MARIANA RIBEIRO BRANCO DE OLIVEIRA

A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS EM PORTUGAL

Dissertação com vista à obtenção do grau de

Mestre em Direito e Segurança

Orientador:
Professora Dra. Paula Espírito Santo

Fevereiro, 2015

FACULDADE DE DIREITO

UNIVERSIDADE NOVA DE LISBOA

MARIANA RIBEIRO BRANCO DE OLIVEIRA

A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS EM PORTUGAL

Dissertação com vista à obtenção do grau de

Mestre em Direito e Segurança

Orientador:
Professora Dra. Paula Espírito Santo

Fevereiro, 2015

Declaração de Compromisso de Anti-Plágio

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 27 de Fevereiro de 2015

Mariana Brandão Alcaide

À Avó Leontina, pelo exemplo
e por demonstrar que o conhecimento
está muito para além das oportunidades
cedidas.

Agradecimentos

O caminho percorrido durante este ano contou com o apoio e a colaboração de várias pessoas, as quais, merecem agora um especial agradecimento.

Agradeço à minha família, por este ano ter sido, tal como em todos os outros, o meu suporte. Não posso deixar de fazer um agradecimento dirigido à Leontina, à Isabel, ao Vitor, à Maria Isabel, à Isabel Margarida e ao José.

Agradeço ao Miguel, que para além de família, é o confidente mais profundo, o companheiro de todos os dias e um motivo de inspiração.

À família do Miguel, que a tenho como minha. Agradeço em particular à Maria Teresa pelo interesse, pelas confidências e pelos momentos de descontração.

Um agradecimento muito especial à Professora Dra. Paula Espirito Santo, por ter aceitado este desafio, demostrando sempre grande determinação, dedicação e me ter encorajado a fazer sempre melhor.

À Faculdade de Direito da Universidade Nova de Lisboa, que sempre se demonstrou disponível para me ajudar. Particularmente ao Professor Dr. Jorge Bacelar Gouveia pelo incentivo inicial, e por ter tornado possível a realização deste Mestrado.

Ao Dr. Rui Costa Fonte, à Dr.ª Ana Costa, ao Dr. Francisco Correia Marques e ao Engenheiro Edgar Carvalho que aceitaram colaborar no estudo desenvolvido, contribuindo assim para o enriquecimento deste trabalho. Um agradecimento especial à Dr.ª Isabel Pais pela disponibilidade demonstrada desde o primeiro contacto.

A todos os amigos pela troca de ideias, o interesse revelado e o apoio incondicional. Por último, à Inês, pela compreensão e pela incansável amizade, permitindo que todos os dias fossem encarados com especial motivação.

Resumo

Portugal, tendo responsabilidades a nível europeu, necessita de assegurar o cumprimento das normas europeias, nomeadamente no que se refere ao Plano de Europeu da Segurança das Infraestruturas Críticas. As infraestruturas críticas (IC) nacionais devem ser um foco de atenção no que respeita à gestão dos riscos públicos, já que representam "um conjunto de serviços que são essenciais para o funcionamento do país e para o funcionamento das forças que asseguram a defesa nacional." (Soares, 2008)

O presente contributo sobre as infraestruturas críticas nacionais tem como objetivo essencial esclarecer o desenvolvimento da estratégia adotada por Portugal na persecução da segurança destas infraestruturas fundamentais. O objetivo deste estudo centra-se no enquadramento jurídico e a realidade em que os Operadores de Infraestruturas Críticas e a Autoridade Nacional de Proteção Civil (ANPC) operam. Pretende-se, nesse sentido, perceber como está a ser desenvolvido o projeto para o programa nacional de segurança das infraestruturas críticas e quais os efeitos das suas junto dos operadores.

Portugal, sendo um país geograficamente periférico, não tem registo de incidentes capazes de provocar contingências em serviços fulcrais para o normal desenvolvimento do Estado. Não apresenta, por isso, um plano estruturado e regulador que substancie a necessidade dos operadores responsáveis pelas IC investirem em segurança. Sem a existência de uma instituição e um sistema regulador, os operadores de IC podem tornar-se menos permiáveis ao cumprimento do enquadramento legal.

Palavras-Chave: Infraestruturas Críticas; Resiliência; Gestão de Continuidade de Negócio

Abstract

Portugal, having responsibilities at European level, needs to ensure compliance with European standards, particularly with regard to the European Security Plan for Critical Infrastructures. National critical infrastructures should be a focus of attention with regard to the management of public risks, since these represent "a set of services that are essential to the functioning of the country and the functioning of the forces that ensure national defense." (Soares, 2008)

This contribution on national critical infrastructures (CI) has the essential objective of clarifying the development of the strategy adopted by Portugal in pursuit of the security of these fundamental infrastructures. The goal lies not only through producing a descriptive document, but also carry a brief confrontation between the legal framework related to these subjects and the reality in which the Critical Infrastructure Operators and the National Civil Protection Authority (ANPC) operate. It is intended, in this sense, to understand the development of the project for the national security program of critical infrastructures and what effects of its measures on operators.

As for the methodology, we followed a methodological strategy, where we combine the literature with data obtained through semi-structured interviews.

Portugal, being a geographically peripheral country and having no record of incidents capable of causing major contingencies in key services for the normal development of society, does not have a structured and regulator plan that substantiates the need for operators responsible for CI to invest in security. This same approach is expected at the State level, believing that even though this theme has be widely explored by international institutions, Portugal has not yet tried to give the attention it deserves. Without the existence of an institution and a regulatory system, CI operators can become less available to comply with the legal framework.

Keywords: Critical Infrastructure; Resilience; Business Continuity Management

Índice

Abstract

Índice de Figuras

Índice de Tabelas

Introdução

Segundo Ulrich Beck a sociedade é caracterizada pelo processo de globalização, encontrando-se em constante desenvolvimento tecnológico e promovendo a individualização. Este tipo de sociedade está em constante mutação, não sendo possível aos indivíduos preverem os acontecimentos, aumentando assim o grau incerteza em relação ao que sucederá no momento seguinte. Por esta razão, o autor designou-a como sociedade de risco.

A globalização tem colocado novos desafios à segurança dos Estados, já que o mundo é cada vez mais conflituoso, ao mesmo tempo que se torna mais opaco, ou seja, não nos é possível perceber o que está a acontecer e principalmente o que está na iminência de ocorrer. Assim o "Estado deixou de ser ator único para passar a partilhar responsabilidades com um conjunto de outros atores-chave que consigo concorrem pelo monopólio da segurança, situando-se estes quer a nível externo, num quadro de relações internacionais cada vez mais complexo, quer a nível interno." (Rocha, 2014)

As componentes principais do novo quadro de ameaças à Segurança Nacional – a violência urbana, a criminalidade transnacional e as novas formas de terrorismo – que acompanham as mudanças da sociedade moderna e que se associam à densificação do conceito de segurança, tornam a reflexão da defesa e da segurança um exercício mais exigente. De facto, quando hoje pensamos em Segurança Nacional a fronteira entre segurança interna e externa já não é tão nítida.

Os atos terroristas foram dos primeiros eventos a levantar preocupações acerca da proteção das Infraestruturas Críticas (IC) pelos Países, contudo, desastres naturais capazes de causar fortes danos deixam os países em alerta.

Conhecer as vulnerabilidades e os riscos a que o nosso território está sujeito contribui fortemente para traçar uma estratégia de proteção das infraestruturas críticas o mais criteriosa e eficiente possível. Apesar de Portugal ser um país periférico, no que concerne ao contato territorial com outros países e de não ser, em principio, um alvo evidente de grupos terroristas, a segurança de áreas vitais

para o país não pode ser vista unilateralmente como um custo mas como um investimento, capaz de evitar acidentes que podem pôr em risco vidas humanas e consequências devastadoras no plano económico e social.

O papel do Estado é garantir a segurança, justiça e o bem-estar económico e social da sociedade. Assim, a segurança das infraestruturas críticas revela-se uma das funções essenciais do Estado Português, algo que não resulta apenas da sua integração europeia. Contudo essa segurança não pode ser analisada do ponto de vista unilateral e direto. A segurança tem de ser pensada em estreita colaboração não só com empresas privadas (Operadores de IC) como também com os Estados. Caso fosse posto em causa o funcionamento de qualquer uma das IC, provocaria a "paralisação das atividades económicas e também reduziria a capacidade de resposta do Estado a qualquer tipo de ameaça" (Pais I. , Sá, Lopes, & Oliveira, 2011). Acresce que este tipo de Infraestruturas, mesmo operadas por privados, funcionam num ambiente de grande interdependência, levando a que os efeitos sentidos numa, tenham consequências relevantes nas outras.

Portugal sendo um país europeu, e tendo a sua quota-parte de responsabilidade no cenário internacional, tem de estar em condições de proteger as suas infraestruturas críticas nacionais, bem como, responder adequadamente a um eventual cenário de interrupção das normais atividades de uma destas infraestruturas. Foi nesse sentido que, através do Decreto-Lei n.º 62/2011, de 9 de Maio, Portugal estabeleceu os procedimentos de identificação e proteção das infraestruturas críticas realçando a importância do debate sobre este tema no nosso país, contribuindo assim para agitar conceções, erguer objetivos, levantar interrogações, contribuindo para tornar uma sociedade mais atenta ao risco. É neste contexto que surge o presente trabalho, procurando não só clarificar o caminho seguido até ao momento, mas também desbravar outras possíveis conceções que se esperam úteis para desenvolvimentos futuros.

O presente contributo sobre as infraestruturas críticas nacionais tem como objetivo essencial esclarecer o desenvolvimento da estratégia adotada por Portugal na persecução da segurança destas infraestruturas fundamentais. O objetivo não passa apenas por produzir um documento descritivo, mas efetivar também, um

breve confronto entre o enquadramento jurídico de que estas matérias se revestem e a realidade em que os Operadores de Infraestruturas Críticas e a Autoridade Nacional de Proteção Civil (ANPC) operam.

Pretende-se, por isso, perceber como está a ser desenvolvido o projeto para o programa nacional de segurança das infraestruturas críticas e quais os efeitos junto dos operadores. Isto obriga-nos por isso, à formulação das perguntas de partida necessárias à orientação na recolha de informação.

Em que fase estamos no Projeto para o Programa Nacional de Segurança das Infraestruturas Críticas?

Encontram-se as empresas alertadas para as especificidades decorrentes da posição que ocupam, enquanto Operadores de Infraestruturas Críticas?

As perguntas de partida levaram-nos a adotar uma metodologia qualitativa acente na realizão de entrevistas semiestruturadas, capazes de efetivar o cruzamento dos dados recolhidos com a pesquisa bibliográfica. As entrevistas focaram os operadores de infraestruturas críticas dos sectores dos transportes e da energia, que servem atualmente de base à Diretiva 2008/114/CE do conselho de 8 de Dezembro de 2008 e do Decreto-Lei n.º 62/2011, de 9 de Maio. Foi também efetuada uma entrevista semiestruturada à responsável pelo Programa Nacional de Proteção das Infraestruturas Criticas e ponto de contacto nacional junto da UE. Quanto à pesquisa bibliográfica foram analisados artigos ciêntificos, livros e legislação que nos permitiu não só contextualizar o tema da dissertação, como também complementar e fundamentar os resultados obtidos das entrevistas realizadas.

Este trabalho estrutura-se em três partes. Na primeira procede-se à contextualização do tema, em que, para além da enunciação e explicação dos conceitos essenciais, são apresentadas as principais diretrizes e reflexões que se consideram essenciais no que ao tema diz respeito. Na segunda parte é apresentado um trabalho de investigação a partir de entrevistas realizadas a Operadores de Infraestruturas Críticas bem como à Autoridade Nacional da Proteção Civil, servindo não só para responder às interrogações levantadas anteriormente como também proceder à recolha de informação relevante. Por último, na conclusão são

apresentadas algumas ideias-síntese resultantes do desenvolvimento do trabalho, bem como algumas reflexões que se consideraram apropriadas para desenvolvimento futuro.

Capitulo 1: A Proteção das Infraestruturas Críticas

Em Portugal, existe um conjunto de serviços estratégicos capacitados para garantir o normal funcionamento da sociedade, nomeadamente na área dos transportes, da energia, da defesa, da saúde, das comunicações, entre outros. Segundo a análise do Center for Protection of National Infrastruture (CPNI), as Infraestruturas Críticas identificadas no caso específico do Reino Unido são, o Governo, Serviço de Emergência, Saúde, Comunicação, Água, Energia, Serviços Financeiros, Transportes e Alimentação. (Alberto, 2011)

Alguns destes serviços são garantidos diretamente pelo Estado, contudo a "produção e distribuição de eletricidade, água e gás, bem como a prestação de serviços de telecomunicações e de transportes, são alguns dos exemplos de serviços básicos sob o comando do setor privado" (Almeida, 2011). Ora, numa avaliação a nível macro, podemos dizer que todas estas infraestruturas necessitam de medidas de segurança capazes de responder de forma célere e o mais adequada possível, sem que se tenha unicamente em conta uma visão financeira. Significa assim que a segurança deste tipo de infraestruturas necessita de ser regulada, a fim de assegurar o seu funcionamento normal.

É neste sentido que o tema da proteção das infraestruturas críticas tem ganho espaço tanto a nível nacional (nomeadamente com o Plano para a Proteção das Infraestruturas Críticas nacionais, iniciado pela Comissão Nacional de Proteção Civil) como a nível internacional, com a abundante legislação produzida pela Comissão Europeia. O interesse nesta matéria justifica-se, em grande parte, com a forte complexidade que lhe é inerente.

Pelas razões acima explanadas as IC são um dos alvos mais apetecíveis quando nos referimos a atos de cariz terrorista. Tal acontece pela complexidade e interdependências que criam entre si, já que, no caso de surgirem perturbações

podem gerar rapidamente efeito cascata, multiplicando as suas consequências em setores análogos ou contíguos.

O próprio conceito de infraestrutura crítica apresenta algumas singularidades, dependendo da instituição ou do governo que o utiliza. Esta diferenciação surge desde logo nos critérios utilizados para a sua definição. Em alguns casos, os critérios enfatizam a finalidade da IC, enquanto noutros salientam o impacto da sua ausência ou do seu funcionamento ineficiente (Natário & Nunes, 2014). De seguida será desenvolvido o conceito na ótica do enquadramento jurídico da União Europeia.

Capítulo 2: Revisão da Literatura

2.1 Concetualização

2.1.2 Infraestruturas críticas (IC)

Podem encontrar-se inúmeras definições de infraestruturas críticas (IC), nomeadamente, a que define IC como "as facilidades básicas, serviços e instalações necessárias ao funcionamento de uma comunidade ou sociedade, tais como sistemas de transporte e comunicações, redes elétricas e de água, e instituições incluindo escolas, postos de correio ou prisões" (Houghton Mifflin Company, 2000). No entanto, o presente trabalho será desenvolvido com base na definição apresentada no *Decreto-lei n.º 62/2011, de 9 de Maio, do Ministério da Defesa Nacional*, que resulta da transcrição da Diretiva 2008/114/CE do Conselho de 8 de Dezembro para a legislação portuguesa e define IC como " (…) componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem- estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções;"

As infraestruturas críticas compreendem vários setores como o financeiro, das informações, do abastecimento alimentar, dos transportes, da energia, da água, da saúde, das comunicações, de resposta a emergências, dos setores da administração civil, do setor da indústria química e nuclear, carecendo por isso cada um de segurança especialmente adaptada às suas especificidades. Contudo, torna-se essencial ter em conta, para a análise desta temática, que alguns destes setores a proteger não se materializam em infraestruturas de facto, mas por vezes em redes de abastecimento que asseguram a chegada ao destino de um produto ou serviço considerado essencial. (Comissão das Comunidades Europeias, 2004)

2.1.3 Infraestruturas Críticas Europeias (ICE)

Em Portugal, o projeto para o Plano de Proteção das Infraestruturas Críticas encontra-se integrado no Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC). Daí resulta que, muitas Infraestruturas Críticas nacionais são qualificadas também como Infraestruturas Críticas Europeias, estando os demais Estados-Membros dependentes do seu bom funcionamento.

De acordo com a alínea b) do artigo.2.º do Decreto Lei n.º 62/2011, de 9 de Maio do Ministério da Defesa Nacional, uma Infraestrutura Crítica Europeia é "(…)a infra- -estrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da União Europeia, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infra -estruturas." Ainda segundo a Comunicação da Comissão COM (2006) 786 final, relativa a um Programa Europeu de Proteção das Infraestruturas Críticas, pode ser considerada uma IC quando a sua perturbação ou destruição afete um único Estado-Membro se a IC estiver localizada noutro Estado-Membro, sendo abrangidas as consequências transfronteiriças resultantes da interdependência entre IC. Consideram-se estas Infraestruturas Críticas as mais importantes para Comunidade Europeia.

Segundo a Diretiva 2008/114/CE do Conselho de 8 de Dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, os sectores abrangidos serão numa primeira fase os sectores da Energia e o dos Transportes, tal como podemos verificar pela Tabela 1.

Tabela 1 Setores das Infraestruturas Críticas

Sector	Subsetor	
I Energia	1. Eletricidade	Infraestruturas e instalações de produção de transporte de eletricidade, em termos de abastecimento
	2. Petróleo	Produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos
	3. Gás	Produção, refinação, tratamento, armazenagem e transporte de gás, por gasodutos Terminais para GNL
II Transportes	4. Transportes rodoviários	
	5. Transportes ferroviários	
	6. Transportes aéreos	
	7. Transporte por vias navegáveis interiores	
	8. Transporte marítimo, transporte marítimo de curta distância e portos	

Fonte: Anexo I da Diretiva 2008/114/CE do Conselho de 8 de Dezembro de 2008

Como podemos verificar, os dois setores subdividem-se criando juntos, oito subsetores, fazendo com que em Portugal os setores da energia e dos transportes "representem cerca de 50% das infraestruturas críticas nacionais" (Pais, 2014). No entanto segundo o mesmo autor a Autoridade Nacional de Proteção Civil já se encontra a desenvolver o seu projeto na area das tecnologias de informação e comunicação, considerando-o já o "(…)terceiro grande setor" (Pais, 2014).

2.1.4 Risco

Uma das definições do conceito de risco sugere que este é a combinação da probabilidade e da(s) consequência(s) da ocorrência de um determinado acontecimento não desejado, com potencial para causar danos.

A segurança efetiva inicia-se com uma compreensão clara de todos os tipos e níveis de risco que uma organização enfrenta. Se estes riscos não são ainda conhecidos e totalmente compreendidos então uma pesquisa de segurança e uma avaliação de risco irão ser essenciais para identificá-los.

O relatório Global Risks do World Económic Forum 2013 dividiu os riscos globais em cinco categorias:

- Económicos (preço da energia, crises de liquidez etc.);

- Ambientais (condições atmosféricas adversas, alterações climáticas);
- Geopolíticos (terrorismo, utilização de armas de destruição massiva);
- Societários (crises de abastecimento de água, pandemias);
- Tecnológicos (falha de sistemas e ciber ataques).

Segundo Cardona (2006), uma eficaz gestão do risco requer que este seja dimensionado. Na prática, esta medição do risco significa que seria necessário levar em conta não só os danos físicos previstos, em termos de número de vítimas e perdas económicas, alargando o âmbito da gestão do risco para que este inclua também fatores sociais, organizacionais e institucionais. Para este autor "a dificuldade em conseguir uma gestão eficaz do risco de desastres tem sido, em parte, o resultado da falta de um quadro conceptual abrangente do risco de desastre que poderia facilitar a avaliação e intervenção multidisciplinar" (Cardona, 2006), sustentando que a maior parte das técnicas de avaliação de risco, assim como os índices existentes, não permitem ter uma imagem clara e correta do risco que pretendem expressar. Se o risco não for transmitido de forma adequada, não atrai as atenções das autoridades de modo a que estas intervenham atempadamente para adoptarem medidas de redução do impacto desastres.

Por outro lado, as preocupações dos vários sectores de governo diferem consoante a extensão geográfica e a população afectada. Assim, o conceito de risco é encarado de forma diferente a nível local, quando este afecta apenas uma comunidade ou uma cidade pequena, do que quando os efeitos são sentidos a nível nacional.

Ainda, de acordo com o mesmo autor (Cardona, 2006) a avaliação do risco é mais pormenorizada quando é realizada numa escala micro-social ou territorial, dado que se perde detalhes quando de trabalha em escalas macro. Nesta perspectiva torna-se imprescindível dispor de instrumentos de avaliação adequados, pois tal como os atores sociais diferem, também as necessidades de informação são significativamente diferentes em cada nível, tornando-se necessário que estes permitam entender o problema e orientar o processo de tomada de decisão.

Numa perspectiva diferente, Chertoff (2009) refere que a percepção do risco é influenciada pela natureza e extensão da ameaça, pelas vulnerabilidades a essa ameaça e pelas consequências que daí podem resultar, pelo que todas estas vertentes têm que ser tidas em conta no momento em que se procede à avaliação desse risco. Assim, segundo Hämmerli & Renda (2010) importa dar prioridade à avaliação do nível de risco associado às IC, utilizando uma abordagem abrangente, de modo a permitir um melhor fluxo de informação e melhorar a eficiência das IC.

Tal como Cardona (2006) também Cornish et al. (2011) alerta que a utilização de técnicas de avaliação inadequadas e o desconhecimento das métricas apropriadas para estimar parâmetros importantes, levam a que muitas avaliações de risco sejam mal conduzidas, exacerbando riscos que podem ser afectados por outros factores e expondo as organizações, uma vez que a sua avaliação não é realizada de modo uniforme.

Carreño et al. (2007), no entanto, tem uma abordagem diferente – holística - pois na sua avaliação de risco – aquilo que ele chama de *Índice de Risco Total* – ele combina o risco "físico" - *Índice de Risco Físico* - com um *Factor de Impacto*, associando a estas duas variáveis a fragilidade social e a falta de resiliência, que podem agravar o resultado final da perda física.

2.1.5 Resiliência

Resiliência deriva do latim "resiliens" e expressa a intenção de voltar ao estado normal depois de ter ocorrido uma perturbação no ciclo habitual. No que se refere especificamente às infraestruturas crítcas resiliência "refere-se à sua capacidade de adaptação contínua face a grandes tendências evolutivas, permitindo ao sistema regional (ou outro) suportar crises e perturbações sem colapsar." Resiliência refere-se especificamente aos " procedimentos a serem adotados para que a instalação, o sistema, ou o serviço voltem a funcionar rapidamente, com um mínimo de tempo de recuperação" No fundo estar resiliente é estar preparado para

responder a quaisquer riscos, incorporando a "ideia de prevenção pré-incidente e resposta pós-incidente." (Austen & Nathan, 2013).

Um dos exemplos mais flagrantes que ilustra a importância deste conceito é avançado pelos mesmo autores (Austen & Nathan, 2013) e refere-se às medidas governamentais adoptadas pelos EUA após os atentados terroristas de 11 de setembro de 2001. Segundo estes investigadores o governo americano negligenciou o papel vital das parcerias público-privadas no domínio da proteção de infraestruturas críticas, concentrando-se mais no pré-incidente e descurando o pós-incidente, dando como exemplo, as centrais nucleares, as barragens e as instalações fabris, que são sistemas extremamente complexos. "A resiliência colocou as infraestruturas criticas dentro de uma imensa rede de atores públicos ou privados, individuais ou colectivos, quer fossem instituições cívicas ou sem fins lucrativos". Esta estratégia possibilitou distribuir o "ónus da protecção por todas as partes interessadas, e especialmente pelas próprias empresas, que possuem ou operam cerca de 85% das infraestruturas críticas dos Estados Unidos."

