



# **Boas Práticas de Resiliência de Infraestruturas Críticas**

## **SETOR PRIVADO E SETOR EMPRESARIAL DO ESTADO**

Atividade do Grupo de Trabalho 4 – Triênio 2015-2017

“Promover as boas práticas de redução do risco e aumento da resiliência das infraestruturas críticas no setor privado e Setor empresarial do Estado”

**2017**

## FICHA TÉCNICA

### Promoção

Plataforma Nacional de Redução de Risco de Catástrofes

### Coordenação

CGD – Caixa Geral de Depósitos S.A.

### Redação

ANPC – Autoridade Nacional de Proteção Civil

CGD – Caixa Geral de Depósitos S.A.

EDP – Energias de Portugal

NOS Comunicações, S.A.

### Participação

DGAE – Direção Geral de Atividades Económicas

EDP Distribuição – Energia, S.A.

EPAL – Empresa Portuguesa de Águas Livres, S.A.

GALP Energia

IP – Infraestruturas de Portugal, S.A.

Siemens, S.A.

SONAE

TAP – Air Portugal

### Revisão

Grupo de Trabalho 4 (2015/2017) da Plataforma Nacional para a Redução do Risco de Catástrofes

### Paginação

ANPC – Autoridade Nacional de Proteção Civil

### Disponibilidade em PDF

[www.prociv.pt](http://www.prociv.pt) / [www.pnrrc.pt](http://www.pnrrc.pt)

### Data de publicação

13 de outubro de 2017

### ISBN

978-989-8343-21-5

### **Grupo de Trabalho 4 (2015/2017) – Plataforma Nacional para a Redução do Risco de Catástrofes Setor Privado e Setor Empresarial do Estado – Resiliência de infraestruturas críticas**

Caixa Geral de Depósitos S. A. – Gabinete de Prevenção e Segurança (José Manuel Gonçalves) – Coordenação

Autoridade Nacional de Proteção Civil – Direção de Serviços de Riscos e Planeamento (Isabel Pais)

Direção-Geral de Atividades Económicas – (Francisco Escoval e Armando Mendes)

EDP – Energias de Portugal – Direção de Gestão de Risco (Ricardo Messias)

EDP Distribuição – Direção de Ambiente, Sustentabilidade e Continuidade de Negócio (Inês Cândido da Silva e Maria Luísa Pestana)

EPAL – Empresa Portuguesa de Águas Livres, S. A. – (Alexandra Cristóvão e Marco Santos)

GALP – Direção de Ambiente Qualidade Segurança e Sustentabilidade (José Almeida)

Infraestruturas de Portugal – Departamento de Safety (Rui Nunes da Silva)

NOS Comunicações, S. A. – Direção de Auditoria e Gestão de Risco (Pedro Gomes da Silva)

Siemens S. A. – (Luís Mourato e Rui Gramunha)

SONAE – Direção de Gestão de Risco (José Luís Amorim)

TAP Air Portugal – Direção de Serviços Gerais e Gestão de Instalações e Direção de Auditoria (Ana Malheiro, Fátima Geada, Maria João Calha e Andreia Afonso)

## NOTA DE ABERTURA

O Quadro de Sendai para a Redução do Risco de Catástrofes 2015-2030, aprovado na 3.<sup>a</sup> Conferência Mundial de Redução das Catástrofes, em março de 2015, reforça nos seus objetivos fundamentais a necessidade do envolvimento de todos os setores da sociedade no esforço de criação de estratégias e desenvolvimento de ações com vista à gestão e à redução do risco de catástrofes, tarefa que envolve inúmeros stakeholders, de forma transversal à sociedade, incluindo naturalmente o setor privado.

Este Quadro preconiza de forma muito clara a necessidade de organização desses stakeholders em plataformas nacionais, por forma a constituírem-se como agentes facilitadores de partilha de informação e de experiências, promovendo o trabalho conjunto.

Neste contexto, no âmbito da Plataforma Nacional para a Redução do Risco de Catástrofes, foi criado um Grupo de Trabalho constituído maioritariamente por entidades pertencentes ao Setor Privado e Setor Empresarial do Estado, com o objetivo de proceder a uma recolha e partilha de boas práticas de resiliência das suas infraestruturas.

Tal iniciativa teve por base a constatação do papel incontornável que o setor privado tem vindo a assumir na construção de sociedades progressivamente mais resilientes e sustentáveis. Com efeito, é o setor privado que detém e ou opera uma larga maioria das infraestruturas que asseguram o fornecimento de bens e serviços vitais para o normal funcionamento das comunidades que servem.

O resultado da reflexão, pesquisa e análise efetuada no Grupo de Trabalho traduz-se no manual que agora se apresenta e que procura reunir um conjunto de recomendações e boas práticas no âmbito da resiliência organizacional, ilustradas por casos de estudo que exemplificam a implementação de medidas de reforço da resiliência por parte dos operadores. A adoção destas boas práticas contribuirá para que as organizações reforcem a sua capacidade de permanecer em funcionamento em situações de acidente grave ou catástrofe, aumentando assim o grau de fiabilidade dos serviços que prestam.

Este manual deve servir, por isso, de estímulo à criação de uma cultura nacional de resiliência, ampliando a perspetiva tradicionalmente existente, assente na continuidade de negócio, para uma visão mais abrangente, centrada na manutenção da prestação de serviços vitais à sociedade e na redução dos impactos de uma disrupção. Até porque, muitas vezes, basta a implementação de programas e procedimentos simples para incrementar consideravelmente a resiliência.

**José Oliveira**  
**Coordenador**  
**Subcomissão da Plataforma Nacional para a Redução**  
**do Risco de Catástrofes**

## NOTA PRÉVIA

O aumento do risco de catástrofe que a Humanidade enfrenta hoje, seja ele de origem natural ou induzido pela atividade humana, coloca um conjunto de desafios que podem ser comparados à escalada de uma montanha

Em Portugal, e sob a égide das Nações Unidas, foi lançada pela Autoridade Nacional de Proteção Civil, a Plataforma Nacional para a Redução do Risco de Catástrofe, com o objetivo de promover o aumento da resiliência das comunidades face à ocorrência de catástrofes, cada vez mais intensas e em maior número. A Plataforma Nacional para a Redução do Risco de Catástrofes congrega várias entidades públicas e privadas e foi dividida em vários grupos de trabalho.

No caso do Grupo de Trabalho 4 “– Promover as boas práticas de redução do risco e aumento da resiliência das infraestruturas críticas no sector privado e sector empresarial do estado”, estabeleceu-se como objetivo principal, a produção de um manual que compile um conjunto de contribuições visando alcançar o aumento da resiliência das infraestruturas críticas do sector privado e empresarial do Estado.

Com este objetivo, reuniu-se um grupo de empresas públicas e privadas, dos mais diversos setores, que partilharam conhecimentos e experiências enriquecedoras, que se encontram agora vertidas no presente manual.

É nossa convicção que as ideias agora transmitidas irão proporcionar ferramentas, processos e sugestões, úteis para empresas e para os cidadãos, tornando-os mais resilientes em eventos futuros.

Em face do exposto, esta Coordenação, expressa o reconhecido agradecimento à entidade promotora e às entidades que nos acompanharam na redação, bem como a todos os participantes, pelo trabalho e disponibilidade demonstrados ao longo destes últimos três anos.

**A Coordenação**  
**Caixa Geral de Depósitos**



## ENQUADRAMENTO

Com o objetivo de promover o aumento da resiliência das comunidades face à ocorrência de catástrofes, as Nações Unidas aprovaram, em 2000, a Estratégia Internacional para a Redução de Catástrofes (International Strategy for Disaster Reduction – ISDR). Desde 2001 que a ANPC (à data, o Serviço Nacional de Proteção Civil) está designada como Ponto Focal Nacional para efeitos da ISDR.

Na sequência da implementação da referida Estratégia, foi aprovado em 2005 o Quadro de Ação de Hyogo 2005-2015 e, em 2015, foi adotado o Quadro de Ação de Sendai para a Redução do Risco de Catástrofes 2015-2030.

O Quadro de Ação de Sendai introduz uma evolução, comparativamente ao seu antecessor Quadro de Hyogo, do conceito de gestão de catástrofes para o conceito de gestão do risco de catástrofes. A tónica incide na ótica preventiva, dando especial importância ao envolvimento dos múltiplos agentes da sociedade civil, públicos e privados, na mitigação do risco, redução das vulnerabilidades e aumento da resiliência das comunidades, através da adoção de boas práticas de carácter multirrisco e multisetorial.

O principal objetivo definido para o atual ciclo de 15 anos é “prevenir novos riscos e reduzir os riscos de catástrofes existentes, através da implementação de medidas integradas e inclusivas ao nível económico, estrutural, legal, social, da saúde, cultural, educacional, ambiental, tecnológico, político e institucional, para prevenção e redução da exposição a perigos e vulnerabilidades a catástrofes, aumentar o grau de preparação para resposta e recuperação, e assim reforçar a resiliência”.

Uma das sete metas definidas no Quadro de Ação de Sendai consiste em “Reduzir os danos em infraestruturas críticas e a afetação dos serviços básicos e essenciais”. Como a grande maioria destas infraestruturas que fornecem os serviços fundamentais para o funcionamento das sociedades pertencem ao setor privado, é indispensável o envolvimento aprofundado e participação ativa daquele no aumento da resiliência das suas infraestruturas.

Para tal, os diferentes stakeholders devem trabalhar em conjunto, criando oportunidades de cooperação, juntando sinergias, partilhando informação e divulgando-a, tanto quanto possível. A atividade empresarial deve integrar a redução do risco nas suas práticas normais de gestão, com vista ao aumento da sua resiliência organizacional, onde é fundamental a sensibilização e informação de todos os direta ou indiretamente envolvidos.

O Quadro de Ação de Sendai destaca, entre outros temas, o reforço da importância das Plataformas Nacionais para a redução do risco de catástrofes, pois constituem fóruns privilegiados de envolvimento dos stakeholders públicos e privados relevantes para a redução do risco e aumento da resiliência das sociedades.

