliação técnica de exercícios/simulacros.

Agilizar contactos entre os operadores de IC e os responsáveis das FS ao nível local (localidade onde se insere cada uma das IC).

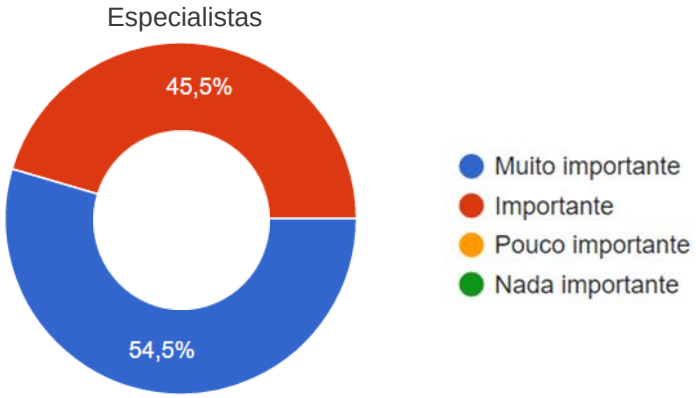
Facilitar e promover a partilha de informação entre responsáveis locais das FS e Agentes de Ligação de Segurança de IC (nível local), com vista a uma intervenção mais adequada, bem como à agilização/treino de procedimentos conjuntos em caso de necessidade de intervenção.



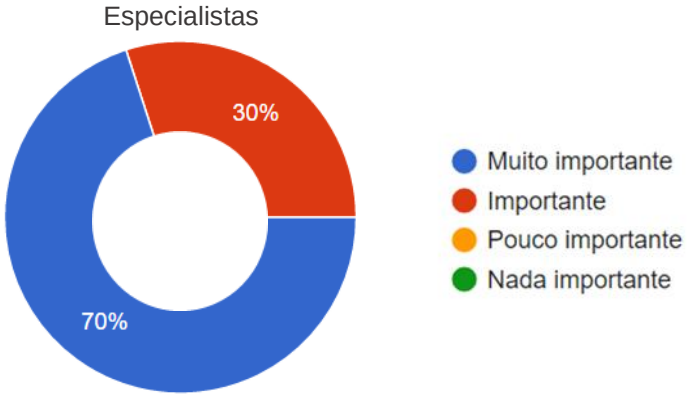
Implementar verificações de segurança a funcionários que venham a desempenhar funções de elevada criticidade no contexto de IC (nos termos de legislação em vigor ou a regulamentar no futuro).



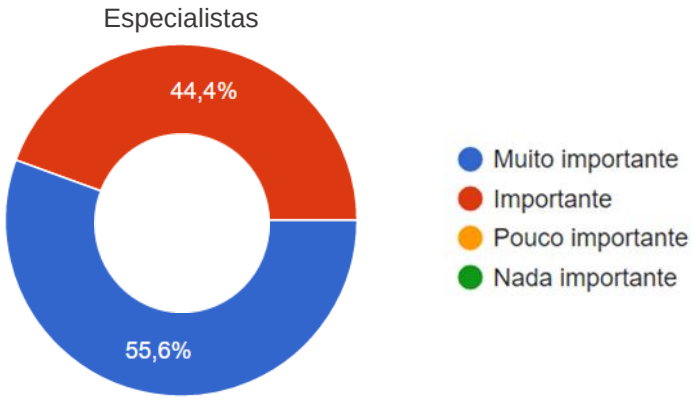
Criar e gerir sistemas de informação geográfica com informação organizada relativa à proteção de IC.



Implementar e gerir uma plataforma de contacto com operadores ou outros atores.



Operacionalizar uma sala de situação (crise) para apoio e coordenação de respostas a incidentes em IC que envolvam a responsabilidade partilhada e a utilização meios de várias entidades, quer públicas quer privadas.



Relativamente à importância da realização do conjunto de atividades de proteção de IC podemos extrair os seguintes resultados finais:

Painel de especialistas:

- **80%** considera «**muito importante**» a realização das atividades de proteção de IC;
- **19.6%** considera «**importante**»;
- **0.4%** considera «**pouco importante**»[84] (representa a opinião de um inquirido, em apenas uma atividade);
- Nenhum especialista considerou «**nada importante**».

Painel de operadores de IC:

- **67%** considera «**muito importante**»;
- **31%** considera «**importante**»;
- **2%** considera «**pouco importante**»;
- Nenhum operador considerou «**nada importante**».

Acumulado do total dos inquiridos[85]:

- **73.5%** considera «**muito importante**»;
- **25.3%** considera «**importante**»;
- **2.4%** considera «**pouco importante**»;
- Nenhum especialista considerou «**nada importante**».

Em suma cerca de 98% dos inquiridos considera como «importante» ou «muito importante» a realização das atividades de proteção mencionadas no inquérito.

[84] Representa a opinião de um inquirido, em apenas uma atividade.
[85] O resultado de 101.2% advém dos arredondamentos realizados nos parciais.

3.4. COMO ORGANIZAR OS RECURSOS – UM PLANO NACIONAL DE PROTEÇÃO DE IC

A comunidade internacional recomenda, como já vimos, a implementação de instrumentos de governação de âmbito nacional, abrangentes e integradores para a proteção de IC. Estes planos servem para determinar as responsabilidades dos vários atores, as atividades a prosseguir pelo Estado, e como deve ser organizada a mobilização de recursos.

Com a bateria de perguntas que se segue, procuramos saber o que tem feito o Estado nesta matéria, e qual o modelo organizativo de proteção de IC que a comunidade considera mais eficiente.

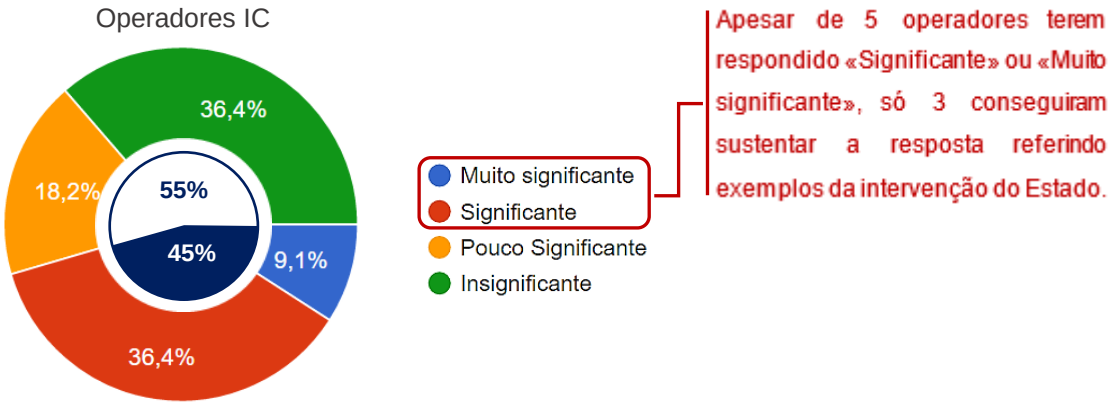
Seguindo a mesma metodologia, a pergunta base foi a seguinte:

«De acordo com a sua experiência e perceção, indique o grau de intervenção/empenho que o Estado tem demonstrado na prossecução das seguintes medidas/atividades:»

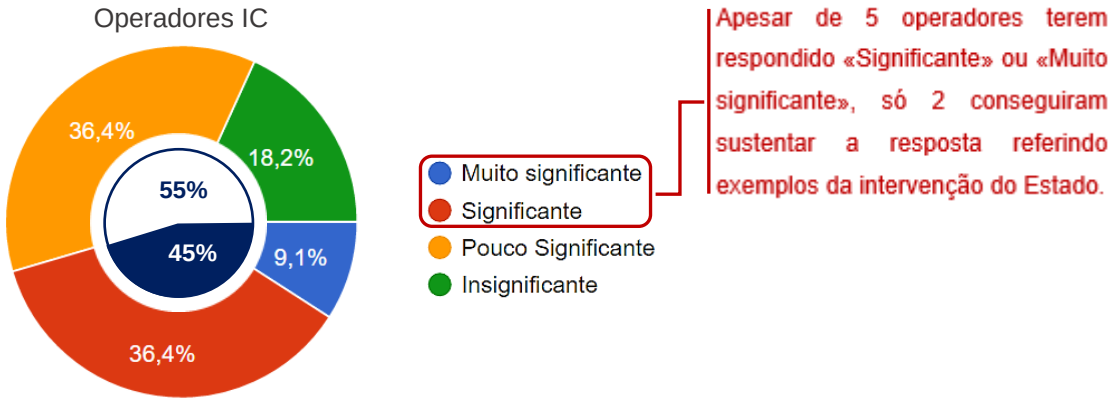
Finalmente, e apenas para o grupo de especialistas, foi colocada a questão: **«existe em Portugal um Plano Nacional de Proteção de IC»**.

Os resultados deste inquérito foram os seguintes:

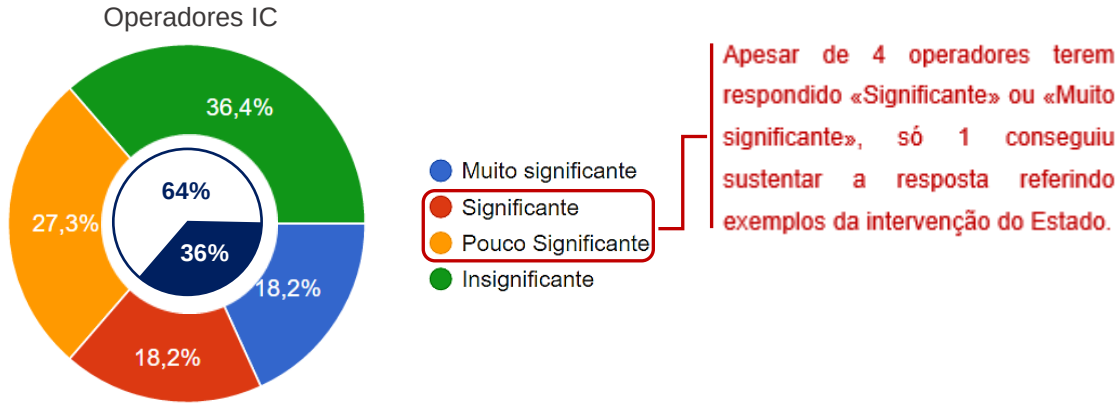
Proporcionar aos operadores de IC informação e conhecimento sobre boas práticas de proteção de Infraestruturas críticas, do seu setor ou de outros, recolhidas tanto a nível nacional como internacional.



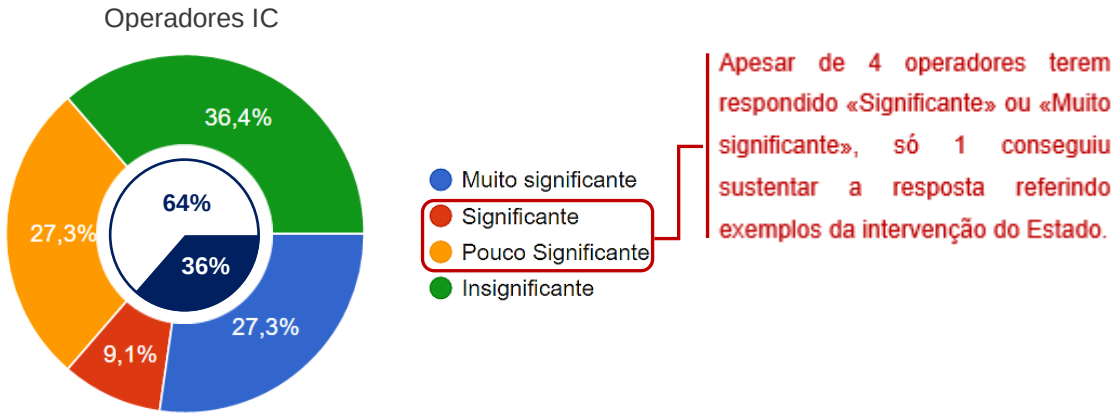
Proporcionar acesso a informação sobre potenciais ameaças a IC, no seu setor ou em outros, que possam contribuir para um melhor nível de proteção.



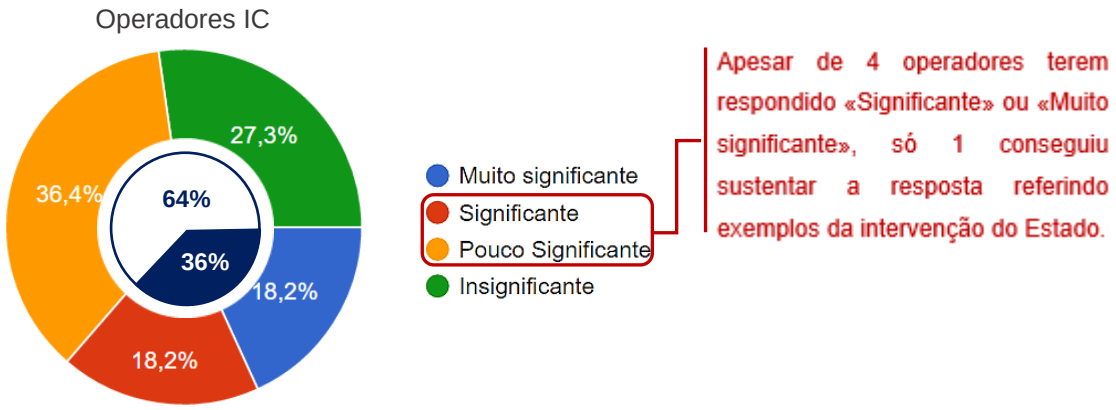
Organizar e proporcionar o acesso a *workshops* com vários OIC, e/ou com outros atores (FSS, Serviços de Informações, entre outros), para discussão e partilha de boas práticas de proteção/resposta a incidentes.