A resiliência apresenta benefícios tanto para os sectores públicos, como para os privados, no entanto, implica também custos para efetivar e potenciar os seus efeitos. Em contextos económicos adversos, em que as empresas procuram cortar nos custos, a proteção das infraestruturas críticas tende a ser descurada, diminuindo assim a sua eficácia.

2.1.6 Gestão de Continuidade de Negócio

Infraestruturas Críticas consideram-se não só as estruturas físicas mas também os serviços e sistemas de dados. De facto, se qualquer um destes setores for posto em causa terá um impacto social, económico e político na segurança do Estado. Na verdade, os ataques terroristas em Nova Iorque, Londres e Madrid, as catástrofes naturais que provocaram o acidente nuclear em Fukushima e tantos outros acidentes provocados pela ação humana ou não, impulsionaram soluções de reação e recuperação em empresas de todo o mundo.

A norma internacional BS25999 do British Standards Institution define o programa de gestão de continuidade de negócio como o "processo de gestão corrente suportado pela Gestão de Topo, com os recursos adequados, de forma a garantir que são identificadas as ameaças potenciais e o seu impacto no negócio sendo desenvolvidas e mantidas estratégias e planos de recuperação, com vista à continuidade dos produtos e serviços da organização caso estas ameaças se venham a concretizar, através da realização de ações de formação, exercícios de simulação e atividades de manutenção e revisão." (BSI, 2006)

Atualmente encontra-se em vigor a ISO 22301 na qual "Continuidade de Negócio" é definida como a capacidade da organização para continuar a sua produção em níveis previamente definidos como aceitáveis, após a ocorrência de um incidente perturbador. (Business Continuity Institute, 2014)

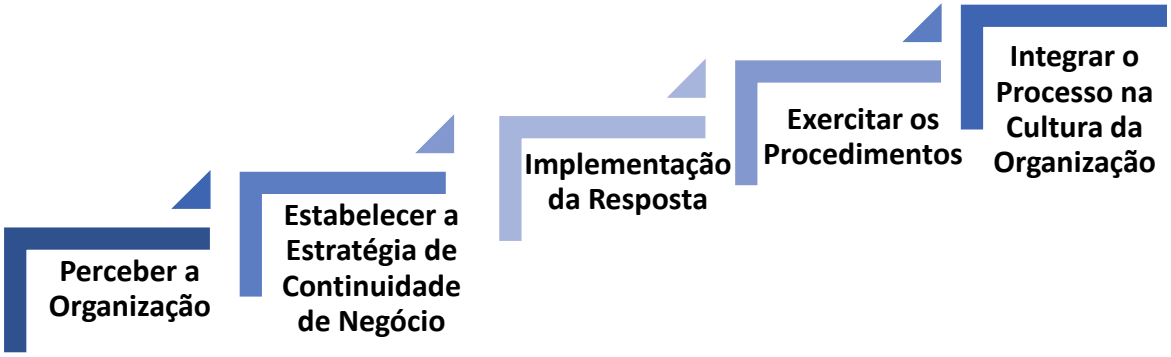

Figura 1 Fases da implementação de um sistema de Gestão de Continuidade de Negócio
Fonte: Adaptado de Alberto, C. (Janeiro de 2011)

De acordo com a Figura 1, torna-se premente numa primeira fase, conhecer a organização e as especificidades do seu funcionamento, onde se incluem as potenciais ameaças para o setor e onde são identificados "Requisitos de Recuperação dos processos críticos (i.e, colaboradores, instalações e sistemas) " (Alberto, 2011). É também nesta fase que se calcula o tempo máximo admissível para cada setor presente no processo, se manter indisponível.

Já na segunda fase estabelece-se uma estratégia a adotar pela organização, na qual são desenhados os seus parâmetros de acordo com os fatores analisados na fase anterior.

A terceira fase, denominada na figura como *Implementação de Resposta* é responsável por elaborar um conjunto de planos como os "Planos de Emergência Internos, Gestão de Crise, Recuperação de Negócio e Recuperação Tecnológica" (Alberto, 2011). Nesta fase ficam formalizados os procedimentos, os colaboradores e os contratos anexos que o plano inclui.

Na quarta fase, a teoria é interpretada e integrada nas práticas da empresa. Os procedimentos são exercitados, recorrendo muitas vezes a simulacros, para os quais se torna essencial que os colaboradores conheçam as suas funções e a conduta a seguir. Havendo uma permanente necessidade de adaptação às novas ameaças, torna-se também crucial, ainda nesta fase, iniciar um processo contínuo de revisão do próprio plano.

Trata-se de um processo complexo com uma forte componente analítica, em que se procura identificar os produtos, serviços e atividades nos quais a empresa se sustenta, a fim de implementar medidas capazes de, em caso de incidente, continuar as suas operações mínimas permitindo uma rápida recuperação nas várias áreas. Tendo estas características, o conceito de gestão de continuidade de negócio deveria ser encarado, neste contexto das IC em especial, como o fator chave na resposta aos incidentes, tal como deveria ser dada uma importância mais adequada a planos de resiliência em termos sectoriais nas infraestruturas em causa (Alberto, 2011).

A Gestão de risco abrange a gestão de continuidade de negócio, já que é o "processo sistemático e analítico para determinar, qualitativa e quantitativamente, a probabilidade de um evento adverso e a gravidade do seu impacto sobre bens, indivíduos, funções e/ou sistemas. É uma função que abrange a identificação de ameaças, vulnerabilidades e consequências e pode incluir cenários em que dois ou mais riscos interajam para criar maior ou menor impacto. Além disso, constitui a base para hierarquização de riscos e priorização de contramedidas, o que permite delinear ações para reduzir o risco e mitigar eventuais consequências de um incidente" (Arruda, 2014).

Figura 2 Gestão de Risco e Gestão de Continuidade de Negócio
Fonte: Adaptado pelo autor de http://www.iso27001standard.com/o-que-e-a-iso-22301

Assim, a implementação de planos de continuidade de negócios nas organizações revela-se como um instrumento capaz de mitigar riscos que possam afetar as suas operações, os seus sistemas de informação ou os seus serviços críticos.

2.2 Contexto Histórico

Os acontecimentos registados ao longo dos últimos anos mostram-nos como as catástrofes naturais e os desastres originados por ação humana podem causar fortes perturbações nos setores fundamentais da sociedade. Esses mesmos acontecimentos têm vindo a conferir aos órgãos responsáveis (Estados-Membros, NATO e EU), uma preocupação acrescida sobre a segurança desse tipo de infraestruturas.

Em 2004 surgiram as primeiras iniciativas concretas da União Europeia sobre a Proteção das Infraestruturas Críticas (PIC). Em Junho desse mesmo ano, o "Conselho Europeu pediu à Comissão que desenvolvesse uma estratégia a nível global para as PIC. (Pais, Sá, & Gomes, 2007)

Ainda com os ataques terroristas de 11 de Setembro de 2001 em Nova Iorque muito presentes, bem como, como os de 11 de Março de 2004 em Madrid, a Comissão Europeia adotou em 2004 a comunicação "*Proteção das*

Infraestruturas Criticas no âmbito da luta contra o terrorismo" focada na prevenção e na sua capacidade de resposta (Pais & Candeias, 2000). Em consequência, em Dezembro desse mesmo ano, a Comissão propôs ao Conselho Europeu a elaboração de um *Programa Europeu de Proteção de Infraestruturas Críticas* (PEPIC) (Pais, Sá, & Gomes, 2007).

Em Novembro de 2005, a Comissão adotou um livro verde relativo ao PEPIC que reforçou a ideia da importância de elaborar um enquadramento regulamentar comunitário para estas matérias. Contudo, foi em Dezembro de 2006, por proposta da União Europeia, que a Comissão lançou uma proposta de Diretiva relativa às Infraestruturas Críticas Europeias, chamando a atenção para a necessidade de aumentar a sua proteção, ao mesmo tempo que lançava "uma comunicação sobre um Programa Europeu de Proteção de IC's" (Pais & Candeias, 2000), recomendando desta forma, a adoção de medidas que tornassem as IC Nacionais mais resilientes através de Programas Nacionais de Proteção das Infraestruturas Críticas.

Por fim, surge em 2008 a Diretiva 2008/114/CE do Conselho, de 8 de Dezembro relativa à identificação e designação das ICE e à avaliação da necessidade de melhorar a sua proteção, sendo da responsabilidade dos Estados-Membros assegurar a respetiva proteção das infraestruturas críticas.

2.3 Programa Europeu de Proteção de Infraestruturas Críticas (PEPIC)

A Comissão Europeia, no âmbito das suas competências comunitárias desenvolve um esforço para garantir a melhor proteção possível das infraestruturas críticas no espaço Europeu. É esse aliás, o objetivo que a move, ao criar um Programa Europeu de Proteção de Infraestruturas críticas, o PEPIC.

Criado esse enquadramento jurídico na União Europeia, cabe à Comissão desenvolver um plano assente nas ameaças reconhecidas nessas áreas. Neste caso a abordagem é ampla, incluindo assim "todos os riscos" tal como descreve a Comunicação da Comissão COM (2006) 786, parte final, relativa a um Programa

Europeu de Proteção das Infraestruturas Críticas, não esquecendo porém, de enfatizar o terrorismo como uma ameaça relevante.

Neste âmbito, torna-se essencial promover a cooperação e o intercâmbio de informações entre Estados-Membro, Operadores e Comissão. Para tal, medidas como a Criação de um Grupo de Contacto PIC que reúne todos os Pontos de Contacto de todos os Estados-Membro, bem como a criação de uma plataforma de intercâmbio das melhores experiências neste sector - Rede de Alerta para as Infraestruturas criticas (RAIC), - tornam-se essenciais para alcançar esse objetivo. É na concretização desta ultima medida que se fundamenta a proteção das IC, isto é, a partilha de informação entre os intervenientes do processo. No entanto para que essa partilha seja concretizada sem constrangimentos desmedidos, tem de se basear numa relação de confiança e privacidade, na qual a manipulação da informação só é feita por pessoas habilitadas pelo Estado-Membro, já que se trata de informação sensível e melindrosa.

2.4 Projeto do Programa Nacional para a Proteção das Infraestruturas Críticas

Portugal tem participado na discussão desta temática, fazendo-se representar no NATO CPC Ad-hoc Working Group on Critical Infrastructure Protection, através de membros da Autoridade Nacional de Proteção Civil. A ANPC encontra-se a liderar o desenvolvimento da antiga "Carta Nacional de Pontos Sensíveis", hoje designado Proteção de Infraestruturas Críticas (Pais & Candeias, 2000).

Através da Deliberação do Conselho de Ministros n.º 51DB/2004, de 18 de Março, foi dado enquadramento jurídico ao plano que se viria a criar no âmbito da proteção das infraestruturas críticas nacionais. Na mesma deliberação foi igualmente nomeado o Conselho Nacional de Planeamento Civil de Emergência (CNPCE), posteriormente substituído pela Autoridade Nacional de Proteção Civil (ANPC), como a entidade responsável pela coordenação de um grupo de trabalho que teria como objetivo a criação da antiga Carta Nacional de Pontos Sensíveis,

bem como o ponto de contacto nacional, junto da União Europeia para questões relacionadas com a proteção das infraestruturas críticas. Posteriormente o CNPCE foi nomeado como ponto de contacto nacional para questões relacionadas com a proteção das Infraestruturas Críticas (Pais & Candeias, 2000). Esta cooperação nacional junto da UE permitiu ao nosso país iniciar um plano capaz de garantir a resiliência das IC nacionais.

No seguimento desta estratégia de aproximação às normas europeias, através do Despacho n.º14128/2010, de 1 de Setembro, foi decidida a elaboração de um projeto de transposição da Diretiva Europeia n.º 2008/114/CE, do Conselho, de 8 de Dezembro, constituindo um grupo de trabalho com os seguintes elementos:

- ✓ Conselho Nacional de Planeamento Civil de Emergência;
- ✓ Secretário-Geral do Sistema de Segurança Interna.

No desenvolvimento desta matéria, a CNPCE celebrou protocolos com outras entidades, com capacidade para gerar valor ao projeto, nomeadamente, o Instituto Superior Técnico e a Fundação para a Computação Científica Nacional (Pais, Sá, & Gomes, 2007). Estas entidades em conjunto com os técnicos da CNPCE têm vindo a trabalhar no sentido de desenvolver um Plano Nacional para a Proteção das Infraestruturas Críticas (PNPIC).

O projeto foi dividido em três fases e cada uma delas em subfases (Pais, Sá, & Gomes, 2007):

1. Identificação e classificação das infraestruturas críticas nacionais;

Como se tratava de um projeto pioneiro a nível nacional, definir uma Infraestrutura Crítica revelava-se uma das prioridades da sua elaboração. Ainda assim, numa primeira fase, foi elaborado um trabalho de identificação e classificação das IC presentes em território nacional. Essa classificação foi assente em critérios hierárquicos, que permitiram, numa fase posterior, priorizar as medidas de proteção a implementar.

Classificação nacional das IC

Para a classificação das IC "foi desenvolvido o algoritmo Adpa, pelo qual se procura medir o potencial de cada infraestrutura em propagar disfunções às que se situem a jusante dela" (Pais, Sá, & Gomes, 2007). Essa propagação

acontece pelas dependências que se criam entre as Infraestruturas, pelos serviços que cada uma presta e pelo respetivo impacto que têm na sociedade. Tabansky considera que os três fatores necessários para definir uma IC são: a sua importância simbólica, ou seja tudo aquilo que representa ao olhar dos outros, a imediata independência daquilo que produz e por último, a rede de dependências a que está ligada. (Tabansky, 2011). Ainda segundo o mesmo autor, recorreu-se ao algoritmo *Macbeth,* que de acordo com Costa, Angulo-Meza, & Oliveira, (2013) trata-se de um método de apoio à decisão utilizando múltiplos critérios e baseando-se em apreciações de caráter qualitativo sobre diferenças de atratividade, dando grande relevância à apreciação do consultor (Figura 3).

Figura 3 Fases do processo MACBETH de apoio multicritério à decisão
Fonte: Adaptação pelo autor de (Costa, Angulo-Meza, & Oliveira, 2013)

A metodologia aplicada possibilitou encontrar valores que permitiram a classificação (de forma relativa) das Infraestruturas Críticas, permitindo que "uma infraestrutura possa ser considerada mais crítica do que outra, se houver uma forte evidência que a sua destruição, ou exploração de uma vulnerabilidade, possa afetar seriamente um dos grandes objetivos presentes na definição de IC." (Pais, Sá, & Gomes, 2007)

Após a sua identificação, os dados obtidos foram agrupados numa base de dados integrada num Sistema de Informação Geográfica (SIG).

2. Análise e avaliação do risco associado à disfunção de infraestruturas críticas e estudo e difusão de medidas eficientes para reforço da sua proteção;

Na segunda fase procura-se identificar as vulnerabilidades face às ameaças que as poderão afetar, a fim de na fase seguinte, se poder implementar medidas eficientes para a redução dessa vulnerabilidade. Trata-se de uma tarefa que terá de ser efetuada de forma contínua, tendo em conta que os contextos são facilmente passíveis de serem modificados. (Autoridade Nacional de Proteção Civil, 2014)

3. Implementação de medidas e monitorização do risco.

A última fase deste processo é da exclusiva responsabilidade dos Operadores, já que são eles que são os responsáveis pela sua própria segurança (Pais , 2014). Estas medidas devem ser implementadas no sentido de garantir a funcionalidade da IC a fim de mitigar e neutralizar as ameaças, os riscos e as vulnerabilidades identificados (Alberto, 2011).

2.5 As infraestruturas críticas em Portugal

Em Portugal assistimos com alguma frequência a incêndios, tempestades, cheias e a nossa localização geográfica torna-nos especialmente vulneráveis à ocorrência de sismos, em especial na zona do Algarve e Vale do Tejo, o que levou a Proteção Civil a preparar planos de emergência e exercícios de simulação, em articulação com as empresas. Por outro lado, não se devem também minimizar a probabilidade da ocorrência de ataques de *hackers* às páginas institucionais.

A maioria das infraestruturas críticas pertencem ao setor privado, sendo que o Estado encontra-se numa posição de relativa dependência na implementação de medidas de segurança. Por esta razão, torna-se fundamental nesta área a cooperação entre os setor público e o setor privado, a fim de cada um reconhecer e aceitar a sua responsabilidade na persecução do reforço de segurança (Pais, Sá, & Gomes, 2007).

Ainda segundo os mesmos autores, cabe aos operadores, ou stakeholders, contribuir de forma ativa para a adoção de medidas de caráter preventivo. No entanto, e tendo em conta os riscos e a incerteza dos tempos atuais, é da competência do Estado proporcionar apoio na elaboração de protocolos de colaboração, tanto a nível nacional como internacional, tendo em vista estimular a comunicação e a cooperação entre as partes envolvidas.

Após a finalização da primeira fase do Plano de Proteção das IC verificaram-se algumas conclusões, nomeadamente:

- ✓ Mais de 65% das IC nacionais podem ser gravemente afetadas por uma ocorrência sísmica, provável ou plausível;
- ✓ Mais de 300 sugerem uma significativa atratividade ou um elevado potencial para ações mal-intencionadas;
- ✓ Algumas infraestruturas encontram-se em zonas de elevado risco de incêndio florestal ou leitos de cheia;

O que estes resultados nos sugerem é a necessidade de implementar medidas que se adaptem a cada uma das IC, com vista a aumentar a sua resiliência, fazendo assim com que a resposta a qualquer incidente seja concretizada com a maior celeridade e eficiência possíveis, evitando a propagação e agravamento do dano, já que as consequências que podem surgir de um evento nocivo como este podem ser devastadoras para os cidadãos, para o meio ambiente e para bens e serviços, em áreas transversais à sociedade.

2.5.1 Interdependências

Portugal, apesar de ser geograficamente periférico, tem responsabilidades para com os parceiros europeus, tendo muitas das suas principais infraestruturas a funcionar de forma interligada com serviços de outros países. Estas interligações criam preocupações adicionais, já que as medidas de segurança implementadas por um Estado-Membro, deverão ser tomadas, preferencialmente, em conjunto e colaboração com outros Estados- Membros. Ou seja, as IC dependem umas das outras, tal qual a sociedade depende delas para o seu correto funcionamento, num

ambiente não só de relações de dependência unidirecionais, mas também de relações de interdependência bidirecionais (Natário & Nunes, 2014). Segundo Kelly (2001) estas interdependências podem ser físicas, ciber, geográficas e lógicas. Físicas, na medida em que o sucesso de uma depende do estado físico da outra. Cibernéticas, caso alguma infraestrutura crítica dependa da informação armazenada e transmitida por outra. Geográficas, no caso de haver uma vulnerabilidade e proximidade tal que um evento ambiental possa causar distúrbios graves. Lógicas, por fim, quando o estado de cada uma depende do estado da outra por meio de um mecanismo que não seja físico, cibernético ou geográfico. (Natário & Nunes, 2014) Atualmente as interdependências de caráter cibernético tendem a ter crescimento exponencial face às outras, podendo fazer crescer bastante as vulnerabilidades.

Na reflexão que faz no Livro Verde – Relativo a um Programa Europeu de Proteção das Infraestruturas Críticas, a Comissão Europeia chama a atenção para a especial questão das interdependências geradas entre IC e para a forte propagação que possa ocorrer no sistema em caso de disfunção. É aliás neste documento que se denota uma forte preocupação em encetar estudos no sentido de identificar potenciais ameaças, dando especial atenção às tecnologias da informação e comunicação. Aliando estes mesmos estudos à cooperação e partilha de informação entre Operadores, Estados-Membros e Comissão, espera-se que resultem em estratégias para a minimização do risco.

2.5.2 Relação entre o Público – Privado

A coordenação entre o setor público e o setor privado no que respeita à proteção de infraestruturas críticas revela-se um enorme desafio.

Os interesses e objetivos de cada uma das partes permitem criar consensos a partir de diálogo e cedências, tendo em vista gerar sinergias que revelem vantagens mútuas. Essas vantagens constatam-se ao nível do crescimento da produtividade e da eliminação da duplicação de esforço, ou seja, no aumento da

eficiência e do cumprimento dos objetivos de uma forma mais eficaz, tendo em consideração o que cada entidade poderia fazer individualmente. (S.Eckert, 2005)

A segurança é um dos pressupostos essenciais no que se refere ao exercício dos direitos fundamentais dos cidadãos. A segurança é garantida por entidades exteriores, nomeadamente pelo Estado. No entanto a privatização no setor da segurança tem crescido nos últimos anos, fruto da cedência de funções, até aí unicamente garantidas pelas autoridades estatais. Esta é uma tendência que parece continuar, já que, tal como defendem Austen Givens e Nathan Bush, "a noção de que o governo sozinho pode efetivamente proteger a grande variedade de instalações, ignora a complexidade dos sistemas." (Austen & Nathan, 2013)

Contudo, essa parceria cria a necessidade de investimento, quer por parte das entidades privadas, quer por parte do Estado, materializando-se, nesse caso, em incentivos financeiros cedidos aos operadores a fim de promoverem as práticas mais corretas no que refere à segurança das IC.

2.6 Setor dos Transportes e Setor da Energia

2.6.1 Transportes

O setor dos transportes inclui o tráfego aéreo, ferroviário, rodoviário, o transporte por vias navegáveis interiores e ainda o transporte marítimo, incluindo curta distância e portos, de acordo com o Decreto-Lei n.º 62/2011, de 9 de Maio. A diversidade e o volume de tráfego que ocorre diariamente é essencial para o desenvolvimento económico e social de um país, bem como para a garantia da própria segurança. O setor dos transportes, tal como o da energia, é transversal à sociedade no que respeita ao panorama económico. Com tais interdependências, um desequilíbrio no normal funcionamento do setor dos transportes pode provocar com facilidade transtornos nos que dependem dele. Deste setor depende não só a mobilidade dos passageiros como também a deslocação de volumes incalculáveis de mercadorias.

Em Portugal, o setor dos transportes começou a adquirir a relevância que

hoje lhe é inerente a partir dos anos 50, constituindo as duas décadas seguintes uma fase de crescimento significativo (ANTROP, 2002). Contudo, foi a partir da revolução de 25 de Abril de 1974 que muitas empresas foram nacionalizadas, desenvolvendo-se o transporte público tal como o conhecemos hoje. No entanto, essa fase da nacionalização viria a inverter-se já nos anos 90, com o início de um período de grande abertura à participação dos privados neste setor, bem como por outro lado, um crescimento da utilização da viatura própria (Lacomblez, 2006).

Como podemos verificar na Figura 4, atualmente metade dos europeus utilizam carro próprio todos os dias, enquanto apenas 16% utiliza os transportes públicos (European Commission, 2013).