Portugal designou formalmente, em 31 de maio de 2010, a Comissão Nacional de Proteção Civil como a Plataforma Nacional para a Redução do Risco de Catástrofes (PNRRC). Foi ainda constituída a Subcomissão da PNRRC, coordenada pela ANPC, que congrega mais de 40 entidades públicas e privadas, da administração pública, municípios, empresas privadas, universidades e ordens profissionais, com o objetivo de promover a implementação do Plano de Atividades da Plataforma, que se desenvolvem atualmente em 6 grupos de trabalho.

O Grupo de Trabalho 4 (GT4) da Plataforma reúne 11 entidades pertencentes maioritariamente ao setor privado e empresarial do Estado. Tem como objetivo central “Promover as boas práticas de redução do risco e aumento da resiliência das infraestruturas críticas no sector privado e setor empresarial do estado”, contribuindo para a redução do risco de catástrofes de origem natural ou induzidas pela atividade humana, sendo que os efeitos de indisponibilidade do serviço que tais situações podem gerar são independentes das causas que lhes deram origem.

Para o efeito, durante o triénio 2015-2017, procedeu-se a uma recolha das principais boas práticas nas empresas envolvidas no GT que os operadores das referidas infraestruturas críticas deverão adotar em termos de prevenção, contenção de efeitos e recuperação das suas atividades perante fatores ou condições adversas suscetíveis de as afetar. A publicação do presente manual pretende sistematizar os resultados dessa recolha em reuniões realizadas nas próprias empresas, discussões e troca de experiências, decorrida ao longo deste triénio. O Manual organiza-se em três partes que se complementam. Na primeira, agregam-se as boas práticas que contribuem para uma maior resiliência das Organizações e das comunidades onde se inserem, permitindo também uma gestão adequada em cada fase do ciclo de uma catástrofe. Na segunda, apresentam-se medidas de resiliência concretas que as Organizações devem adotar, abrangendo diversas vertentes da proteção de pessoas, bens, edifícios e outras infraestruturas, bem como medidas a considerar na Gestão da Continuidade de Negócio e na gestão dos seguros. Na terceira, reúnem-se exemplos reais de como as Organizações colocaram em prática as referidas boas práticas de resiliência.

**ÍNDICE**

Nota de abertura .....	3
Nora prévia .....	4
Enquadramento .....	5
<b>PARTE I – RESILIÊNCIA NO CICLO DA CATÁSTROFE .....</b>	<b>7</b>
<b>1. Prevenção e Mitigação .....</b>	<b>8</b>
1.1. Apreciação do risco .....	8
1.1.1. Fontes de informação .....	9
1.2. Legislação e regulamentação .....	10
1.3. Normas internacionais e certificações .....	12
<b>2. Preparação .....</b>	<b>13</b>
2.1. Elaboração de Medidas de Autoproteção, Planos de Contingência e Planos de Continuidade do Negócio .....	13
2.2. Desenvolvimento de mecanismos de coordenação e comunicação interna e externa .....	14
2.3. Formação e exercícios .....	16
<b>3. Alerta .....</b>	<b>17</b>
3.1. Ativação .....	17
3.2. Monitorização .....	17
3.3. Preparação .....	17
<b>4. Resposta .....</b>	<b>17</b>
4.1. Coordenação da resposta .....	17
<b>5. Recuperação .....</b>	<b>18</b>
5.1. Avaliação de danos .....	18
5.2. Restabelecimento de infraestruturas e serviços .....	18
5.3. Comunicação empresarial .....	19
5.4. Avaliação do evento (lições aprendidas) .....	19
<b>PARTE II – MEDIDAS DE RESILIÊNCIA .....</b>	<b>21</b>
<b>1. Critérios para avaliação da criticidade .....</b>	<b>22</b>
<b>2. Medidas para Proteção de Pessoas, Bens e Infraestruturas .....</b>	<b>23</b>
2.1. Proteção de pessoas .....	23
2.2. Localização da infraestrutura .....	23
2.3. Características construtivas .....	23
2.4. Sistemas de energia .....	24
2.5. Proteção contra incêndio .....	24
2.6. Proteção contra inundação .....	25
2.7. Proteção contra sismos .....	26
2.8. Proteção contra tsunamis .....	28
2.9. Proteção contra intrusão .....	28
2.10. Formação e exercícios .....	39
<b>3. Gestão da Continuidade de Negócio .....</b>	<b>31</b>
<b>4. Gestão de Seguros .....</b>	<b>32</b>
4.1. Tipos de seguros .....	32
4.2. Boas práticas .....	34
<b>PARTE III – APLICAÇÃO DE BOAS PRÁTICAS DE RESILIÊNCIA .....</b>	<b>35</b>
1. Programa Caixa Segura (Caixa Geral de Depósitos).....	36
2. Sistema de apoio ao colaborador em viagem (Siemens) .....	38
3. Sistema de alerta e fecho automático de células de reservatórios de água em caso de sismo (EPAL) .....	40
4. Sistema anti-sísmico em transformadores de potência (EDP Distribuição) .....	42
5. Centro de Comando Operacional (Infraestruturas de Portugal) .....	44
6. Kit de Instrumentos de Gestão de Crise (NOS) .....	46
7. Aplicação para Gestão de Crises (SONAE) .....	48
8. Assistência Humana – Care Team e Assistance Team (TAP) .....	50
Agradecimentos .....	53



# PARTE I

## Resiliência no Ciclo da Catástrofe

Centro de Despacho e Condução da EDP-Distribuição

Os operadores de infraestruturas críticas, conscientes da sua função na Comunidade onde se inserem, devem desenvolver esforços permanentes com vista à redução do risco, mantendo-o em níveis aceitáveis.

Tal significa que, para além dos esforços de prevenção e mitigação, as Organizações têm de desenvolver ações de preparação, mecanismos de alerta, capacidade de resposta e de recuperação e ainda por fim serem capazes de melhorar continuamente na pós-catástrofe. Nesta parte exploram-se as boas práticas que vão além da legislação vigente em cada setor.



## 1. PREVENÇÃO E MITIGAÇÃO

Como Prevenção e Mitigação entende-se a atividade de implementação de medidas estruturais e não estruturais, empreendidas antes da ocorrência de eventos adversos, destinadas a reduzir a possibilidade da sua ocorrência (prevenir) ou o impacto negativo (mitigar) que tais eventos possam causar na sociedade ou nas Organizações, nomeadamente quando esses impactos evoluem para efeitos graves.

A implementação e atualização destas medidas só são possíveis através de um estabelecimento cíclico do contexto da Organização, que possibilita a análise do impacto na Organização da indisponibilização dos seus serviços se uma ou várias vertentes (pessoas, infraestruturas físicas, infraestruturas tecnológicas e fornecedores) que os suportam forem afetadas, devendo esta análise considerar o impacto à medida que o tempo de indisponibilidade aumenta.

Este estabelecimento cíclico do contexto permite a apreciação do risco da Organização, composta por:

- **Identificação do risco** (contempla as ameaças a que a Organização está exposta e as vulnerabilidades que podem ser exploradas por essas ameaças);
- **Análise do risco** (contempla as medidas já implementadas de Prevenção e/ou Mitigação);
- **Avaliação do risco** (contempla a valoração do risco identificando-se as situações acima do apetite de risco da Organização).

A apreciação do risco permite à Organização a priorização de medidas concretas de tratamento. Subjacente a este ciclo descrito está a sua monitorização e revisão, uma vez que só assim se garante a efetividade do ciclo aliado à comunicação e consulta de todos os envolvidos. Só é possível uma prevenção e mitigação efetiva em Organizações onde todos se sentem “donos” do risco, comunicando todas as situações que potenciam perdas.

### 1.1. Apreciação do risco

Uma apreciação do risco eficaz envolve a identificação, análise e avaliação do risco, sendo para tal necessário o entendimento de quais as ameaças a que a Organização está exposta, para posteriormente identificar e avaliar as



vulnerabilidades existentes, que podem ser exploradas por essas ameaças.

Uma vez que estamos a avaliar situações com efeitos potencialmente graves, ou seja, situações que vão para além da emergência do dia-a-dia, mais do que procurar uma probabilidade histórica que, conjuntamente com o impacto, permite quantificar o risco, a Organização deve focar-se na probabilidade de determinada ameaça explorar as vulnerabilidades identificadas.

O risco quantificado deve ser então confrontado com as medidas já implementadas pela Organização, de modo a perceber se essas medidas permitem uma redução do impacto e/ou da probabilidade, que permita desta forma trazer a quantificação do risco para um nível abaixo do apetite de risco<sup>1</sup> da Organização.

Na fase posterior de tratamento do risco a Organização deverá propor medidas a implementar, priorizando essas medidas através da quantificação efetuada, tomando em especial consideração as situações acima do apetite identificado pela Organização. Estas medidas preventivas (estruturais e não estruturais) deverão estar alinhadas com estratégias que permitem evitar/mitigar/transferir/aceitar<sup>2</sup> o risco, atenuando as consequências da materialização da ameaça, aumentando desta forma a resiliência da Organização e, por inerência, de todas as partes interessadas.

Caso a estratégia seja de aceitar o risco (por exemplo por falta de recursos ou falta de solução técnica), então deverá ser comunicado a todas as partes interessadas, para todos estarem conscientes da situação.

<sup>1</sup> Considera-se “Apetite de Risco” o nível de risco que uma organização está disposta a alcançar ou a reter, permitindo estabelecer um limite a partir do qual devem ser implementadas medidas de controlo adicionais (adaptado da Edição da NP EN 22301:2017 – “Segurança nas sociedades. Sistemas de gestão da continuidade. Requisitos”).