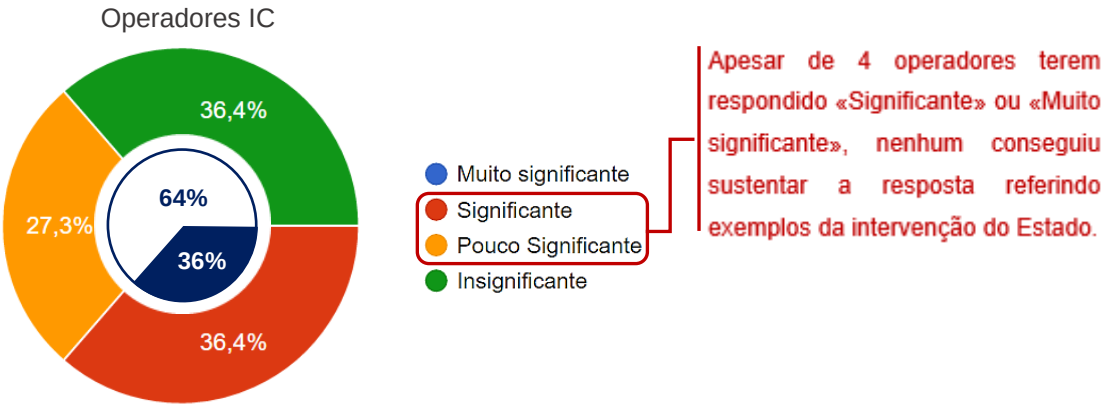
Proporcionar apoio técnico na deteção de vulnerabilidades da IC (se solicitado pelo operador de IC) através de especialistas das FS e/ou outros organismos de reconhecida competência (LNEC, universidades, reguladores).



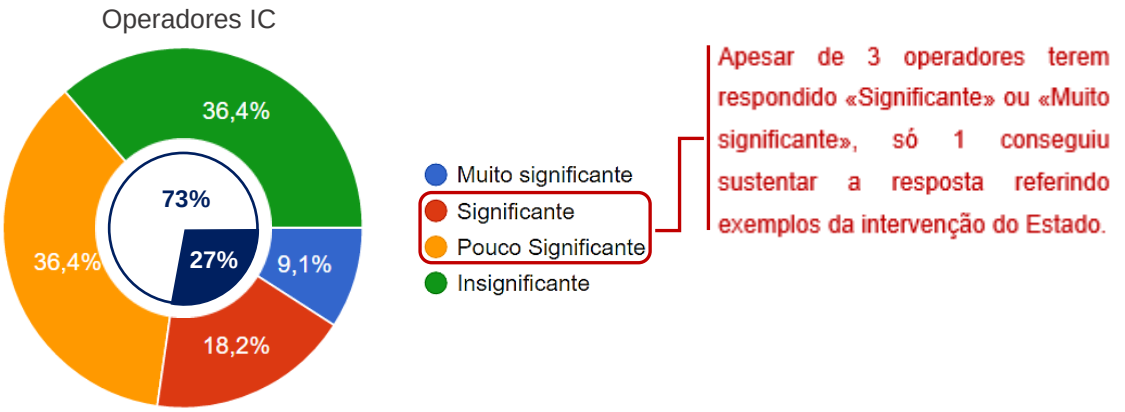
Organização de exercícios de tomada de decisão, ou simulacros, abrangendo IC do mesmo setor.



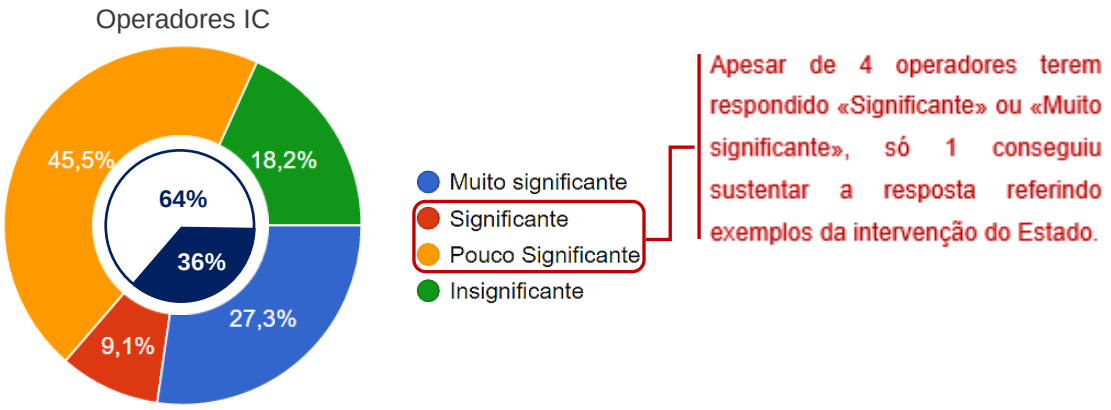
Organização de exercícios de tomada de decisão, ou simulacros, abrangendo IC de diversos setores, e exploração de efeitos sistémicos.



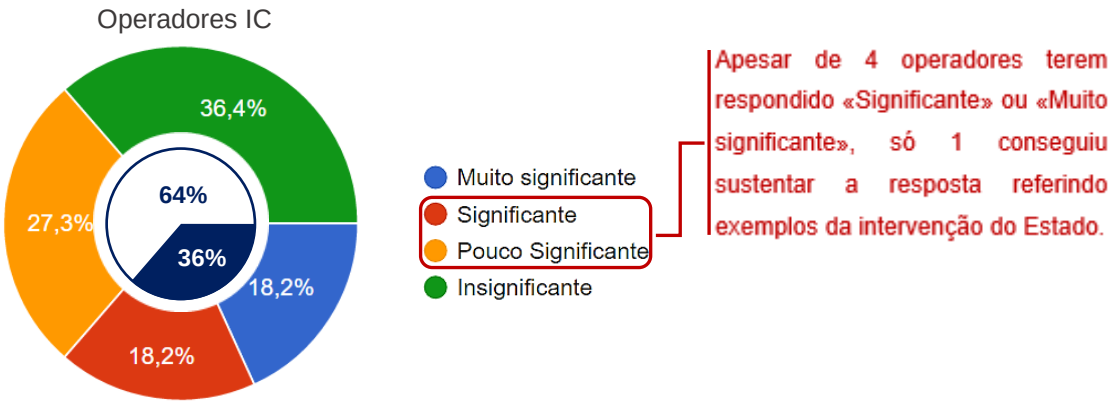
Disponibilização de equipas de peritos/observadores, provenientes de organismos de reconhecida capacidade no âmbito *security*, para observação e avaliação técnica de exercícios/simulacros.



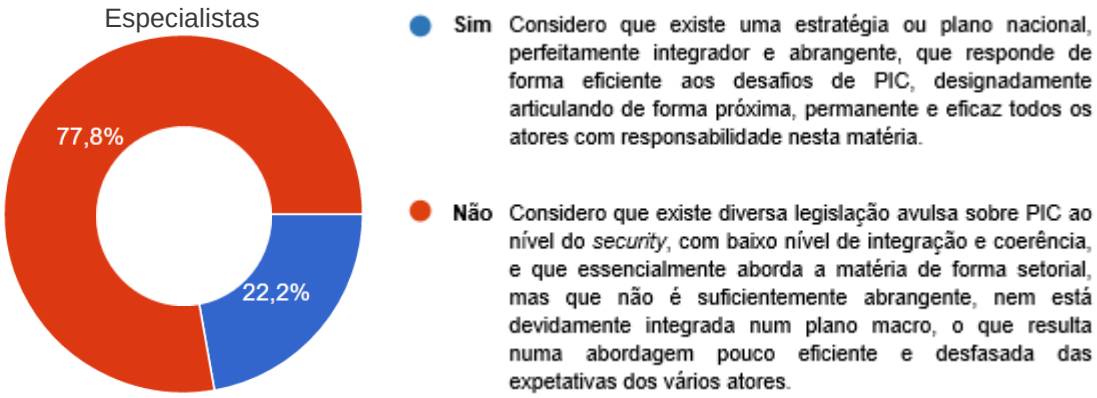
Agilização de contactos com os responsáveis locais das FS (ao nível da localidade onde se insere cada uma das IC).



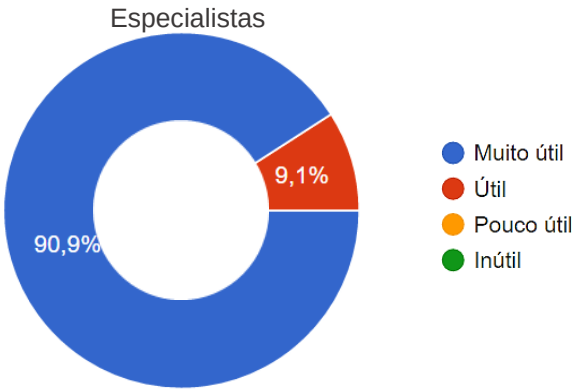
Facilitação/promoção da partilha de informação entre responsáveis locais das FS e das IC (nível local), com vista a uma intervenção mais adequada, e ao treino de procedimentos conjuntos em caso de necessidade de intervenção.



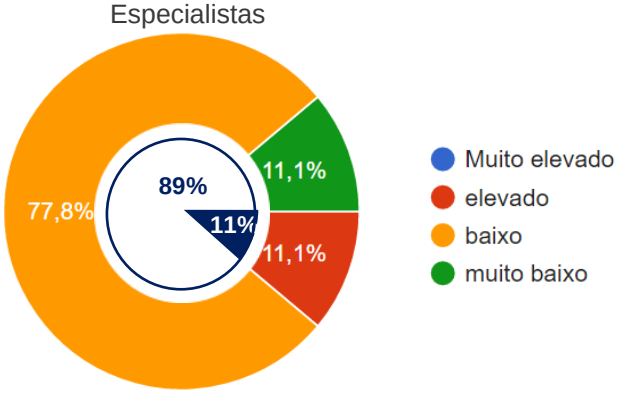
Considera existir em Portugal uma estratégia ou um plano nacional (integrador, abrangente e transversal) para a PIC, que envolva de forma eficiente e empenhada os vários atores (operadores de IC, FSS, entidades reguladoras)?



Tendo em conta que no ordenamento jurídico nacional existe mais de uma dezena de diplomas legais, que fazem menção expressa à PIC, considera útil a elaboração de uma estratégia ou de um PNPIC, único, abrangente, concertado e integrador, que garanta uma maior atenção do Estado no domínio da PIC?



Considerando que o quadro jurídico português atribui um vasto conjunto de competências ao SGSSI, em matéria de articulação da PIC, qual lhe parece ser o nível de comprometimento e resultados alcançados até ao momento?



Quanto ao grau de intervenção do Estado na promoção destas medidas, os operadores de IC responderam da seguinte forma:

- **15%** considera a intervenção do Estado «**muito significativa**»;
- **23%** considera «**significativa**»;
- **32%** considera «**pouco significativa**»;
- **31%** considera «**nada significativa**».

Refira-se que apesar de 38% de inquiridos ter indicado a resposta «significativo» ou «muito significativo», **apenas 5%** conseguiu sustentar a sua escolha com exemplos concretos da intervenção do Estado nestas atividades.

Em termos de agrupamento temos os seguintes resultados:

- **38%** dos inquiridos considera a intervenção do Estado «**significativa**» ou «**muito significativa**»;
- **63%** considera «**pouco significativa**» ou mesmo «**nada significativa**».

Quanto ao painel de especialistas registamos que:

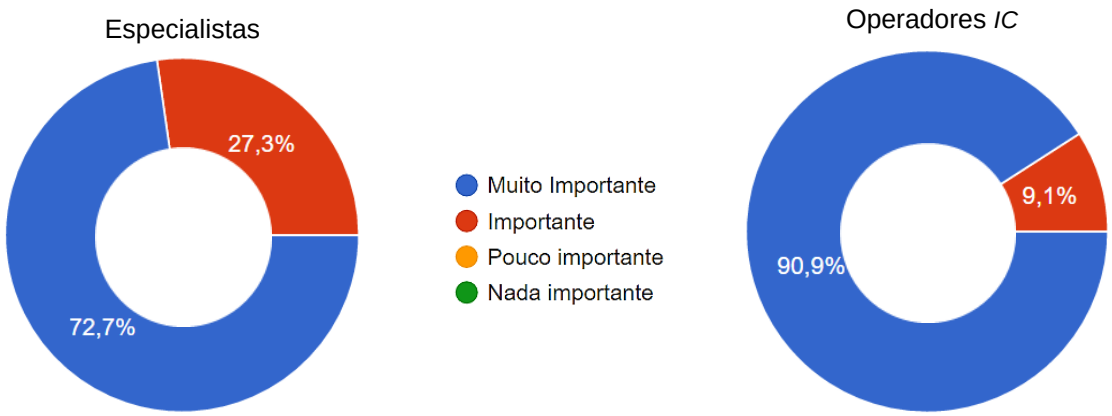
- **78%** considera não existir em Portugal um Plano Nacional de Proteção de IC ou uma estratégia de proteção de IC;
- **100%** considera «muito útil» ou «útil» a elaboração de um Plano Nacional;
- **89%** considera «muito baixo» ou «baixo» o comprometimento e resultados alcançados pelo SGSSI na proteção de IC.

3.5. COMO IMPLEMENTAR O PLANO – UM ORGANISMO

São inúmeras, já o referimos, as recomendações doutrinárias sobre a criação de um organismo específico, de caráter interministerial, no seio da administração pública, que coordene e as atividades de proteção de IC.

Também relativamente a este tema, quisemos saber a opinião dos especialistas, e dos operadores de IC. Os resultados constam do gráfico seguinte.