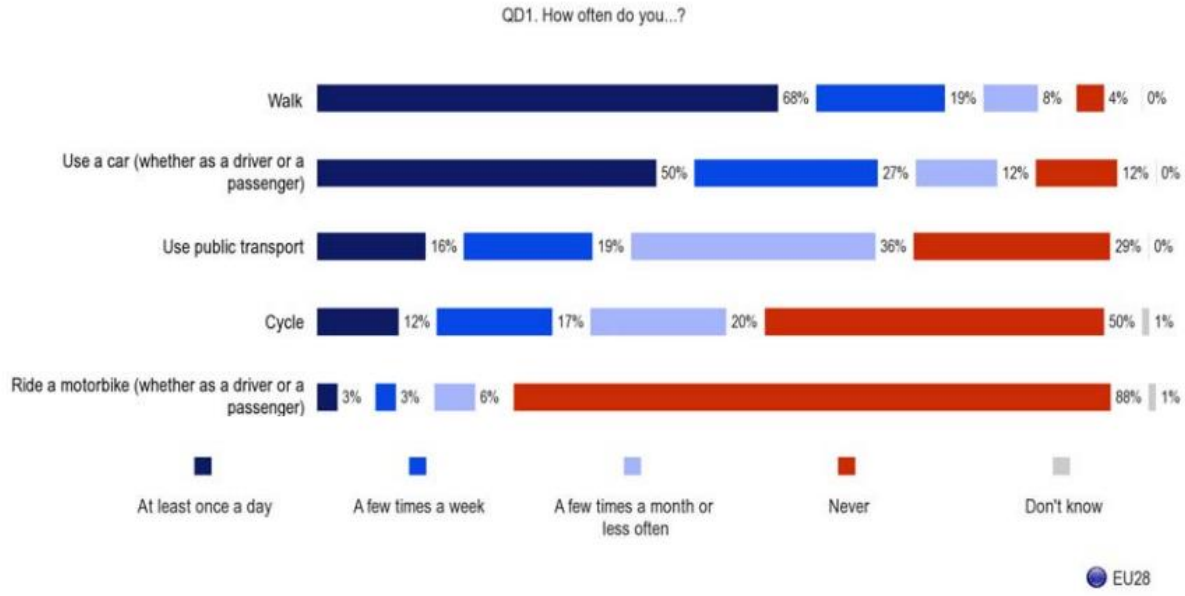

Figura 4 Meios de transporte utilizados pelos Europeus
Fonte: (European Commission, 2013)

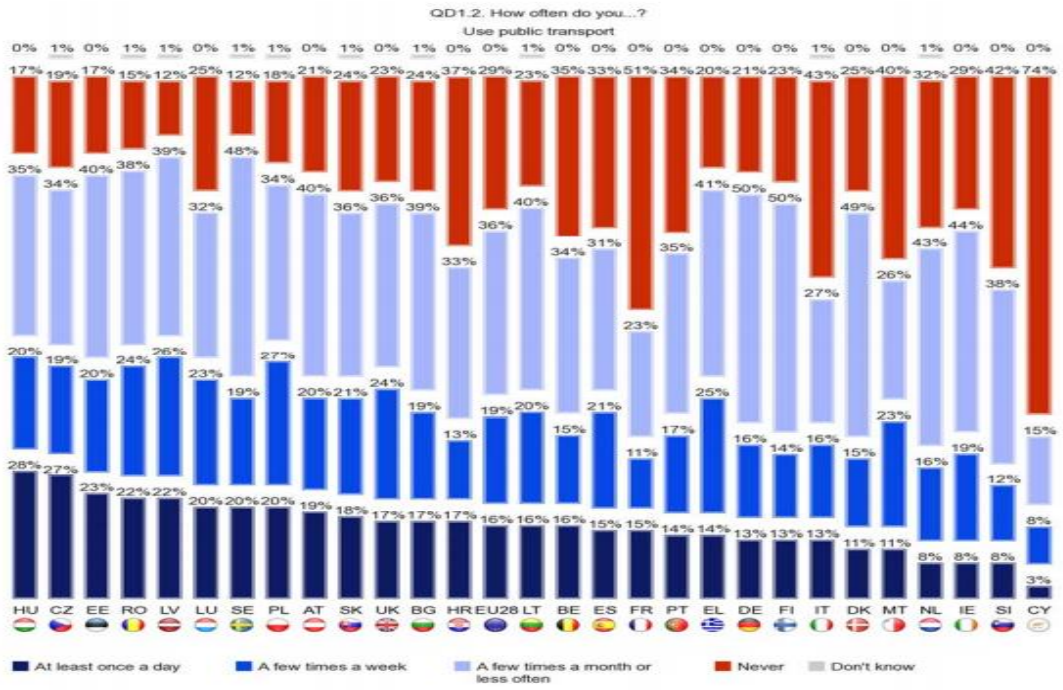

Figura 5 Utilização dos Transportes Públicos
Fonte: *(European Commission, 2013*)

Verifica-se uma contraposição entre a utilização de viatura própria e o esforço desenvolvido pelos operadores de serviços de transportes públicos no sentido de incentivar à sua utilização. Em 2012, o volume de negócio das empresas do setor dos transportes registou uma redução de 2,4%, no entanto, os meios de transporte "não seguiram um padrão homogéneo: se, por um lado, as empresas cuja atividade principal era o transporte por água (…) registaram diminuição de 7,5%, em contrapartida as empresas de transporte aéreo viram o respetivo volume de negócio crescer quase 3,0%" (Instituto Nacional de Estatistica, 2013). Uma possível explicação para este facto pode encontrar-se na análise dos dados disponibilizados pelo *Special Eurobarometer 406* que foi desenvolvido pela Comissão Europeia e que é refletido na Figura 5. Em Portugal, 69% dos cidadãos ou nunca utilizam os transportes públicos ou utilizam-nos raramente.

2.6.2 Energia

No contexto que é apresentado e de acordo com o Decreto-Lei n.º 62/2011, de 9 de Maio, o sector da energia inclui as:

a) "Infra-estruturas e instalações de produção e de transporte de eletricidade;

b) Infra-estruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos; e

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

Atualmente a energia é produzida com recurso à transformação de várias fontes primárias, tal como o petróleo, o gás natural, combustíveis sólidos, o Sol e o vento. Na Figura 6 podemos comparar a produção de energia primária num conjunto de 19 países. Portugal, a par com o Luxemburgo, são os únicos países em que a produção de energia primária se restringe às energias renováveis.

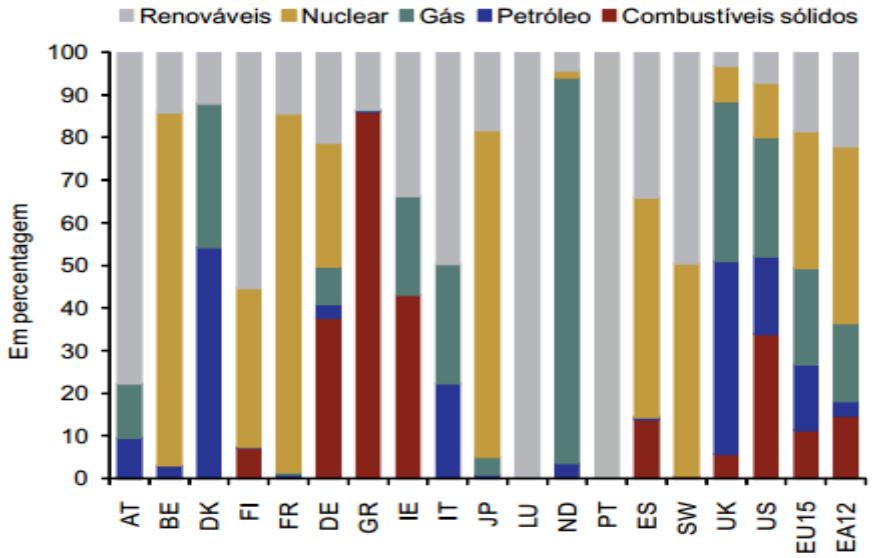

Figura 6 Países da OCDE selecionados 2008
Fonte: Agência Internacional de Energia (AIE) e (Amador, 2010)

Em Portugal, o número de produtores de energia tem aumentado significativamente uma vez que têm surgido muitas centrais térmicas e hídricas com o sentido de produzir energias renováveis (Rede Energética Nacional, 2014). Segundo dados do INE, no ano de 2008 existiam 79 589 empresas do setor das indústrias transformadoras capazes de produzir 78 956 milhões de euros (Instituto Nacional de Estatística, 2008). No entanto, para além das infraestruturas de produção existem todas as outras de igual criticidade,

responsáveis pela distribuição de baixa, média e alta tensão desde o produtor até ao consumidor. Esta distribuição é atualmente da responsabilidade de uma única empresa – a REN, Redes Energéticas Nacionais através da Rede Nacional de Transporte.

O consumo de produtos energéticos em Portugal tem registado um forte crescimento, contribuindo para tal o setor industrial (cerca de 32,1%) como também o consumo doméstico (cerca de 29,1%). (Instituto Nacional de Estatística, 2008). A importância reconhecida da energia no nosso dia-a-dia justifica facilmente o elevado consumo registado, bem como a diversidade de distribuidoras e a volatilidade dos preços. Segundo dados avançados pela REN, em Portugal Continental existem 6,1 milhões de consumidores de eletricidade, "sendo a sua esmagadora maioria de Baixa Tensão, 23500 de Média Tensão e cerca de 350 em Alta e Muito Alta Tensão." (Rede Energética Nacional, 2014)

Sabendo que, em 2013 a população de Portugal Continental consumiu mais de 49 mil milhões de KWh, encontra-se a explicação para que este setor sirva, conjuntamente com o setor dos transportes, de base à legislação que regula esta área. De facto uma elevada dependência energética gera uma forte correlação entre cortes de energia e instabilidade política, económica e securitária (Amador, 2010).

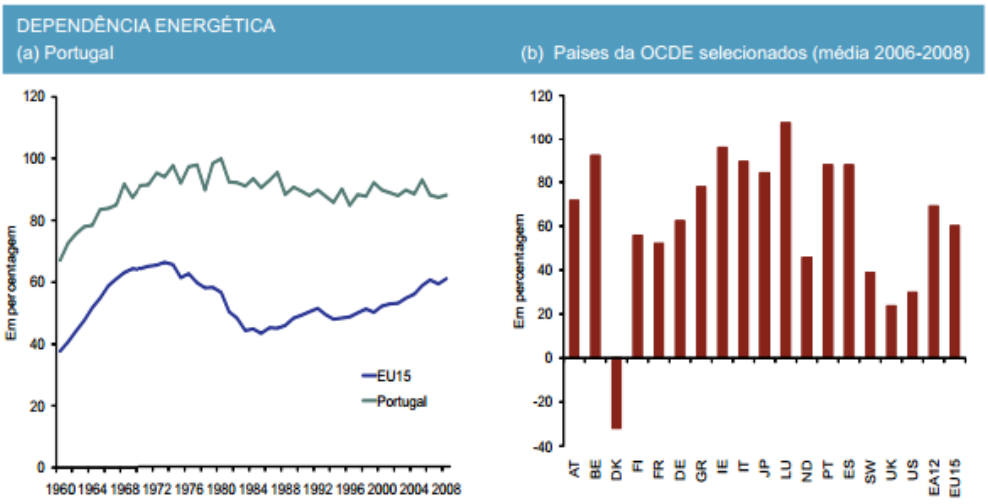

Figura 7 Dependência Energética

Fonte: Agência Internacional de) Energia (AIE e (Amador, 2010)

Na Figura 7 podemos verificar em percentagem a dependência energética de Portugal face à EU. Em 2008, Portugal apresentava 30 pontos percentuais acima da média da EU, podendo este facto ser explicado através das razões avançadas pelo Banco de Portugal, nomeadamente condições estruturais, escolhas tecnológicas e políticas nacionais. (Amador, 2010) Para além do mais, infraestruturas como as centrais hidroelétricas, parques solares fotovoltaicos, parques eólicos ou mesmo linhas aéreas e postes de média, alta e muito alta tensão, para além de serem construções de grande magnitude, apresentam uma vulnerável exposição às condições meteorológicas.

2.7 Enquadramento Legal

2.7.1 Livro Verde - RELATIVO A UM PROGRAMA EUROPEU DE PROTECÇÃO DAS INFRAESTRUTURAS CRÍTICAS

O *Livro Verde* relativo a um programa Europeu de Proteção das Infraestruturas Críticas surgiu no seguimento do 2º seminário de Proteção das Infraestruturas críticas da EU e contou com a participação dos Estados-Membros e das associações industriais. Este documento é datado de 17 de Novembro de 2005, e descreve as opções tomadas em relação ao Programa Europeu de Proteção das Infraestruturas Críticas.

Este documento tem por objetivo acolher as reações dos Operadores, a fim de dar início à preparação de um pacote estratégico PEPIC. Pretende-se, desta forma, desenvolver o pensamento crítico, encontrando soluções no âmbito da prevenção e reação a incidentes em IC, que viabilizem a segurança dos cidadãos dos Estados-Membros.

Numa primeira fase, o (COM (2005) 576 final) Livro Verde relativo a um Programa Europeu de Proteção das Infraestruturas Críticas, apresentado pela

Comissão a 17 de Novembro de 2005, sugere as abordagens mais convenientes a adotar neste âmbito:

a) Abordagem exaustiva de todos os riscos: **"**trata-se de uma abordagem global que atenda a riscos quer de ataques intencionais quer de catástrofes naturais, que assegura que as sinergias entre as medidas de proteção sejam aproveitadas ao máximo, sem atribuir qualquer ênfase específico ao terrorismo;"

b) Abordagem de todos os riscos com prioridade para o terrorismo: **"**trata-se de uma abordagem flexível para assegurar a articulação com outros tipos de riscos, como a ameaça de ataques intencionais e catástrofes naturais, que desse no entanto prioridade ao terrorismo. Se as medidas de protecção de um dado sector industrial fossem consideradas adequadas, as partes interessadas poderiam centrar a sua atenção nas ameaças em relação às quais fossem ainda vulneráveis."

c) Abordagem em relação aos riscos de terrorismo: *"*trata-se de uma abordagem centrada no terrorismo que não prestaria qualquer atenção específica a ameaças mais comuns. "

O mundo atual está exposto a diversos riscos, sejam eles causas naturais ou por ação do Homem, como é o caso do terrorismo. Por este facto e dada a complexidade de fatores que se geram em redor da temática da segurança, é de considerar absolutamente redutora a visão da terceira abordagem. O terrorismo tem de facto uma grande expressão no paradigma atual, principalmente pelo impacto que causa e pelo alarme social que cria. No entanto, não é possível aceitá-lo como o único risco necessário a ter em conta. Tal acontece sobretudo no contexto da proteção das Infraestruturas Críticas, em que as catástrofes naturais ou os incidentes provocados de forma não intencional pelo homem, se tornam um perigo iminente a considerar, já que têm potencial para gerar graves consequências.

Como abordado anteriormente os ataques terroristas são um motivo de preocupação no que concerne à defesa de um Estado, apesar de não merecerem uma atenção exclusiva, merecem pelo menos uma atenção cuidada. Do ponto de vista do alvo a atingir, os ataques terroristas podem ser, certamente, tão

inesperados como um desastre natural. No entanto, sendo os primeiros planeados por indivíduos, tornam-se passíveis de investigação preventiva. Nestas circunstâncias, a "abordagem de todos os riscos com prioridade para o terrorismo", é aquela que se considera mais adequada à realidade atual. Reflexo disso é o facto da:

- Comissão ter adotado, a 20 de Outubro de 2004, uma comunicação relativa à proteção das infraestruturas críticas no âmbito da luta contra o terrorismo, "que apresenta sugestões sobre como reforçar a prevenção, o estado de preparação e a capacidade de resposta da Europa a atentados terroristas que envolvam infra-estruturas críticas."

- Decisão do Conselho de 12 de Fevereiro de 2007 que cria, para o período de 2007 a 2013, no âmbito do Programa Geral sobre Segurança e Proteção das Liberdades, o programa específico «Prevenção, preparação e gestão das consequências em matéria de terrorismo e outros riscos relacionados com a segurança»

No mesmo Livro Verde podemos verificar uma preocupação especial no que refere à ligação de Infraestruturas críticas em rede. Esta preocupação é aceite como um resultado natural do desenvolvimento atual, no entanto, essa ligação cria grandes preocupações quanto às fragilidades resultantes dessa situação. Para colmatar tal debilidade, criaram-se enquadramentos legais comuns, a fim de criar um padrão de proteção adotado por todos os Operadores.

No que se refere aos critérios a adotar quanto à identificação das Infraestruturas Críticas, torna-se necessário numa primeira instância, criar um acordo em relação à lista comum de definições e setores de IC, e posteriormente criar uma base comum de critérios identificativos. Tendo em conta a disparidade existente entre setores das IC, e mesmo entre Infraestruturas da mesma área de atuação económica, o documento recomenda que o trabalho seja efetuado na sua generalidade, ao nível sectorial, não descurando o nível multissectorial.

No seguimento do desígnio inicial do Livro Verde, pode-se apreender um dos pilares fundamentais pelo qual se desenvolve o futuro Programa Europeu de Proteção das Infraestruturas Críticas, ou seja: "o estabelecimento de um enquadramento comum para o PEPIC (objetivos e metodologias comuns, por exemplo para estabelecer comparações e interdependências), do intercâmbio de boas práticas e da observância de mecanismos de controlo. O enquadramento comum poderá abranger os seguintes elementos:

• Princípios comuns de PIC;

• Códigos/normas comummente acordados;

• Definições comuns com base nas quais se possa chegar a acordo sobre definições sectoriais específicas (o Anexo 1 inclui uma lista indicativa de definições);

• Uma lista comum dos sectores das IC (o Anexo 2 inclui uma lista indicativa de sectores);

• Áreas prioritárias em matéria de PIC;

• Descrição das responsabilidades das partes interessadas;

• Parâmetros estabelecidos de comum acordo;

• Metodologias para comparar e atribuir prioridade às infra-estruturas dos diferentes sectores. "

Constata-se um reforço da importância da criação de um enquadramento jurídico adequado e bem definido no que concerne às responsabilidades e direitos que cada Estado-Membro, cada operador e a Comissão Europeia devem fruir.

O Capitulo 6 do documento apresenta uma abordagem específica às Infraestruturas Críticas Europeias, não avançando com uma definição mas apontando elementos necessários, que devem constar na mesma, nomeadamente:

- "O seu efeito transfronteiras, que indica se o incidente pode ter consequências graves fora do território do Estado-Membro em que a instalação está localizada;"
- "As ICE podem incluir recursos físicos, serviços, dispositivos de tecnologias da informação, redes e componentes de infra-estruturas que,

caso sejam danificados ou destruídos, podem ter consequências graves para a saúde, segurança e bem-estar económico ou social."

O mesmo capítulo avança com a proposta para as fases de implementação das ICE, que tal como veremos mais à frente não se coaduna com o aplicado atualmente.

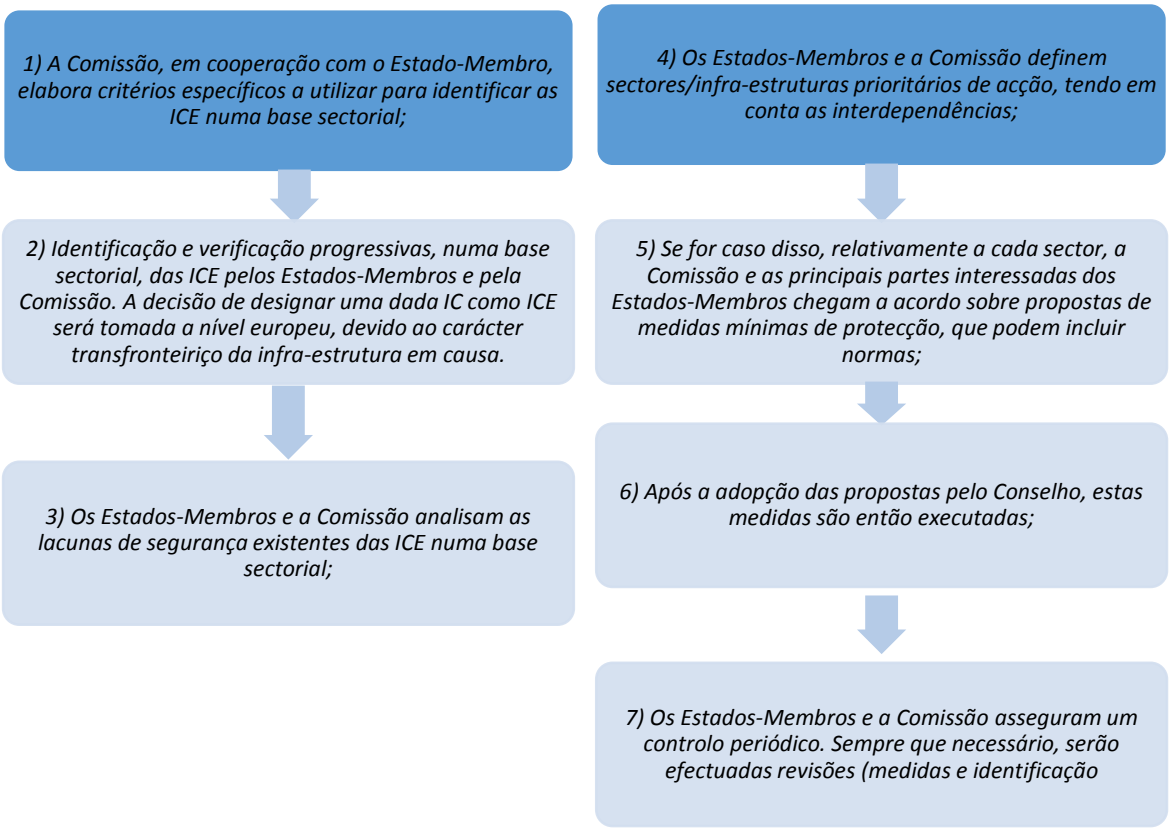

Figura 8 Fases de implementação das ICE
Fonte: Adaptado pelo autor

Todas as ICE são Infraestruturas Criticas Nacionais, e nesse sentido o diploma aponta para a necessidade dos Estados-Membros aproximarem as suas legislações tendo em vista a partilha entre si de um enquadramento comum. A Comissão apresenta, no entanto, alguma abertura no ponto 7.2, ao referir que os Estados-Membros devem desenvolver os seus próprios Programas Nacionais de Proteção de Infraestruturas Críticas, podendo mesmo, aplicar medidas mais restritas do que as previstas no PEPIC.

Em sequência, foi sugerida a elaboração de uma lista de sete itens, para identificar as infraestruturas como ICN, nos termos apresentados na Figura 9.