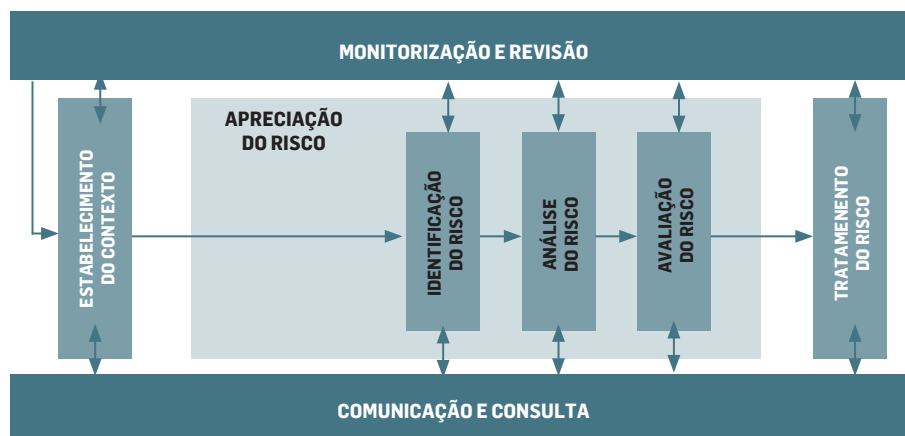
<sup>2</sup> Evitar: eliminar, sempre que possível, o risco ou a sua condição ou ainda proteger a Organização dos impactos desse risco.

Mitigar: reduzir a probabilidade e/ou consequência de um evento de risco. Desenvolver ações preventivas que reduzam a probabilidade da ocorrência de um risco ou o seu impacto para a Organização é mais eficaz que posteriormente tentar reparar as suas consequências.

Transferir: deslocar a consequência de determinado evento disruptivo para terceiros. Ao transferir o risco, não o eliminamos, apenas responsabilizamos terceiros pelas consequências que esse risco pode provocar à Organização. Inclui normalmente seguros e contratos.

Aceitar: não desenvolver nenhuma ação referida anteriormente para controlo do risco; apenas monitorizar e acompanhar a sua evolução.





Ciclo do processo de gestão de risco (Fonte: Adaptado de ISO 31000).

### 1.1.1. Fontes de informação

Como fontes de informação relativas à exposição a ameaças, fundamentais na apreciação do risco, salientam-se as seguintes:

- Para informação **geral** sobre riscos e vulnerabilidades, destaca-se:

- Avaliação Nacional de Risco – inclui a identificação e caracterização dos perigos de génese natural, tecnológica ou mista, suscetíveis de afetar o território nacional. Fonte: ANPC (<http://www.prociv.pt/pt-pt/RISCOSPREV/AVALIACAONACIONALRISCO/Paginas/default.aspx>)
- Avaliações de risco contidas nos Planos Municipais de Emergência de Proteção Civil (Fonte: Serviços Municipais de Proteção Civil).

- Para informação sobre **inundações** podem ser consultados:

- Cartas de risco de inundação (Decreto-Lei n.º 115/2010, de 22 de outubro). Fonte: Sistema Nacional de Informação de Recursos Hídricos (<http://snirh.apambiente.pt>).
- Cartografia de risco existente nos Instrumentos de Gestão do Território (IGT): Planos Regionais de Ordenamento do Território (PROT); Planos Diretores Municipais (PDM). Fonte: Sistema Nacional de Informação Territorial ([www.dgterritorio.pt](http://www.dgterritorio.pt))

- Para informação sobre **sismos e tsunamis** podem ser consultados:

- Cartas de zonamento sísmico para as estruturas. Fonte: Decreto-Lei n.º 235/83, de 31 de maio – Regulamento de Segurança e Ações para Estruturas de Edifícios (RSA)

- ([http://www.oern.pt/documentos/legislacao/d\\_dl\\_dr/DL235\\_83.pdf](http://www.oern.pt/documentos/legislacao/d_dl_dr/DL235_83.pdf));

- Cartas de perigosidade sísmica do território nacional para o Sismo Afastado (Tipo I) e Sismo Próximo (Tipo II). Fonte: Eurocódigo 8 - Documento Nacional de Aplicação (DNA), citado por Ordem dos Engenheiros<sup>3</sup> ([http://www.ordemengenheiros.pt/fotos/dossier\\_artigo/20111118\\_eca\\_rvalho\\_12886089014eca753f6b3bc.pdf](http://www.ordemengenheiros.pt/fotos/dossier_artigo/20111118_eca_rvalho_12886089014eca753f6b3bc.pdf));

- Cartas de danos do simulador nacional de danos sísmicos e dos simuladores sísmicos para a Área Metropolitana de Lisboa e Concelhos Limítrofes e Algarve. Fonte: disponibilizados a pedido pela ANPC;

- Cartografia de risco detalhada para zonas da costa mais suscetíveis a tsunamis. Fonte: disponibilizados a pedido pela ANPC.

- Para informação sobre **incêndios florestais** pode ser consultado:

- Mapa de Perigosidade de Incêndios Florestais (<http://www.icnf.pt/porta/florestas/dfci/inc/cartografia/map-perig-incend-flor>);

- Portaria 1056/2004, de 19 de agosto – zonas críticas face ao risco de incêndio

- (<http://dre.pt/pdf1sdip/2004/08/195B00/54505453.pdf>);

- Planos Municipais/intermunicipais de Defesa da Floresta Contra Incêndios.

<sup>3</sup> Deve-se ter em conta que: (i) as cartas são feitas com base nos valores das acelerações sísmicas, calculadas na rocha (a tabela das acelerações é também apresentada no DNA). Os efeitos precisos que podem verificar-se no local de implantação de cada instalação necessitam ser calculados multiplicando por um fator que depende da natureza do solo, que varia muito e necessita de estudos locais para cada instalação; (ii) o DNA inclui o coeficiente de importância que deve ser associado aos edifícios e equipamentos da instalação e que a ela deve ser aplicado. Este fator destina-se, em particular, a aumentar o nível de segurança das construções cujo colapso ou inoperacionalidade tenha consequências superiores ao colapso de edifícios correntes de habitação e escritórios (por exemplo hospitais, escolas, instalações de serviços e agentes de proteção civil, edifícios governamentais, instalações das redes de infraestruturas e outras infraestruturas críticas, instalações importantes para o funcionamento da economia, etc.).

## 1.2. Legislação e regulamentação

Uma gestão adequada na fase de Prevenção e Mitigação, passa primeiramente pelo cumprimento da legislação e regulamentação, onde exista, quer transversal, quer própria do setor.

De seguida destaca-se um conjunto de legislação e regulamentação vigente que é transversal a vários setores de atividade.

### Segurança face a riscos coletivos

- Decreto-Lei n.º 220/2008, de 12 de novembro, com a alteração dada pelo Decreto-Lei n.º 224/2015, de 9 de outubro, que aprovou o **Regime Jurídico da Segurança Contra Incêndio em Edifícios (RJ-SCIE)**. A introdução deste regime jurídico recomenda que se proceda à avaliação, em tempo oportuno, do seu impacto na efetiva redução do número de ocorrências, das vítimas mortais, dos feridos, dos prejuízos materiais, dos danos patrimoniais, ambientais e de natureza social, decorrentes dos incêndios urbanos e industriais que se venham a verificar;
- Portaria n.º 1532/2008, de 29 de dezembro, que aprovou o **Regulamento Técnico de Segurança contra Incêndio em Edifícios (RT-SCIE)**, nomeadamente as disposições técnicas gerais e específicas de SCIE referentes às condições exteriores comuns, às condições de comportamento ao fogo, isolamento e proteção, às condições de evacuação, às condições das instalações técnicas, às condições dos equipamentos e sistemas de segurança e às condições de autoproteção;
- Decreto-Lei n.º 150/2015, de 5 de agosto, que estabelece o **regime de prevenção de acidentes graves que envolvem substâncias perigosas** e de limitação das suas consequências para a saúde humana e para o ambiente, transpondo a Diretiva n.º 2012/18/UE, do Parlamento Europeu e do Conselho, de 4 de julho, relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas;
- Decreto-Lei n.º 174/2002, de 25 de julho, que estabelece as regras aplicáveis à **intervenção em caso de emergência radiológica**, transpondo para a ordem jurídica interna as disposições do título IX "Intervenção", da Diretiva 96/29/EURATOM;
- Decreto-Lei n.º 165/2002, de 17 de julho, com as alterações introduzidas pelo Decreto-Lei n.º 215/2008, de 10 de novembro, e pelo Decreto-Lei n.º 156/2013, de 5 de novembro – **proteção contra radiações ionizantes**;
- Decreto-Lei n.º 147/2008, de 29 de julho, que estabelece o regime jurídico da **responsabilidade por danos ambientais** e transpõe para a ordem jurídica nacional a Diretiva n.º 2004/35/CE, do Parlamento Europeu e do Conselho, de 21 de abril, que aprovou, com base no princípio do poluidor-pagador, o regime relativo à responsabilidade ambiental aplicável à prevenção e reparação dos danos ambientais;
- Decreto-Lei n.º 344/2007, de 15 de outubro, que aprova

### o Regulamento de Segurança de Barragens;

- Decreto-Lei n.º 409/93, de 14 de dezembro, que aprova o **Regulamento de Pequenas Barragens**;
- Decreto-Lei n.º 293/2009, de 13 de outubro, que assegura a execução, na ordem jurídica nacional, das obrigações decorrentes do Regulamento (CE) n.º 1907/2006, do Parlamento Europeu e do Conselho, de 18 de dezembro, relativo ao **registo, avaliação, autorização e restrição dos produtos químicos (REACH)**;
- Decreto-Lei n.º 63/2008, de 2 de abril, que procede à primeira alteração ao Decreto-Lei n.º 82/2003, de 23 de abril, que aprova o **Regulamento para a Classificação, Embalagem, Rotulagem e Fichas de Dados de Segurança de Preparações Perigosas**, transpondo para a ordem jurídica interna as Diretivas n.º 2004/66/CE, do Conselho, de 26 de Abril, 2006/8/CE, da Comissão, de 23 de janeiro, e 2006/96/CE, do Conselho, de 20 de novembro;
- Decreto-Lei n.º 41-A/2010, de 29 de abril, que regula o **transporte terrestre, rodoviário e ferroviário, de mercadorias perigosas**, transpondo para a ordem jurídica interna a Diretiva n.º 2006/90/CE, da Comissão, de 3 de novembro, e a Diretiva n.º 2008/68/CE, do Parlamento Europeu e do Conselho, de 24 de setembro, alterado pelo Decreto-Lei n.º 206-A/2012, de 31 de agosto, pelo Decreto-Lei n.º 19-A/2014, de 7 de fevereiro, e pelo Decreto-Lei n.º 246-A/2015, de 21 de outubro;
- Decreto-Lei n.º 124/2006, de 28 de junho, alterado e republicado pelo Decreto-Lei n.º 17/2009, de 14 de janeiro, que aprova o **Sistema Nacional de Defesa da Floresta Contra Incêndios**.