Indique, qual a importância de ser constituído um organismo, que se dedique especificamente às matérias de facilitação e coordenação da PIC, com vista a prosseguir as atividades mencionadas nas questões anteriores, e apoiando todos os atores intervenientes e criando pontes entre o setor público e privado.



3.6. SÍNTESE

O inquérito aplicado revela os seguintes dados:

- Os atores atribuem relevância às atividades de proteção de IC, já que 98% dos inquiridos as consideram «importante» ou «muito importante».
- A intervenção do Estado é percecionada como deficitária, por 63% dos inquiridos que a caraterizou como sendo «pouco significante» ou «insignificante». Dos restantes, só 5% justificaram a sua escolha.
- Não existe em Portugal, um PNPIC ou uma estratégia concertada, de acordo com 78% dos especialistas inquiridos.
- A necessidade de elaboração de um plano é incontestável, de acordo 100% dos especialistas.

- O papel do SGSSI, nos últimos 10 anos, motiva reflexão, já que 89% dos inquiridos considera insuficientes os resultados alcançados.
- Todos os especialistas e operadores, consideram basilar o reforço da capacidade do Estado, em especial nas competências de coordenação, através da criação de um organismo especificamente dedicado à proteção de IC.

CAPÍTULO 4

CONCLUSÕES E RECOMENDAÇÕES

4.1. INTRODUÇÃO

No presente capítulo apresentamos as conclusões do trabalho.

Começaremos por verificar se os objetivos do trabalho foram atingidos para, de seguida, confrontarmos a nossa hipótese com as respostas às questões da investigação.

Propomo-nos ainda registar as reflexões mais importantes que o trabalho nos sugere, e tentaremos avançar algumas recomendações que possam de algum modo dar resposta aos problemas que a matéria encerra.

Finalmente, umas breves notas à possibilidade de desenvolvimento de novas linhas de pesquisa, capazes de complementar este e outros trabalhos já produzidos na mesma área.

4.2. CONFIRMAÇÃO DOS OBJETIVOS DO TRABALHO

As metodologias de investigação escolhidas permitiram-nos atingir os seis objetivos específicos do trabalho:

OE1 Foi aferido o grau de inteligibilidade, eficiência e articulação do quadro legal relativo à proteção de IC;

OE2 Foram diagnosticadas as atividades mais valorizadas pelos principais atores e avaliado o grau de implementação dessas atividades;

OE3 Foram identificadas boas práticas, recomendadas pela Comissão Europeia, relativamente quer à organização de uma política de proteção, quer também às atividades concretas a desenvolver no âmbito dessa política e adaptáveis ao contexto nacional;

OE4 Foi medido o grau de importância atribuído à criação de um Plano Nacional de Proteção de IC, pela literatura e pelo painel de especialistas nacionais e internacionais;

OE5 Foi recolhida e explorada informação suficiente para concluir sobre o grau de (in)capacidade do Estado na implementação de medidas de proteção de IC, muito em especial no domínio da coordenação, e sobre a criação, útil para a solução do problema, de um organismo dedicado;

OE6 Foram apontados elementos essenciais à construção de um plano nacional, com os seus princípios, os atores investidos de o executar, a relação que deve ser estabelecida entre eles e finalmente as atividades que se destinam a uma efetiva melhoria do nível de proteção das nossas IC.

4.3. RESPOSTAS ÀS QUESTÕES DA INVESTIGAÇÃO

Em linha com a hipótese levantada o nosso estudo fornece as seguintes respostas às perguntas derivadas:

PD1 Existe em Portugal um plano ou uma estratégia nacional para a proteção de IC?

Não. A pesquisa demonstrou que a legislação vigente, apesar de abundante, carece de ordem, coerência, e alinhamento com uma visão estratégica de natureza transversal, características essenciais a um verdadeiro plano nacional. De resto, esta resposta foi confirmada por 80% dos membros do painel de especialistas.

PD2 Que necessidades são sentidas pelos diferentes atores no domínio da proteção de IC?

Todas as atividades apresentadas registaram elevada adesão tanto por parte do painel de operadores como por parte do painel de peritos (98% consideram «importante» ou «muito importante»).

Quando questionados sobre o grau de intervenção do Estado na promoção dessas atividades 63% dos operadores indicaram ser «pouco significativo» ou «nada significativo».

Em suma, os diversos atores consideram as atividades de proteção muito importantes, mas a maior parte dos seus destinatários – os operadores – entendem que o Estado não tem atendido de forma satisfatória à sua implementação.

PD3 Que modelos de governação e boas práticas são seguidas em outros países europeus?

A generalidade dos países europeus preparou um plano nacional de proteção de IC. Em alguns deles existem organismos de coordenação específicos, noutros são reforçados organismos já existentes na área da segurança interna ou na dependência direta do Primeiro-Ministro. Estes organismos garantem a implementação do plano através da coordenação de medidas como a identificação de IC, a criação e/ou estabilização de doutrina, a partilha de informações entre entidades públicas e operadores de IC, a promoção de exercícios e a gestão de plataformas informáticas que permitam dar apoio à gestão do risco.

Em suma, promovem e facilitam o contacto entre os operadores e as entidades da administração pública, e realizam atividades específicas com vista a potenciar o trabalho de todos os atores.

PD4 Há necessidade de um plano ou de uma estratégia para a proteção de IC em Portugal?

A revisão da literatura revela que há necessidade de conferir coerência ao atual quadro legal.

Um plano ou uma estratégia nacional para a proteção de infraestruturas criticas, que estabilize as opões políticas relativas ao papel do Estado na proteção de IC, são referidos sistematicamente como boas ferramentas de trabalho.

A maioria dos países da União Europeia, os EUA, o Canadá e a Nova Zelândia, entre outros, dispõe de um plano que funciona como moldura para todas as atividades que visem a proteção de IC.

É também sintomático que 91% do painel de especialistas considerem a elaboração de um plano «muito útil» e os restantes 9% a considerem «útil».

PD5 A implementação e condução de um plano ou uma estratégia para a proteção de IC requer a criação de um organismo dedicado e especializado?

A implementação e condução de um plano com esta abrangência requer o compromisso político e a correspondente capacitação da administração pública.

Em alguns países da Europa essa capacitação foi conseguida através do reforço de organismos já existentes. Noutros casos (os de maior sucesso) foram mesmo criados organismos específicos de coordenação.

Todos os inquiridos consideram positivo uma maior capacitação do Estado, indicando como «muito importante»[86] ou «importante»[87] a criação de um organismo de coordenação dedicado à proteção de IC.

Em Portugal, no atual quadro do Sistema de Segurança Interna, o SGSSI parece ser o órgão do Estado mais vocacionado para assumir este papel de coordenação e liderança. No entanto, por falta de quadro orgânico e de compromisso político induzido neste órgão não tem conseguido alcançar os resultados desejáveis (89% dos inquiridos considera «insuficientes» os resultados alcançados nos últimos 10 anos).

PD6 Considerando a realidade nacional, que desenho e configuração deverá ter um plano nacional de proteção de IC?

Tendo em conta…

86 Referiram «muito importante» 73% dos especialistas e 91% dos operadores.
87 Referiram «importante» 27% dos especialistas e 9% dos operadores.

- A multiplicidade de competências que a lei atribui a uma pluralidade de entidades, em matéria se proteção de IC;
- A existência de um órgão de coordenação no Sistema de Segurança Interna cujos poderes têm ampla sustentação legal;
- As idiossincrasias existentes entre a generalidade dos operadores e a administração pública;
- A mobilização tendencialmente voluntária dos operadores privados, para irem ao encontro das exigências do Estado, em matéria de segurança;
- As atividades de proteção mais valorizadas pelos operadores, e tidas como necessárias pela comunidade de especialistas;

…entendemos que um plano nacional deveria assentar nos seguintes princípios:

- Modelo de matriz "semi-intervencionista" (aspas do autor), em que o posicionamento do Estado passa essencialmente pela coordenação e facilitação de medidas junto dos diversos atores, embora com uma presença significativa ao nível da coordenação e supervisão do desenvolvimento das ações delineadas;
- Reconhecimento e reforço das competências dos diversos organismos em matéria de proteção de IC, mas ao mesmo tempo clarificação de sobreposições negativas.
- Fortalecimento das competências do SGSSI, em matéria de proteção de IC, através do reforço do seu quadro ou, em alternativa, através da criação de um organismo de coordenação, na dependência daquele, principal responsável pela condução do "macromodelo de segurança" (Torres, 2015);
- Paradigma de intervenção "Baixo custo – Alto impacto" (aspas do autor), assente em investimento técnico/intelectual e tecnologicamente suportado, focado na coordenação, exploração de sinergias, bem como partilha de conhecimento e de informações.

- Reconhecimento, por parte dos principais atores do domínio da cibersegurança e proteção civil, do papel coordenador do SGSSI, como garante de uma abordagem integral.
- Encorajamento do modelo de parceria público-privada entre operadores e Estado, através da criação de um centro de perícia (*expertise)* de segurança, apelativo e aberto.
- Criação de grupos de trabalho com entidades públicas (representantes dos ministérios envolvidos, reguladores setoriais e atores do SSI), nos quais tenham assento os operadores, assim se garantindo a necessária sintonia e alinhamento entre todos os envolvidos.
- Relação jurídica de caráter tendencialmente não sancionatório, mas em que as responsabilidades e as atividades a desenvolver estejam detalhadamente enunciadas, quer relativamente aos atores privados, quer ao Estado.
- Para a prossecução dos objetivos traçados e das metas definidas o plano deve enumerar as seguintes atividades:
    - Construção de taxonomia específica, quer no campo dos conceitos gerais, quer no campo das métricas (estabilização de definições, indicadores de criticidade, metodologias de gestão do risco e avaliação de interdependências, entre outras), com a participação dos vários atores, assegurando-se a sua plena difusão;
    - Organização de *workshops* envolvendo operadores e as competentes entidades do Estado;
    - Criação de bolsas de especialistas, de caráter multidisciplinar, para execução de missões de apoio técnico, tendo em vista a identificação de vulnerabilidades em IC (regime *Ad hoc*);
    - Organização de exercícios de tomada de decisão, com os operadores de IC e entidades do Estado;

- Criação de um manual de boas práticas (*toolkit)* estabelecendo os aspetos estruturantes da dinâmica a estabelecer entre as forças de segurança e os operadores de IC ao nível local (partilha de contatos, preparação dos planos de proteção exterior, visitas técnicas, organização de simulacros à escala local, etc);
- Implementação de testes de stresse à segurança das IC*,* em coordenação com os respetivos operadores;
- Desenvolvimento e gestão de uma plataforma de centralização da informação relativa à proteção de infraestruturas críticas, de configuração modelar, que integre componentes de avaliação de ameaça, gestão do risco, geração de cenários e gestão de crises, a qual possa ser alimentada e explorada por vários atores, mediante políticas de utilização previamente definidas;
- Estabelecimento de parcerias com o CNPIC-Espanha, e outros organismos semelhantes, para troca de experiências e partilha de recursos (*know-how*);
- Exploração sistemática dos fundos europeus disponíveis para iniciativas nesta matéria, bem como das ferramentas de apoio técnico, acessíveis no âmbito da Comissão Europeia;
- Inclusão desta temática nos conteúdos programáticos dos cursos de formação policial, de nível universitário, e em formação específica para outros cargos dirigentes;
- Revisão dos requisitos legais do agente de ligação de segurança, designadamente ao nível da sua formação.

4.4. REFLEXÕES FINAIS

Tal como um relógio assenta no funcionamento do seu mecanismo, e na interação articulada das suas engrenagens, o desenvolvimento das sociedades modernas, como a nossa, depende do exercício regular e sincronizado das

suas infraestruturas críticas. Mas esta condição também faz delas um dos alvos de maior interesse, no quadro das ameaças extremas.

O baixo número de ataques a IC na Europa, não nos deve iludir nem tranquilizar: qualquer investida, bem-sucedida, numa destas instalações, pode destruir ou desestabilizar muitas outras, num efeito dominó, conduzindo à paralisação da generalidade das funções vitais do país. Voltando à metáfora inicial: para bloquear o relógio, basta comprometer uma única das suas engrenagens.

É certo que, como em qualquer outra atividade humana, também aqui existe um risco estrutural e intrínseco, impossível de suprir em toda a sua extensão.

No entanto, o Estado e os operadores dessas infraestruturas têm a obrigação de, em conjunto, empregar esforços que possibilitem a aproximação a esse limiar mínimo de risco.

A respeito deste esforço, Portugal constitui caso único (conhecido) na Europa: a sua administração não dispõe de um único funcionário incumbido em exclusividade desta esta missão.

Como acontece em qualquer sistema (e neste âmbito falamos sempre de sistemas), a mobilização de um componente anima todos os outros provocando um efeito de contágio, de elevado impacto.

Não são, por isso, necessários investimentos avultados, pelo menos numa primeira fase, para introduzir melhorias significativas: um elementar sinal do compromisso do Estado, por via da **harmonização do quadro legal** e do **reforço da massa crítica da Administração**, multiplicará os seus efeitos, potenciando sinergias e a melhoria do nível de proteção das nossas IC.

Como é referido num documento da Comissão: “a opção «não mudar de política» não apresenta qualquer vantagem evidente…”.

Em Portugal, como resulta da comparação com a situação de outros países, urge atalhar caminho, numa prudente atitude de evitar tempestivamente a ocorrência de situações que comprometam de forma grave infraestruturas críticas e, por arrasto, a normalidade da vida social e a segurança nacional.