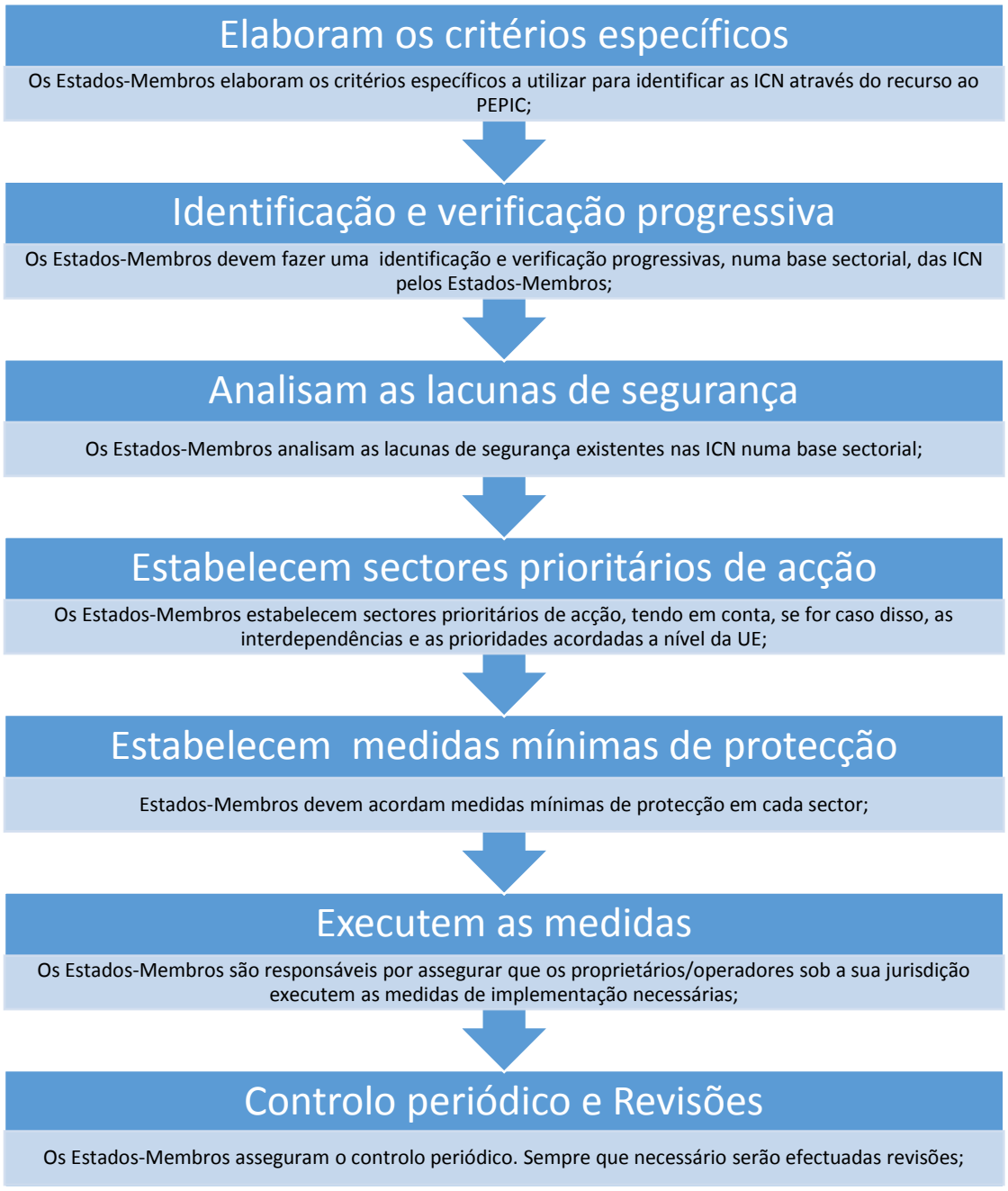

Figura 9 Fases da nomeação de uma infraestrutura como ICN
Fonte: Efetuado pela autora

O documento propõe ainda a adoção por cada país de um organismo para "coordenar, controlar e fiscalizar a execução do PEPIC no seu território e construir o principal ponto de contacto (…) com a Comissão. "Em Portugal, como anteriormente foi referido, é a ANPC que tem competências para estabelecer os contactos nestas matérias com a Comissão Europeia. Porém, a função fiscalizadora a que o documento se refere não é executada atualmente.

O ponto 8.1 encarrega-se de atribuir responsabilidades também aos Operadores e Utilizadores das IC, nomeadamente:

1- "Notificação ao organismo pertinente de PIC do Estado-Membro em causa do facto de uma infra-estrutura poder ter um carácter crítico;"

2- "Designação de um representante de alto nível para agir como funcionário de ligação de segurança (FLS) entre o proprietário/operador e a autoridade PIC competente do Estado-Membro (…);"

3- "Elaboração, execução e actualização de um plano de segurança dos operadores.(…);"

4- "Participação, mediante pedido, no desenvolvimento de um plano de emergência em relação às IC (…);"

Por último, a Comissão avança com quatro medidas de apoio ao Programa Europeu de Infraestruturas Críticas. A primeira prende-se com a criação de um sistema em rede que permite partilhar informação, nomeadamente dados que possam contribuir para ajustar medidas de segurança em IC de outros Estados-Membros. A segunda, são metodologias comuns a adotar no que se refere aos níveis de alerta de cada Estado-Membro, já que uma possível disfunção de uma IC pode, nestas circunstâncias, ter interpretações diferentes. A terceira medida surge no âmbito de uma decisão da Comissão em disponibilizar sete milhões de euros para o financiamento de um conjunto de ações de âmbito antiterrorista, onde se inclui a proteção às IC e mais especificamente o desenvolvimento do PEPIC. Esse esforço financeiro aplica-se em projetos de investigação na área da proteção de infraestruturas críticas. Por último, a quarta fase é destinada à avaliação e ao acompanhamento do PEPIC, o qual necessita da cooperação entre todos os intervenientes no processo.

2.7.2 Diretiva 2008/114/CE do Conselho, de 8 de Dezembro de 2008

A Diretiva 2008/114/CE do Conselho de 8 de Dezembro, pode ser considerada a pedra angular da longa construção que se espera que seja o Programa Europeu de Proteção das Infraestruturas Criticas. Tal como enuncia o ponto 5 do preâmbulo, a Diretiva aborda apenas os setores dos transportes e da energia, deixando no entanto a indicação da necessidade da inclusão de outros sectores de atividade em revisões posteriores.

No Artigo 2.º a Comissão apresenta a definição de ICE adotada:

"(…) Infra-estrutura crítica situada nos Estados-Membros cuja perturbação ou destruição teria um impacto significativo em pelo menos dois Estados-Membros. O significado do impacto deve ser avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infra-estruturas; Este compromisso indica que serão consideradas como infraestruturas críticas europeias aquelas cuja perturbação ou destruição poderá ter implicações diretas em dois ou mais Estados-Membros."

No que diz respeito à identificação das ICE, tal como abordado no n.º1 do artigo 3.º, é atribuída aos Estados-Membros a responsabilidade de identificar as potenciais Infraestruturas Críticas Europeias, localizadas no seu território, e informar os Estados vizinhos potencialmente afetados. Para tal é essencial uma cooperação e negociação entre responsáveis, procurando-se a definição de estratégias conjuntas para melhorar a proteção das IC e minimizar os impactos transfronteiriços. O artigo refere que a Comissão poderá, por um lado, ser chamada a auxiliar os Estados-Membros na identificação das ICE, bem como indicar espontaneamente infraestruturas que sejam passíveis de preencher os requisitos. Essa identificação é efetuada através de comunicação anual à Comissão, incluindo o número de ICE designadas em cada sector, bem como os Estados-Membros dependentes de cada uma, tal como indica o n.º 4 do artigo 4.º.

Os Operadores de ICE, de acordo com o n.º 5 do artigo 4.º, devem ser informados que as mesmas foram designadas como tal. Nesse contexto ficou definida a obrigatoriedade da existência de Planos de Segurança (designados como Planos de Segurança do Operador – PSO), para cada Infraestrutura Crítica Europeia.

A Diretiva contempla ainda a obrigatoriedade de existência de um Oficial de Ligação de Segurança, o qual assegurará a ligação entre o operador da Infraestrutura Crítica e a autoridade competente do Estado-Membro, designadamente funcionando como ponto de contacto para os fluxos de informação sobre riscos e ameaças identificadas (n.º 2; artigo 2º). Tal qual descrito no n.º 3 do artigo citado anteriormente é da responsabilidade do Estado-Membro, garantir que é elaborado um PSO ou plano equivalente, como por exemplo os Planos de Emergência, devendo estes ser sujeitos a uma revisão periódica anual.

Por último, a fim de imprimir um carácter mais regulador ao processo, o artigo 7º. refere que cada Estado-Membro deverá efetivar uma avaliação das ameaças e riscos a que cada sector está sujeito e entregar de dois em dois anos um relatório sobre a matéria. A Comissão exige, por força do n.º 1 do artigo 9º., que todas as pessoas que trabalham com informação confidencial no âmbito destes processos, devem ser sujeitas a "um procedimento de habilitação de segurança adequado. "

2.7.3 Decreto-Lei n.º 62/2011, de 9 de Maio

O Decreto-Lei n.º 62/2011, de 9 de Maio, contribuiu significativamente para o desenvolvimento da matéria relativa à Proteção das Infraestruturas Críticas em Portugal. Resulta da transposição para o ordenamento jurídico Português da Diretiva n.º 2008/114/CE do Conselho de 8 de Dezembro, estabelecendo os procedimentos de identificação e de proteção das Infraestruturas essenciais para a sociedade nos setores específicos da energia e dos transportes.

O preâmbulo refere que "Portugal adquire uma maior capacidade de intervenção ao nível da segurança e resiliência das infraestruturas que venham a ser sectorialmente consideradas críticas".

Este Decreto-Lei promove a necessidade de uma profunda cooperação tanto a nível nacional como Europeu, baseada na comunicação, coordenação e partilha de informação estratégica. Este ponto de contacto é definido no artigo 15.º deste diploma, atribuindo tais competências ao CNPCE (atual ANPC).

No artigo 2.º, encontramos os primórdios da construção do pensamento sobre esta matéria, isto é, a definição de Infraestruturas Críticas e Infraestruturas Críticas Europeias, que suportam os procedimentos explanados no artigo 4.º. É aliás no nº 3 deste artigo que são apresentados os critérios necessários à sua identificação, sendo eles:

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

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

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

Ainda no que concerne à identificação das ICE, de acordo com o n.º 1 do artigo 5º o processo compreende quatro fases.

Na primeira são aplicados critérios sectoriais tendo em vista efetuar a primeira seleção das IC dentro de determinado setor. Após essa seleção, a definição de ICE é aplicada às IC selecionadas sectorialmente. Na terceira fase do processo é aplicado o elemento transfronteiriço. Por fim, a quarta fase é caracterizada pela adequação dos critérios transversais da fase anterior às potenciais ICE, mas que desta feita não tenham sido identificadas nos termos dos números anteriores. Este processo culminará com a elaboração de uma base de

dados de ICE. Contudo, tal como indica o n.º 7, todas as potenciais ICE que no final do processo de identificação não tenham preenchido os critérios de qualquer uma das fases anteriores, não podem ser consideradas como tal. No entanto, prevê-se de acordo com o artigo 9.º, que caso o Estado Português considere poder sofrer uma afetação por parte de uma IC presente no território de outro Estado, poderá comunica-lo à Comissão Europeia, a fim de ser desencadeado um processo de negociação bilateral ou mesmo multilateral.

Nos artigos 10.º 11.º, são apresentadas duas responsabilidades por parte dos Operadores. Na primeira encontram-se descritas as especificidades dos Planos de Segurança dos Operadores. De acordo com o n.º 1 do artigo 10.º este plano de segurança é para os Operadores de ICE de caráter obrigatório e com aprovação necessária até um ano após a designação como Infraestrutura Crítica Europeia, estando também prevista a sua revisão anual. Nos termos do n.º 4, o mesmo plano terá de ser revisto anualmente pelos operadores e submetido a parecer prévio pela força de segurança territorialmente competente e pela Autoridade Nacional de Proteção Civil. A última fase do processo prevê a validação pelo Secretário-Geral do Sistema de Segurança Interna.

O Plano dos Operadores de ICE, como indica o n.º 2 do mesmo artigo, terá de conter os seguintes elementos:

a) "Identificação dos elementos importantes";
b) "Uma análise de risco baseada em cenários de ameaça grave, na vulnerabilidade de cada elemento e nos impactos potenciais";
c) "A identificação, seleção e prioridade de contramedidas e procedimentos de segurança permanente";
d) "A identificação, seleção e prioridade de contramedidas e procedimentos de segurança progressivos, a ativar consoante o grau de ameaça aplicável à ICE ou o estado de segurança decretado."

O Plano de Segurança do Operador será sempre articulado com o plano desenvolvido pela força de segurança territorialmente competente e pela Proteção Civil – Plano de segurança e Proteção Exterior, tal qual é assinalado no n.º 5.

Como referido atrás, o artigo 11.º, preconiza outra das responsabilidades dos Operadores, designadamente a necessidade da presença de um agente de ligação de segurança que cumpra os requisitos da categoria de diretor de segurança, referida na Lei nº 34/2013, de 16 de Maio[1]. O agente serve de ponto de contacto entre o proprietário da ICE e o Secretário-Geral do Sistema de Segurança Interna.

No artigo 14º, determina-se o nível de proteção a que é sujeita a informação relacionada com as ICE. Toda a informação (escrita e não escrita), é classificada e nessa medida, todas as pessoas que trabalham com essa informação, de acordo com o n.º 2, devem ser submetidas a um procedimento de habilitação adequado concedido pela Autoridade Nacional de Segurança.

O artigo 15º do referido Decreto-Lei dispõe que o ponto de contacto junto da Comissão Europeia para a proteção das Infraestruturas Críticas Europeias é a Comissão Nacional de Proteção Civil de Emergência, atual Autoridade Nacional de Proteção Civil, especificamente no que se refere à designação das ICE. Já no que ao plano de segurança se refere, é tal como indica o n.º 2 do mesmo artigo, o Secretário-Geral do Sistema de Segurança Interna que exerce a função de ponto de contacto.

É crucial que na prossecução da análise deste Decreto-Lei se tenha em linha de conta, que tudo o que se encontra disposto é aplicável às restantes infraestruturas críticas nacionais, tal como descrito no artigo 17.º.

Por último, o artigo 18.º estipula que, todo o processo anteriormente descrito de identificação e designação das ICE deveria ficar concluído até dia 31 de Dezembro de 2011.

[1] Estabelece o regime do exercício da atividade de segurança privada.

2.8 Resenha de práticas noutros Países

Como vimos no capítulo respeitante à definição de Infraestruturas críticas, a classificação que é efetuada pelos países baseia-se em diferentes critérios. Estas diferenças podem ser facilmente explicadas mediante a adoção de diferentes abordagens influenciadas por diversos fatores sociais, políticos e económicos (Natário & Nunes, 2014). Esta discricionariedade permite uma diferenciação entre países quanto ao reconhecimento que os próprios fazem dos seus setores críticos.

SECTORES \ PAÍSES	AUS	AUT	BRA	CAN	EST	FRA	FIN	DEU	HUN	IND	ITA	JPN	KOR	MAL	NLD	NOR	NZL	POL	RUS	SWE	SGP	ESP	CHE	GBR	USA
Banca e Finanças	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Governo Central		•		•	•	•		•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•
Indústria Química e Nuclear				•						•				•	•			•				•	•		•
Serviços de Emergência	•		•	•	•	•			•	•	•		•	•		•	•	•	•				•	•	•
Electricidade/Energia	•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•			•	•	•	•	•
Agricultura/Alimentação	•			•	•	•	•	•	•		•	•			•	•					•	•	•	•	•
Serviços de Saúde	•		•	•	•	•	•		•		•			•	•	•					•	•	•	•	•
Comunicação/Media	•	•				•	•		•		•		•		•	•			•	•	•		•		•
Defesa						•			•	•			•	•		•			•					•	•
Monumentos Nacionais	•																								•
Esgotos/Resíduos	•									•			•	•	•			•					•	•	•
Telecomunicações	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•		•	•
Transportes/Logística	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•
Distribuição de Água	•		•		•	•	•	•	•		•	•		•	•	•				•	•	•	•	•	•

Figura 10 Setores Críticos em diversos países
Fonte: Brunner e Suter (2008) e (Natário & Nunes, 2014)

Pode-se verificar, pela análise do quadro 10, particularidades tais como o facto do setor da Banca e das Finanças serem considerados setores críticos por todos os países visados, o sector da Eletricidade/Energia não se encontrar entre as opções de países como o Brasil, Malta, Rússia e Suécia, bem como, o facto de os Estados Unidos da América (EUA) considerarem todos os setores do estudo, setores críticos.

2.8.1 Estados Unidos da América

Antes do ataque terrorista às torres gémeas decorrido a 11 de Setembro de 2001, em Nova Iorque, não existia uma preocupação muito acentuada em relação à segurança das Infraestruturas Críticas do país. Contudo, o ataque envolveu recursos privados (aviões comerciais), um setor de Infraestruturas Crítica (setor dos transportes), tendo como objetivo atingir recursos públicos e privados (como o World Trade Center e o Pentágono), colocando assim muitas infraestruturas críticas em risco. (S.Eckert, 2005)

Neste contexto, surge em 2002, o *Homeland Security Act of 2002: Critical Infrastructure Information Act*[2], que propõe a criação de um novo departamento responsável pela avaliação das vulnerabilidades das IC dos Estados Unidos, abrangendo, tal como podemos verificar pela Figura 10, os sistemas de água e alimentação, agricultura, saúde, serviços de emergência, informação e telecomunicações, banca e finanças, energia, transporte, indústrias químicas e de defesa, entidades postais e de transporte, e monumentos e ícones nacionais.

Em 2003, é lançado o *Homeland Security Presidential Diretiva 7*[3] dando competências aos departamentos federais de identificar, priorizar e encontrar medidas para proteger as IC.

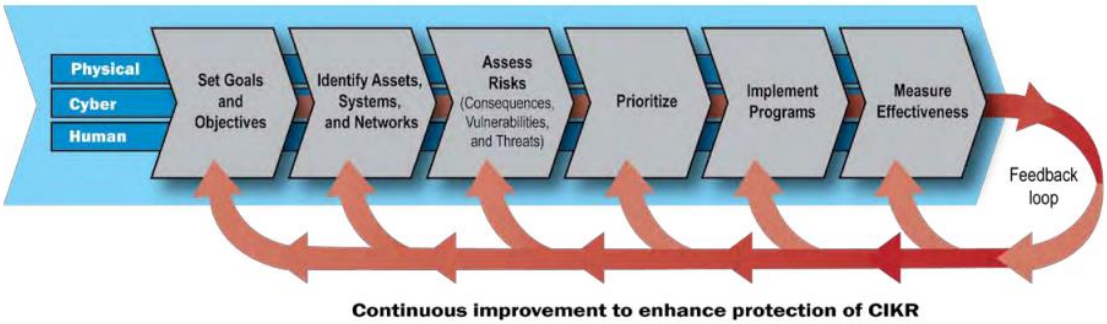

Figura 11 NIPP Risk Management Framework
Fonte: (Homeland Security, 2013)

[2] http://fas.org/sgp/crs/RL31762.pdf
[3] http://www.dhs.gov/homeland-security-presidential-directive-7#1

No mesmo ano, a *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*[4] apresenta os objetivos e os princípios orientadores a nível nacional, para manter as infraestruturas vitais em segurança. Neste documento são identificadas seis áreas que devem ser tidas em conta no que à proteção das IC diz respeito – *Homeland Security Critical Mission Areas.* Estas áreas incluem:

- Inteligência e de advertência;
- Segurança das fronteiras e transporte;
- Contra terrorismo;
- Proteger infraestruturas críticas e ativos-chave;
- Defender contra o terrorismo catastrófico;
- Preparação e resposta a emergências.

Em 2007 é publicado o *Homeland Security Appropriations Act*, legislação específica para instalações químicas de alto risco.[5]

Por fim, em 2009 é emitido o Plano Nacional para a proteção das infraestruturas críticas, com o objetivo de construir "uma América mais segura, e mais resistente, para prevenir, impedir, neutralizar ou mitigar os efeitos da esforços deliberados por terroristas para destruir, incapacitar, ou exploram elementos de CIKR (...) e para fortalecer nacional preparação, resposta oportuna e rápida recuperação de CIKR no caso de um ataque, catástrofe natural, ou outra emergência." (Homeland Security of United States, 2014)

É na Lei de Segurança Interna dos Estados Unidos da América, que se encontra plasmada a responsabilidade do Departamento de Segurança Interna (DHS) de desenvolver e aplicar as medidas que garantam a segurança das Infraestruturas Críticas da Nação, ou seja, a responsabilidade de desenvolver o Plano Nacional de Segurança para a Proteção das IC. O Plano em causa desenvolve uma cuidada gestão de risco contínua e adaptada, aferindo a eficácia e o grau de resiliência das

[4] http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
[5] http://www.gpo.gov/fdsys/pkg/BILLS-109hr5441enr/pdf/BILLS-109hr5441enr.pdf

instituições, mediante a execução de simulacros, contribuindo para a mitigação do risco.

2.8.2 França

Em França, a Proteção das IC encontra-se centralizada no *Secrétariat General de la Défense Nationale*, que está na dependência do Presidente, tornando-se, por isso um órgão "transversal aos setores." (Pais, 2014)

As Infraestruturas Críticas encontram-se divididas em doze setores, que por sua vez se subdividem em três áreas, tal como é apresentado na Figura 12.

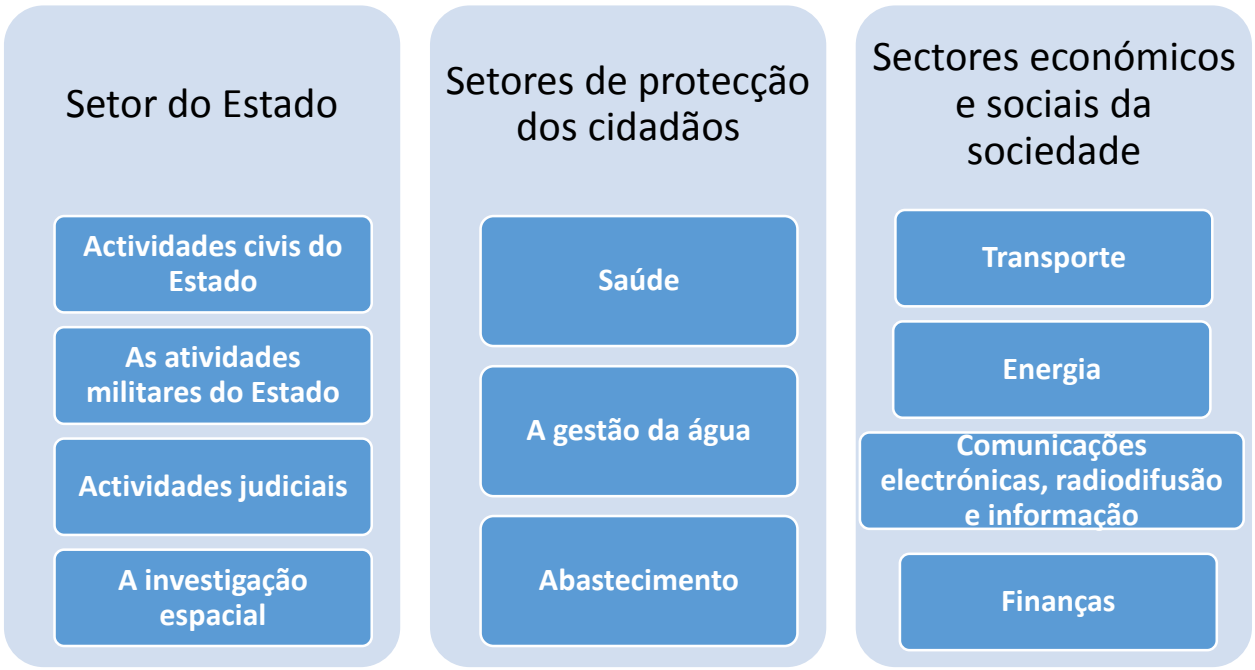

Figura 12 Setores IC Francês
Fonte: Adaptado pelo autor

De acordo com o *Secrétariat General de la Défense Nationale*, os operadores têm de respeitar três requisitos legais. O primeiro é a obrigação de formar responsáveis e diretores de segurança para as suas infraestruturas. O segundo obriga a proceder à avaliação dos riscos e das ameaças e à elaboração dos Planos de Segurança dos Operadores. O terceiro, obriga à identificação dos pontos críticos que

serão incluídos nos Planos Particulares de Proteção[6] e nos Planos de Proteção Externo[7].