### Segurança de Bens

- Lei n.º 34/2013, de 16 de maio, que estabelece o regime do **exercício da atividade de segurança privada** e as medidas de segurança a adotar por entidades públicas ou privadas com vista a prevenir a prática de crimes;
- Portaria n.º 273/2013, de 20 de agosto, com a alteração dada pela Portaria n.º 106/2015, de 13 de abril, que regula as condições específicas da **prestação dos serviços de segurança privada**, o modelo de cartão profissional e os procedimentos para a sua emissão e os requisitos técnicos dos equipamentos, funcionamento e modelo de comunicação de alarmes;
- Portaria n.º 148/2014, de 18 de julho, que estabelece o conteúdo e a duração dos **cursos do pessoal de segurança privada**<sup>4</sup>.

### Segurança de Infraestruturas Críticas

- Lei n.º 62/2011, de 9 de maio, que estabelece os procedimentos de identificação e de **proteção das infraestruturas essenciais para a saúde, a segurança** e o bem-estar económico e social da sociedade nos sectores da energia e transportes, transpondo a Diretiva n.º 2008/114/CE, do Conselho, de 8 de dezembro.

## Segurança da Informação

- Lei n.º 67/1998, de 26 de outubro – **Lei da Proteção de Dados Pessoais** – relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. Aplica-se à generalidade dos sectores de atividade em Portugal, podendo existir leis ou regulamentos específicos nacionais sobre proteção de dados pessoais aplicáveis a determinados setores de atividade;
- Regulamento n.º 2016/679 da UE, de 27 de abril – **Regulamento Geral sobre a Proteção de Dados** – relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Tem aplicação direta e obrigatória nos Estados-Membros da UE, sem necessidade de existir legislação que transponha para a ordem jurídica portuguesa. Aplica-se à generalidade dos sectores de atividade na União Europeia, podendo existir diretivas ou regulamentos europeus específicos sobre proteção de dados pessoais aplicáveis a determinados setores de atividade;
- Decreto-Lei n.º 7/2004, de 7 de janeiro (alterado pelo Decreto-Lei n.º 62/2009, de 10 de março, e pela Lei n.º 46/2012, de 29 de agosto) – **Regime do Comércio Eletrónico** – que aborda, entre outras, as seguintes temáticas: o âmbito dos serviços da sociedade da informação (qualquer serviço prestado à distância por via eletrónica mediante remuneração ou pelo menos no âmbito de uma atividade económica); as obrigações para as comunicações de marketing/publicitárias por via eletrónica; as exigências legais e a informação mínima a disponibilizar em processos de Contratação Eletrónica; a força probatória das declarações eletrónicas;
- Lei n.º 109/2009, de 15 de setembro – **Lei do Cibercrime** – que estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico. Esta lei transpõe para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, de 24 de fevereiro, relativa a ataques contra sistemas de informação e adapta o direito português à Convenção sobre Cibercrime do Conselho da Europa;
- Decreto-Lei n.º 69/2014, de 9 de maio, estabelece que o **Centro Nacional de Cibersegurança** funciona no âmbito do Gabinete Nacional de Segurança (GNS) – O Centro Nacional de Cibersegurança (CNCS) tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação,

à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

## Seguros

- A **ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões** disponibiliza no seu website (<http://www.asf.com.pt/NR/exeres/380168E0-EB92-4F21-8F7E-866B231382AD.htm>) toda a legislação e regulamentação existente sobre seguros;
- De acordo com a ASF, os **seguros obrigatórios** em vigor na ordem jurídica Portuguesa (<http://www.asf.com.pt/NR/exeres/121FAB2D-E3DB-4517-A4E1-1F63774D8D-FC.htm>), aplicáveis à generalidade dos setores de atividade, são os relativos a:
  - Acidentes de Trabalho;
  - Acidentes em Serviço;
  - Acidentes Pessoais;
  - Assistência a Pessoas;
  - Danos;
  - Doença;
  - Incêndio;
  - Caução;
  - Responsabilidade Civil;
  - Furto e Roubo;
  - Vida.

<sup>4</sup> A Portaria n.º 148/2014 regula a emissão de certificados de aptidão e qualificação profissional do pessoal de segurança privada e a aprovação, certificação e homologação dos respetivos cursos de formação profissional

### 1.3. Normas internacionais e certificações

As Organizações devem procurar ir além dos requisitos mínimos impostos pela legislação e regulamentação. Hoje em dia os esforços na resiliência levaram à publicação de informação nacional e normas internacionais de boas práticas nas mais diversas áreas, possibilitando às Organizações obterem a certificação em algumas destas normas. Embora de observação e implementação voluntária, o alinhamento com a informação disponibilizada e com os requisitos das normas, permite às Organizações criarem mecanismos de certificação, quando aplicável, e de auditoria garantindo não só uma conformidade real, como também um ciclo de melhoria contínua.

A nível internacional, a International Organization for Standardization (ISO) promove a normalização de empresas e produtos, com o objetivo de manter a qualidade permanente, através da publicação de normas que fornecem requisitos, especificações, diretrizes ou características que podem ser usados de forma sólida para assegurar que os materiais, produtos, processos e serviços são adequados para os fins.

Na categoria da segurança e resiliência existem algumas normas internacionais vigentes, onde se salientam, entre outras:

- NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs, 2013 Edition;
- ISO 9000 Series – Quality management;
- ISO 14000 Series – Environmental Management;
- ISO 22000 Series – Food safety management;
- ISO 22300 Series – Societal Security Management;
- ISO 26000 Series – Social Responsibility;
- ISO 27000 Series – Information Security Management;
- ISO 31000 Series – Risk Management;
- ISO 45000 Series – Occupational Health and Safety;
- ISO 50000 Series – Energy Management;
- ISO 55000 Series – Asset Management.

A maioria destas normas apresentam uma estrutura bastante completa, no sentido de irem além da gestão da fase de Prevenção e Mitigação. No entanto, relativamente a esta fase as normas apresentam partes comuns, nomeadamente o enfoque na gestão do risco, que permitem às Organizações orientar e direcionar esforços, como referido no início deste capítulo.

Outra parte comum das normas, nesta fase, é a relevância na sensibilização interna e externa, pretendendo-se o conhecimento generalizado dos fatores que conduzem às catástrofes e as ações que podem ser tomadas individualmente ou coletivamente, de forma a reduzir a exposição e vulnerabilidade às ameaças.

Esta é uma componente essencial de uma Prevenção e Mitigação eficiente, sem a qual não se consegue obter uma participação empenhada de todos, absolutamente necessária na fase de Preparação da resposta.



## 2. PREPARAÇÃO

Como Preparação da resposta entende-se a antecipação do conhecimento e das capacidades necessárias para gerir eficazmente todos os tipos de disrupções, desde o momento em que ocorrem até às fases da Resposta e da Recuperação. Com uma correta preparação as Organizações alcançam a prontidão, que é a capacidade de rapidamente responder, quando necessário, a qualquer situação.

A Preparação é baseada numa análise de risco rigorosa e na correta ligação com sistemas de alerta precoce, e inclui atividades de:

- Elaboração de medidas de autoproteção, planos de contingência e de continuidade do negócio;
- Desenvolvimento de mecanismos de coordenação e comunicação, internamente e com as partes interessadas;
- Formação e exercícios.

### 2.1. Elaboração de Medidas de Autoproteção, Planos de Contingência e Planos de Continuidade do Negócio

Apresentam-se de seguida as medidas de autoproteção bem como os Planos de Contingência e de Continuidade de Negócio que as Organizações deverão considerar.

#### 2.1.1. Medidas de Autoproteção

O Regime Jurídico da Segurança Contra Incêndio em Edifícios<sup>5</sup> (RJ-SCIE) obriga a que as entidades exploradoras gestoras (espaços comuns) ou os seus proprietários de edifícios ou recintos elaborem e implementem Medidas de Autoproteção (MAP) dos mesmos.

As MAP estabelecem a organização e gestão da segurança durante a exploração ou utilização de um edifício ou recinto, destinando-se a mitigar os riscos e a planear a resposta às emergências. Apesar das MAP se encontrarem vocacionadas para o risco de incêndio, considera-se como boa prática a inclusão neste conjunto de medidas de prevenção, preparação e resposta a inclusão de outros cenários de origem natural, tecnológica ou intencional.