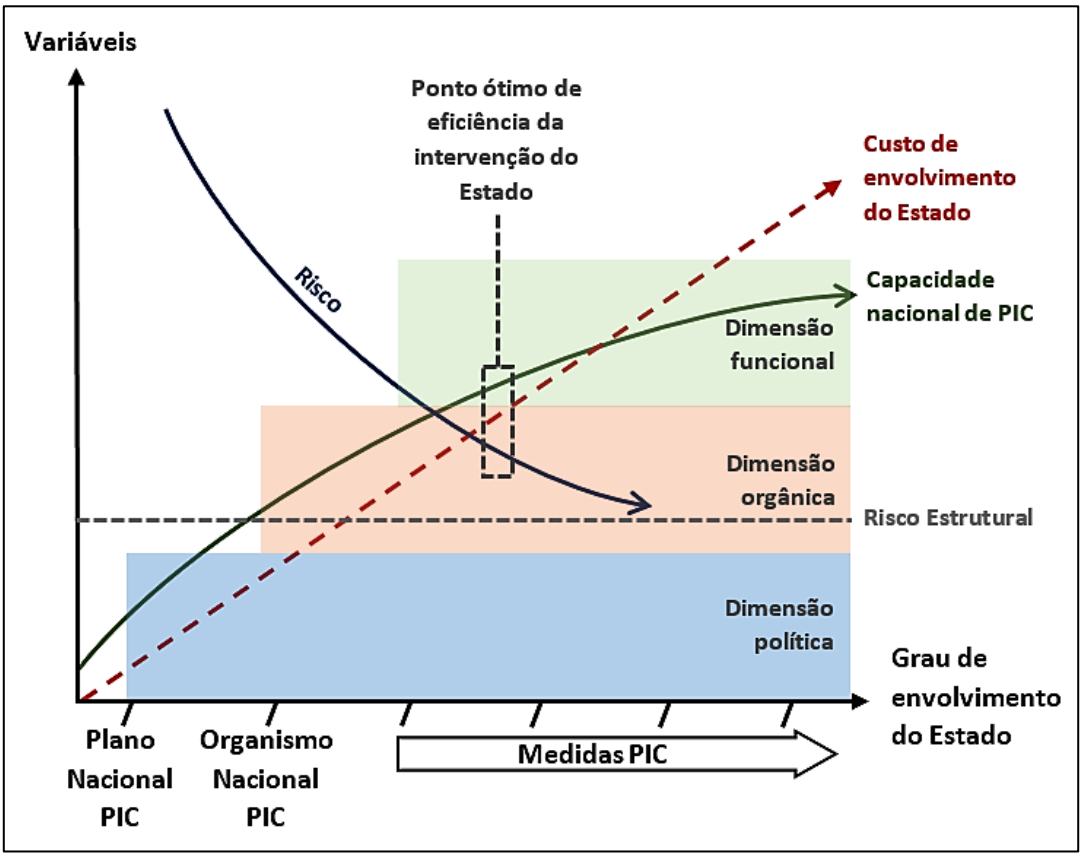


Figura 16: Paradigma **«**Baixo custo - alto impacto» - Relação das variáveis «risco» e «proteção» em função do envolvimento do Estado
Fonte: elaboração própria do autor.

4.5. RECOMENDAÇÕES

O presente estudo evidencia fragilidades que urge colmatar. Parece-nos particularmente relevante a atuação em três vertentes, interligadas:

- **Vertente política**: Elaboração de um documento de enquadramento (plano ou estratégia) que permita a clarificação e estabilização do atual panorama jurídico;
- **Vertente orgânica**: Reforço do Estado para fazer face aos exigentes desafios que esta temática coloca, por via do reforço do quadro atual do SGSSI ou, em alternativa, da criação de um organismo de coordenação, na dependência daquele.
- **Vertente funcional**: Desenvolvimento de medidas de proteção de IC, que visem a exploração de sinergias entre as entidades da administração pública e do setor privado.

Na ilustração que se segue, e com a qual damos por finalizado o nosso trabalho, sugerimos um possível modelo de abordagem à proteção de infraestruturas criticas, escalpelizando as principais missões dos vários atores, e os respetivos patamares de atuação.

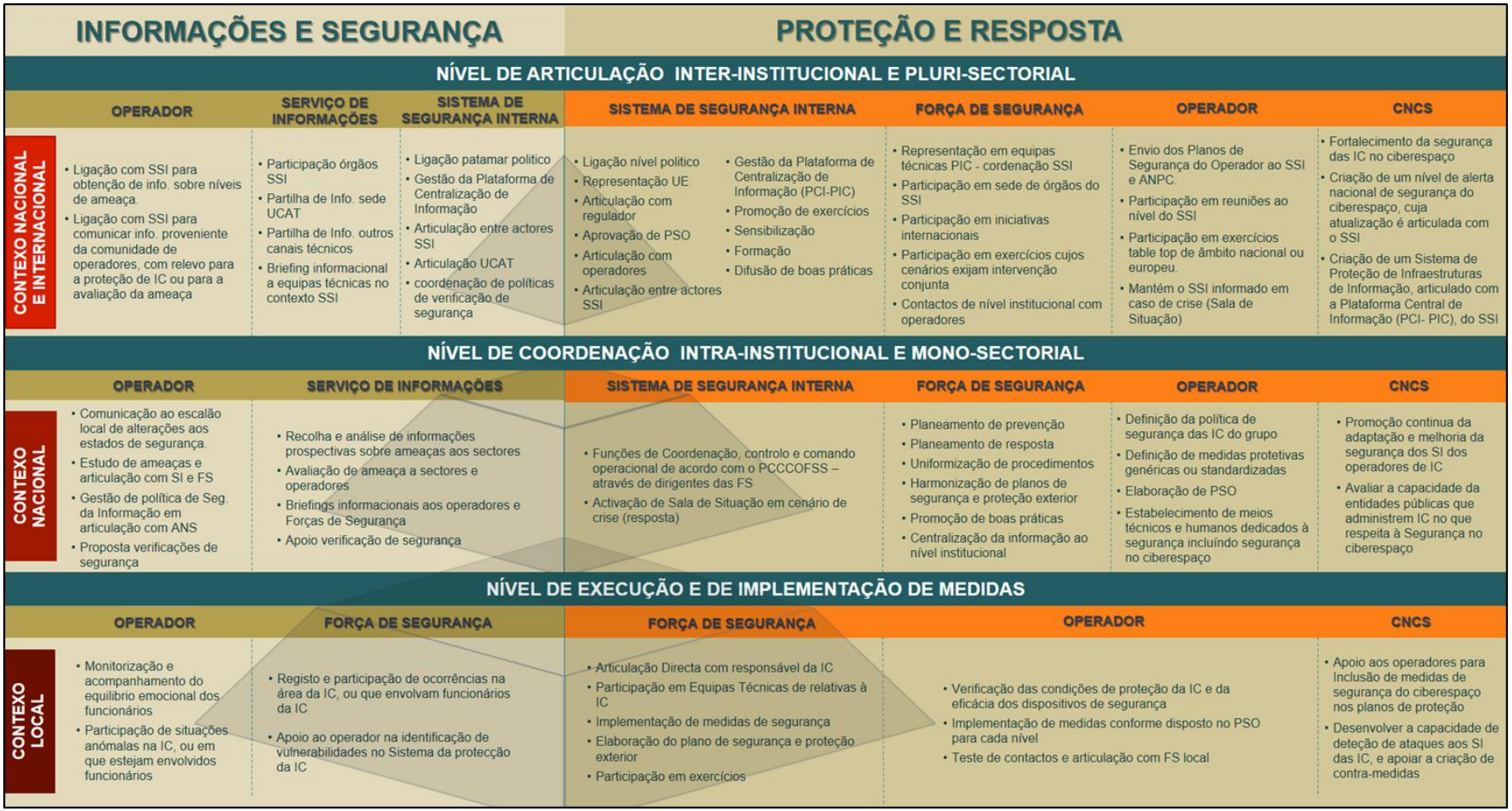


Figura 17: Proteção de IC - Plano geral dos atores, das atividades e domínios de intervenção
Fonte: elaboração própria do autor.

4.6. LIMITES DA INVESTIGAÇÃO

Durante o trabalho foram sentidas as seguintes dificuldades:

- A classificação de segurança atribuída a alguma informação comprometeu, nalguns casos, uma exposição mais detalhada;
- A escassez de documentação técnica nacional ligada nesta área obrigou a uma consulta intensiva de autores estrangeiros.

4.7. INVESTIGAÇÕES FUTURAS

O grau de maturidade e envolvimento dos operadores é fundamental para definir a natureza da sua relação com o Estado. Apesar de haver um histórico positivo de relacionamento, o facto de apenas metade dos inquiridos ter respondido ao questionário, aliado à circunstância de uma percentagem significativa de operadores ainda não ter elaborado os seus planos de segurança, levanta dúvidas sobre o verdadeiro grau de comprometimento (voluntário) em matéria de proteção de IC. Um estudo mais detalhado sobre o grau de compromisso do setor privado poderia colmatar esta carência.

Uma outra linha de investigação pertinente prende-se com a formação dos agentes de ligação de segurança. O currículo do curso de Diretor de Segurança, que atualmente constitui requisito para a assunção da função de ALS, não parece estar suficientemente vocacionado para a temática específica da proteção de IC.

Lisboa, 20 de junho de 2016

_____

João Franca da Fonseca Pestana

Comissário

BIBLIOGRAFIA

DIRECTIVA 2008/114/CE DO CONSELHO de 8 de Dezembro de 2008, Pub. L. No. DIRECTIVA 2008/114/CE (2008).

Assembleia da República (2008). Lei n.º 53/2008. Diário da República. *Diário da República*. 1ª Série, n.º 167, 29 de agosto.

Assembleia da República (2015). Lei n.º 59/2015. Diário da República. *Diário da República*. 1ª Série, n.º 121, 24 de junho.

Centre for European Policy Studies (2010). CESP *Task Force Report – Protecting Critical Infrastruture in the EU*. p. 77. Bruxelas.

COM(2006) 786 final da Comissão das Comunidades Europeias, de 12 de dezembro. *Programa Europeu de Protecção das Infra-Estruturas Críticas*. Retrieved from:http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52006DC0786&from=PT.

EC COM(2006) 787 final, de 12 de dezembro. *Diretiva do Concelho para a identificação e designação de IC europeias e da necessidade de melhorar a sua proteção.*

Fernandes, L. (2014). *Intelligence e Segurança Interna*. Lisboa. ISCPSI.

Ministério da Defesa Nacional (2011). Decreto-Lei n.º 72/2011 de 09 de maio. *Diário da República*. 1ª Série, n.º 89, 09 de maio.

Oliveira, M. (2015). *A Segurança das Infraestruturas Críticas em Portugal*. Lisboa. UNL-Faculdade de Direito.

Oliveira, V. (2008). *Protecção de infra-estruturas críiticas - duas abordagens*. Lisboa. ISCPSI.

Pais, I & Gomes, H (2007). *Proteção de infraestruturas Críticas. A cooperação público privada.* Em C. Soares, A. Teixeira, & P. Antão, Riscos Públicos e Industriais (pp. 65-8). Lisboa. Edições Salamandra.

Presidência do Conselho de Ministros (2015). Resolução do Conselho de Ministros n.º 7-A/2015. *Diário da República*. 1ª Série, n.º 36, 20 de fevereiro.

Presidência do Conselho de Ministros (2015). Resolução do Conselho de Ministros n.º 36/2015. *Diário da República*. 1ª Série, n.º 113, 12 de junho.

Torres, J. (2015). *Gestão de Riscos – No planeamento, execução e auditoria de segurança*. Lisboa. ISCPSI-ICPOL.

RECIPE. Retrieved from: http://repository.tudelft.nl/view/tno/uuid%3A29f15365-8885-4278-82fe-996567858ae9/

Rodrigues, N. (2008). *A protecção e segurança das infra-estruturas críticas*. Lisboa. ISCPSI. Lisboa.

.

APÊNDICES

APÊNDICES

APÊNDICE A: Pedido autorização para a realização de Inquéritos

APÊNDICE B: Lista e dados técnicos dos especialistas e *policy-makers* inquiridos

APÊNDICE C: Guião do questionário aplicado aos especialistas e *policy-makers*

APÊNDICE D: Guião do questionário aplicado aos especialistas e *policy-makers* (CNPIC e SAIV) – versões em inglês e português

APÊNDICE E: Lista e dados técnicos dos operadores de IC inquiridos

APÊNDICE F: Guião do questionário aplicado aos operados de IC

APÊNDICE G: Quadro jurídico

APÊNDICE H: Lista de organismos dos EM e respetivos planos nacionais de proteção de IC

APÊNDICE I Glossário

APÊNDICE A

PEDIDO AUTORIZAÇÃO PARA A REALIZAÇÃO DE INQUÉRITOS

De: João Franca Da Fonseca Pestana
Enviado: terça-feira, 24 de maio de 2016 10:19
Para: ISCPSI - Direcção Ensino
Cc: Sergio Ricardo Felgueiras
Assunto: II CCDP - Pedido de autorização para realização de inquérito
Anexos: inquérito - perspetiva dos operadores de IC).pdf; Entrevista especialistas responsáveis e policy makers.pdf; Questionário modelos de governação.pdf

Exmo. Sr. Superintendente-Chefe Pedro Clemente

M.I. Diretor do ISCPSI,

A Portaria 199/2014, de 3 de outubro, aprova a estrutura curricular e o plano de estudos, bem como as normas de admissão, frequência, avaliação e organização do Curso de Comando e Direção Policial (CCDP).

Dos seus termos resulta que o CCDP integra uma componente letiva e compreende a realização de um relatório final sobre uma temática relevante para a segurança interna de entre os previamente definidos por Despacho exarado por S.Exa. o Diretor Nacional da PSP.

Neste sentido, João Franca da Fonseca Pestana, Comissário, N/M148125, subordinará o seu estudo sobre o macro tema n.º 14 – Sistema de Segurança Interna, tendo como objeto: ***A Proteção de Infraestruturas Críticas – Modelos de Governação, Atores e Papeis – Contributos para o desenvolvimento de um Programa Nacional de Proteção de Infraestruturas Críticas,*** do qual é orientador o Sr. Subintendente Tito Eurico Miranda Fernandes, Adjunto do Gabinete do Secretário Geral do Sistema de Segurança Interna.