O Plano apresentado na Figura 13 é o Plano do Sistema de Alerta de Segurança Nacional Francês (Vigipirate).

Cabe a cada operador identificar os componentes críticos tendo em vista a tomada das medidas de proteção adequadas às especificidades daquelas infraestruturas. Este documento aponta as eventuais ameaças, identifica as vulnerabilidades, define os requisitos de proteção e determina medidas para a sua execução. Este processo tem em conta a intensidade da ameaça, de acordo com o plano do governo - *Vigipirate*. Foram aprovadas pelo Primeiro-ministro francês vinte e uma Diretrizes Nacionais de Segurança (DNS). Nelas são especificadas as ameaças, os riscos e as vulnerabilidades correspondentes a fim de traçarem os objetivos de segurança. (Secrétariat Général de la Défense et de la Sécurité Nationale, 2014)

A estruturação do Plano para a Proteção das IC está representada na Figura 13. A primeira fase do plano é de carácter conceptual, na qual foram redigidas as normas nacionais de segurança. Após a fase de identificação foram considerados cento e cinquenta operadores de IC, distribuídos por sete sectores: Agrícola; Água; Energia: Saúde e Transportes. Posteriormente, cada operador desenvolveu o seu próprio plano de segurança, apoiado no Plano Particular de Proteção e no Plano de Proteção Externo. (Secrétariat Général de la Défense et de la Sécurité Nationale, 2014)

[6] Plan particulier de sécurité (PPP) trata-se de um documento que define o conjunto de medidas para prevenir os riscos associados com a operação de uma empresa num determinado local. (Tissot Éditions, 2014)

[7] Plan de protection externe (PPE) é um documento complementar ao PPP que define medidas de vigilância, prevenção, proteção e resposta fornecidas pelo governo, incluindo pelas forças de segurança.

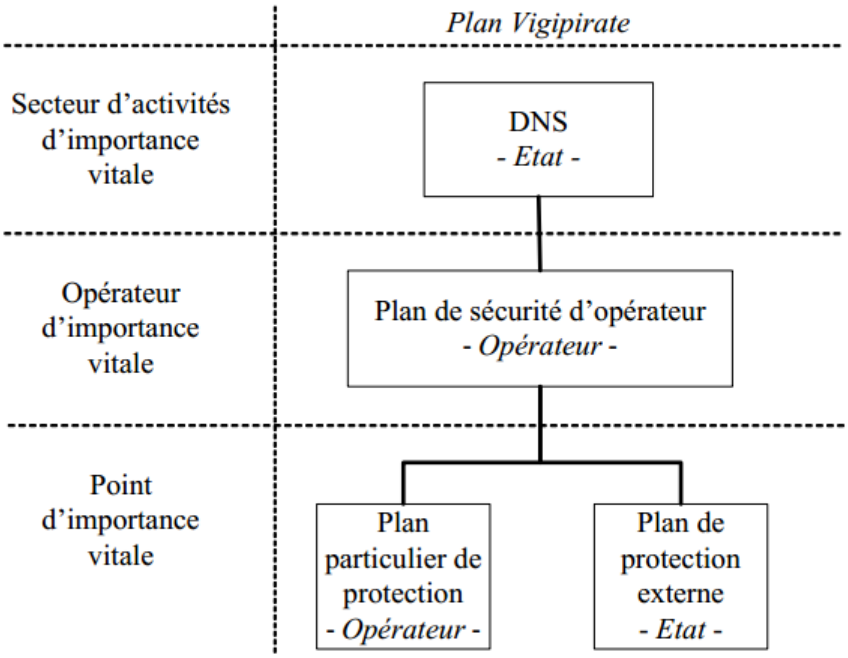

Figura 13 Plano para a Proteção das IC
Fonte: (Secrétariat Général de la Défense et de la Sécurité Nationale, 2014)

2.8.3 Espanha

O sector das IC encontra-se regulado no Real Decreto 704/2011, de 20 de Maio, que resulta da transposição da Diretiva 2008/114/CE do Conselho e estabelece as estratégias adequadas a adotar e as responsabilidades partilhadas pelos intervenientes, tal como indica o seu artigo 1.º.

Este regulamento através do artigo 7.º, determina a criação do Centro Nacional para la Protección de las Infraestruturas Críticas (CNPIC), responsável pela coordenação, supervisão e promoção de todas as atividades relacionadas com a proteção das IC, encontrando-se sob a dependência da Secretaria de Estado da Segurança. Este organismo, para além de ser o ponto de contacto junto da Comissão, tem vários objetivos a concretizar, sendo de salientar os seguintes:

- Determinar a criticidade das instalações incluídas no Catálogo Nacional de Infraestrutura Estratégica[8] e manutenção operacional e atualizar o mesmo;
- Definir o conteúdo mínimo dos Planos de Segurança dos Operadores, de Planos de Proteção, Planos e operações de apoio específico, supervisionando o processo de preparação;
- Avaliar os Planos de Segurança do Operador e propor, se necessário, para aprovação, ao Secretário de Estado da Segurança.

Foram identificadas 3.500 instalações, distribuídas por onze sectores tal como se pode verificar na Figura 14:

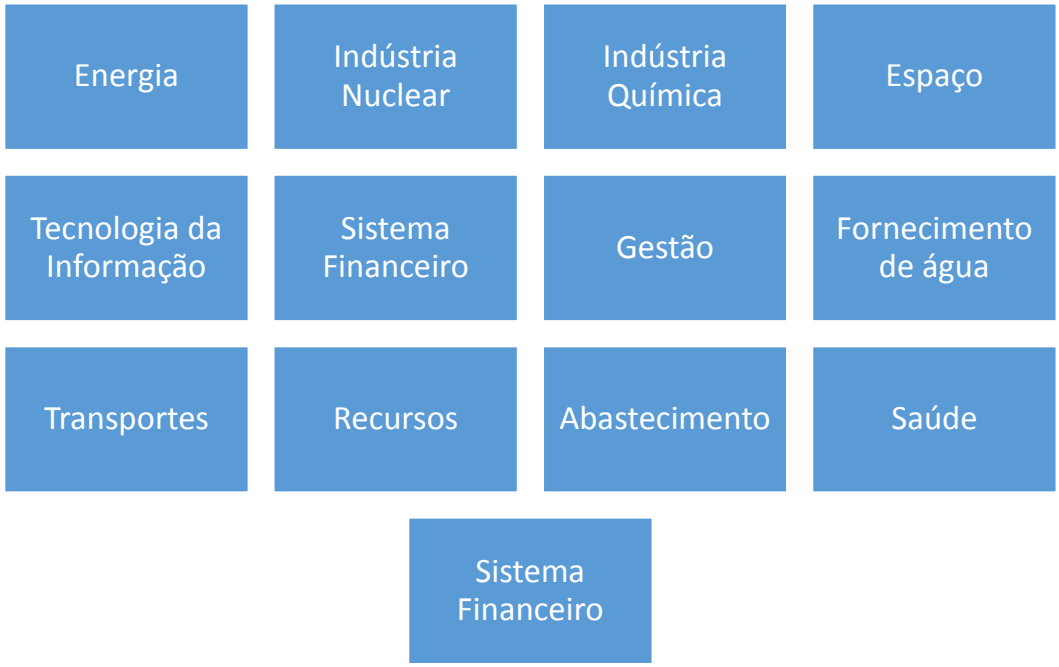

Figura 14 Setores Infraestruturas Críticas Espanholas
Fonte: Adaptado pelo autor

Com a Ley 8/2011, de 28 de Abril, que estabelece medidas para a proteção das Infraestruturas Críticas, foi possível desenvolver um Plano Nacional neste âmbito[9]. Desse plano nasceu o Plano Estratégico do Sector (PES), Planos de

[8] O Catálogo Nacional de Infraestruturas Estratégicas é uma base de dados informatizada que contém a lista completa e atualizada das Infraestruturas do país com a sua caracterização detalhada. (CNPIC, 2014)
[9] Plan Nacional de Protección de las Infraestructuras Críticas

Segurança dos Operadores (PSO), Planos de Proteção e Específicos (PPE) e Planos de Suporte Operacional (PAO). O *Plan Nacional de Protección de las Infraestructuras Críticas* (PNPIC), estabelece orientações específicas para a mobilização das administrações públicas, em estreita cooperação com os Operadores. O PES permite determinar quais são os serviços essenciais em cada setor estratégico, o seu funcionamento normal, as vulnerabilidades que lhes são intrínsecas e as potenciais consequências da sua inatividade (CNPIC, 2014).

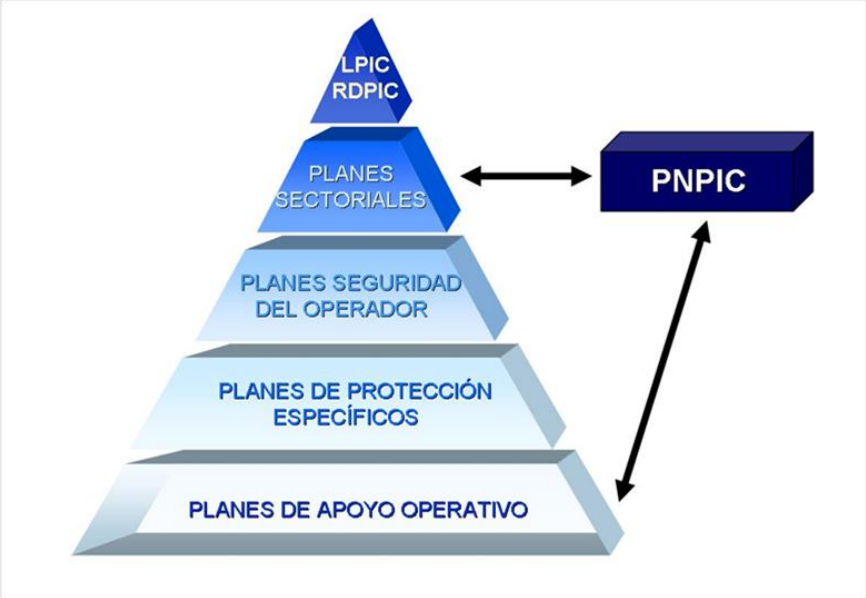

Figura 15 Distribuição dos Planos de segurança em Espanha

Fonte: (CNPIC, 2014)

O PSO e o PPE são planos da responsabilidade do Operador, nos quais estão plasmadas as medidas que têm de ser seguidas em situação de distúrbio. Por último, o PAO é desenvolvido em estreita concordância com o PPE e incluí as medidas de vigilância, prevenção e reação que devem ser prestadas pelas autoridades públicas em caso de ativação do PNPIC. A esquematização deste sistema encontra-se retratada na Figura 15. Todos estes planos indicam quais as medidas a tomar e quem deve ser responsável por acioná-las. Atribui responsabilidades do ponto de vista técnico e funcional.

Capitulo 3: Apresentação e Análise de Resultados;

3.1 Metodologia

No que concerne à metodologia a aplicar decidimos adotar uma estratégia metodológica mista, onde conjugámos a análise de documentação, fruto da pesquisa bibliográfica e do levantamento da legislação nacional e das normas Europeias. Foi posteriormente cruzada a informação com os resultados obtidos através da análise das entrevistas semiestruturadas, realizadas aos operadores de infraestruturas críticas nacionais, do setor dos transportes e da energia.

Quanto ao levantamento bibliográfico, foi selecionado um conjunto de estudos sobre o tema recorrendo a artigos ciêntificos, livros, monografias,dados estatísticos e legislação relacionada. A escassez de estudos realizados em Portugal, sobre esta temática, constituiu uma das limitações que tivemos de superar, a qual, felizmente pudemos colmatar com o recurso às entrevistas realizadas.

Assim, terminada a contextualização anterior, assim como o respetivo enquadramento legal, necessários para a transparência dos resultados subsequentes, seguir-se-á uma análise das práticas dos operadores nacionais, desenvolvida e fundamentada com os dados recolhidos.

As entrevistas semiestruturadas foram realizadas aos operadores de infraestruturas críticas dos sectores dos transportes e da energia, os quais servem atualmente de base à Diretiva 2008/114/CE do conselho de 8 de Dezembro de 2008 e do Decreto-Lei n.º 62/2011, de 9 de Maio. Foi também efetuada uma entrevista semiestruturada à Dr.ª Isabel Pais[10], responsável pelo Programa Nacional de Proteção das Infraestruturas Criticas e ponto de contacto nacional junto da UE.

[10] Visão institucional da Autoridade Nacional de Proteção Civil

Capitulo 3: Apresentação e Análise de Resultados;

Ao nível do conteúdo, o conjunto das entrevistas procurou compreender em que ponto o PNPIC se encontra e se os Operadores de IC se encontram empenhados no cumprimento das normas especificas da lei base[11]. Teve como objetivos específicos perceber como esta estruturada a resposta dada pelos operadores a situações de emergência e de que forma estão a ser envolvidos no projeto desenvolvido pela ANPC. No que se refere à ANPC pretendeu-se analisar a sua visão quanto ao projeto desenvolvido, ao enquadramento legal vigente e aos resultados obtidos junto dos operadores.

Para tal, procurou-se através da utilização desta tecnica – a da entrevistas semiestruturadas - criar proximidade entre o investigador e o entrevistado, fazendo com que os elementos pertinentes para a investigação fossem mais facilmente disponibilizados e apreendidos. Houve contudo um cuidado na distância estabelecida entre o entrevistador e o entrevistado, imprimindo sempre uma postura adequada e nunca esquecendo o objetivo da entrevista. Ao salvaguardar a posição do entrevistador face ao seu objeto de estudo, contribui para minimizar a possibilidade de surgir respostas consideradas socialmente pouco aceitáveis (Santo, 2010). As entrevistas foram semiestruturadas, apresentando um guião prévio, permitindo desta forma criar flexibilidade e dinamismo. Neste tipo de entrevista são apresentadas perguntas ao entrevistado, concedendo no entanto ao entrevistador a possibilidade de realizar questões complementares para entender melhor o fenómeno em causa (Manzini, 2012).O guião da entrevista obedeceu a cuidados quanto à formulação e estruturação das perguntas, procurando que estas fossem "claras, curtas quanto possível, não tendenciosas, não ambíguas, com um ou poucos e não incluindo múltiplos tópicos de análise" (Santo, 2010). Com a entrevista “não se procura nem é apropriada a representatividade dos resultados em termos extensivos. Pelo facto de se tratar de uma técnica de recolha de dados intensiva ou em profundidade, privilegia-se a qualidade da informação na técnica de entrevista” (Santo, 2010). Esta opção metodológica procurou obter informações sobre a disposição da direção de segurança no contexto organizacional, recolher

[11] Decreto-Lei n.º 62/2011, de 9 de Maio

dados relevantes referentes aos planos de segurança desenvolvidos e perceber os objetivos futuros na estratégia traçada.

Procuramos utilizar a comparação a fim de potenciar o resultado da informação recolhida através do método qualitativo. Tendo em conta as perguntas de partida, pareceu-nos importante contrapor as várias práticas e visões dos entrevistados, procurando chegar sempre a um fluxo de causalidade. Existindo intenção de estabelecer comparação, é "fundamental a definição de pressupostos quer metodológicos quer teóricos específicos (...)" (Santo, 2010). Assim, tivemos em atenção a amostra pretendida, o conjunto de perguntas a aplicar bem como o próprio período de recolha de dados.

O estudo que apresentamos em seguida é fruto de um processo participativo, envolvendo gestores das infraestruturas, empresas utilizadoras e entidades reguladoras.

3.2 Limitações no desenvolvimento do Trabalho

A primeira limitação no desenvolvimento deste projeto prendeu-se com o reduzido volume de informação bibliográfica sobre estas matérias em Portugal, motivo pelo qual as entrevistas conseguidas foram sobejamente importantes.

A mais significativa limitação deste trabalho estabeleceu-se ao nível das autorizações formais junto dos Operadores de IC. Várias direções de segurança dos Operadores de Transportes e Energia foram contactadas, no entanto, na maior parte dos casos o convite foi declinado.

3.3 Análise dos resultados

Tornou-se necessário entender a posição organizacional ocupada pela Direção de Segurança (DS) de cada empresa. Este tópico permite perceber que influência decisória a DS tem, dependendo da posição hierárquica que ocupam. Através da análise das entrevistas expostas na Tabela 2, podemos verificar que, no caso da REFER e do METRO, a posição ocupada permite responder diretamente

à administração. Já no caso da ANA, apesar da área de segurança estar inserida na Direção Técnica Aeroportuária e de, por esse motivo, hierarquicamente responder ao Diretor da mesma, considera que a representação dos seus interesses não é posta em causa. Já no caso do Porto de Lisboa, a Direção de Segurança encontra-se na vertente da Autoridade Portuária, contribuindo por isso para que, segundo o seu próprio diretor, exista um fraco envolvimento nas decisões tomadas em questões de segurança. No que concerne ao Grupo EDP, este divide-se em duas vertentes, sendo que a vertente *Safety* está integrada na EDP Valor, respondendo hierarquicamente à Direção de Segurança e Saúde, enquanto que a vertente de *Security* – onde estão integradas as ICN (Infraestruturas Críticas Nacionais) – é gerida nas empresas que as detêm, consoante a atividade, na EDP Produção e na EDP Distribuição. Estas áreas têm uma relação com a Direção de Gestão de Risco da EDP. Porém, todos os Operadores consideram vantajosa uma posição hierarquicamente próxima da administração da empresa, apontando vantagens ao nível da eficácia e da possibilidade de maior perceção das necessidades no momento da decisão. Para além desta vantagem, uma posição hierárquica mais próxima dos órgãos decisórios, cria na sua génese um sentimento de maior confiança por parte dos seus colaboradores.

Tabela 2 Posição organizacional

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Posição organizacional	"Na REFER A Direção de Segurança responde diretamente ao Conselho de Administração. As principais vantagens são o facto de ser mantido um relacionamento próximo com a mesma e poder tratar os assuntos diretamente com quem decide."	"A Direção de segurança do ML (ASC) insere-se na área corporativa da estrutura, diretamente dependente do Conselho de Administração."	"(…) temos uma unidade geral de segurança da ANA inserida na Direção Técnica Aeroportuária. A Direção responde diretamente à Administração da Ana. No entanto a área de segurança responde ao Diretor da Direção Técnica Aeroportuária. No entanto, apesar da área da segurança não ser independente, não sinto que não tenha uma voz ativa e que esteja distanciada da Administração. É muito regular fazer reuniões ou trabalhar em projetos com o Vogal da Administração. (…)"	"A Direção de Segurança e Pilotagem da APL, insere-se na organização na vertente da Autoridade Portuária." (…) Embora esteja inserida na vertente da Autoridade Portuária, nem sempre é devidamente envolvida em todos os processos desse âmbito."		No Grupo EDP a vertente *Safety* está integrada na EDP Valor (empresa de Serviços Partilhados do Grupo) e é "Corporativa (Direção de Segurança e Saúde); a vertente de *Security* – onde estão integradas as ICN (Infraestruturas Críticas Nacionais) – é gerida nas empresas que as detêm, consoante a atividade, na EDP Produção e na EDP Distribuição. Estas áreas têm uma relação com a Direção de Gestão de Risco da EDP (Holding).

No que se refere aos riscos identificados, os Operadores referem, tal como refletido na Tabela 3, que as maiores preocupações recaem sobre os riscos naturais e os provocados pela intervenção humana, sejam estes últimos com propósitos de vandalismo ou mesmo de apropriação de componentes das próprias infraestruturas. No caso do Metro de Lisboa são também identificados riscos tecnológicos, como a falta de energia ou mesmo problemas nos controladores.

Nesta situação torna-se importante salientar a visão global da ANPC, a qual considera que, a nível nacional, os maiores riscos identificados são o risco sísmico e atualmente os ciberataques. No entanto como a maior parte das IC nacionais são fábricas, os incidentes registados com mais frequência são explosões e incêndios.

Tendo por base o entendimento apresentado por cada um dos Operadores, verifica-se que os riscos naturais estão presentes na preocupação de todos os

Operadores, apesar de funcionarem em contextos físicos tão distintos. A ANPC partilha a mesma preocupação, no entanto, tendo por base uma visão necessariamente mais macro, evidencia o risco sísmico como o mais alarmante no que ao panorama nacional se refere, já que "é o único capaz de destruir várias coisas ao mesmo tempo e com uma enorme abrangência" (Pais, 2014). No caso dos Operadores ferroviários é notória a preocupação que recai sobre os riscos naturais, nomeadamente no que às inundações se refere. A precipitação abundante permite, em caso de fraco escoamento, bloquear caminhos e mover e/ou danificar equipamentos, podendo culminar na inutilização das operações. A Linha Ferroviária do Norte é precisamente distinguida pelo relatório da avaliação nacional de risco como uma infraestrutura que se encontra marcadamente exposta à possibilidade de ocorrência cheias.

Tabela 3 Maiores Riscos que a empresa foi alvo no último ano

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Maiores Riscos que a empresa foi alvo no último ano	"Tem muitas vezes a ver com fatores de ordem natural, como queda de objetos nas linhas. Também podem acontecer intervenção humana como roubo de equipamento fundamental à circulação. E as quedas nas linhas é claro"	"Essencialmente enfrentámos inundações decorrentes de situações de elevada pluviosidade e mau funcionamento da rede de efluentes públicos (…) situações decorrentes de riscos tecnológicos (…) e situações provocadas por terceiros quer de vandalismo quer de atos intencionais."	Principalmente fenómenos meteorológicos como o caso do Vulcão da Islândia este ano, ou o tornado que levou o teto do aeroporto de Faro em 2011.		"A maior parte das IC são fábricas ou equipamentos desse tipo e os riscos que acabam por ser os mais frequentes são incêndios, as explosões (…) a emissão de uma matéria perigosa para a atmosfera (…) agora, há alguns riscos que são mais abrangentes e mais preocupantes e o principal dentro dos riscos naturais é o risco sísmico. (…) Depois há os ataques terroristas e etc, em que não somos muito conhecidos por sermos um grande alvo.(…) Os ataques via virtuais são das maiores ameaças agora."	"Na EDP Distribuição a tempestade GONG, em 2013, pela disrupção criada no abastecimento de energia e dificuldades nas telecomunicações. Na EDP Produção nos últimos 3 anos não ocorreram riscos que colocassem em causa o normal funcionamento da companhia em si, e das suas instalações em particular.