As Medidas de Autoproteção, previstas no RJ-SCIE, exigíveis para cada categoria de risco nas diversas utilizações-tipo<sup>6</sup>, contemplam:

- a) Medidas preventivas, as quais, conforme a categoria de risco, tomam a forma de:
  - i. Procedimentos de Prevenção; ou
  - ii. Planos de Prevenção;
- b) Medidas de intervenção em caso de incêndio, as quais, conforme a categoria de risco tomam a forma de:
  - i. Procedimentos em Caso de Emergência; ou
  - ii. Planos de Emergência Internos;
- c) Registo de segurança, no qual devem constar:
  - i. Os relatórios de vistoria ou inspeção;
  - ii. A relação de todas as ações de manutenção das instalações técnicas, equipamentos e sistemas, direta ou indiretamente relacionadas com a SCIE;
  - iii. A relação das ocorrências (não apenas de incêndio, mas de todas as que estiverem consideradas nas MAP.
- d) Formação em SCIE, sob a forma de ações de sensibilização destinadas a todos os funcionários e colaboradores<sup>7</sup> das entidades exploradoras, ou de formação específica, destinada aos delegados de segurança, a elementos que possuem atribuições especiais de atuação em caso de emergência e outros que lidam com situações de maior risco de incêndio;
- e) Simulacros/exercícios, para testar os procedimentos de emergência / do plano de emergência interno e treinar os ocupantes e equipas de segurança tendo em vista a criação de rotinas de comportamento e de atuação, bem como o aperfeiçoamento de procedimentos em causa. As MAP estão sujeitas a parecer obrigatório da ANPC.

#### 2.1.2. Planos de Contingência

Para além da elaboração do conjunto de documentos que constituem o Plano de Segurança Interno, anteriormente descrito, a Organização deverá elaborar Planos de Contingência. O seu objetivo é identificar e descrever uma série de procedimentos alternativos, estruturais e não estruturais, a serem executados para controlar rapidamente uma disrupção, de origem natural ou tecnológica, e minimizar as consequências negativas, no sentido de repor os processos vitais da Organização

<sup>5</sup> Decreto-Lei n.º 220/2008, de 12 de novembro, alterado pelo Decreto-Lei n.º 224/2015, de 9 de outubro.

<sup>6</sup> De acordo com o estabelecido no Decreto-Lei n.º 220/2008, de 12 de novembro, alterado e republicado pelo Decreto-Lei n.º 224/2015, de 9 de outubro, os edifícios e recintos estão do ponto de vista da segurança contra incêndio, classificados de acordo com o seu uso em 12 utilizações-tipo, correspondendo a cada uma das utilizações-tipo 4 categorias de risco (1.ª, 2.ª, 3.ª e 4.ª), sendo a 1.ª e a 4.ª categorias de risco as de menor e de maior risco de incêndio respetivamente.

As Organizações devem aferir no RJ-SCIE qual a constituição das medidas de autoproteção exigíveis, a qual para cada edifício ou recinto depende da(s) utilização(ões) tipo, respetivas categorias de risco e locais de risco. A determinação da categoria de risco depende de vários fatores de risco, tais como: altura da utilização-tipo; n.º de pisos abaixo do plano de referência; área bruta ocupada pela utilização-tipo ou o efetivo da utilização-tipo.

<sup>7</sup> Nomeadamente, os funcionários e colaboradores das entidades exploradoras dos espaços afetos às utilizações-tipo; Todas as pessoas que exerçam actividades profissionais por períodos superiores a 30 dias por ano nos espaços afectos às utilizações-tipo; Todos os elementos com atribuições previstas nas atividades de autoproteção.

o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos.

O processo de desenvolvimento de um Plano de Contingência pode ser dividido em 6 etapas fundamentais:

- Identificar a ameaça;
- Avaliar o seu impacto na Organização;
- Definir a estrutura de coordenação;
- Elaborar o plano de resposta operacional, os controlos adequados e a resposta às necessidades de comunicação;
- Testar o plano através de simulacro;
- Planear o restabelecimento da atividade normal de forma rápida e segura.

### 2.1.3. Planos de Continuidade do Negócio

Dada a diversidade de cenários causadores de disrupção do negócio com que uma Organização se poderá deparar, o planeamento baseado em causas de disrupção não só implica um grande esforço, dado o elevado número de planos necessários, como se pode revelar um esforço em vão pelo facto de não ser possível prever todos os cenários que podem ocorrer.

Assim, enquanto as medidas de autoproteção e os planos de contingência se focam em cenários inerentes à natureza das infraestruturas, na continuidade do negócio o planeamento é baseado na perda de recursos, considerando-se quatro categorias de recursos – pessoas, infraestruturas físicas, infraestruturas tecnológicas e fornecedores –, sendo estas categorias endereçadas, nos Planos de Continuidade, dependendo da criticidade de cada uma delas para a continuidade do serviço.

O processo de desenvolvimento de um Plano de Continuidade do Negócio deverá estar inserido num ciclo de Gestão de Continuidade do Negócio, que garanta que o plano, ou planos, são os que efetivamente respondem às necessidades da Organização.

Este ciclo, segundo as boas práticas, deverá contemplar:

- Contexto: Avaliar a missão, processos, atividades e envolvente, definindo o âmbito e planeando o processo de continuidade;
- Análise de impacto no negócio: Através de entrevistas, identificar as necessidades de recuperação e priorização de atividades;
- Análise e Avaliação de Risco: Analisar as atividades críticas identificadas na análise de impacto no negócio, incluindo-se a análise das medidas implementadas e proposta de medidas a implementar;
- Estratégia de continuidade do negócio: Estabelecer e implementar a estratégia de continuidade do negócio, através de planos de continuidade, de gestão de crise e de comunicação;
- Exercícios: Realizar e definir um programa evolutivo de

exercícios e testes, que valide a estratégia estabelecida;

- Responsabilidade: Definir responsabilidades pelo ciclo de Continuidade do Negócio, nomeadamente através da criação de comités que permitam a implementação efetiva da continuidade.

Os planos de Continuidade do Negócio devem, no mínimo, ser compostos pelos seguintes pontos:

- Âmbito, outros documentos a considerar, definições relevantes, objetivos, recursos mínimos, entidades internas e externas envolvidas;
- Funções e responsabilidades;
- Cenários de indisponibilidade (pessoas, infraestruturas físicas, infraestruturas tecnológicas e fornecedores), cada um descrevendo a estratégia de continuidade do negócio, os recursos necessários para a ativação, as ações a desenvolver e o retorno à normalidade.

## 2.2. Desenvolvimento de mecanismos de coordenação e comunicação interna e externa

Na sua maioria, as dificuldades encontradas na resposta a uma situação de crise são devidas a uma insuficiente preparação, treino e organização de todos os intervenientes na gestão deste tipo de eventos. Tal exige o conhecimento dos protocolos e procedimentos de atuação quer das Organizações, quer dos agentes de proteção civil e de outras entidades envolvidas.

A resposta de uma Organização a uma situação de crise, independentemente da sua origem, assenta na capacidade da sua equipa de gestão, na coordenação e controlo dos meios existentes e posteriormente na sua boa articulação com os meios externos.

### 2.2.1. Equipa de Gestão de Emergência

A Organização deve dispor de uma Equipa de Gestão de Emergência devidamente formada, rotinada e preparada para a resolução de situações de emergência e crise, capaz de gerir os recursos humanos e técnicos disponíveis, bem como assegurar a coordenação das operações previstas nos planos e nos protocolos de atuação das equipas de segurança.

Esta Equipa pode ser constituída por um representante responsável de cada uma das áreas da Organização, sendo exemplos:

- Administração ou gerência da Organização;
- Gestão do Risco;
- Operação (áreas com atividades críticas, tais como produção, despachos, centros de segurança);
- Continuidade do Negócio;
- Segurança física e vigilância;
- Manutenção dos edifícios e outras infraestruturas;
- Recursos Humanos;
- Gestão de Ativos;



Centro de Comando Operacional – Infraestruturas de Portugal

- Logística;
- Gestão de Fornecedores;
- Gestão de Clientes
- Sistemas de Informação;
- Comunicação e Imagem;
- Saúde e Segurança no Trabalho.

### 2.2.2. Articulação com entidades de proteção civil e socorro

As entidades de proteção civil e socorro são um elemento fundamental naquilo que será a resposta a um evento de exceção, mitigando as consequências diretas e indiretas para as Organizações.

Desta forma é fundamental que sejam desenvolvidos mecanismos de articulação de resposta a incidentes (que podem derivar em protocolos de atuação), concretizando-se na implementação de procedimentos específicos de articulação com entidades externas (comunicações, estabelecimento do alarme e alerta, programa de visitas, etc.) a integrar no planeamento de emergência das Organizações.

### 2.2.3. Requisitos com os fornecedores

A Organização deve avaliar e selecionar os fornecedores com base na capacidade que eles detêm em fornecer artigos, equipamentos ou serviços indispensáveis ao normal funcionamento da Organização, num período de tempo considerado aceitável, de modo a que, em caso de

catástrofe, a Organização tenha uma maior capacidade de resiliência e recuperação perante condições adversas.

A materialização destas premissas deve consubstanciar-se na introdução de cláusulas específicas aquando da celebração de contratos que assegurem, caso ocorram eventos suscetíveis de provocarem perturbação no normal desenrolar das atividades da Organização, o fornecimento imediato de materiais, equipamentos diversos ou serviços que sejam imprescindíveis para a recuperação atempada da atividade.

### 2.2.4. Requisitos dos clientes

Se no ponto anterior se referem as Organizações como clientes, e como se devem gerir os fornecedores, as Organizações também são elas próprias fornecedoras de alguém. Devem, por isso, ter em consideração as necessidades dos seus clientes no planeamento em situação de interrupção.

Em várias Organizações, a definição contratual de requisitos de fornecimento para com os clientes, em caso de crise, é nevrálgica, devendo assim ser clara a prioridade no restabelecimento do serviço. Para tal é fundamental a incorporação desses requisitos nos mecanismos de coordenação e comunicação da Organização, de modo a que, especialmente em situação de crise, eles sejam respeitados.

### 2.3. Formação e exercícios

A formação prevista no RJ-SCIE, engloba as ações de sensibilização destinadas a todos os funcionários e colaboradores das entidades exploradoras, e a formação específica, destinada aos delegados de segurança (e elementos que possuem atribuições especiais de atuação em caso de emergência) e outros elementos que lidam na sua atividade profissional normal com situações de maior risco de incêndio.