Ambicionando a solidez, fundamentação e a credibilidade dos dados analisados, deseja recorrer a entrevistas semi-estruturadas, e a inquéritos nos seguintes moldes:

Inquérito "perspetiva dos Operadores de IC" (anexo):
Operadores de Infraestruturas Críticas

- EDP - Gestão da Produção de Energia S.A.
  (Security Officer)" Dr. Carlos Carvalho
- TURBOGÁS Prod. Energética S.A
  Engº Daniel Pereira (Director Produção)
- Centro de Produção de Energia Eléctrica do PEGO
  Engº Felicissimo Matos (Resp. Química e Eficiência)
- EDP - Distribuição Energia S.A.
  Engª Maria Luisa Pestana (Dep. de continuidade de Negócio)
- REN - Redes Energéticas Nacionais S.A.
  Engº Francisco Parada (Seg, Ambiente, Qualidade)
- GALPENERGIA SGPS
  Engº José Almeida (HSEQ Ambiente, Qualidade e Segurança)
- SIGÁS, Armazenagem de Gás ACE
  Engº Francisco Ventura da Silva

- CLC, Companhis Logística de Combustíveis, S.A.
  Engª Helena Adão (Dir. Qualidade)

- PORTSINES S.A.
  Engº Francisco Mocho (Resp. Segurança)

- AICEP GLOBAL PARQUES (esteira de pipelines)
  Dr. Miguel Borralho (Diretor da aicep Global Parques, Sines)"

- NAV PORTUGAL E.P.E. - Nav. Aérea de Portugal
  CTA José Matos (Adjunto Dir. Operações de Lisboa)

- ANA - AEROPORTOS DE PORTUGAL S.A.
  Engº Vitor Figueiredo

- ADMINISTRAÇÃO DOS PORTOS DO DOURO E LEIXÕES S.A.
  Comandante Rui Cunha

- ADMINISTRAÇÃO DO PORTO DE AVEIRO S.A.
  Comand. Armando Santos

- ADMINISTRAÇÃO DO PORTO DE LISBOA S.A.
  Comand. Esteves Cardoso

- ADMINISTRAÇÃO DOS PORTOS DE SESIMBRA E SETÚBAL S.A.
  Comand. Carlos Marques

- ADMINISTRAÇÃO DO PORTO DE SINES S.A.
  Comandante Brazuna Fontes

- TCL, TERMINAL DE CONTENTORES DE LEIXÕES
  Engº Álvaro Sérgio

- LISCONT, OPERADORES DE CONTENTORES S.A.
  Engº Alexandre Gonçalves

- TERSADO, TERMINAIS PORTUÁRIOS DO SADO, S.A.
  Engº Ricardo Lemos

- PSASINES - TERMINAIS DE CONTENTORES S.A.
  Engª Susana Romão

- DIRECÇÃO GERAL RECURSOS NATURAIS, SEGURANÇA E SERVIÇOS MARÍTIMOS
  Dr. Miguel Serrão

Inquérito "modelos europeus" (anexo):

- Bibiane Andujar - Responsável no Centro Nacional de Protección de Infraestruturas Críticas (Espanha)

- Samuel Donikian - Responsável no organismo *Securité des Activités D´Importance Vitale*, do Secretariado Nacional de Defesa e Segurança Nacional (França)

Entrevista "especialistas, responsáveis e policy makers" (anexo):

- Procuradora Geral Adjunta Maria Helena Fazenda (SGSSI)
- Superintendente-Chefe Paulo Lucas (PSP),
- Intendente Luís Elias - Gab. 1.º Ministro,
- Subintendente Norberto Rodrigues (PSP)
- Dr.ª Isabel Pais (ANPC),
- Eng. Miguel Serrão (DGRM),
- Eng. Francisco Parada (REN),
- Eng.ª Luísa Pestana (EDP),
- Tenente-Coronel Inglês (GNR);
- Comandante Pedro Daniel Vinhas Silva (AMN);
- Dr.ª Carla Pinto (ANAC)

Com os melhores cumprimentos,

João Pestana
Comissário

APÊNDICE B

LISTA E DADOS TÉCNICOS DOS ESPECIALISTAS E *POLICY-MAKERS* INQUIRIDOS

NOME	FUNÇÕES RELACIONADAS COM PIC
Superintendente-Chefe Paulo Lucas	Secretário-Geral Adjunto do Sistema de Segurança Interna Diretor Nacional Adjunto para a Unidade Orgânica de Operações e Segurança – PSP
Intendente Alexandre Coimbra	Chefe de gabinete do Secretário-Geral Sistema de Segurança Interna Chefe de gabinete do Diretor do Serviço de Informações de Segurança
Intendente Luís Elias	Assessor do gabinete do Primeiro-Ministro 2.º Comandante do Comando Metropolitano de Lisboa – PSP Chefe da Área Operacional – Comando Metropolitano de Lisboa – PSP
Tenente-Coronel Inglês	Oficial de Ligação da GNR junto do SP do Gabinete Coordenador de Segurança Oficial responsável pela área de proteção de IC no Sistema de Segurança Interna
Dr. Ricardo Carrilho (MAI)	Secretário-Geral Adjunto do Ministério da Administração Interna Coordenador das Relações Internacionais e da Gestão de Fundos Comunitários do MAI Responsável pela Avaliação Schengen
Capitão-de-fragata Pedro Daniel Vinhas Silva	Oficial de Ligação da Autoridade Marítima Nacional junto do SP do Gabinete Coordenador de Segurança
Subintendente Norberto Rodrigues	Chefe da Divisão de Policiamento e Ordem Pública do Departamento de Operações da DN/PSP Oficial de Ligação da PSP junto do SP do Gabinete Coordenador de Segurança Investigação científica no âmbito do Mestrado em Direito e

	Segurança da Faculdade de Direito da Universidade Nova de Lisboa
Eng. Miguel Serrão (DGRM)	Regulador no setor dos Transportes
Dr.ª Carla Pinto (ANAC)	Chefe do Departamento de Controlo e Qualidade AVSEC
Samuel Donikian	*Securité des Activités D´Importance Vitale - Le Secrétariat Général de la Défense et de la Sécurité Nationale*
Bibiane Andujar	*Centro Nacional de Protección de Infraestruturas Críticas*

APÊNDICE C

GUIÃO DO QUESTIONÁRIO APLICADO AOS ESPECIALISTAS E *POLICY-MAKERS*

A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS - "Questionário especialistas"

Desenvolvido no âmbito do 2.º Curso de Comando e Direção Policial, o presente questionário/entrevista tem por fim consolidar dados para o Relatório Final subordinado ao tema:

"A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS - CONTRIBUTOS PARA O DESENVOLVIMENTO DE UM PLANO NACIONAL DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS"

Neste contexto, as questões que compõem o questionário/entrevista visam obter a perspetiva de pessoas que têm, ou tiveram, num passado recente, responsabilidades operativas e de policy making, sobre qual deve ser, no futuro, o papel do Estado enquanto ator no apoio aos Operadores de Infraestruturas Críticas (IC), e na agilização das atividades de proteção de IC, tanto na vertente da prevenção como no domínio de resposta a ameaças deliberadas (Security).

Este breve inquérito tem uma duração estimada de resposta de entre 5 a 10 minutos.

Para que possa ser integrada no estudo, o seu contributo deverá ser enviada até ao dia 06 de junho.

As suas respostas são fundamentais para o sucesso deste estudo, pelo que desde já agradecemos a sua inestimável colaboração.

João Pestana
Comissário da PSP

Identificação

1. **Nome:**

_____

2. **Função actual:**

_____

3. **Funções ou cargos relacionadas com proteção de IC no presente ou no passado:**

_____

_____

_____

_____

_____

Instrumentos de governação no âmbito da proteção de IC

4. **Considera existir em Portugal um estratégia ou um plano nacional (integrador, abrangente e transversal), para a proteção de IC, que envolva de forma eficiente e empenhada os vários atores (Operadores de IC, Forças e Serviços de Segurança (FSS), Entidades reguladoras, universidades, entre outros)?**
Marcar apenas uma oval.

- ◯ Sim. Considero que existe uma estratégia ou plano nacional perfeitamente integrador e abrangente, que responde de forma eficiente aos desafios de proteção de IC, designadamente articulando de forma próxima, permanente e eficaz todos atores com responsabilidades nesta matéria.
- ◯ Não. Considero que existe diversa legislação avulsa sobre proteção de IC ao nível do security, com baixo nível de integração e coerencia, e que essencialmente aborda a matéria de forma setorial, mas que não é suficientemente abrangente, nem está devidamente integrada num plano macro, o que resulta numa abordagem pouco eficiente e desfasada das expetativas dos vários atores
- ◯ Outro: _____

5. **Se escolheu "outro" justifique**

_____

_____

_____

_____

_____

6. **Considerando que, quer a Lei n.º 53/2008 de 29 de agosto (Lei de Segurança Interna) quer o próprio Decreto-Lei n.º 62/2011 de 09 de maio, atribuem um vasto conjunto de competências ao Secretário-Geral do Sistema de Segurança Interna (SGSSI) em matéria de articulação da proteção de IC, nos domínios da prevenção e da coordenação na resposta a incidentes, qual lhe parece ser o nível de comprometimento e resultados alcançados até ao momento (na área da proteção de IC)?**
Marcar apenas uma oval.

- ◯ Muito elevado
- ◯ elevado
- ◯ baixo
- ◯ muito baixo

7. **Tendo em conta que no ordenamento jurídico nacional existe mais de uma dezena de diplomas legais, que fazem menção expressa à proteção de IC, bem como outros tantos que aludem indiretamente ao tema, e finalmente não esquecendo a intensa atividade da Comissão Europeia nesta área, considera útil a elaboração de uma estratégia ou de um plano nacional de proteção de IC, único, abrangente, concertado e integrador, que garanta uma maior atenção do Estado no domínio da proteção de IC? Por favor explicite a sua resposta**

   Marcar apenas uma oval.

   - ◯ Muito útil
   - ◯ Útil
   - ◯ Pouco útil
   - ◯ Inútil

8. **No caso de ter indicado "muito útil" ou "útil", considera importante que essa estratégia ou plano nacional contemple uma concentração de competências de governance e apoio aos diferentes atores na proteção de IC, que explore sinergias e know-how (atualmente disperso), criando para a sua implementação e execução um Organismo especializado e totalmente dedicado a esta matéria, à semelhança de alguns modelos europeus (Espanha, Inglaterra, entre outros)?**

   Marcar apenas uma oval.

   - ◯ Muito Importante
   - ◯ Importante
   - ◯ Pouco importante
   - ◯ Nada importante

O papel do Estado no apoio à proteção de IC

De acordo com a sua experiência, indique o grau de intervenção/empenho que o Estado deverá ter na prossecução das seguintes medidas/atividades:

9. **Proporcionar aos diferentes atores (Operadores de IC, FSS, Entidades reguladoras) informação e conhecimento sobre boas práticas de proteção de IC, do seu setor ou de outros, recolhidas tanto a nível nacional como internacional.**

   Marcar apenas uma oval.

   - ◯ Muito importante
   - ◯ Importante
   - ◯ Pouco importante
   - ◯ Nada importante

10. **Proporcionar acesso a informação sobre potenciais ameaças a IC, que possam contribuir para um melhor nível de proteção.**

    Marcar apenas uma oval.

    - ◯ Muito importante
    - ◯ Importante
    - ◯ Pouco importante
    - ◯ Nada importante

11. **Organizar e proporcionar o acesso a workshops com vários Operadores de IC, e com outros atores (FSS, entre outros), para discussão e partilha de boas práticas de proteção/resposta a incidentes, rentabilizando desta forma o know-how que se encontra disperso entre o setor público e o setor privado.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

12. **Proporcionar apoio técnico na deteção de vulnerabilidades em IC (quando, e na medida do solicitado pelo Operador de IC) através de especialistas das Forças de Segurança e/ou de outros Organismos de reconhecida competência (Laboratório Nacional de Engenharia Civil, universidades, Entidades reguladoras, entre outros).**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

13. **Organizar exercícios de tomada de decisão, ou simulacros, abrangendo IC do mesmo setor e outros atores (Forças de Segurança, Entidades reguladoras, entre outros).**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

14. **Organizar exercícios de tomada de decisão, ou simulacros, abrangendo IC de diversos setores, com exploração de efeitos sistémicos como os "fenómenos de cascata".**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

15. **Disponibilizar equipas de peritos/observadores, provenientes de Organismos de reconhecida competência no âmbito da segurança (Security), para observação e avaliação técnica de exercícios/simulacros.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada Importante

16. **Agilizar contactos entre os Operadores de IC e os responsáveis das Forças de Segurança ao nível local (localidade onde se insere cada uma das IC).**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada Importante

17. **Facilitar e promover a partilha de informação entre responsáveis locais das Forças de Segurança e Agentes de ligação de segurança de IC (nível local), com vista a uma intervenção mais adequada, bem como à agilização/treino de procedimentos conjuntos em caso de necessidade de intervenção.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

18. **Implementar verificações de segurança a funcionários que venham a desempenhar funções de elevada criticidade no contexto de IC (nos termos de legislação em vigor ou a regulamentar no futuro).**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

19. **Criar e gerir sistemas de informação geográfica com informação organizada relativa à proteção de IC.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

20. **Implementar e gerir uma plataforma de contacto com Operadores ou outros atores.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada Importante

21. **Operacionalizar uma sala de situação (crise) para apoio e coordenação de respostas a incidentes em IC que envolvam a responsabilidade partilhada e a utilização meios de várias Entidades, quer públicas quer privadas.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada Importante

APÊNDICE D

GUIÃO DO QUESTIONÁRIO APLICADO AOS ESPECIALISTAS E *POLICY-MAKERS* (CNPIC E SAIV) – VERSÕES EM INGLÊS E PORTUGUÊS-

2ND POLICE DIRECTION AND COMMAND TRAINNING COURSE - 2016

FINAL REPORT

CRITICAL INFRASTRUTURE PROTECTION

EUROPEAN UNION BEST PRACTICES SURVEY

1. Has your country developed a national plan or equivalent strategy specially focused on CIP?

2. Does your country have, within the national administration, a central and coordinator public organ or agency (such as a Centre, a Bureau, a Directorate or equivalent entity) responsible for establishing and implementing CIP measures?