A Tabela 4 é referente à adequação das medidas de segurança adotadas pelos Operadores considerando a posição específica que os mesmos ocupam como IC.

Todos os Operadores reconhecem não existir uma adaptação específica a essa posição, considerando no entanto suficientes as medidas de segurança implementadas resultantes da sua normal atividade. Nesse sentido, todos os Operadores indicam que já tinham previamente medidas de segurança plasmadas em vários regulamentos, como os Planos de Emergência e/ou os Planos de Continuidade de Negócio, sendo neste sentido os mesmos utilizados para satisfazer as necessidades do Plano de Segurança do Operador. A ANPC indica por sua vez que desenvolveu e entregou uma lista de conteúdo a incluir nos Planos do Operador, reconhecendo no entanto que muita da informação é transcrita de Planos de Segurança que as empresas anteriormente detinham.

Tabela 4 Adequação das medidas à posição de operador de IC

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Adequação das medidas à posição de operador de IC	"A REFER tem Planos de Emergência para toda a Rede Ferroviária, nomeadamente Planos de emergência gerais e Planos de Emergência para pontos específicos. A escolha da especificidade desses pontos tem em conta não a possível quantidade de ocorrências mas sim o impacto que essas mesmas ocorrências têm/podem ter."	"As medidas de segurança são adequadas através da constante evolução técnica, quer dos equipamentos quer dos diversos materiais que incorporam as infraestruturas do ML, bem como existe uma constante análise aos fatores de risco externos de modo a garantir de modo permanente a segurança dos trabalhadores e dos passageiros. Os regulamentos e os planos de segurança que construímos são revistos regularmente para manter os procedimentos de emergência atualizados."	"Antes de começarem os trabalhos na CNPC nós já tínhamos diversos planos de segurança, como os de emergência ou de continuidade de negócio. Nesse sentido não se introduziram medidas novas porque as que já tínhamos se adequavam. Na verdade nós somos regidos por regulamentos muito mais exigentes em termos de medidas a adotar do que o Decreto de Lei 62 impõe."	"Todas as infraestruturas críticas da APL estão devidamente identificada e estão cobertas por medidas preventivas de proteção aprovadas pela ACPTMP – AUTORIDADE COMPETENTE PARA A PROTECÇÃO DO TRANSPORTE MARÍTIMO E DOS PORTOS;"	"A ANPC fez um estudo apurado sobre os planos mais variados que conseguiam encontrar fizeram uma checklist de conteúdo que esses planos deviam ter na parte safety e security e deram aos operadores para eles terem uma chave guia. Depois eles não precisam de fazer planos novos, vão sim aproveitar os muitos planos que eles já têm. Vão la buscar grande parte da informação para completarem estes planos do operador"	"De acordo com as disposições legais constantes da legislação em vigor nesta matéria (DL 62/2011, de 9 de Maio). A EDP Produção e a EDP Distribuição produziram e entregaram à ANPC – Autoridade Nacional de Proteção Civil e GCSI – Gabinete Coordenador de Segurança Interna, os seus PSO – Planos de Segurança do Operador.

A relação que os Operadores estabelecem com a Autoridade Nacional de Proteção Civil foi também alvo de análise. De acordo com as respostas registadas na Tabela 5, existem três Operadores – REFER, EDP e ANA – que atualmente estabelecem contacto com a ANPC no que concerne à proteção das IC,

participando em reuniões periódicas e procurando cumprir os objetivos do projeto atualmente desenvolvido. Já de acordo com o Porto de Lisboa e o Metro de Lisboa, o contacto estabelecido nestas matérias ocorreu apenas com o anterior Conselho Nacional de Planeamento Civil de Emergência, extinto em 2012, não tendo sofrido desenvolvimentos ou atualizações com a integração das suas competências, na atual ANPC. No entanto, a ANPC indica que está a trabalhar com todos os Operadores notificados e que se encontra a desenvolver o programa em coordenação com os mesmos.

Tabela 5 Envolvimento no trabalho desenvolvido pela ANPC sobre as IC

	REFER	**METRO DE LISBOA**	**ANA – AEROPORTOS DE PORTUGAL**	**PORTO DE LISBOA**	**ANPC**	**EDP**
Envolvimento no trabalho desenvolvido pela ANPC sobre as IC	"Sim o contacto é permanente (com a ANPC). A REFER tem a sua presença semanal no Briefing da ANPC. Relativamente sobre a segurança das Infraestruturas, há um contacto, porque nós somos operador. .	O ML colaborou no trabalho desenvolvido pelo grupo de trabalho criado no âmbito do CNPCE (…) procedeu à identificação e classificação das Infraestruturas nacionais; tentou arrancar com a elaboração do Programa Nacional para a Proteção de Infraestruturas Críticas e elaborou uma definição de infraestrutura (…). Até à presente data ainda não houve contato (com a ANPC). O contato anterior foi com o CNPCE."	Sim a ANA está. "Primeiro na identificação das IC e das ICE onde fizemos propostas."	"Sim. Mas Ainda sem conhecimento do desenvolvimento do programa (…) Sem conhecimento de existência de contacto."	"Nos estamos a trabalhar com os nossos operadores todos que notificamos. Depois do trabalho de identificação de IC feito, há um ofício que sai, para notificar o operador."	"Sim."

Em relação à concretização das fases do projeto de Proteção das IC, através da Tabela 6 identificamos uma clara disparidade nas fases em que cada Operador de IC se encontra.

No caso da REFER e do Porto de Lisboa, a identificação das suas IC ainda se encontra em progresso. Foi entregue por ambas uma primeira proposta que incluía a lista detalhada de todas as infraestruturas passiveis de serem designadas como ICN. Porém, no caso da REFER, esse número obrigou a uma reformulação

dos critérios utilizados, encontrando-se a empresa atualmente a redefinir os mesmos. No caso do Metro de Lisboa, apesar de ter sido elaborada uma lista com as ICN identificadas pelo Operador, esse trabalho não foi prosseguido, estando por essa razão de momento estagnado. Quanto à EDP, revela já ter entregue os PSO, encontrando-se neste momento a aguardar os comentários aos mesmos. A ANA é o único Operador que revela estar a desenvolver este projeto em conjunto com a ANPC, encontrando-se de momento a elaborar o conjunto de documentos necessários à adequação ao enquadramento jurídico. Tal como a ANPC reconhece, o plano traçado não está a ter uma aplicação uniforme, sucedendo assim uma disparidade muito definida entre posições tomadas pelos Operadores e orientações dadas pela ANPC. No entanto, decompondo as respostas dos dois intervenientes no projeto, parece clara a existência de uma disparidade entre a evolução do projeto por parte da ANPC, que descreve a existência de um contacto permanente com os Operadores, e por outro lado, o contacto pouco próximo e desacompanhado indicado pelas empresas entrevistadas.

Tabela 6 Atual fase do projeto

	REFER	**METRO DE LISBOA**	**ANA – AEROPORTOS DE PORTUGAL**	**PORTO DE LISBOA**	**ANPC**	**EDP**
Em que fase do projeto se encontra	"(…)atualmente ainda estamos na fase de identificar as IC." A ANPC pediu-nos um levantamento das IC com base nas possíveis IC (pontes e túneis) com mais de X metros mas a lista era tão extensa que o levantamento não foi aprovado e voltou para nós para reformularmos os critérios utilizados (como o numero de metros). Atualmente ainda estamos em conversações para definir esse critério."	"O ML indicou um conjunto das estações de interface e de correspondência com outros modos de transporte para serem considerados como ICN. (…) Não foi recebida informação do resultado final de avaliação pelo CNPCE (entretanto extinto)."	"Definimos quantas e quais as IC. Agora no que se refere à elaboração do conjunto de documentos que nos pediram e que ainda estamos em conversações com a Dr.ª Isabel Pais. Para nós têm sido positivos e enriquecedores."		"Para já nem todos os sectores, subsectores, operadores estão a trabalhar ao mesmo, é normal. (…) Há sectores que nos já estamos claramente na terceira fase. Depois há sectores que nos já estamos claramente na terceira fase."	"Aguardam os comentários aos PSO entregues."

Os simulacros são um importante instrumento no que à aplicação das medidas de segurança se refere. Neste sentido, todos os Operadores participantes indicam realizar exercícios capazes de simular situações de incidentes, permitindo dessa forma avaliar a eficácia dos planos por si desenvolvidos. A distinção assenta,

por sua vez, na periodicidade com que são realizados, no número de exercícios efetuados e no contexto em que são aplicados.

Em relação aos tipos de exercícios realizados, a REFER e a ANA executam dois tipos distintos. No caso da REFER, um deles é capaz de simular uma situação de impacto para circulação, como é exemplo a queda de uma árvore na linha ferroviária, e outra na qual esse impacto não se verifique. Por seu lado, a ANA desenvolve um grande exercício, no qual são acionados todos os meios previstos nos planos, e outro que não implica o acionamento desses mesmos meios mas no qual são revistos todos os procedimentos a tomar por cada área responsável.

Quanto à periodicidade com que são realizados, verifica-se uma grande disparidade entre os Operadores. A REFER desenvolve oito simulacros por ano (metade com impacto na circulação e outra metade sem impacto), enquanto o Porto de Lisboa desenvolve trimestralmente exercícios nos terminais operacionais. No caso do Metro de Lisboa são realizados simulacros de dois em dois anos nos seus edifícios e anualmente em duas das estações da cidade. A EDP realiza, no mínimo um simulacro por ano nas UO dos Centros Produtores e anualmente nos Centros de Comando e Condução da Rede de Distribuição de Eletricidade. Por último, a ANA desenvolve um grande exercício bianual e outro anualmente que não envolve acionamento dos meios.

Tabela 7 Realização de Simulacros

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Realização de Simulacros	"A REFER tem dois tipos de simulacros: Um que simule uma situação com impacto para a circulação e outro que simule uma que não o tenha. São feitos em média 4 por ano de cada situação. Estes simulacros são articulados com a Proteção Civil"	"Realizamos simulacros de dois em dois anos nos edifícios e anualmente em 2 estações/zonas da rede."	"Fazemos no mínimo um grande exercício de dois em dois anos, no qual acionamos todos os meios que seriam necessários para a situação. Integramos os trabalhadores no mesmo exercício. Fazemos também um outro anualmente sem ativar meios. (…) Nós chamamos uma Table Top, em que cada um leva os documentos e os procedimentos pelos quais é responsável e mediante um cenário, cada um diz o que teria de fazer."	"Realizam-se simulacros de proteção nos terminais operacionais, geridos pela APL com carácter trimestral"		"As UO Centros Produtores realizam no mínimo 1 (um) simulacro /ano. Nas instalações Críticas da Distribuição realizam-se simulacros anuais nos Centros de Comando e Condução da Rede de Distribuição de Eletricidade.

Nas entrevistas realizadas, foi questionado se os Operadores equacionavam poder sofrer problemas operacionais considerados graves, capazes de originar uma interrupção dos processos críticos até 24h. Apurou-se que atualmente todos os Operadores consideram esse cenário possível, apesar de a EDP sustentar que tal só será possível para algumas das suas instalações individualmente e não para o total da operação. Segundo este Operador é altamente improvável que todas as suas instalações produtivas críticas sejam simultaneamente afetadas, pondo dessa forma em causa a normal atividade da companhia. O Metro de Lisboa e a ANA apontam as causas de origem natural, como as mais prováveis a gerarem um cenário como esse, dando os exemplos da ocorrência de um sismo e, no caso da ANA, de um acontecimento como o registado em Maio de 2010 na Islândia, com a emissão vulcânica de uma nuvem de cinzas. Se no caso da REFER foram os acidentes ferroviários que foram mencionados, no Porto de Lisboa foi atribuída especial preocupação aos conflitos sociais, como são exemplos as greves e o absentismo. Na EDP Distribuição esse risco pode concretizar-se, embora normalmente circunscrito a áreas afetadas, e em resultado de eventos de grande dimensão ligados a riscos naturais, como um sismo de grande intensidade, riscos tecnológicos, como, por exemplo um incêndio de grandes proporções e ações sociais, como seria o caso de um ato terrorista ou de sabotagem. No que concerne ao setor dos transportes, este tópico sugere uma reflexão sobre as alternativas à circulação em caso de perturbação do seu normal funcionamento. No caso específico da REFER e do Metro de Lisboa, tendo em conta que operam sob carris, o desafio em encontrar caminhos alternativos é exigente e, por vezes, tal qual se encontra citado na Tabela 8, inexequível.

Segundo a visão da ANPC, atualmente os Operadores estão preparados para responder a um cenário anómalo. Essa preparação baseia-se, em grande parte, nas medidas presentes anteriormente a serem consideradas IC. No entanto, ressalva que, perante uma grande catástrofe, pode ser facilmente espectável que muitas dessas mesmas infraestruturas não se mostrem resilientes.

Tabela 8 Possibilidade de sofrer problemas operacionais, interrompendo os processos de negócio críticos até 24h

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Possibilidade de sofrer problemas operacionais, capazes de originar uma interrupção dos processos de negócio críticos até 24h	"Sim, isso pode acontecer, bastando para isso haver um incidente grave em alguma das linhas ferroviárias em que não haja alternativas de linhas complementares. Exemplo disso foi o acidente de Alfarelos/Granja que decorreu em Janeiro passado e impediu a utilização daquela linha"	"Atualmente só pensamos poder sofrer repercussões como as referidas se resultantes de risco natural de intensidade muito grave. O motivo que consideramos será o sismo."	"Sim, principalmente como resultado de fenómenos meteorológicos. A maioria deles em 24h conseguem-se resolver. Há sempre possibilidade de alocar os voos para outros Aeroportos da ANA. A única forma de deixar de existir possibilidade de operar é se algo o impedir No espaço aéreo, como foi o caso da nuvem de cinzas vulcânicas provocada pelo vulcão na Islândia"	"Sim. Como principais motivos de preocupação temos os conflitos sociais."	"No global (os Operadores) têm uma resposta preparada. Eles antes de iniciarmos o plano já tinham muitos planos feitos. Planos de Continuidade de Negócio, Planos de Emergência Interna, Planos de Segurança, Planos contra incêndios, Planos de segurança física. Agora num caso de grande catástrofe é claro que as coisas podem falhar. Para coisas menos catastróficas eles estão preparados."	"Na EDP Produção para algumas das suas instalações individualmente, negativa para o total da operação, uma vez que é altamente improvável que todas as suas instalações produtivas críticas sejam simultaneamente afetadas, pondo dessa forma em causa a normal atividade da companhia. Na EDP Distribuição esse risco pode concretizar-se, embora normalmente circunscrito a áreas afetadas, e em resultado de eventos de grande dimensão ligados a riscos naturais (eg. sismo de grande intensidade), riscos tecnológicos (eg. incêndio de grandes proporções) e ações sociais (eg. Sabotagem/terrorismo)

Foi possível apurar que à exceção do Porto de Lisboa, os restantes quatro Operadores desenvolveram Programas de Continuidade de Negócio, tal como se encontra indicado na Tabela 9. Estes Planos resultam da colaboração de várias áreas da organização. No caso da REFER, o plano encontra-se sob a alçada da Direção de Operações, enquanto no caso da ANA apenas é atribuído de forma formal a sua responsabilidade à área Técnica, indicando no entanto que a sua aplicação é partilhada por todos os membros do grupo multissectorial criado para o desenvolver. No que respeita à EDP, tanto o setor da Produção como o da Distribuição possuem áreas de gestão vocacionadas para o efeito.

Tabela 9 Programa de Continuidade de Negócio

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Programa de Continuidade de Negócio	"Não esta diretamente sobre a alçada da Direção de Segurança. Esse plano é feito pela área da segurança contudo é disponibilizado à Direção de Operações."	"Sim. Em função da situação ocorrida, temos procedimentos definidos para a reposição do serviço, eventualmente em parte da rede ou da linha, até à resolução completa do problema."	"A ANA tem um, onde são incluídos todos os Aeroportos. Foi desenvolvido por um grupo de trabalho de diferentes áreas de atividade. O responsável formal é o Diretor da área Técnica."			"A EDP Produção e a EDP Distribuição têm áreas de gestão vocacionadas para o efeito."

Os Planos de Emergência são instrumentos orientadores que se tornam fundamentais na resposta aos incidentes. Questionados sobre a frequência e a eficiência da sua aplicação, apurou-se que, à exceção do Porto de Lisboa, os Operadores acionam os seus PE com frequência, nomeadamente a REFER que em média o aciona uma vez por semana, e a ANA que o faz uma vez por mês (Tabela 10). Ainda segundo a ANA, grande parte das vezes não se torna necessário concretizá-lo, contudo os meios necessitam de estar no terreno caso a ameaça se concretize. Quanto á EDP, este Operador considera que a avaliação feita em cada situação permite melhorar continuamente a resiliência da Empresa, e isso passa também por formação, sensibilização e preparação para situações de stress, em toda a organização.

Tabela 10 Aplicação do Plano de Emergência

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Aplicação do Plano de Emergência; Resultados	"Os Planos de emergência principalmente são ativados com bastante frequência. A média é mesmo um por semana. Há é planos especiais para linhas especiais. Resposta que temos dado mostra que a empresa é resiliente."	"Sim. Decorrente de questão natural ou tecnológica. Correu de acordo com o plano de emergência definido (…) Aplicámos por exemplo na sequência de acidente ocorrido num término da linha vermelha. "	"Sim, várias vezes. Com muita frequência mesmo. Pelo menos uma vez por mês. Felizmente a maior parte das vezes não é necessário concretiza-lo mas temos de o acionar e os meios têm de estar preparados para intervir, se necessário."	"Não."		"A avaliação feita em cada situação permite melhorar continuamente a resiliência da Empresa, e isso passa também por formação, sensibilização e preparação para situações de stress, em toda a organização."

Por fim, tentou apurar-se a perceção que os responsáveis de segurança têm sobre a consciência coletiva dos colaboradores da empresa em questões de segurança.

De acordo com as respostas registadas na Tabela 11, se aplicarmos a fórmula da média aritmética, verificamos que o resultado é positivo (7,6), contribuindo no entanto três dos Operadores (Metro de Lisboa, EDP e ANA) para o aumento deste resultado, tendo atribuído 8, 9 e 9 pontos respetivamente. Segundo estes três Operadores, a segurança é sobejamente valorizada no interior da organização, sendo que no caso particular da ANA existe um programa de formação na vertente da segurança com frequência obrigatória para todos os colaboradores que integram a empresa. Por outro lado, a EDP vai mais longe afirmando que se poderia situar até num nível acima de 9, devido ao trabalho feito ao longo de dezenas de anos em termos de formação e cultura de segurança, aliado à consciência técnico-profissional que os próprios colaboradores têm acerca da importância das atividades que desenvolvem (produção e distribuição de eletricidade) e das consequências para o País no caso de existir uma falha grave no desenvolvimento dessas atividades. Nos casos da REFER e do Porto de Lisboa registam-se os valores mais baixos, 7 e 5 pontos respetivamente, resultantes, segundo os mesmos, da baixa cultura de segurança presente na organização.

Tabela 11 consciência coletiva dos colaboradores da empresa em questões de segurança

	REFER	METRO DE LISBOA	ANA – AEROPORTOS DE PORTUGAL	PORTO DE LISBOA	ANPC	EDP
Numa escala de 0 – 10 a consciência coletiva dos colaboradores da empresa em questões de segurança	"Diria 7, porque é positiva mas a segurança é um pouco secundarizada, é muitas vezes vista como um impedimento."	"8 – A cultura de segurança é intrínseca ao ML"	"9 – Só não digo 10 porque é sempre possível melhorar, contudo cada colaborador quando inicia atividades com a ANA tem de ter um mínimo de formação de 4h com teste avaliativo no final. A Segurança é uma bandeira e pilar na empresa. Exemplo disso é a recetividade dos colaboradores em participarem nos simulacros."	"Pontuamos com 5"		"Situa-se certamente num nível muito elevado (acima de 9). Por um trabalho feito ao longo de dezenas de anos em termos de formação e cultura de segurança, aliado à consciência técnico-profissional que os próprios colaboradores têm acerca da importância das atividades que desenvolvem (produção e distribuição de eletricidade) e das consequências para o País no caso de existir uma falha grave no desenvolvimento dessas atividades."

De acordo com os operadores entrevistados, apesar da perceção da posição que ocupam enquanto operadores de IC, o trabalho desenvolvido pelas respetivas áreas de segurança, não têm um foco especial nesse âmbito, havendo mesmo bastantes requisitos impostos pela Lei base que não são cumpridos. No que à resposta aos incidentes se refere, a maioria dos operadores apesar de se considerarem resilientes consideram a possibilidade de poder sofrer um incidente de tal ordem capaz de afetar a continuidade das funções essenciais para a empresa operar.

Ao nível da própria integração nos trabalhos desenvolvidos pela ANPC, apesar de todos os operadores indicarem já terem anteriormente mantido contacto com a ANPC nesse âmbito, revelam-se pouco familiarizados com os trabalhos que foram e estão atualmente a ser desenvolvidos. Neste sentido verificou-se uma falta de concordância entre a informação prestada pela ANPC e a prestada pelos operadores participantes no presente trabalho, já que durante a entrevista a ANPC indicou que a boa comunicação e relação de proximidade existente entre ambas as partes, no âmbito da segurança dasIC, era um pilar que sempre existiu e continua a ser essencial em todo o processo.

Conclusões e Contributos para Investigação Futura

Na base do funcionamento da sociedade encontram-se os serviços considerados básicos, suportados por infraestruturas Críticas. Entende-se, neste sentido, que qualquer disfunção que possa colocar em risco o funcionamento normal destas Infraestruturas tem de ser encarada como um problema nacional, com necessidade de resolução integrada entre as entidades públicas e privadas (caso se tratem de Operadores privados). A importância que é automaticamente aprovisionada a estas infraestruturas, bem como a complexidade resultante da sua ligação em rede, torna a segurança das Infraestruturas Críticas, uma matéria cada vez mais atual e progressivamente mais debatida.

Neste contributo procurou-se estabelecer um retrato atual da segurança das infraestruturas críticas no panorama nacional, bem como, entender em que moldes Portugal se insere a nível europeu. Nesse sentido, foi necessário contextualizar historicamente, geograficamente e juridicamente, através da análise específica de três diplomas. Este enquadramento permitiu construir um trabalho de investigação, sustentado conjuntamente na análise bibliográfica e na informação veiculada pelas entrevistas realizadas. Procurou-se, por último, entender a influência que o trabalho desenvolvido pela ANPC, no âmbito da proteção das IC, tem nos diversos Operadores analisados e a adaptação que os demais têm procurado fazer à posição de Operadores de IC.

Portugal, apesar de ter vindo a abrir progressivamente espaço para a reflexão das temáticas da segurança, ainda apresenta um baixo envolvimento nestas questões, facto que decorre de razões históricas, sociopolíticas, mas sobretudo culturais. Muito por termos a ideia de sermos um “País de brandos

costumes" identifica-se em geral – nas empresas, organização estadual e consciência coletiva - uma subvalorização da segurança.