A realização de simulacros / exercícios, para testar os procedimentos de emergência / plano de emergência interno e treinar os ocupantes e equipa de segurança é essencial para garantir a atualização e adequação dos procedimentos a ter em caso de emergência. A sua obrigatoriedade depende da utilização-tipo, da categoria de risco e dos locais de risco da Organização. No entanto, é aconselhável que todas as Organizações considerem a sua realização como uma boa prática ao nível da gestão da segurança.

Como referido anteriormente, a realização de formação e exercícios não se podem cingir aos incêndios em edifícios, mas devem ser aplicados também a todos os cenários previstos nas medidas de autoproteção, assim como ao previsto nos planos de contingência.

Apenas existirá uma resposta eficaz se os colaboradores da Organização forem instruídos, tiverem consciência dos riscos a que estão expostos, compreenderem as medidas e procedimentos de prevenção, procedimentos de atuação em caso de emergência previamente definidos.

O Plano formativo para os colaboradores da Organização poderá abranger, entre outras, as seguintes ações:

- Visita aos edifícios e infraestruturas com o objetivo de identificar os locais de risco;
- Regras de exploração e comportamento, nomeadamente as que estabelecem os procedimentos de exploração e utilização dos espaços, no dia a dia;
- Procedimentos de alarme;
- Procedimentos gerais de atuação em caso de emergência, nomeadamente os de evacuação, tendo conhecimento das equipas de evacuação e do ponto de encontro;
- Formação em primeiros socorros;
- Utilização dos meios de primeira intervenção (extintores portáteis e bocas de incêndio tipo carretel);
- Formação específica para funcionários e colaboradores com atividade em locais de risco C, D ou F, respetivamente locais de risco agravado de incêndio, locais com permanência de pessoas diminuídas nas suas capacidades (ex. pessoas acamadas e crianças com idade inferior a 6 anos) e locais destinados a atividades essenciais na Organização);
- Formação para o delegado de segurança, elementos da equipa de intervenção, elementos da equipa de primeiros socorros e para os elementos da equipa de evacuação;
- Sensibilização sobre riscos naturais e antropogénicos, e o modo como afetam a Organização e os seus colaboradores.

A eficácia da formação ministrada só poderá ser medida com a realização de exercícios que testem a capacidade de coordenação e intervenção em situações simuladas, o mais perto da possível realidade.



Sala de formação – Infraestruturas de Portugal



### 3. ALERTA

Cada Organização deve desenvolver os parâmetros que levam à ativação dos respetivos níveis de alerta definidos no seu planeamento de emergência interno, que são os parâmetros que separam o regime normal da atividade desenvolvida, de um regime perturbado. Os níveis de alerta definidos por cada Organização podem ou não ter correspondência com os níveis de alerta emitidos pelas entidades oficiais, caso estes sejam ativados.

A fase de alerta nas Organizações pode dividir-se em:

- Ativação;
- Monitorização;
- Preparação.

#### 3.1. Ativação

As Organizações devem ativar os seus níveis de alerta pré-definidos, na iminência ou ocorrência de um acidente com gravidade que o justifique. Pode tratar-se de uma ocorrência súbita (por exemplo, um sismo, um ataque terrorista, um acidente tecnológico), ou de uma ocorrência que se pode antecipar e que tem uma evolução progressiva (por exemplo, um fenómeno meteorológico extremo, uma cheia, etc.). Em qualquer dos casos, a Organização decidirá os níveis de alerta a ativar, podendo alinhá-los com os estados de alerta declarados por entidades externas competentes.

A Organização deverá, face à ativação do alerta, convocar as respetivas Equipas de Gestão de Emergência, de modo a desencadear e adequar as ações preventivas e preparatórias.

#### 3.2. Monitorização

A Equipa de Gestão de Emergência, imediatamente após ter conhecimento da ativação do alerta, deverá efetuar um rigoroso acompanhamento da situação. Caso seja algo externo à Organização, esse acompanhamento poderá ser feito através dos avisos emitidos pelas autoridades de proteção civil ou por entidades sectoriais em razão do risco (ex.: Instituto Português do Mar e da Atmosfera, Agência Portuguesa do Ambiente, Direção-Geral da Saúde, etc.).

#### 3.3. Preparação

Face ao evoluir da situação, para um nível que se considere iminente o impacto na Organização, a Equipa de Gestão de Emergência deverá informar todos os colaboradores da situação e convocar as equipas de emergência para uma pronta intervenção, no sentido de minimizarem os efeitos negativos expectáveis, colocando os meios humanos e materiais de prevenção.

### 4. RESPOSTA

A fase de Resposta a uma situação de acidente grave ou catástrofe é a etapa que corresponde à operacionalização de todas as ações identificadas e previstas na fase de Preparação.

O objetivo fundamental da fase de Resposta é a preservação da vida humana, minimização dos danos provocados e a proteção de bens e propriedade da Organização, permitindo providenciar os serviços em níveis mínimos aceitáveis durante, ou imediatamente após, um acidente grave ou catástrofe, salvaguardando a continuidade do negócio.

#### 4.1. Coordenação da Resposta

Na coordenação da Resposta à ameaça deverão ser convocados os colaboradores da Organização que compõem a Equipa de Gestão de Emergência e as equipas de segurança vocacionadas para a atuação em situações de catástrofe, colocando em prática as medidas de prevenção constantes nos planos de emergência, contingência e continuidade do negócio, previamente elaborados e testados, e a articulação com os agentes de proteção civil e outras entidades.

Dado que um acidente grave ou catástrofe pode consumir de imediato todos os recursos das forças e serviços de proteção civil, compete à Equipa de Gestão de Emergência definir a prioridade das atividades de Resposta.

Uma sequência das atividades de Resposta a situações de crise poderá ser:

- Evacuação dos colaboradores para local seguro;
- Prestação de primeiros socorros a colaboradores afetados;
- Comunicação aos familiares de colaboradores afetados;
- Ativação de equipas, de infraestruturas físicas e de infraestruturas tecnológicas redundantes;
- Implementação de ações para a supressão do incidente;
- Contacto e receção de agentes de proteção civil a informar do incidente;
- Remoção de bens para local seguro;
- Implantação de ações de rescaldo, vigilância e recuperação do local.

## 5. RECUPERAÇÃO

Como Recuperação entende-se a fase imediatamente posterior às atividades de Resposta. Nesta fase, uma equipa multidisciplinar procurará identificar recursos alternativos (por ex. instalações, equipamento, tecnologia de informação e fornecedores alternativos) ou métodos alternativos (por ex. como realizar as atividades “manualmente” sem recurso a meios “modernos”) para iniciar as atividades que conduzam ao retorno à normalidade.

Em situações mais gravosas, a Recuperação implica a reabilitação e reconstrução, devendo estas ser baseadas em estratégias pré-definidas. Nestes casos, os programas de Recuperação oferecem importantes oportunidades para desenvolver e implementar novas medidas de redução de risco de catástrofe e para aplicar o princípio de “construir de novo melhor” (build back better).

A fase da Recuperação poderá ainda ser dividida em:

- Avaliação de danos;
- Restabelecimento de infraestruturas e serviços;
- Comunicação empresarial;
- Avaliação do evento.

### 5.1. Avaliação de danos

Imediatamente após ter terminado a fase de Resposta à situação, a Equipa de Gestão de Emergência deverá, de acordo com os planos preestabelecidos e devidamente treinados, propor a realização de uma avaliação a toda a Organização.

Uma equipa pluridisciplinar de avaliação de danos, constituída por um conjunto de técnicos especializados, internos ou externos, deverá verificar desde a integridade estrutural da(s) infraestrutura(s), aos sistemas de apoio (eletricidade, água, comunicações, acesso à informação, AVAC, etc.) recolhendo informação específica sobre os estragos provocados pela situação, e as suas consequências para a Organização, nomeadamente no que se refere a:

- Ocorrência de danos estruturais e estabilidade das estruturas;
- Ocorrência de danos não estruturais e operacionalidade dos sistemas auxiliares implantados;
- Condições de segurança para os colaboradores e partes interessadas;
- Condições de habitabilidade/salubridade das instalações;
- Condições de armazenagem de produtos;
- Existência de produtos combustíveis, poluentes ou perigosos sem segurança.

Com base nos dados recolhidos, a equipa elabora um

relatório de avaliação preliminar de danos, apuramento das causas que desencadearam a situação (se possível) e as oportunidades de melhoria para evitar que a Organização seja atingida de novo por este evento ou que o impacto seja reduzido.

### 5.2. Restabelecimento de infraestruturas e serviços

Entende-se por restabelecimento de infraestruturas e serviços o processo que se inicia imediatamente após a conclusão da avaliação dos danos que de algum modo afetaram a Organização.

As ações a tomar dependem diretamente do relatório de avaliação de danos previamente elaborado e entregue à Equipa de Gestão de Emergência, e deve incidir especialmente na proteção dos colaboradores, na atenuação dos efeitos provocados pela situação e no rápido restabelecimento das condições laborais e no potencial produtivo da Organização.

Uma sequência padrão das ações a realizar pode ser:

- Garantir a segurança dos colaboradores e partes interessadas;
- Ativação dos contratos de fornecedores críticos;
- Promover a demolição, desobstrução e remoção dos destroços ou obstáculos, a fim de restabelecer a circulação (se necessário);
- Adotar as medidas necessárias à urgente recuperação da capacidade de prestação do serviço e à normal atividade da Organização;
- Adotar medidas que visem a minimização dos riscos patrimoniais e as perdas de exploração;
- Assegurar que as necessidades dos clientes são colmatadas;
- Proceder à análise e quantificação dos danos pessoais e materiais, elaborando um relatório sobre as operações realizadas.



Reparação de danos da rede elétrica – EDP-Distribuição

### 5.3. Comunicação empresarial

De modo a evitar desinformação prejudicial ao desenrolar das atividades de recuperação da Organização, e como parte integrante na Equipa de Gestão de Emergência, o responsável pela Comunicação deverá manter permanentemente atualizada internamente a Organização e externamente os órgãos de comunicação social, clientes e partes interessadas prioritárias, do bom andamento dos trabalhos de recuperação da Organização, através da elaboração de um plano de comunicação, que contemple entre outros:

- Briefings e comunicados internos;
- Briefings e comunicados aos órgãos de comunicação social (danos humanos e materiais, andamento dos trabalhos de recuperação da Organização, etc.);
- Atualização contínua da informação através das redes sociais;
- Comunicados aos fornecedores.