3. How important do you consider the setting up and activity of such a public body/agency? Choose one of the following options: a) essential; b) very important; c) important; d) not so important; e) not important at all. Please give some reasons for your choice, according to your own experience.

4. In case of having such a Body/Agency where is it settled (Ex. Prime Minister Bureau, Minister of the Interior, National Police, other entity) and to whom does it report.

5. What kind of concerns, problems and challenges does this public agency addresses (security, safety/natural hazards, cybersecurity...)?

6. Who are the beneficiaries, the ones who profit from the work of this public agency? Ex: central administration, local administration, security forces (police authorities), intelligence services, critical infrastructures operators, sector regulators, general public (ex: by launching public campaigns, etc.) other entities.

7. Which tasks/assignments are to be carried out in your Country by the aforesaid central CPI agency? specify if you think any adjustment is required to meet your CPI agency activities.

   (Answer *Yes* or *No* and, in any case, specify how in your opinion each task might be important by adding: *Very important* / *Important* / *Not important, Not important at all*)

   a. National Contact Point for the European Directive (2008/114/CE)

   b. Identification/Designation of CI at both national and European level

   c. CIP policy making and definition of general guidelines to be implemented at national level by other public entities, sector regulators and CI operators.

   d. Preparation and development of technical studies on issues related to CIP (even if in collaboration with other entities)

   e. Information and intelligence sharing among CI operators and other relevant entities, regarding potential threats posed to security of CI (in general, or targeting a specific CI).

   f. Promotion and organization of workshops, training courses or seminars attended by the core CPI actors (including, inter alia, CI operators, sector regulators, intelligence services and security forces) aimed to approach and discuss a wide variety of CIP topics, promote preparedness, improve response to crisis and share experience, know-how and good practices.

   g. Making expert support teams available to provide assistance for assessment of CI vulnerabilities and security improvement (upon request by operators)

h. Promoting/conducting table-top, decision making and/or simulation exercises involving actors from the same sector/CPI area.

i. Promoting/conducting table-top, decision making and/or simulation exercises involving actors from different CPI areas, in order to explore and learn about the systemic "cascading effects".

j. Providing expert teams and highly qualified observers in the field of security for CPI exercises monitoring and assessment (upon request by operators)

k. Promoting and encouraging, at local level, open and permanent communication channels between CI operators and other relevant actors, such as municipal/regional/provincial authorities and local security forces.

l. Maintaining an fostering dialogue and information-sharing amongst CI operators (Security Liaison Officers) and local authorities directly concerned, such as police forces, as well as promoting training exercises for the implementation of suitable procedures to be applied in the event of a real crisis, aiming to facilitate, strengthen and speed up mutual collaboration, with the ultimate purpose of ensuring the highest possible levels of cooperation and coordination.

m. Security Vetting Checks implementation

n. Setting up and management of IT data base(s) containing organized information related with CI (such as location, contact numbers, main characteristics...)

o. Setting up and managing a national IT platform connecting different operators (or other relevant actors) and CIP central body/agency.

p. Activating crisis/emergency room to support and/or coordinate the public-private response to CI incidents.

q. Providing (to the core CIP actors) updated knowledge and innovative proceedings regarding best practices on CI protection, collected by the CIP agency, both at national and international level.

Thank you for your collaboration
João Pestana

2º CURSO DE COMANDO E DIREÇÃO POLICIAL - 2016

RELATÓRIO FINAL

PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

INQUÉRITO DE BOAS PRÁTICAS NA UNIÃO EUROPEIA

1. No seu país existe um plano nacional ou uma estratégia específico para a proteção de IC?

2. No seu país existe um organismo (tal como um Centro, um Gabinete, um Departamento ou uma entidade equivalente) da Administração Pública responsável por estabelecer e implementar medidas de proteção de IC?

3. Considera essencial a existência de um organismo desta natureza para a implementar e desenvolver um plano nacional de proteção de IC? Escolha uma das seguintes opções: a) essencial; b) muito importante; c) importante; d) pouco importante; e) nada importante. De acordo com a sua experiência, indique, por favor, algumas razões que justificam a escolha.

4. Em termos de posicionamento no aparelho do Estado, onde se insere o organismo (Ex.: gabinete do Primeiro-Ministro, do Ministro da Administração Interna, da Polícia, outra entidade) e de quem depende?

5. Que vertentes de proteção de Infraestruturas Críticas este organismo desenvolve (*security*, *safety*, cibersegurança)?

6. Quem são os beneficiários do trabalho deste organismo? (Ex.: administração central, administração local, forças de segurança (autoridades policiais), serviços de informações / inteligência, operadores de IC, reguladores setoriais, público em geral e outras entidades.

7. Quais as competências e atividades que este organismo prossegue?

(Responda *Sim* ou *Não e*, especifique a importância de cada tarefa, adicionando: *Muito importante / Importante / Pouco importante, Nada importante*)

a. Ponto de contacto no âmbito da Diretiva n.º 2008/114/CE, do Conselho, de 8 de dezembro

b. Identificação e designação de infraestruturas críticas (Nacionais e Europeias)

c. Produção de políticas ou de diretivas de âmbito nacional na área da proteção de IC.

d. Produção de estudos e trabalhos técnicos no âmbito da proteção de IC.

e. Partilha de informação sobre potenciais ameaças com os operadores de IC ou outros atores relevantes com vista a uma melhor proteção de IC.

f. Organização de *workshops* com vários atores (operadores de IC , forças e serviços de segurança, serviços de Informações, entre outros), para discussão e partilha de boas práticas de poteção de IC, bem como para resposta a incidentes.

g. Proporcionar apoio técnico na deteção de vulnerabilidades da IC, através de especialistas das forças de segurança e/ou de outros organismos competentes).

h. Organização de exercícios de tomada de decisão ou de simulacros, abrangendo IC do mesmo setor.

i. Organização de exercícios de tomada de decisão ou de simulacros, abrangendo IC de diversos setores, com exploração de efeitos sistémicos como "fenómenos cascata".

j. Disponibilização de equipas de peritos/observadores, provenientes de organismos de reconhecida competência no âmbito da segurança (*security*), para observação e avaliação técnica de exercícios/simulacros.

k. Promover e incentivar, a nível local, canais de comunicação permanentes entre os operadores de IC e outros atores relevantes, tais como as autoridades municipais / regionais / provinciais e forças de segurança locais

l. Manter e fomentar o diálogo e intercâmbio de informações entre os operadores de IC (oficiais de ligação de segurança) e as autoridades locais diretamente envolvidas, tais como as forças policiais, bem como a promoção de exercícios de treino para a implementação de procedimentos adequados a serem aplicados em caso de uma crise real, com o objetivo de facilitar, reforçar e acelerar a colaboração mútua, com o objetivo final de garantir os mais altos níveis possíveis de cooperação e coordenação.

m. Implementação de procedimentos de *security vetting check*

n. Criação e gestão de sistemas de informação com informação organizada relativa à proteção de IC.

o. Implementação e gestão de plataforma de contacto com operadores ou outros atores.

p. Operacionalização de Sala de Crise para apoio e coordenação de resposta a incidentes em IC.

q. Providing (to the core CIP actors) updated knowledge and innovative proceedings regarding best practices on CI protection, collected by the CIP agency, both at national and international level.

Agradecido pela sua colaboração
João Pestana

APÊNDICE E

LISTA E DADOS TÉCNICOS DOS OPERADORES DE IC INQUIRIDOS

SETOR / SUBSETOR	OPERADORES
Energia Elétrica	EDP - Gestão da Produção de Energia S.A.
Energia Elétrica	Centro de Produção de Energia Elétrica do PEGO
Energia Elétrica	EDP - Distribuição Energia S.A.
Energia Elétrica Gás Natural	REN - Redes Energéticas Nacionais S.A.
Combustíveis	GALPENERGIA SGPS
Combustíveis	SIGÁS, Armazenagem de Gás ACE
Combustíveis	CLC, Companhia Logística de Combustíveis, S.A.
Combustíveis	PORTSINES S.A.
Combustíveis	AICEP GLOBAL PARQUES (esteira de pipelines)
T. Aéreo	NAV PORTUGAL E.P.E. - Nav. Aérea de Portugal
T. Aéreo	ANA - AEROPORTOS DE PORTUGAL S.A.
T. Marítimo	ADMINISTRAÇÃO DOS PORTOS DO DOURO E LEIXÕES S.A.
T. Marítimo	ADMINISTRAÇÃO DO PORTO DE AVEIRO S.A.
T. Marítimo	ADMINISTRAÇÃO DO PORTO DE LISBOA S.A.
T. Marítimo	ADMINISTRAÇÃO DOS PORTOS DE SESIMBRA E SETÚBAL S.A.
T. Marítimo	ADMINISTRAÇÃO DO PORTO DE SINES S.A.
T. Marítimo	TCL, TERMINAL DE CONTENTORES DE LEIXÕES
T. Marítimo	LISCONT, OPERADORES DE CONTENTORES S.A.
T. Marítimo	TERSADO, TERMINAIS PORTUÁRIOS DO SADO, S.A.
T. Marítimo	PSASINES - TERMINAIS DE CONTENTORES S.A.
T. Marítimo	DG RECURSOS NATURAIS, SEGURANÇA E SERVIÇOS MARÍTIMOS

APÊNDICE F

GUIÃO DO QUESTIONÁRIO APLICADO AOS OPERADORES DE IC

Proteção de Infraestruturas Críticas - Questionário operadores de IC

Desenvolvido no âmbito do 2.º Curso de Comando e Direção Policial, o presente inquérito tem por fim consolidar dados para o Relatório Final subordinado ao tema:

"A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS - CONTRIBUTOS PARA O DESENVOLVIMENTO DE UM PROGRAMA NACIONAL DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS"

Neste contexto, as questões que compõe o inquérito visam obter a perspetiva dos vários Operadores de Infraestruturas Críticas (OIC) sobre qual deverá ser o papel do Estado enquanto ator no apoio aos OIC, e na agilização das actividades de Proteção de Infraestruturas Críticas (IC), tanto na vertente da prevenção como na vertente de resposta a ameaças deliberadas (Security).

As suas respostas - fundamentais para o sucesso deste estudo - serão rigorosamente anónimas e serão tratadas de forma agregada com as respostas dos restantes operadores, não permitindo a identificação individual.

Estimamos que o inquérito tenha uma duração de preenchimento de aproximadamente 15 minutos, e ficará disponível online até ao dia 06 de Junho.

É fundamental que "valide" o inquérito no final, clicando no campo próprio

Desde já agradecemos a sua inestimável colaboração.

Caracterização

1. **Qual o Sector a que pertence enquanto Operador de IC**
   Marcar apenas uma oval.

   - ◯ Energia
   - ◯ Transportes

As Atividades de Proteção de Infraestruturas Críticas

Indique, na perspectiva do Operador de Infraestrutura Crítica (OIC) de que forma valoriza as seguintes actividades de proteção

---

2. **Acesso a informação e conhecimento sobre boas práticas de Proteção de Infraestruturas críticas (IC), do seu sector ou de outros, recolhidas tanto a nível nacional como internacional.**
   Marcar apenas uma oval.

   - ◯ Muito importante
   - ◯ Importante
   - ◯ Pouco importante
   - ◯ Nada importante

3. **Acesso a informação sobre potenciais ameaças a IC, no seu sector ou em outros, que possam contribuir para um melhor nível de proteção.**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

4. **Acesso a workshops com vários OIC, e/ou com outros actores (Forças e Serviços de Segurança, Serviços de Informações, entre outros), para discussão e partilha de boas práticas de proteção/resposta a incidentes**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

5. **Apoio técnico na deteção de vulnerabilidades da IC (quando, e na medida do solicitado pelo OIC) através de especialistas das Forças de Segurança e/ou de outros organismos competentes (Laboratório Nacional de Engenharia Civil, Universidades, Entidades reguladoras, entre outros)**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada Importante

6. **Participação em exercícios de tomada de decisão, ou em simulacros, abrangendo IC do mesmo sector**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

7. **Participação em exercícios de tomada de decisão, ou em simulacros, abrangendo IC de diversos sectores, com exploração de efeitos sistémicos como os "fenómenos de cascata".**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

8. **Possibilidade de solicitar equipas de peritos/observadores, provenientes de organismos de reconhecida competência no âmbito da segurança (Security), para observação e avaliação técnica de exercícios/simulacros**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

9. **Maior proximidade e facilidade de acesso aos responsáveis locais das Forças de Segurança (ao nível da localidade onde se insere cada uma das IC)**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

10. **Disponibilização de elementos de informação sobre a IC (nível local) aos responsáveis das Forças de Segurança, que permitam uma intervenção mais adequada, e agilização/treino de procedimentos conjuntos em caso de necessidade de intervenção**
Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

11. **Indique sumariamente outras atividades que considere relevantes para o aumento da proteção de IC**

_____

_____

_____

_____

_____

O papel do Estado no apoio à proteção de IC

De acordo com a sua experiência e perceção, indique o grau de intervenção/empenho que o Estado tem demonstrado na prossecução das seguintes medidas/actividades:

12. **Proporcionar aos OIC informação e conhecimento sobre boas práticas de proteção de Infraestruturas críticas, do seu sector ou de outros, recolhidas tanto a nível nacional como internacional.**
Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco Significante
- ◯ Insignificante

13. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

14. **Proporcionar acesso a informação sobre potenciais ameaças a IC, no seu sector ou em outros, que possam contribuir para um melhor nível de proteção**
Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

15. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

16. **Organizar e proporcionar o acesso a workshops com vários OIC, e/ou com outros atores (Forças e Serviços de Segurança, Serviços de Informações, entre outros), para discussão e partilha de boas práticas de proteção/resposta a incidentes**
Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

17. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

18. **Proporcionar apoio técnico na deteção de vulnerabilidades da IC (quando, e na medida do solicitado pelo OIC) através de especialistas das Forças de Segurança e/ou outros organismos de reconhecida competência (Laboratório Nacional de Engenharia Civil, Universidades, Entidades reguladoras, entre outros)**

Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

19. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

20. **Organização de exercícios de tomada de decisão, ou simulacros, abrangendo IC do mesmo sector**

Marcar apenas uma oval.