A cultura gerada em torno desta temática, não só a nível nacional como também europeu, não tem na sua génese um forte caráter legislativo. Este trabalho não procura defender a criação de uma legislação rígida, mas sim a necessidade de incluir um caráter mais regulador e exigente, já que medidas não vinculativas, não permitem definir funções e atribuir responsabilidades. Para tal, deveria ser designado um órgão que garantisse, não só o acompanhamento, como também regulasse a execução das medidas previstas pelos respetivos diplomas. O órgão em causa deveria ser transversal a todos os setores de atividade. Por essa razão, consideramos que poderia ser integrado no Gabinete Nacional de Segurança, ficando desta feita na dependência do Primeiro-Ministro.

Como podemos verificar pelas respostas obtidas nas entrevistas realizadas, há operadores, pertencentes a um dos setores que serve de base ao Decreto-Lei n.º62/2011, de 9 de Maio, que não se encontram integrados nos trabalhos desenvolvidos pela ANPC. Verificou-se, de igual forma que apenas a ANA detém um agente de ligação de segurança em cada Aeroporto, nos termos do n.º 3 do artigo 11.º do diploma referido anteriormente. Atualmente e de acordo com os dados recolhidos, os Planos de Segurança dos Operadores não são elaborados nos moldes do que está plasmado na atual legislação nacional. São, no entanto, utilizados para o mesmo fim, os Planos de Emergência e os demais planos de segurança concebidos anteriormente a esta lei. Segundo a ANPC, nos parâmetros atuais a forma mais viável de promover o cumprimento das normas por parte dos Operadores é pela via da sensibilização, já que não existe a função fiscalizadora.

A potencial designação de uma infraestrutura como crítica é transversal a qualquer setor de atividade. Encontramos, também por essa razão, IC com especificidades totalmente distintas entre si. Compreendendo desta forma o atual contexto, torna-se crucial atender às características próprias de cada setor de atividade e de cada infraestrutura especificamente. A complexidade que cada

Infraestrutura Crítica comporta, carece de um estudo de todo o sistema na qual se insere e sob o qual se desenvolve. Não se procura uma individualização mas sim por outro lado, a perceção da distinta realidade em que se tem de pensar a segurança.

Portugal deveria implementar um Programa de Proteção das Infraestruturas Críticas, tal qual recomenda a Diretiva 2008/114/CE do Conselho, de 8 de Dezembro. Este programa deveria assentar numa análise recorrente das vulnerabilidades, das possíveis ameaças e dos riscos associados. Incluiria um estudo a nível macro e micro, focando-se, numa primeira instância, nas características comuns entre IC, e seguidamente, ajustada às características mais específicas de cada setor de atividade Seria de incluir nesta fase, o conhecimento claro das relações de interdependência que as IC geram entre si.

Porém, a segurança das IC não pode ser apenas da responsabilidade do Estado, havendo necessidade de um estreita cooperação entre o setor público e privado. A complexidade gerada em torno da segurança deste tipo de infraestruturas pode motivar investimentos avultados. Contudo, sendo a maioria dos operadores pertencentes ao setor privado, o critério financeiro tende a priorizar-se. Assim, o trabalho do departamento de segurança no seio da organização é mostrar aos decisores como é que os investimentos feitos em segurança conseguem materializar-se, ainda que indiretamente, em ganhos para a empresa. Neste ponto, o Estado pode ter um papel fundamental, não só no sentido de sensibiliza-los para esta matéria, mas também num trabalho de cooperação, procurando encontrar as melhores práticas.

Face aos objetivos propostos, considera-se que os mesmos foram alcançados. Foi possível responder às duas perguntas de partida, sendo possível entender, primeiro lugar, que as três fases definidas no projeto para Proteção das Infraestruturas Críticas pela ANPC resultaram de uma divisão feita de forma puramente académica. Deste facto resulta, que atualmente se esteja a trabalhar em simultâneo em todas as fases, isto é, dependendo do nível de integração do

operador no projeto, assim se desenvolvem os procedimentos e aquilo que lhe é solicitado. Por outro lado, verificou-se que a adequação dos Operadores às normas vigentes carece de maior atenção, quer por parte da ANPC, quer por parte das organizações que gerem as ditas IC. Verificou-se uma fraca adaptação e sensibilização para a adequação de medidas específicas à posição ocupada como Operador de IC, prova disso é inexistência de um plano de segurança do operador e de um agente de ligação de segurança que cumpra o requisito de diretor de segurança, plasmados respetivamente no artigo 10º e 11º do Decreto-Lei n.º 62/2011, de 9 de Maio.

Apesar de atualmente as Infraestruturas Críticas de Informação não se encontrarem previstas pelo Decreto-Lei que estabelece os procedimentos de identificação e de proteção das IC, há uma integração natural das Tecnologias de Informação e Comunicação nas funções vitais da sociedade.

Cada vez mais se terá de pensar a segurança das Infraestruturas Críticas, indissociável da segurança das informações. Esta simultaneidade está atualmente a ser promovida através de conversações entre a ANPC e o Gabinete Nacional de Cibersegurança. Será necessário portanto, começar a explorar esta área com mais ímpeto.

Bibliografia

Homeland Security of United States. (26 de Junho de 2014). *Critical Infrastructure Security; Homeland Security*. Obtido de Homeland Security: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Alberto, C. (Janeiro de 2011). Infra-estruturas críticas nacionais: proteção, prevenção e resposta a ameaças. *Revista Segurança e Defesa nº16*, pp. 14-22.

Almeida, A. O. (2011). *Metodologia Multicritério de Identificação e Priorização de Infra-Estruturas Críticas.* Lisboa: Instituto Superior Técnico .

Amador, J. (2010). *PRODUÇÃO E CONSUMO DE ENERGIA EM PORTUGAL:FACTOS ESTILIZADOS.* Lisboa: Banco de Portugal.

ANTROP. (2002). *Linhas de orientação estratégica para o sector de transportes colectivos rodoviários de passageiros. Caracterização do sector e aspectos particulares.* Edições ANTROP.

Arruda, P. A. (13 de Junho de 2014). *ciclo de estudos estratégicos*. Obtido de eceme: http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XCEE/paper/viewFile/10/17

Austen, D. G., & Nathan, E. B. (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *Critical Infrastructure protection*, 31-50.

Autoridade Nacional de Proteção Civil. (13 de Junho de 2014). *Infraestruturas Críticas*. Obtido de Autoridade Nacional de Proteção Civil: http://www.proteccaocivil.pt/RISCOSVULNERABILIDADES/Pages/InfraestruturasCriticas.aspx

BSI. (2006). *Business continuity management. Code of practice.* Londres: British Standards Institution.

Business Continuity Institute. (14 de Junho de 2014). *What is BC?* Obtido de Business Continuity Institute: http://www.thebci.org/index.php/resources/what-is-business-continuity

Cardona, O. D. (2006): "A System of Indicators for Disaster Risk Management in the Americas - Measuring Vulnerability to Natural Hazards", in Birkmann, United Nations University Press,189-209.

Carreño M.L., Cardona O.D., Barbat A.H., (2007): "Urban Seismic Risk Evaluation: A Holistic Approach", Natural Hazards, Vol.40(1):pp:137-172.

Chertoff, M. (2009). National Infrastructure Protection Plan. *Department of Homeland Security*.

Clemente, D. (2013). *Cyber Security and Global Interdependence: What is Critical?* London: Chatham House.

CNPIC. (30 de Outubro de 2014). *CNPIC - ¿Qué es el CNPIC?* Obtido de Centro Nacional para la Protección de las Infraestruturas Criticas: http://www.cnpic.es/Preguntas_Frecuentes/Que_es_el_CNPIC/index.html

Comissão das Comunidades Europeias. (20 de 10 de 2004). Protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo. *Comunicação da Comissão ao Conselho*.

COMISSÃO DAS COMUNIDADES EUROPEIAS. (2005). *LIVRO VERDE RELATIVO A UM PROGRAMA EUROPEU DE PROTECÇÃO DAS INFRAESTRUTURAS CRÍTICAS.* Bruxelas.

Costa, C. A., Angulo-Meza, L., & Oliveira, M. D. (2013). *O método Macneth e aplicação no Brasil.* Rio de Janeiro: Rio Climate Challenge.

Costa, C. B., Angulo-Meza, L., & Oliveira, M. D. (21 de Outubro de 2013). *O MÉTODO MACBETH E APLICAÇÃO NO BRASIL*. Obtido de Universidade Federal Fluminence: https://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.uff.br%2Fengevista%2Fseer%2Findex.php%2Fengevista%2Farticle%2Fdownload%2F484%2F217&ei=8qAVVIWLJJHgaOTCguAG&usg=AFQjCNFMMaRnOMdFyZSBUsiPImsQEBj

European Commission. (2013). *Attitudes of Europeans Towards Urban Mobility.* Bruxelas: European Commission.

Federal Republic of Germany. (2009). *National Strategy for Critical Infrastruture Protection.* Berlim: Bundesministerium des Innern.

Freire, V. (Maio de 2012). Cibersegurança e ciberdefesa: a inevitabilidade de adoção de uma estratégia nacional. *Revista Segurança e Defesa*, pp. 53-63.

Hämmerli, B., & Renda, A. (2010). *Protecting Critical Infrastructure in the EU*.

Centre for European Policy Studies.

Homeland Security. (2013). *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*. Homeland Security.

Homeland Security. (26 de Junho de 2014). *Chemical Security Laws and Regulations; Homeland Security*. Obtido de Homeland Security: http://www.gpo.gov/fdsys/pkg/BILLS-109hr5441enr/pdf/BILLS-109hr5441enr.pdf

Houghton Mifflin Company. (2000). *The American Heritage Dictionary* . Boston: Houghton Mifflin Company.

Instituto Nacional de Estatística. (2008). *Indústria e Energia em Portugal.* Lisboa: Instituto Nacional de Estatistica Statitics Portugal.

Instituto Nacional de Estatistica. (2013). *Estatística dos Transportes e Comunicações 2012.* Lisboa: INE.

International Organization of Standards. (2012). *ISO 22301*. Geneva: International Organization of Standards.

Lacomblez, L. C. (2006). Mudanças no sector dos transportes em Portugal: que caminhos para a actividade de serviço público e para a preservação do interesse geral? Em Laboreal, *Volume II* (pp. 26-37). Porto: Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto.

Manzini, E. J. (2012). Uso da Entrevista em Dissertações e Teses produzidas em um programa de Pós-Graduação em Educação. *Revista Percurso - NEMO*, pp. 149-171.

Monteiro, M. H. (2007). Infra-estruturas Críticas e Vulnerabilidades Sociais: o paradigma do mundo mais desenvolvido. *Planeamento Civil de Emergência*, pp. 9-13.

Natário, R. M., & Nunes, P. F. (2014). Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. Em *Revista Militar* (pp. 249-286). Lisboa: Revista Militar.

Oliveira, M. (2008). *Acesso Distribuido e Interoperável à Informação Geográfica para Suporte à Gestão de Infra-estruturas Críticas.* Braga: Universidade do Minho.

Pais, I. (21 de Novembro de 2014). A Segurança das Infraestruturas crítica em Portugal. (M. B. Oliveira, Entrevistador)

Pais, I., & Candeias, J. (2000). O significado da transposição para Portugal da diretiva europeia. Para proteção das infra-estruturas criticas. *Revista Planeamento Civil de Emergência nº22*, pp. 20-22.

Pais, I., & Sá, F. M. (2009). Paradigmas da Proteção de Infra-estruturas Críticas e o Estado da Arte em Portugal. *Planeamento Civil de Emergência nº 21*, pp. 36-42.

Pais, I., Sá, F. d., & Gomes, H. (2007). Proteção de Infra-Estruturas Críticas - A Cooperação Publico-Privada. Em C. Soares, A. Teixeira, & P. Antão, *Riscos Públicos e Industriais* (pp. 65-84). Lisboa: Edições Salamandra.

Pais, I., Sá, F. M., Lopes, M., & Oliveira, C. S. (2011). Infraestruturascríticas: Propostas para a redução do risco sísmico. *Planeamento civil de emergência nº23*, pp. 16-21.

Rede Energética Nacional. (30 de Setembro de 2014). *O que fazemos*. Obtido de REN: http://www.ren.pt/o_que_fazemos/eletricidade/o_setor_eletrico/

Rocha, M. T. (24 de Maio de 2014). *Investigação*. Obtido de Miguel Trindade Rocha web site: http://www.migueltrindaderocha.com/investiga%C3%A7%C3%A3o-1/

S.Eckert. (2005). Protecting Critical Infrastructure: The Role of the Private Sector. Em P. Dombrowski, *Guns and Butter: The Political Economy of International Security.* Colorado: Lynne Rienner Publishers.

Secrétariat Général de la Défense et de la Sécurité Nationale. (10 de Outubro de 2014). *L'organisation*. Obtido de SGDSN: http://www.sgdsn.gouv.fr/site_rubrique70.html

Tabansky, L. (2011). *Critical Infrastructure Protection against Cyber Threats.* Militaru and Strategic Affairs.

Tissot Éditions. (30 de Outubro de 2014). *Définition Plan particulier de sécurité et de protection de la santé* . Obtido de Editions Tissot: http://www.editions-tissot.fr/droit-travail/dictionnaire-droit-travail-st-definition.aspx?idDef=1407&definition=Plan+particulier+de+s%C3%A9curit%C3%A9+et+de+protection+de+la+sant%C3%A9+%28PPSPS%29

Wenk, D. (2013). Turning Business Continuity Into A Competitive Advantage. *Disaster Recovery*.

Legislação Complementar

- (COM (2004) 702 final) Comunicação da Comissão ao Conselho e ao Parlamento Europeu – Proteção das Infra-estruturas críticas no âmbito da luta contra o terrorismo, datado de 20.10.2004;
- (COM (2005) 576 final) Livro Verde relativo a Um Programa Europeu de Proteção das Infra-estruturas Críticas, apresentado pela Comissão, datado de 17.11.2005;
- (COM(2006) 786 final) Comunicação da Comissão relativa a um Programa Europeu de Proteção das Infra-estruturas Críticas, datado de 12.12.2006;
- Deliberação do Conselho de Ministros n.º 51-DB/2004, de 18 de Março, designou o Conselho Nacional de Planeamento Civil de Emergência (CNPCE) como entidade coordenadora de um grupo de trabalho para a elaboração da Carta Nacional de Pontos Sensíveis;
- Diretiva 2008/114/CE do Conselho de 8 de Dezembro de 2008, relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção;

- Decreto-Lei n.º 62/2011, de 9 de Maio, estabelece os procedimentos de identificação e de protecção das infra -estruturas essenciais para a saúde, a segurança e o bem -estar económico e socia da sociedade nos sectores da energia e transportes;

Anexos

Entrevista Drª Isabel Pais

O presente questionário será efetuado no âmbito da conclusão do Mestrado em Direito e Segurança a realizar-se na Faculdade de Direito da Universidade Nova de Lisboa. O objetivo é analisar a adequação dos operadores das Infraestruturas Críticas à realidade nacional. Entrevista efetuada à Responsável pela Área da Proteção de Infraestruturas Críticas e Ponto de Contacto Nacional junto da UE.

1 **E: O que é o plano de ação para a proteção das IC iniciado pela ANPC?**

I.: A designação de Programa Nacional vem do Programa Europeu para a proteção das infraestruturas criticas, em que a Comissão Europeia recomendou (porque o que ela pode fazer é recomendar) aos Estados que elaborassem os seus programas nacionais de IC mas na verdade acaba por ser um nome, porque o que interessa neste momento é que os Estados Membros trabalhem nesta área, desenvolvam ações para a identificação das IC e a redução do risco que correm e a maior capacidade de recuperarem em caso de sofrerem uma disfunção, ou seja aumentarem a resiliência, mais do que chamar um nome. O nome em si nós chamamos inicialmente, mas depois como em termos de legislação foi proposto haver uma legislação que cobrisse esse nome mas como depois não houve por falta de vontade política (enfim, também se legisla mal no pais, nós sabemos isso) e portanto não esta na lei. E como não esta na Lei, nos decidimos para não haver problemas…quer dizer no fundo ninguém contesta qualquer nome mas pode haver algum purista e acabamos por neste momento deixar cair o nome mas estão todos a trabalhar nesta área.
Estive ontem em Bruxelas e la estavam os 28 Estados Membros com os seus representantes a trabalhar na área e a discutir. O tema continua bastante aceso.

2 **E: Os trabalhos foram divididos em três partes. Em que fase nos encontramos?**
I: Essa divisão em fases já tem uns anos e foi feita de uma forma académica. Porque quando se aborda um assunto a tendência é dividir em fase para ter qualquer coisa que nos oriente. Hoje temos as 3 fases a decorrer ao mesmo tempo e é o que vai acontecer. Para já nem todos os setores, subsetores, operadores estão a trabalhar ao mesmo, é normal. Depois há setores que nos já estamos claramente na terceira fase…a fase 2 é a principal, é a faze onde está o principal trabalho, que é reduzir o risco e planear melhor para aumentar a resiliência e que no fundo nunca se deixa de estar, porque está-se sempre a trabalhar. E depois à que

implementar as medidas e quem o faz são os operadores das infraestruturas, nunca é o Estado, porque eles é que são os responsáveis pela sua segurança. E há operadores que já identificaram uma serie de carências que têm e já estão a fazer os seus planos de investimento, na sequencia deste trabalho, para nos próximos anos colmatarem e melhorarem cada vez mais essas falhas. Outros estão a fazer os planos, a estudar os riscos. Noutros setores ainda estamos a identificar as infraestruturas. Estamos por exemplo a começar agora em cheio no setor das comunicações, tecnologias de informação e comunicação, Internet, ciber. Transportes e Energia são as infraestruturas que representam mais de 50% das infraestruturas estruturas em Portugal.

Já há um levantamento das infraestruturas todas! Mas agora até tem de ser atualizado e tem de sofrer a segunda e terceira fase da identificação, porque uma coisa é meter os dados todos que nos temos e recolhemos num modelo de classificação e isso tem como out put as listas das IC, o que no fundo faz uma ordenação das ICs, classifica-as e depois é falar com os operadores e com os respetivos reguladores para naqueles resultados que saem do modelo eles poderem analisar e ver se aquilo faz algum sentido para eles (e normalmente faz porque os dados até são dados por eles) e há uma serie de perguntas que nos fazemos nos inquéritos do levantamento que são eles que respondem. Mas de qualquer forma eles vão fazer a análise daqueles resultados, fazem a sua alteração (exemplo este elemento já não existe ect, abriu outra e fechou aquela).

Estamos a trabalhar nas energias e nos transportes mesmo assim não estão todas ao mesmo ritmo, é impossível, são 160 ICs. E por outro lado estamos a começar a rever todo o setor das chamadas TIC que digamos é o 3º grande setor e temos outros a seguir. Há medida que vamos andando também vamos ficando mais experientes e andamos mais depressa, mas quando começarmos a chegar ao fim deste os planos estão sempre a precisar de se atualizar e isto não para nunca. Portanto a implementação já é uma fase e a monitorização já é coisa própria dos operadores mas eles depois fazem-na de acordo com o seu próprio ritmo e de acordo com a sua própria disponibilidade financeira.

As 3 fases vão estar sempre a correr ao mesmo tempo.

3 E: Como se procedeu em cada fase?

I:Há varias formas que pode acontecer, na primeira o operador pode chamar a atenção - atenção a esta que esta abriu ou abriu aquela ali ao lado portanto aquela deixou de ser critica. Depois é obrigatório por lei cada ano haver uma revisão dos planos dos operadores, está na lei. Ora quando fizerem essa revisão, de certeza que tem de rever a lista das infraestruturas críticas e aí é uma maneira de manter as coisas atualizadas… porque se não é terrível manter a base de dados.

4 E: Quais os maiores riscos que considera que Portugal corre no que se refere à proteção das IC?

I: Há vários tipos de riscos. A maior parte das IC são fábricas ou equipamentos desse tipo e os riscos que acabam por ser os mais frequentes são incêndios, as explosões, aquelas coisas que as fabricas se deparam. Mas não é bem isso que nos preocupa. Aliás pode preocupar se for por exemplo a emissão de uma matéria perigosa para a atmosfera ao abrigo da Diretiva SEVESO (diretiva que armazenam e manuseiam matérias perigosas). Agora, há alguns riscos que são mais abrangentes e mais preocupantes e o principal dentro dos riscos naturais é o risco sísmico porque é o único que é capaz de destruir varias coisas ao mesmo tempo e com uma abrangência enorme, Normalmente os outros são mais localizados. Depois há os ataques terroristas e etc., em que não somos muitos conhecidos por sermos um grande alvo e quem tem de se preocupar mais com isso e o SIS e o Sistema de Segurança Interna porque isso é uma parte mais security. E há uma dentro destas que é a cibersegurança. Os ataques via virtuais são das maiores ameaças agora porque de facto podem fazer muito mal sem se dar por ela, não se ouve e não se vêm e de repente são os sistemas de controlo todos invadidos e a partir daí as consequências security e safty são incontáveis. A proteção civil, inicialmente não tinha essa competência na sua origem porque na sua origem estaria a análise da ameaça que é feita pelo SIS. Agora as consequências a nível safty são imensas, porque se as infraestruturas entrarem em disfunção e não houver eletricidade, não houverem comunicações e não houverem uma serie de coisas que decorrem disso há afetação de pessoas e bens e aí esta já a Proteção Civil. Há vários exercícios que se está agora a fazer na área da cibersegurança mesmo a nível internacional NATO, como europeu, na União Europeia como já a nível nacional (centro nacional de cibersegurança). O próprio centro tem a proteção das IC na sua competência e agora temos de nos articular para melhor protegermos as IC.

5 E: Com a transferência do CNPCE para a ANPC houve algo que tenha mudado na estratégia adotada, nos objetivos definidos ou mesmo no ritmo de trabalho?

I: O CNPCE tinha 10 comissões de planeamento civil de emergência que eram coordenadas pelo respetivo ministério que tutela agregavam entidades públicas e privadas dentro do setor que se referiam, por exemplo a comissão de planeamento civil de energia era coordenada pela direção geral de geologia e geologia e tinha todos os operadores públicos e privados nesta área, o da saúde ect… Elas faziam vários trabalhos não só este, faziam tudo ao nível do planeamento civil de

emergência. Mas nos tentamos refazer um bocado o esquema sema a construção das comissões. A ANPC tem dado algum apoio porque esta área requer investimento de dinheiro, tempo, recursos de maneira que não se sentido alterações negativas.

6 **E: Em que consistiu o trabalho de sensibilização da necessidade de adequação das medidas de segurança ao Decreto-Lei n.º62/2011, de 9 de Maio?**

I: Nos estamos a trabalhar com os nossos operadores todos que notificamos. Depois do trabalho de identificação de IC feito, há um ofício que sai, para notificar o operador. Essa notificação indica a lista de IC que o operador tem e como tal indica que este tem de desenvolver para elas os planos de segurança do operador e tem de ter um agente de ligação de segurança. A partir daí em articulação com o Secretario geral de segurança interna para a parte security e a ANPC para a parte safety começam a trabalhar com os operadores para fazerem o seu plano de segurança. A ANPC fizeram um estudo apurado sobre os planos mais variados que conseguiam encontrar fizeram uma check list de conteúdo que esses planos deviam ter na parte safty e security e deram aos operadores para eles terem uma chave guia e depois eles não precisam de fazer planos novos, vão sim aproveitar os muitos planos que eles já têm. Vão la buscar grande parte da informação para completarem estes planos do operador e é aí que vão detetar grande parte das carências que têm e é nessas carências que vão trabalhar. Ou trabalham ou identificam uma serie de carências e falhas e fazem os planos de investimento e começam já a trabalhar.
Quanto ao agente de ligação de segurança, como tem de ter o curso de Diretor de Segurança a empresa tem de disponibilizar o trabalhador durante um semestre. E nesse sentido a ANPC está a tentar negociar com a Secretaria de Segurança Interna prazos para formarem os trabalhadores.