### 5.4. Avaliação do evento (lições aprendidas)

Como avaliação do evento entende-se a apreciação da atuação das Organizações nas várias fases do evento: Alerta, Resposta e Recuperação. Para tal é essencial que durante essas fases se recolham elementos, à medida que os acontecimentos vão evoluindo, que servirão de base à avaliação da atuação durante o evento.

É assim considerada uma boa prática que, após a emergência, seja promovido:

- A realização de reuniões de avaliação da atuação durante o evento, com a participação dos coordenadores dos diferentes níveis de apoio e operacionais, que se justifique convocar;
- A análise dos pontos fortes e fracos registados durante a gestão do evento e revisão dos procedimentos internos e de ligação com entidades externas;
- O planeamento e execução de ações corretivas, ao nível da construção e da operação das instalações (caso exista a necessidade de reabilitação ou reconstrução devendo este ponto ser antecipado), dos sistemas e dos processos, ao nível das disposições contratuais com prestadores de serviços/fornecedores e ainda da formação e exercício dos colaboradores e dos prestadores com base nas lições aprendidas.







Linha de montagem com tecnologia Siemens

## PARTE II

# Medidas de Resiliência

Esta parte apresenta medidas de resiliência concretas que as Organizações devem adotar, tendo em conta a especificidade da sua realidade, abrangendo diversas vertentes da proteção de pessoas, bens, edifícios e outras infraestruturas.

Apresenta também medidas que devem ser consideradas pelas Organizações na Gestão da Continuidade de Negócio. Refere ainda uma sistematização de diversos tipos de seguros aplicáveis ao património e às atividades das Organizações assim como uma identificação de boas práticas a seguir nos processos de gestão de seguros.

## 1. CRITÉRIOS PARA AVALIAÇÃO DA CRITICIDADE

Antes de se aplicarem medidas de resiliência, dado que nem todos os riscos têm o mesmo nível de criticidade e que as Organizações têm recursos limitados, deve-se analisar a priorização dessas medidas. Torna-se deste modo necessário que as Organizações adotem ferramentas que permitam apurar e comparar o nível de risco ou de criticidade dos seus recursos (pessoas, bens e infraestruturas).

De seguida apresenta-se, como exemplo, um conjunto de critérios que podem servir de base à definição de Parâmetros de Avaliação de Criticidade das Infraestruturas da Organização, devendo aplicar-se parâmetros de avaliação também aos restantes recursos.

### A. Critérios das Atividades/Serviços dependentes da Infraestrutura

#### A.1. Pessoas

- Número de pessoas que utilizam o edifício ou infraestrutura;
- Tipos de autorizações e cartões de acesso (por ex. acesso permitido apenas a colaboradores internos perante autorização específica vs. cartões de acesso 24h atribuídos a colaboradores externos);
- Acesso a pessoas e atendimento ao público/terceiros (por ex. sem atendimento ao público/terceiros vs. atendimento corrente ao público/terceiros).

#### A.2. Ativos Físicos

- Valor estimado dos equipamentos ou existências dentro do edifício ou infraestrutura.

#### A.3. Ativos de Informação

- Nível de confidencialidade da informação existente no edifício ou infraestrutura.

#### A.4. Serviços/Atividades Críticos da Organização

- Prioridades dos serviços/atividades;
- Número de clientes/utilizadores impactados.

### B. Critérios de Operação e Segurança da Infraestrutura

#### B.1. Primeiras intervenções

- Criticidade das primeiras intervenções pela equipa de Vigilantes (por ex. confirmação de alarmísticas, combate a incêndio, etc.).

#### B.2. Sistemas de suporte críticos

- Sistemas de suporte críticos para o edifício ou infraestrutura (por ex. nível de dependência face a sistemas de energia socorrida).

#### B.3. Serviços de Emergência Externos

- Tempo/distância das instalações das Forças de Segurança;
- Tempo/distância das instalações dos Corpos de Bombeiros.

### C. Critérios de Tipologia e Localização da Infraestrutura

#### C.1. Incêndio

- Fontes internas de ignição e de combustível de fogo (por ex. armazenamento de existências, máquinas, combustíveis, etc.);
- Localização em zonas de risco de fogo (por ex. tipos de edifícios na envolvente, vegetação, etc.);
- Sistemas de deteção e extinção (por ex. infraestrutura com sistemas de deteção e de extinção automáticos e com alarmística e operação remota vs. infraestrutura sem sistemas de deteção e de extinção automáticos).

#### C.2. Inundação

- Localização do edifício ou infraestrutura em áreas suscetíveis de serem inundáveis (por ex. zona de alta vulnerabilidade a cheias, etc.);
- Natureza e extensão do risco de inundação na zona (por ex. histórico de ocorrências na zona);
- Tipologia do edifício ou infraestrutura e sistemas de deteção de inundação (por ex. edifício com pisos térreos ou subterrâneos e sem sistemas automático de deteção de inundação).

#### C.3. Sismo e Tsunami

- Localização em zona de alta perigosidade sísmica;
- Localização em zona suscetível de ser afetada por um tsunami;
- Tipologia da infraestrutura e forma como se encontra construída.

#### C.4. Intrusão

- Vulnerabilidade do edifício ou infraestrutura à intrusão (por ex. edifício predominantemente fechado e não identificável do exterior vs. edifício com portas e janelas exteriores em vidro sem proteção);
- Existência de sistemas de deteção (por ex. sensores) e dissuasão (por ex. sirene de alarme).



## 2. MEDIDAS PARA PROTEÇÃO DE PESSOAS, BENS E INFRAESTRUTURAS

### 2.1. Proteção de pessoas

Para efeitos da proteção das pessoas que permaneçam nos seus edifícios ou infraestruturas ou que se encontrem em deslocação, a Organização deve prever a existência de:

- Equipas de emergência, podendo ser constituídas pelos Grupos de Primeira Intervenção (GPI) que são responsáveis por conduzir os utilizadores dos edifícios ou infraestruturas para os pontos de encontro exteriores numa situação de emergência, bem como pelas Equipas de Resposta a Emergência (ERE) que são elementos pertencentes aos GPI, com formação diferenciada nas áreas do socorrismo e combate a incêndios, e que podem atuar em primeiro alarme em caso de acidente, em complemento das equipas de vigilantes;
- Caixas/malas/armários de primeiros socorros, devendo o seu conteúdo, bem como a quantidade e respetiva localização e acessibilidade destes equipamentos, serem definidos em função do número e dispersão dos utilizadores dos edifícios ou infraestruturas, do tipo de atividade da Organização e dos fatores de risco profissional, em linha com a Informação Técnica<sup>9</sup> publicada pela Direção-Geral da Saúde (DGS);
- Equipamentos de DAE (Desfibrilhação Automática Externa), incluindo a existência de elementos operacionais DAE formados em número suficiente para assegurar a utilização dos equipamentos de forma eficaz e eficiente, especialmente em edifícios com elevado número de utilizadores internos e/ou de grande afluência de público, em articulação com o Programa Nacional de DAE regulado pelo Instituto Nacional de Emergência Médica (INEM)<sup>10</sup>;
- Medidas de apoio aos colaboradores em deslocação ao estrangeiro que incluam, entre outros, contactos de emergência no estrangeiro, informação situacional sobre destinos de risco, recomendações sobre alimentação em locais exóticos, recomendações de segurança para proteção individual e de bens em viagem, equipamentos básicos de proteção individual (máscaras, medicamentos, etc.).

### 2.2. Localização da infraestrutura

A localização das infraestruturas da Organização é fundamental para a sua resiliência, em caso de acidente grave ou catástrofe.

As infraestruturas da Organização, em especial as que

forem consideradas críticas, não devem preferencialmente estar localizadas:

- Perto de encostas ou declives suscetíveis a movimentos de vertente, que possam ser atingidas por derrocada de pedras ou deslizamento de terras;
- Numa zona com risco significativo de inundações, por ex. em zonas de leito de cheia ou de difícil escoamento de águas pluviais;
- Em zonas de perigosidade sísmica elevada;
- Próximo do mar em zonas sujeitas a galgamentos costeiros, de modo a não serem atingidas por ondas, em caso de tempestade;
- Perto do mar e/ou a uma cota altimétrica suficientemente baixa, de modo a não serem atingidas em caso de tsunami;
- Em áreas suscetíveis à ação das ondas de inundações provenientes de rotura total ou parcial de barragens;
- Perto de uma área industrial onde se processam matérias perigosas ou produtos inflamáveis, de condutas por onde circulem matérias perigosas ou próximas de estações de abastecimento de combustíveis;
- Perto de vias de comunicação onde reiteradamente circulem veículos de transporte de matérias perigosas;
- Na proximidade de áreas de elevado risco de incêndio florestal de modo que possam ser afetadas se um incêndio ocorrer, respeitando sempre as faixas de segurança à volta previstas na Lei.

Caso as infraestruturas da Organização se encontrem nas condições anteriormente descritas, deverão adotar medidas complementares de segurança adequadas à sua exposição ao risco.