- ◯ Muito Significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

21. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

22. **Organização de exercícios de tomada de decisão, ou simulacros, abrangendo IC de diversos sectores, com exploração de efeitos sistémicos como os "fenómenos de cascata"**

Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

23. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

24. **Disponibilização de equipas de peritos/observadores, provenientes de organismos de reconhecida capacidade no âmbito da segurança (Security), para observação e avaliação técnica de exercícios/simulacros**

Marcar apenas uma oval.

- ◯ Muito Significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

25. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

26. **Agilização de contactos com os responsáveis locais das Forças de Segurança (ao nível da localidade onde se insere cada uma das IC)**

Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco significante
- ◯ Insignificante

27. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

28. **Facilitação e promoção da partilha de informação entre responsáveis locais das Forças de Segurança e responsáveis de segurança de IC (nível local), com vista a uma intervenção mais adequada, bem como à agilização/treino de procedimentos conjuntos em caso de necessidade de intervenção**

Marcar apenas uma oval.

- ◯ Muito significante
- ◯ Significante
- ◯ Pouco Significante
- ◯ Insignificante

29. **Caso tenha respondido "Significante" ou "Muito significante" enumere exemplos da intervenção/iniciativa do Estado**

_____

_____

_____

_____

_____

Plano Nacional de Proteção de Infraestruturas Críticas

Nota prévia: Consideramos que não existe, em Portugal, e ao contrário de outros países, um verdadeiro Plano Nacional de Proteção de Infraestruturas Críticas (PNPIC), embora existam algumas decisões e escolhas governativas que enquadram a temática

30. **Indique, tendo em conta as respostas anteriores, e o conhecimento da realidade de outros países como Espanha, França, Inglaterra entre outros, qual a importância de ser constituído um Organismo, que se dedique especificamente às matérias de facilitação e coordenação da proteção de IC, com vista a prosseguir as atividades mencionadas nas questões anteriores, dando, desta forma, apoio a todos os atores intervenientes e criando pontes entre o sector público e privado.**

Marcar apenas uma oval.

- ◯ Muito importante
- ◯ Importante
- ◯ Pouco importante
- ◯ Nada importante

APÊNDICE G

QUADRO JURÍDICO

	Normativo	Conteúdos	atores
ESPECÍFICO - INFRAESTRUTURAS CRITICAS			
Comunicação da Comissão relativa a um Programa Europeu de PIC	**Índice**	**1. CONTEXTO** **2. OBJECTIVOS, PRINCÍPIOS E CONTEÚDO DO PEPIC** **2.1. Objectivo do PEPIC** **2.2. Tipos de ameaças abrangidas pelo PEPIC** **2.3. Princípios** **2.4. Enquadramento PEPIC** **2.5. Grupo de Contacto PIC** **3. INFRA-ESTRUTURAS CRÍTICAS EUROPEIAS (ICE)** **4. MEDIDAS DESTINADAS A FACILITAR O DESENVOLVIMENTO E A APLICAÇÃO DO PEPIC** **4.1. Plano de Acção PEPIC** **4.2. Rede de Alerta para as Infra-Estruturas Críticas da União Europeia (RAIC)** **4.3. Grupos de peritos** **4.4. Processo de intercâmbio de informações sobre a protecção das infra-estruturas Críticas** **4.5. Identificação de interdependências** **5. INFRA-ESTRUTURAS CRÍTICAS NACIONAIS (ICN)** **6. PLANOS DE EMERGÊNCIA** **7. VERTENTE EXTERNA** **8. MEDIDAS DE ACOMPANHAMENTO FINANCEIRO** **ANEXO - Plano de Acção PEPIC**	Estados Membros
Dir. 2008/114/CE	Índice	*Artigo 1.o* **Objecto** *Artigo 2.o* **Definições** *Artigo 3.o* **Identificação das ICE** *Artigo 4.o* **Designação das ICE** *Artigo 5.o* **Planos de segurança dos operadores** *Artigo 6.o* **Agentes de ligação de segurança** *Artigo 7.o* **Relatórios** *Artigo 8.o* **Apoio da Comissão às ICE** *Artigo 9.o* **Informações sensíveis relacionadas com a protecção das ICE** *Artigo 10.o* **Pontos de contacto para a protecção das ICE** *Artigo 11.o* **Revisão** *Artigo 12.o* **Execução** *Artigo 13.o* **Entrada em vigor** *Artigo 14.o* **Destinatários** *ANEXO I* **Lista dos sectores de ICE** *ANEXO II* **Procedimento aplicável ao PSO das ICE** *ANEXO III* **Procedimento aplicável à identificação EM das IC susceptíveis de serem designadas como ICE nos termos do artigo 3.o**	Estados Membros

	Normativo	Conteúdos	Acores
ESPECÍFICO - INFRAESTRUTURAS CRITICAS			
DL 62/2011	10.º n.º 1	Elaboram PSO	OIC
	4 e seg.	Identificação das IC	ANPC
	Art.º 8	Designação: informa anualmente à CE quais as ICE identificadas	ANPC
	10 n. º4	parecer da FSTC sobre o PSO	FSTC
	10 n. º4	Validação do PSO	SGSSI
	10 n. º5	Plano de Segurança e Proteção Exterior	FSTC
	11.º n. º1	Agente de Ligação de Segurança	OIC
	11.º n.º 1	Articulação entre ALS e SGSSI	SGSSI/FS/ OIC
	11 n. º2	troca de informações relativas a riscos e ameaças	SGSSI / FSTC / OIC
	12 n.º 1	Avaliação de Ameaça aos subsectores	SGSSI/FSS
	12 n. º2	Relatório bienal de dados para a Comissão Europeia	SGSSI
	13 n. º1	Apoiar os OIC facultando acesso às melhores práticas e metodologias, formação	Entidades competentes
	14 n. º2	Qualquer pessoa que trate informação classificada é sujeita a procedimento de habilitação de segurança	ANS
	15 n. º1	Ponto de contacto CE no plano da designação de ICE	ANPC
	15 n. º2	Ponto de contacto CE no plano da segurança de ICE	SGSSI

	Normativo	Conteúdos	Acores
SEGURANÇA INTERNA			
Lei de segurança interna 53/2008 - Alterada pela lei 59/2015	16n.º2 b)	Coordenar ações conjuntas de formação, aperfeiçoamento e treino das forças e dos serviços de segurança;	SGSSI - através de FSS
	16 n. º2 c)	Reforçar a colaboração entre todas as forças e os serviços de segurança, garantindo o seu acesso às informações necessárias	
	16 n. º2 d)	Garantir a coordenação entre as forças e os serviços de segurança e os serviços de emergência médica, segurança rodoviária e transporte de e segurança ambiental, no âmbito da definição e execução de planos de segurança e gestão de crises	
	18 n. º2 b)	Articulação das FSS necessários à gestão de incidentes tático-policiais graves	
	18 n. º3 a)	Classifica Incidentes tático-policiais graves - os que ocorram em IC	
	Art.º 19.º	**1** - Em situações extraordinárias, determinadas pelo PM após comunicação fundamentada ao PR, de ataques terroristas ou de acidentes graves ou catástrofes que requeiram a intervenção conjunta e combinada de diferentes FSS e, eventualmente, do SIOP, estes são colocados na dependência operacional do SGSSI, através dos seus dirigentes máximos.	
	Art.º 35.º	As FA colaboram em matéria de SI nos termos da Constituição e da lei, competindo ao SGSSI e ao CEMGFA assegurarem entre si a articulação operacional.	

	Normativo	Conteúdos	atores
SEGURANÇA INTERNA			
Estratégia Nacional de Combate ao Terrorismo RCM 7-A/2015	c) proteger	Proteger - Fortalecer a segurança dos alvos prioritários, reduzindo quer a sua vulnerabilidade, quer o impacto de potenciais ameaças terroristas. A proteção concretiza-se no aumento da segurança das pessoas, das fronteiras, da circulação de capitais, das mercadorias, dos transportes, da energia e das IC, nacionais e ou europeias.	SGSSI - UCAT
	c) *vi)*	Desenvolver um registo central de identificação de infraestruturas criticas, em todos os setores de atividade económica e social, e prover à sua atualização;	
	c) *vii)*	Desenvolver o Plano de Ação para a Proteção de Aumento da Resiliência das IC nacionais e europeias, com os respetivos PSO e planos de segurança externos da responsabilidade das FSS e da ANPC	
	c) *x)*	Avaliar periodicamente as vulnerabilidades resultantes de infraestruturas essenciais, nacionais e europeias, para transportes e energia,	
	c) *xi)*	avaliar as vulnerabilidades dos sistemas de informação críticos e manter e acompanhar a adoção das medidas de correção face a ciber-ataques;	
	e) *vi)* responder	Reforçar a cooperação e a colaboração com todos os agentes de proteção civil e de emergência médica	
	6 A) *i)*	a cooperação entre as FA e as FSS é aprofundada em situações de intervenção perante agressões terroristas de acordo com o Plano de Articulação e Operacional que contempla medidas de coordenação e a interoperabilidade de sistemas de equipamentos, serviços de proteção civil, emergência médica e FA	
	6 A) *ii)*	De acordo com o PNPIC, atribuindo ainda especial atenção à vigilância e ao controlo das acessibilidades marítima, aérea e terrestre ao território nacional.	

	Normativo	Conteúdos
Estratégia Nacional de Segurança no Ciberespaço RCM 36/2015	objetivos estratégicos	**c)** fortalecer e garantir a segurança do ciberespaço, das IC e dos serviços vitais nacionais.
	Eixo 1 - Estrutura de Segurança do ciberespaço	2) consolidar papel de coordenação do Coordenação Operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às IC, do CNCS
		d) desenvolve e aplica medidas que visem a capacitação humana e tecnológica das IC com vista à prevenção e à reação de e a incidentes de cibersegurança
		e) com vista à eficácia operacional e a uma melhor avaliação situacional, devem ser criados mecanismos de reporte de incidentes de cibersegurança para entidades públicas e para os OIC. A desejada avaliação situacional resulta na criação de condições para a identificação de um nível de alerta nacional em matéria de segurança do ciberespaço, partilhado entre todas as entidades envolvidas.
		f) em articulação com as autoridades competentes e a comunidade nacional de segurança do ciberespaço o CNCS deve criar uma base de conhecimento que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades públicas e os OIC
	Eixo 3 - proteção do ciberespaço e das infraestruturas. Medidas a adotar	1) avaliar a maturidade e a capacidade das entidades públicas e privadas que administrem IC ou serviços vitais de informação, no que respeita à segurança do ciberespaço;
		2) promover a adaptação e melhoria contínua da segurança dos sistemas de informação das entidades públicas, dos OIC e dos serviços vitais de informação, para assegurar uma maior resiliência nacional, adaptando-os aos novos riscos e ameaças do ciberespaço.
		4) desenvolver a capacidade de deteção de ataques aos sistemas de informação, especialmente os das entidades publicas e as IC nacionais, a qual deve permitir alertar as entidades competentes, ajudar a entende a natureza dos ataques e criar as necessárias contramedidas;
		5) promover a aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os OIC de IC;
		6) incluir medidas de segurança do ciberespaço nos planos de proteção de IC nacionais, seguindo uma abordagem baseada na gestão de risco
		7) incluir medidas para fazer face a ameaças no ciberespaço nos planos de segurança dos OIC nacionais e europeias
		10) os OIC têm o dever de reportar falhas e interferências de segurança do ciberespaço nos seus sistemas. Por outro lado, deve ser estabelecido, em cada um destes OIC, um conjunto de meios técnicos e humanos mínimos dedicados à função de segurança do ciberespaço.
		13) garantir a proteção das infraestruturas de informação críticas, através de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN)
	Eixo 4 - Educação, sensibilização	7) promover formação especializada junto dos decisores e gestores públicos e de IC, numa ótica de consciencialização e prevenção para a necessidade de salvaguardar os interesses e informação crítica nacional