7. **E: Como tem sido/foi a aceitação dos Operadores?**

I: Muito boa. A ANPC não quer aplicar taxas para a revisão dos planos porque acreditam que é dissuasor. Em todo o mundo com a nossa cultura a visão tem sido de não ir muito pela parte legislativa porque quanto mais leis há mais maneiras se arranjam de não as cumprir. Vamos pela sensibilização. Por isso por vezes diz-se, esta lei é muito precária, mas eu antes quero a lei precária do que leis muito rígidas (não quer dizer que ela não devesse em muitos aspetos ser alterada). Porque essas Leis muito rígidas, espartilham-nos de tal maneira que nós não conseguimos fazer nada e de maneira que utilizamos muito a via da

sensibilização. Porque se não for da vontade de eles próprios não se consegue nada. Contudo talvez se venham a criar taxas (é preciso falar com a Secretaria da Segurança Interna e isso precisa de ser baseado numa portaria) para os não cumpridores.

8. **E: Há fiscalização aos operadores para verificar o cumprimento das normas instituídas? A quem compete essa função?**
   I: Não há nem está prevista. Porque não temos funções de fiscalizadoras. Mas então como funciona: Os Operadores também sabem que se um dia acontecer alguma coisa e se eles declararem nos planos que têm determinadas coisas que depois não têm podem deixar de ser certificados e por isso de perder a capacidade de funcionar e por exemplo os próprios seguros não lhs pagam. Essas taxas para os nãos cumpridores baseava-se apenas em não entregarem os planos a tempo, porque o que acabam por ter la dentro já é a parte, porque não esta prevista uma equipa para fazer a verificação. O que dizem é, se não tiverem os seus planos de segurança dos operadores arriscam-se, caso algo a aconteça a ficar sem a capacidade de trabalhar.

9. **E: Se acontecesse agora um sismo de grande magnitude (entre 7- 8 na escala de Ritcher) – Considera que algumas das atividades criticas de Portugal poderiam ficar comprometidas? Quais?**
   I: Bastantes! As IC mais modernas já são mais resistentes, porque tem uma nova construção etc. O problema é que quando pensamos em infraestruturas não podemos só pensar em termos de colapso físico, porque as edificações podem ficar compostamente em pé mas os equipamentos dentro por razoes as vezes de nada podem por em causa o funcionamento. E aí não há legislação! Aí é que há uma grande dose de sensibilização junto dos operadores para que evitem que determinadas coisas. Aqui é importante formar e sensibilizar os operadores e aí é um trabalho que se tem de fazer muito com a parte técnica e científica.
   Neste momento, com as interdependências que as IC têm de certeza que seria uma afetação muito razoável.

10. **E: Ainda equacionando o cenário anterior, quais os setores que considera poderem ser mais afetados?**
    I: Podem ficar todos afetados mas o setor da energia tinha mais probabilidade. A energia é a Mae de todos os setores. Logo que falte a energia começa a faltar quase tudo. As comunicações estão muito ligadas à energia e a energia às comunicações. Olhem as Smartgreeds da eletricidade, estão todas ligadas em comunicações.

11. **E: Considera que os Operadores das IC em Portugal são resilientes?**
    I: No global têm uma resposta preparada. Eles antes de iniciarmos o plano eles já tinham muitos planos feitos. Planos de Continuidade de Negócio, Planos de Emergência Interna, Planos de Segurança, Planos contra incêndios, Planos de segurança física. Agora num caso de grande catástrofe é claro que as coisas podem falhar. Agora para coisas menos catastróficas eles estão preparados. É que eles também têm regulamentos internacionais muito rígidos. Agora com os planos de segurança dos operadores ainda ficam mais preparados. No fundo a resiliência constrói-se todos os dias.

12. **E:Considera que de um modo geral Portugal se encontra mais resiliente desde que o Plano de ação para a proteção das IC se iniciou?**

    I: O que se conseguiu foi um maior alerta, uma maior sensibilização, ganhar o respeito deles, a consideração pela relação e pela maneira como se aproximam de nós. No fundo isto é um negócio de relação de confiança porque se não for assim não há mais resultado. Eles estão muito mais alerta.

13. **E: Que objetivos existem para o futuro?**
    I: Continuar o caminho. Avançar para mais setores, como a água, saúde. E claro continuarmos atentos às novas ameaças que vão surgindo e continuarmos a trabalhar de uma forma ativa. Com a experiencia conseguimos ir incorporando o novo know how e ir andando mais rápido. Até resultante da cooperação de outras instituições nacionais e internacionais mesmo. Porque há fóruns internacionais, no âmbito da EU e da NATO no âmbito das IC. Nós não estamos sozinhos.

14. **E: Quais as maiores dificuldades para Portugal criar um Programa Nacional de Proteção das IC?**
    I: A área legislativa precisa de ser francamente melhorada. Precisa e ser organizado um programa. Nós se conhecermos as componentes do programa, tanto as que estão na Lei como as que estão associadas mas que não estão. Agora, precisava de um corpo legislativo bem construído e uma coordenação bem definida. Não dividida em entidades (porque esta Lei divide as responsabilidades em 3 entidades diferentes: O CNPCE; a ANPC e o Sistema de segurança interna na pessoa do Secretário Geral do SSI). Neste momento, como a ANPC herdou as funções do antigo conselho nacional ficaram 2 mas na verdade há na parte dos planos de segurança do operador a primazia do Secretário-geral do Sistema de Segurança interna, porque os valida mas de resto há responsabilidades divididas e o que deveria haver era um organismo que assumisse a coordenação…há países

que têm isso, são gabinetes próximos do primeiro-ministro para poderem ter poderes transversais aos setores todos. Não deviam de estar dentro de um ministério como aqui está mas devia estar acima dos ministérios. Se houvesse um órgão deste tipo…há varias soluções, há quem o tenha na Administração Interna, outros na Justiça. Mas a mais correta como tem a França é num gabinete de Segurança e Defesa que está na Presidência do Conselho de ministro deles, ou seja perto do Primeiro-ministro (no caso deles, do presidente) o que faz todo o sentido para ser transversal aos setores. O CNPCE pertencia ao conselho de ministro pertencia ao Conselho de ministros mas as funções do conselho estavam delegadas no ministro da defesa e por isso é que se diz que aquilo era Ministério da Defesa mas não era, daí ter-se conseguido ter as comissões de planeamento de emergência que eram transversais aos setores todos pela posição que o conselho tinha. Em termos de posicionamento este tipo de trabalhos deveriam ser transversais. Felizmente o facto de estar na Administração Interna, nunca tivemos problemas, até porque a ANPC já tem muitos representantes no que diz respeito ao Socorro e portanto não temos tido problemas mas se vier algum ministro mais embirrante podemos vir a ter prolemas.

15. **E: Atualmente apenas os setores da Energia e dos transportes servem de base tanto à Diretiva 2008/114/CE do conselho de 8 de Dezembro de 2008 como ao Decreto-Lei n.º 62/2011, de 9 de Maio. Há algum trabalho que esteja a ser realizado especificamente junto destes operadores?**

I: Essa parte da Diretiva não é coisa que funcione muito bem, não funciona porque a maior parte das ICE não são Infraestruturas que se possam designar pelo procedimento que está no Decreto-Lei, nomeadamente quando diz "negociação entre os Estados". Quando falamos de certas IC como o exemplo da Região de Informação de voo de Lisboa e de Sta. Maria, cobrem uma parte do Atlântico, ou seja, elas quando se afetadas não afetam o nosso pais e os vizinhos, não! Afetam a Europa inteira, o Brasil, a América Latina, para Africa porque eles têm de obrigatoriamente de passar por ali. Ora este tipo de infraestruturas têm de ser obrigatoriamente designadas pela União Europeia porque é uma IC Europeia por natureza! Isto já evoluiu um bocado, agora já há um Staff Working Paper em que se está a caminhar claramente para um entendimento de que há ICE que não podem ser designadas por este processo, portanto aí tem de ser a Comissão Europeia que tem de designa-las e trabalhar para a sua segurança que já esta alias a ser feito neste momento. Elas têm então de ser designadas nacionais e posteriormente têm de passar para Europeias por natureza, já não é bem este de ter de negociar com o vizinho, isto não faz sentido. Nós temos IC que são ICE e como a Diretiva não dá resposta a este tipo de informações (Portugal tem uma

região de informação de voo enorme, das maiores em todo o mundo, tal como tem uma zona Costeira onde passam os navios de todo o mundo enorme. É pela própria situação geográfica e portanto essas IC são Europeias por natureza. Temos outra que é pelo Sistema Galileu que é um sistema de comunicação Europeia e é Europeu por natureza. Ele pertence à Comissão Europeia e tem estações em terra e nós temos uma nos Açores. Naturalmente pela legislação do Sistema galileu é imediatamente uma ICE por natureza e então vieram pedir-nos para que ela fosse designada por IC nacional, aí até foi ao contrária. Isto acaba por ser intermutável e o conceito é um bocadinho diferente do que aquele que a Diretiva preconizava e que se mostrou um bocadinho inapropriado. Mas todos os anos temos de informar na mesma, que elas existem, quantas são e as que são Europeias por natureza.

Entrevista Engenehiro Edgar Carvalho

O presente questionário será efetuado no âmbito da conclusão do Mestrado em Direito e Segurança a realizar-se na Faculdade de Direito da Universidade Nova de Lisboa. O objetivo é analisar a adequação dos operadores das Infraestruturas Críticas à realidade nacional. Entrevista efetuada ao responsável de segurança da ANA – Aeroportos de Portugal.

E: Entrevistador;
R: Responsável de Segurança.

1. **E: No panorama organizacional da empresa onde se insere a direção de segurança do Aeroporto de Lisboa?**
   R: Nós temos uma unidade geral de segurança da ANA inserida na Direção Técnica Aeroportuária. A Direção responde diretamente à Administração da Ana. No entanto a área de segurança responde ao Diretor da Direção Técnica Aeroportuária. Contudo, apesar da área da segurança não ser independente, não sinto que não tenha uma voz ativa e que esteja distanciada da Administração. É muito regular fazer reuniões ou trabalhar em projetos com o Vogal da Administração.
   No caso do Aeroporto de Lisboa este tem um Gestor de segurança que é responsável pela segurança do Aeroporto que responde diretamente à Administração do Aeroporto.

1. **E: O Aeroporto de Lisboa é um operador de infraestrutura crítica em Portugal. Como adequa as medidas de segurança a essa posição específica?**

   R: Antes de começarem os trabalhos na CNPC nós já tínhamos diversos planos de segurança, como os de emergência ou de continuidade de negócio. Por isso não se introduziram medidas novas porque as que já tínhamos se adequavam. Na verdade nós somos regidos por regulamentos muito mais exigentes em termos de medidas a adotar do que o Decreto de Lei 62 impõe.

2. **E: O Aeroporto de Lisboa esta a ser parte envolvida no projeto para a proteção das infraestruturas críticas que esta a ser realizado pela Autoridade Nacional da Proteção Civil?**

R: Não especificamente o Aeroporto de Lisboa mas sim a ANA. Primeiro na identificação das IC e das ICE onde fizemos propostas e definimos quantas e quais as IC e agora no que se refere à elaboração do conjunto de documentos que nos pediram e que ainda estamos em conversações com a Dr.ª Isabel Pais.

3. **E: E como avalia os desenvolvimentos desse trabalho?**
   R: Para nós têm sido positivos e enriquecedores. Temos aprendido mutuamente e temos (a meu ver) alcançado os objectivos.

4. **Existe contacto entre o Aeroporto de Lisboa e a ANPC no âmbito do programa para a proteção das Infraestruturas críticas?**
   R: Em várias matérias. Mas sim, como lhe disse anteriormente, estamos em conversações com eles para acertar os pontos…por acaso na anterior reunião não fui eu que estive presente, mas sempre que posso também vou.

5. **E: Considera que a empresa cumpre todos os parâmetros do Decreto-lei n.º 62/2011 de 9 de Maio, que estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais?**

   R: Penso que sim. Temos tudo, nomeadamente os relatórios e temos no Aeroporto de Lisboa um gestor de segurança com o curso de Diretor de Segurança.

6. **E: O Aeroporto de Lisboa tem ou já iniciou um programa de Gestão de Continuidade de Negócio?**
   R: A ANA tem um, onde são incluídos todos os Aeroportos. Foi desenvolvido por um grupo de trabalho de diferentes áreas de atividade. Reuniram-se diferentes elementos e cada um deu o seu contributo, claro que no final alguém fica responsável. O responsável formal é o Diretor da área Técnica, portanto da área onde se insere o departamento de segurança.

7. **E: Com que frequência se realizam simulacros e como se distribuem pelas infraestruturas que gerem?**
   R: Fazemos no mínimo um grande exercício de dois em dois anos, no qual acionamos todos os meios que seriam necessários para a situação e integramos os trabalhadores no mesmo exercício. Fazemos também um outro anualmente sem ativar meios. Este funciona com os intervenientes da empresa. Não são acionados meios e o que acontece é o que nós chamamos uma Table Top, em que cada um leva os documentos e os procedimentos pelos quais é responsável e mediante um cenário, cada um diz o que teria de fazer.

8. **E: Quais as principais ameaças identificadas à segurança do Aeroporto de Lisboa?**

   R: Para além dos fenómenos meteorológicos há também cada vez mais premente a situação do ciberterrorismo que pode causar problemas na navegação aérea por exemplo. Outra ameaça para o nosso negócio a possibilidade da falência de um cliente. Imaginando que a TAP agora falia….

2. **E: Quais os maiores riscos que a empresa foi alvo nos últimos 3 anos?**

   R: Principalmente fenómenos meteorológicos como o caso do Vulcão da Islândia este ano, ou o tornado que levou o teto do aeroporto de Faro em 2011.

9. **E: Nos últimos 3 anos sofreu algum incidente em que tenha sido necessário aplicar o plano de emergência?**
   R: Sim, várias vezes. Com muita frequência mesmo. Pelo menos uma vez por mês. Felizmente a maior parte das vezes não é necessário concretiza-lo mas temos de o acionar e os meios têm de estar preparados para intervir, se necessário. Posso dizer-lhe que mesmo não saindo nas noticias, é com bastante frequência que aqui mesmo no Aeroporto de Lisboa, os meios de emergência sejam chamados e fiquem preparados para intervir. Por exemplo pode haver uma discussão dentro do Avião em que pode mesmo chegar a haver agressões e aí temos de estar preparados para reagir em terra. Muitas das vezes nem entram de facto em acção.

10. **E: A resposta dada mostrou que a empresa era resiliente?**
    R: Sim, até agora sempre reagimos muito bem.

11. **E: No que se refere à vigilância física existe subcontratação de serviços externos?**
    R: Toda a vigilância de segurança que é feita no recinto do Aeroporto é efetuada pelos agentes de Policia de segurança pública, que são os únicos autorizados para o mesmo. Contudo temos empresas subcontratadas nos Aeroportos. No entanto essas empresas de segurança privada são prestadores de serviços e os seus colaboradores fazem Controlo de Acessos e rastreio de pessoas e bens.
    E: Porquê essa opção?

R: A ANA já tem tantos colaboradores, que essa área seria tão específica que teria de haver um investimento muito grande da nossa parte...formação especializada por exemplo. Isso tem elevados custos.

12. **E: Considera poder sofrer problemas operacionais graves capazes de originar uma interrupção dos processos de negócio críticos até 24h?**
    R: Sim, principalmente como resultado de fenómenos meteorológicos.
    E: **Quais os principais motivos?**
    R: A maioria deles em 24h conseguem-se resolver. A ANA tem uma vantagem, é que se acontecer alguma coisa, há sempre possibilidade de alocar os voos para outros Aeroportos da ANA. A única forma de deixar de existir possibilidade de operar é se algo o impedir no espaço aéreo. Por isso sim pode acontecer, sem qualquer dúvida.

13. **Numa escala de 0 – 10 em que zero é muto reduzida e 10 muito elevada, como considera ser a consciência coletiva dos colaboradores da empresa em questões de segurança?**
    R: Nove!
    E: Porquê?
    R: Só não digo 10 porque é sempre possível melhorar, contudo cada colaborador quando inicia atividades com a ANA tem de ter um mínimo de formação de 4h com teste avaliativo no final. A Segurança é uma bandeira e pilar na empresa. Exemplo disso é a recetividade dos colaboradores em participarem nos simulacros. Quando fazemos, juntam-se mesmo muitos trabalhadores para participarem livremente.

Entrevista Dr. Rui Costa Fonte

O presente questionário será efetuado no âmbito da conclusão do Mestrado em Direito e Segurança a realizar-se na Faculdade de Direito da Universidade Nova de Lisboa. O objetivo é analisar a adequação dos operadores das Infraestruturas Críticas à realidade nacional. Entrevista efetuada ao responsável de segurança da REFER – Rede Ferroviária Nacional,

E: Entrevistador;
R: Responsável de Segurança.

3. **E: No panorama organizacional da empresa onde se insere a direção de segurança da REFER?**
   R: A direção de segurança responde diretamente ao conselho de administração e estamos hierarquicamente equiparados ao departamento…por exemplo… de economia e finanças. Quanto à organização dentro da própria direção de segurança, tem três departamentos, o de Pessoas e Bens, o Ferroviário e o de Gestão de Segurança e Emergência (que tem também a parte de segurança no trabalho).
   E: Qual a sua opinião sobre a posição?
   Só vê vejo vantagens. Principalmente duas: a de manter um relacionamento próximo com o conselho e também poder tratar os assuntos diretamente com quem decide.

14. **E: A REFER é um operador de infraestrutura crítica em Portugal. Como adequa as medidas de segurança a essa posição específica?**

    R: A REFER tem Planos de Emergência para toda a Rede Ferroviária, nomeadamente Planos de emergência gerais e Planos de Emergência para pontos específicos. A escolha da especificidade desses pontos tem em conta não a possível quantidade de ocorrências mas sim o impacto que essas mesmas ocorrências têm/podem ter.

15. **E: A REFER esta a ser parte envolvida no projeto para a proteção das infraestruturas críticas que esta a ser realizado pela Autoridade Nacional da Proteção Civil?**

    R: Há um contacto mas atualmente ainda estamos na fase de identificar as IC. A ANPC pediu-nos um levantamento das IC com base nas possíveis IC (pontes e tuneis) com mais de X metros mas a lista era tão extensa que o levantamento não foi aprovado e voltou para nós para reformularmos os critérios

utilizados…como o número de metros (risos). Atualmente ainda estamos em conversações para definir esse critério. Também considero que não estamos adaptados plenamente à legislação vigente, nomeadamente um Diretor de segurança por área etc.

16. **E: E como avalia os desenvolvimentos desse trabalho?**
R: Não sei muito bem. No nosso caso foi como disse, tem havido conversações mas ainda estamos na primeira fase.

17. **E: Considera que a empresa cumpre todos os parâmetros do Decreto-lei n.º 62/2011 de 9 de Maio, que estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais?**

R: …ter um diretor de segurança por exemplo?

E: Sim, estes artigos aqui (é mostrada a legislação)

R: No caso do diretor de segurança não. De facto não. Haver um plano também não porque nós já temos os nossos que cumprem os requisitos. Contudo no final das conversações devem ter de se fazer adaptações sim.

18. **E: A REFER tem ou já iniciou um programa de Gestão de Continuidade de Negócio?**
R: Sim também temos. Não esta diretamente sobre a alçada da Direção de Segurança. Foi feito pela nossa área da segurança mas foi disponibilizado à Direção de Operações e são eles que o aplicam.
E: Já sentiram necessidade de o aplicar muitas vezes?
R: O plano de Continuidade de Negócio não propriamente muitas vezes mas os planos de emergência são ativados com bastante frequência. Ainda ontem tivemos o caso de uma senhora na linha de Cascais em que se teve de ativar o plano específico desse troço.
E: Como se processa quando há um incidente?
R: O plano de emergência é acionado e a situação é resolvida. O relatório de emergência é feito sobre tudo o que se passou e depois é avaliado pela Direção de segurança, a fim de verificar se foi tudo cumprido e se há algo que se deva mudar no próprio Plano.

19. **E: Com que frequência se realizam simulacros e como se distribuem pelas infraestruturas que gerem?**
R: A REFER tem dois tipos de simulacros: um que simule uma situação com impacto para a circulação e outro que não tenha esse impacto. São feitos em

média 4 por ano de cada situação. Estes simulacros, por exemplo, são articulados com a Proteção Civil, nomeadamente com os CDOS.

20. **E: Quais as principais ameaças identificadas à segurança da REFER?**

R: Os fenómenos de ordem natural, quedas por causa de tempestades ou inundações, os roubos.

4. **E: Quais os maiores riscos que a empresa foi alvo nos últimos 3 anos?**

R: Tem muitas vezes a ver com fatores de ordem natural, como queda de objetos nas linhas. Também o roubo de equipamento fundamental à circulação aconteceu muito. O roubo de metais aconteceu muito nos últimos anos, e isso pode parar por completo as operações num troço. Ah! As quedas nas linhas é claro.

E: Nos últimos 3 anos sofreu algum incidente em que tenha sido necessário aplicar o plano de emergência?

R: Sim, claro, bastantes. Exemplo disso foi o acidente de Alfarelos/Granja que decorreu em Janeiro passado e impediu a utilização daquela linha, não sei se recorda mas foram semanas sem transporte.

21. **E: A resposta dada mostrou que a empresa era resiliente?**
R: Sim, de um modo geral cumprimos os objetivos traçados.

22. **E: No que se refere à vigilância física existe subcontratação de serviços externos?**
R: Sim temos, até nos próprios comboios.
E: Porque tomaram essa opção?
R: As razões são em primeiro lugar a económica, já que acaba por compensar contratar e também razões de ordem prática, já que os serviços de autoproteção se tornam legalmente muito morosos. Não é fácil ter serviços de autoproteção.

23. **E: Considera poder sofrer problemas operacionais graves capazes de originar uma interrupção dos processos de negócio críticos até 24h?**
R: Sim a qualquer momento! Isso pode acontecer, bastando para isso haver um incidente grave em alguma das linhas ferroviárias em que não haja alternativas de linhas complementares. Exemplo disso foi o acidente de Alfarelos/Granja que decorreu em Janeiro passado e impediu a utilização daquela linha durante muito tempo.

24. **Numa escala de 0 – 10 em que zero é muto reduzida e 10 muito elevada, como considera ser a consciência coletiva dos colaboradores da empresa em questões de segurança?**

R: Eu diria 7...é positiva mas a segurança é um pouco secundarizada. É muitas vezes vista como um impedimento.