	Normativo	Conteúdos	atores
DEFESA E ESTADOS DE EXCEÇÃO			
Conceito Estratégico de Defesa Nacional	VI. Conceito de ação Estratégica Nacional	Para responder eficazmente à ameaça das redes terroristas, Portugal deve desenvolver uma estratégia nacional e integrada que articule medidas diplomáticas, de controlo financeiro, judiciais, de informação pública e de informações policiais e militares. Deve ainda atribuir especial atenção à vigilância e controlo das acessibilidades marítima, aérea e terrestre ao território nacional. Neste domínio, adquire grande acuidade a implementação de um ***Programa Nacional de Proteção das Infraestruturas Críticas***	FA
		Definem-se como linhas de ação prioritárias: garantir a ***proteção das infraestruturas de informação críticas***, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN)	
Lei Orgânica n.º 1-A/2009 Lei Orgânica de Bases da Organização das FA	4.º n.º 1 e)	Incumbe às FA: cooperar com as FSS tendo em vista o cumprimento conjugado das respetivas missões no combate a agressões ou ameaças transnacionais;	
	4.º n.º 2	As FA podem ser empregues, nos termos da Constituição e da lei, quando se verifique o estado de sítio ou de emergência.	
	9.º n.º 4	Organização do EMGFA: O Comando Operacional Conjunto (COC), dotado das valências necessárias de comando, controlo, comunicações e sistemas de informação, é o órgão permanente para o exercício, por parte do CEMGFA, do comando de nível operacional das forças e meios da componente operacional em todo o tipo de situações e para as missões específicas das FA consideradas no seu conjunto…	COC/FA/CEMGFA
	9.º n.º 5	O COC assegura ainda a ligação com as FSS e outros organismos do Estado relacionados com a segurança e defesa e a Proteção Civil, no âmbito das suas atribuições.	COC/FA/CEMGFA/ANPC
	11.º n. º1 x)	Compete ao CEMGFA exercer, em estado de guerra ou de exceção, o comando operacional das FS quando, nos termos da lei, aquelas sejam colocadas na sua dependência	CEMGFA/FSS
	11.º n.2 d)	Compete ainda ao EMGFA.assegurar, com o SGSSI, a articulação operacional relativa à cooperação entre as FA e as forças e os serviços de segurança para os efeitos previstos na alínea e) do n.º 1 do artigo 4.º;	CEMGFA/SGSSI/FSS/FA
	26.º n. º1	As FA e as forças e os serviços de segurança cooperam tendo em vista o cumprimento conjugado das suas missões para os efeitos previstos na alínea e) do n.º 1 do artigo 4.º	FA/FSS
	26.º n.º 2	Para assegurar a cooperação prevista no número anterior, são estabelecidos as estruturas e os procedimentos que garantam a interoperabilidade de equipamentos e sistemas, bem como o uso em comum de meios operacionais	
	26.º n.º 3	Compete ao CEMGFA e ao SGSSI assegurar entre si a articulação operacional, para os efeitos previstos nos números anteriores.	CEMGFA/SGSSI

	Normativo	Conteúdos	atores
DL n.º 138/2014 Regime de Salvaguarda dos ativos Estratégicos Essenciais	1.º Objeto	salvaguarda de ativos estratégicos essenciais para garantir a defesa e segurança nacional e a segurança do aprovisionamento do País em serviços fundamentais para o interesse nacional, nas áreas da energia, dos transportes e comunicações, enquanto interesses fundamentais de segurança pública.	Conselho de Ministros sob proposta do Ministro da respetiva área
	2.º a)	«Ativos estratégicos», as principais infraestruturas e ativos afetos à defesa e segurança nacional ou à prestação de serviços essenciais nas áreas da energia, transportes e comunicações;	
	2.º b)	«Controlo», a possibilidade de exercer uma influência determinante sobre o ativo estratégico, nos termos do n.º 3 do artigo 36.º da Lei n.º 19/2012, de 8 de maio;	
	3.º n. º1	…opor -se à realização de operações das quais resulte, direta ou indiretamente, a aquisição de controlo, direto ou indireto, por uma pessoa ou pessoas de países terceiros à União Europeia e ao Espaço Económico Europeu, sobre ativos estratégicos, independentemente da respetiva forma jurídica, nos casos em que se determine que estes possam pôr em causa, de forma real e suficientemente grave, a defesa e segurança nacional ou a segurança do aprovisionamento do País em serviços fundamentais para o interesse nacional,	
	3.º n. º2	2 — O caráter real e suficientemente grave de ameaça à defesa e à segurança nacional ou à segurança do aprovisionamento do País em serviços fundamentais para o interesse nacional a que se refere o número anterior é apreciado tendo em conta exclusivamente os seguintes critérios:	
	3.º n.º 2 a)	A segurança física e a integridade dos ativos estratégicos;	
	3.º n.º 2 b)	A permanente disponibilidade e operacionalidade dos ativos estratégicos...	
	3.º n.º 2 c)	A continuidade, regularidade e qualidade dos serviços de interesse geral prestados pelas pessoas que controlem os ativos estratégicos;	
	3.º n.º 2 d)	A preservação da confidencialidade, imposta por lei ou contrato público, dos dados e informações obtidos no exercício da sua atividade pelas pessoas que controlem os ativos estratégicos e do património tecnológico necessário à gestão dos ativos estratégicos	

	Normativo	Conteúdos
Regulamento (UE) N. o 513/2014 Fundo para a Segurança Interna	15	No quadro global do Fundo, a assistência financeira prestada ao abrigo do Instrumento deverá dar apoio à … proteção das pessoas e das IC contra incidentes relacionados com a segurança e a gestão eficaz dos riscos relacionados com a segurança e das crises,
	35	Atendendo a que os objetivos do presente regulamento, nomeadamente a proteção de IC contra incidentes relacionados com a segurança, não podem ser suficientemente alcançados pelos Estados-Membros, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5. o do TUE…
	3.º n.º 2. b)	Objetivos específicos: b) reforçar a capacidade dos Estados-Membros e da União para … preparar e proteger as pessoas e as IC contra ataques terroristas e outros incidentes relacionados com a segurança
	3.º n.º 3. e)	Objetivos operacionais: e) Medidas destinadas a reforçar a capacidade administrativa e operacional dos Estados-Membros para proteger as IC em todos os setores da atividade económica, incluindo através de parcerias entre os setores público e privado, e de uma melhor coordenação, cooperação, intercâmbio e divulgação de conhecimentos e experiências dentro da União e com os países terceiros relevantes;
	Anexo I - Lista das Prioridades Estratégicas	Medidas destinadas a reforçar a capacidade administrativa e operacional dos Estados-Membros para proteger as IC em todos os setores económicos, incluindo os abrangidos pela Diretiva 2008/114/CE do Conselho (1), nomeadamente projetos que promovam a criação de parcerias entre os setores público e privado, com vista a reforçar a confiança e a facilitar a cooperação, a coordenação, a elaboração de planos de contingência e o intercâmbio e divulgação de informações e boas práticas entre os agentes públicos e privados.
	Anexo II - Lista de indicadores comuns para a avaliação dos objetivos específicos	b) reforçar a capacidade dos Estados-Membros e da União para gerir de forma eficaz os riscos relacionados com a segurança e as crises, e preparar e proteger as pessoas e as IC contra ataques terroristas e outros incidentes relacionados com a segurança.
		i) Número de ferramentas postas à disposição e/ou melhoradas com a ajuda do Instrumento para facilitar a proteção de IC pelos Estados-Membros em todos os setores da economia;
		ii) Número de projetos relacionados com a avaliação e a gestão de riscos no domínio da segurança interna apoiados pelo Instrumento;
		iii) Número de reuniões de peritos, *workshops*, seminários, conferências, publicações, sítios *web* e consultas em linha organizados com a ajuda do instrumento.
		Para efeitos dos relatórios anuais de execução a que se refere o artigo 54. o do Regulamento (UE) n. o 514/2014, este indicador é subdividido em subcategorias: — relacionadas com a proteção de IC, ou — relacionadas com a gestão de riscos e crises.

APÊNDICE H

LISTA DE ORGANISMOS DOS EM E RESPETIVOS PLANOS NACIONAIS DE PROTEÇÃO DE IC

PAÍS	SITE	LINK PLANO NACIONAL	POSICIONAMENTO
Espanha	http://www.cnpic.es/	http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf	Ministro do Interior
Inglaterra	http://www.cpni.gov.uk/	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf	Primeiro Ministro
França	http://www.sgdsn.gouv.fr/	https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006053323&dateTexte=vig	Primeiro Ministro
Malta	http://opm.gov.mt/en/MCIP/Pages/CIP-Directorate.aspx		Primeiro Ministro
Suíça		http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/grundstrategie.parsysrelated1.78229.downloadList.33808.DownloadFile.tmp/grundstrategieen.pdf	
Eslovénia	http://www.mo.gov.si/en/areas_of_work/critical_infrastructure_protection/	http://www.pisrs.si/Pis.web/pregledPredpisa?id=RESO61#	
Roménia	http://ccpic.mai.gov.ro/desprenoi_en.html Centre for coordination of critical infrastructure protection	http://ccpic.mai.gov.ro/strategia_en.html	Ministro do Interior
Polonia	http://rcb.gov.pl/en/	http://rcb.gov.pl/wp-content/uploads/REGULATION-on-NATIONAL-CRITICAL-INFRASTRUCTURE-PROTECTION-PROGRAMME-AB.pdf	Primeiro Ministro
Bélgica	http://centredecrise.be/fr/content/infrastructure-critique-0	http://centredecrise.be/sites/5052.fedimbo.belgium.be/files/loi_du_1er_juillet_2011_sur_les_ic_0.pdf	Ministro do Interior
Finlândia		http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf	Primeiro Ministro
Alemanha	http://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html	http://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile	Ministro do Interior

APÊNDICE I

GLOSSÁRIO

GLOSSÁRIO

O presente glossário contem uma compilação de definições, relativas aos conceitos mais frequentemente utilizados no contexto da proteção de infraestruturas críticas.

Por serem conceitos transversais a várias disciplinas, existe uma pluralidade de definições possíveis para cada um deles. No nosso trabalho, e por uma questão de alinhamento optámos por apresentar - sempre que ela exista - a definição adotada pela generalidade da "comunidade internacional de proteção de IC".

Proteção de Infraestruturas Criticas (PIC) – Todas as atividades destinadas a assegurar a funcionalidade, continuidade e integridade de infraestruturas críticas, por forma a impedir, mitigar e neutralizar uma ameaça, risco ou vulnerabilidade.[88] (tradução livre da responsabilidade do autor).

Gestão de Crises – Processo contínuo, tipicamente constituído por cinco fases cíclicas, que se sucedem a uma crise: 1) resposta; 2) recuperação; 3) mitigação; 4) Prevenção; 5) regresso à normalidade[89] (tradução livre da responsabilidade do autor).

Gestão do Risco – Aplicação sistemática de políticas de gestão, procedimentos e práticas, relativas à comunicação, auditoria, contextualização, identificação, análise, avaliação, tratamento, monitorização e revisão do risco[90] (tradução livre da responsabilidade do autor).

Vulnerabilidade – Característica de um elemento do desenho, implementação ou operação de uma IC, suscetível de sofrer disrupção ou destruição por ação de

[88] Disponível em: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Protection [em linha] [consulta em 13 de junho de 2016].

[89] Disponível em: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Crisis_Management [em linha] [consulta em 13 de junho de 2016].

[90] *Cfr.* ISSO/IEC 27000:2014, Informação tecnologia – Segurança

uma ameaça e acarretando consequências noutras IC de si dependentes.[91] (tradução livre da responsabilidade do autor).

(Inter)dependência – "…Relação bidirecional entre duas infraestruturas em que o estado de cada uma influencia ou está correlacionado com o estado da outra" (Rinaldi & Kelly, 2001, 14)[92].

Risco – Probabilidade de uma determinada ameaça explorar uma vulnerabilidade potencial do sistema resultando um determinado impacte num ativo crítico para a missão e objetivos de uma entidade, instituição ou nação (Torres, 2009).

Risco Estrutural – Nível de rico que permanece ativo independentemente da taxa de esforço garantida para o contrariar (Torres, 2015).

[91] *Vide* EC COM(2006) 787 final, de 12 de dezembro. *Diretiva do Concelho para a identificação e designação de IC europeias e da necessidade de melhorar a sua proteção*.
[92] Tradução livre da responsabilidade do autor.

APÊNDICE J

MATRIZ DE PERGUNTAS DOS QUESTIONÁRIOS

Objetivo Específico	Questionário Operadores de IC	Questionário Especialistas e policy-makers	Questionário Peritos estrangeiros
OE1 - Compreender se o panorama atual de PIC é suficientemente inteligível, eficiente e articulado, e se obedece a uma visão integrada do setor público e do setor privado sobre a PIC.		S2 P1	
		S2 P2	
OE2 - Diagnosticar as funcionalidades e disfuncionalidades do atual panorama nacional, e em particular as necessidades sentidas pelos atores relevantes (Governação, Regulação e Operadores de IC)		S2 P2	
		S3 P3	
	S3 P2 e S4 P2	S4 P2	7 e)
	S3 P3 e S4 P3	S4 P3	
	S3 P4 e S4 P4	S4 P4	7 g)
	S3 P5 e S4 P5	S4 P5	7 h)
		S3 P2	
	S3 P6 e S4 P6	S4 P6	7 i)
	S3 P7 e S4 P7	S4 P7	7 j)
	S3 P8 e S4 P8	S4 P8	7 k)
	S3 P9 e S4 P9	S4 P9	7 l)
		S4 P10	7 m)
		S4 P11	7 n)
		S4 P12	7 o)
		S4 P13	7 p)
	S3 P1 e S4 P1	S4 P1	7 q)
		S3 P1	
OE3 - Identificar tendências e boas práticas no contexto europeu, quer no campo do modelo organizativo, quer no campo dos instrumentos e atividades de proteção, que possam ser adaptadas ao contexto nacional;			P1
			P2
			P3
			P4
			P5
			P6
			P7
OE4 - Aferir da necessidade de criação de uma estratégia ou plano nacional de PIC.		S2 P1	
		S2 P3	
OE5 - Aferir da necessidade ou mais valia de criação de um organismo público especificamente dedicado à PIC.	S5 P1	S2 P4	3
OE6 - Identificar as linhas essenciais de uma estratégia ou um plano nacional de PIC e as missões e competências de um organismo dedicado à PIC em Portugal	Todas as questões contribuem para este objetivo		