### 2.3. Características construtivas

As infraestruturas da Organização devem ser projetadas e construídas de modo a:

- Existir espaço exterior suficientemente amplo para as viaturas de socorro poderem manobrar em caso de incêndio ou de outra catástrofe;
- Terem uma correta implementação e manutenção das barreiras corta-fogo aplicáveis no edifício, incluindo as seguintes situações: classe de resistência ao fogo adequada das portas corta-fogo e das paredes; funcionamento correto das portas corta-fogo; selagem dos atravessamentos e das condutas de cabos; separação

<sup>9</sup> Informação Técnica 2/2010, de 12.07.2010, Emergência e Primeiros Socorros em Saúde Ocupacional - Anexo I, Informação Técnica 1/2009, Primeiros Socorros no Local de Trabalho [https://www.dgs.pt/saude-ocupacional/documentos-so/inf\\_tecnica\\_02\\_2010-pdf.aspx](https://www.dgs.pt/saude-ocupacional/documentos-so/inf_tecnica_02_2010-pdf.aspx)

<sup>10</sup> Programa Nacional de Desfibrilhação Automática Externa (PND AE), <http://www.inem.pt/category/entidades/programa-dae/>



ETA da Asseiceira (EPAL). © Francisco Piqueiro

corta-fogo para áreas com postos de transformação de energia; separação corta-fogo para áreas com geradores de emergência; etc.;

- Possuírem medidas adequadas para efetuar uma armazenagem segura de substâncias e preparações perigosas, caso existam;
- Dispirem de um sistema de para-raios adequado;
- Limitar-se a utilização de materiais inflamáveis, incluindo na fachada exterior, cobertura, divisões interiores e revestimentos exteriores/interiores, devendo ser mantida uma ficha técnica com as características dos revestimentos.

## 2.4. Sistemas de energia

A Organização deverá providenciar a instalação de sistemas de energia que garantam a segurança e a continuidade das atividades/serviços críticos da Organização.

As infraestruturas da Organização devem ter:

- Geradores elétricos de emergência que possibilitem, em caso de falha da rede pública de energia, a continuidade de fornecimento de energia aos diversos espaços e equipamentos da infraestrutura;
- Sistemas de UPS (Uninterruptible Power Supply) que assegurem a operacionalidade ininterrupta/imediata em caso de falhas (incluindo micro falhas) nos circuitos de energia que alimentam os sistemas informáticos ou sistemas de segurança críticos.

Estes sistemas críticos deverão estar fornecidos por, pelo menos, dois circuitos de energia independentes e alternativos;

- Mecanismos que inibam a sobrecarga e picos de energia nos circuitos de alimentação (estabilizadores de tensão);
- Mecanismos para proteção física das linhas de energia, recorrendo às melhores práticas existentes e/ou recomendadas pelos fornecedores;
- Separação física das linhas de comunicação face às linhas de energia, de forma a evitar a contaminação das linhas de comunicação com o ruído introduzido pela carga eletromagnética das linhas de energia.

## 2.5. Proteção contra incêndio

Nos edifícios e recintos das instalações das Organizações é obrigatória a existência de um responsável pela segurança contra incêndio (RS), a quem compete, entre outros, assegurar a manutenção das condições de segurança contra risco de incêndio e a implementação das medidas de autoproteção durante todo o ciclo de vida das instalações.

A Organização deve manter as condições de segurança contra risco de incêndio, definidas e aprovadas nas medidas de autoproteção e no projeto de segurança contra incêndio ou ficha de segurança (caso exista), sem introduzir quaisquer alterações:



- Ao uso, total ou parcial dos edifícios ou recintos sem que seja dado cumprimento às exigências legais de SCIE, nomeadamente ao projeto de segurança e medidas de autoproteção (se a alteração ao projeto implicar a alteração da categoria de risco ou da utilização-tipo, as medidas de autoproteção devem ser apreciadas pela ANPC);
- Aos meios de compartimentação ao fogo e ao isolamento e proteção, não sendo permitida a abertura de vãos de passagem ou de novas comunicações entre espaços que agravem o risco de incêndio;
- Aos elementos com capacidade de suporte de carga, estanquidade e isolamento térmico, para classes de resistência ao fogo com desempenho inferior ao exigido, que agrave o risco de incêndio;
- Aos materiais de revestimento e acabamento das paredes e tetos interiores, para classes de reação ao fogo inferiores ao exigido, no que se refere à produção de fumo, gotículas ou partículas incandescentes;
- Aos equipamentos e sistemas de segurança contra incêndio, bem como de instalações técnicas com interesse para a segurança contra incêndio de que o edifício disponha e a legislação exija.



Sinalização de segurança – SONAE

A Organização deve ainda:

- Manter as saídas e caminhos/vias de evacuação praticáveis, não trancando, obstruindo ou introduzindo elementos que possam reduzir a respetiva largura;
- Dispor de instalações técnicas, equipamentos e sistemas de segurança em boas condições de funcionamento e manutenção;
- Não ocupar ou usar as zonas de refúgio, se existentes;
- Não armazenar líquidos e gases combustíveis em violação dos requisitos determinados para a sua localização ou quantidades permitidas;
- Não obstruir, reduzir, ocultar ou anular as portas resistentes ao fogo que façam parte dos caminhos de evacuação, das câmaras corta-fogo, das vias verticais ou horizontais de evacuação ou saídas de evacuação.

Recomenda-se que a Organização adote as seguintes boas práticas:

- Quando existam sistemas de controlo de acessos, os mesmos devem ser dotados de dispositivos que, perante situações de emergência, permitam ser desativados/libertados, de modo a permitir a livre circulação dos utilizadores em áreas restritas, caso essas áreas façam parte das vias de evacuação;
- Regras para fumar ou acender qualquer tipo de chama dentro do edifício ou infraestrutura;
- Processos implementados para limitar, autorizar e executar a realização de trabalhos a quente, quando necessários, como por exemplo soldaduras ou outros trabalhos com chama/calor (Procedure for Hot Work).

No âmbito do RJ-SCIE, consoante a utilização-tipo e a categoria de risco da instalação, a organização pode ter a necessidade de solicitar à ANPC, com carácter periódico, a realização de inspeções regulares às suas instalações (cuja periodicidade depende da categoria de risco das mesmas), para verificação da manutenção das condições de segurança contra incêndio e a implementação das medidas de autoproteção.

A Organização deve ter presente que a instalação ou a manutenção dos equipamentos e sistemas de segurança contra incêndio deve ser obrigatoriamente efetuada por entidades registadas na ANPC, de acordo com a Portaria n.º 773/2009, de 21 de julho, que as divulga no seu sítio na internet. O registo obriga ao cumprimento de determinados requisitos que garantem a adequação técnica necessária à realização destas atividades.

## 2.6. Proteção contra inundação

A Organização deverá providenciar a instalação de medidas de segurança contra inundação, de modo a prever e mitigar eventuais danos, caso a criticidade e a localização do edifício ou infraestrutura em causa justifique o investimento nessas medidas.

O conceito de “projetar à prova de inundações” pode ser definido como o conjunto de medidas para reduzir as perdas em zonas inundáveis, durante a ocorrência das inundações. Para tal, podemos considerar medidas do tipo estruturais e do tipo não estruturais. As medidas estruturais são medidas de carácter permanente, nas quais a ação humana modifica o sistema ribeirinho ou costeiro existente na tentativa de minimizar eventos de inundações.

As medidas não-estruturais são as de carácter não permanente, e podem, em conjunto com as estruturais, minimizar significativamente os prejuízos suscetíveis de serem causados às Organizações pelas inundações, muitas vezes com custos avultados.

No que respeita às medidas estruturais, a Organização deve:

- Elevar estruturas existentes que contenham elementos críticos ou construir novas estruturas elevadas ou sobre estacas;
- Construir pequenas paredes ou diques circundando as estruturas;
- Elevar a entrada do edifício ou proteger a entrada com barreiras físicas resistentes à inundação;
- Construir paredes resistentes no exterior do edifício, capazes de resistir à pressão hidrostática, e usar material resistente à água em cotas inferiores à referência de inundação;

No que respeita às medidas não estruturais, a Organização deve:

- Instalar um sistema de deteção de inundação que cubra as áreas da infraestrutura onde esse risco é mais relevante, com alarme e ligação à central de segurança;
- Instalar um sistema de drenagem que inclua corte geral de água e bombas de escoamento de água com descarga para o exterior da infraestrutura.
- Localizar os serviços essenciais (incluindo os associados à rede elétrica) em níveis do edifício ou infraestrutura acima da cota prevista de inundação;
- Implementar regulamentação interna sobre o uso do solo no espaço do edifício ou infraestrutura, por exemplo localizando equipamentos críticos em andares superiores acima da cota prevista de inundação;
- Confinar esses equipamentos em espaços protegidos com barreiras;
- Construir plataformas interiores amovíveis para colocação de equipamentos e conteúdos críticos;
- Instalar vedação temporária ou permanente nas aberturas das estruturas edificadas;

- Instalar barreiras amovíveis de emergência nas portas;
- Instalar tampas em grelhas de ventilação;
- Instalar válvulas de retenção na rede de drenagem;
- Prever mecanismos de tamponamento nas sanitas.

A Organização deverá ainda considerar as seguintes recomendações de carácter geral:

- Executar procedimentos periódicos de prevenção de inundação, tais como a manutenção da cobertura e calhas de escoamento de águas pluviais e a limpeza preventiva de fossas e calhas de escoamento de águas pluviais;
- Integrar no seu planeamento de contingência medidas face ao risco de inundação, incluindo planos de evacuação que definam caminhos a seguir pelos utilizadores do edifício ou infraestrutura, com indicação dos pontos de encontro e locais de refúgio;
- Assegurar a ligação a sistemas externos de alerta precoce para o risco de inundação ou adaptar à sua realidade um que já esteja em utilização;
- Coordenar a resposta com os serviços de emergência e outras entidades participantes no socorro, se uma inundação ocorrer;
- Proceder a formação e treino regular dos procedimentos de evacuação e outros a acionar em caso de inundação.

## 2.7. Proteção contra sismos

A Organização deverá ter em conta medidas e recomendações para reduzir o risco e conter efeitos nas infraestruturas em caso de ocorrência sísmica, quer do ponto de vista estrutural, quer em relação aos equipamentos e elementos não estruturais, caso a localização da infraestrutura em causa justifique o investimento nessas medidas. A implementação de medidas específicas implica um estudo detalhado dos elementos mais críticos da instalação.



Acondicionamento de baterias UPS – NOS



Bastidores – Siemens

No que respeita à componente estrutural, as infraestruturas da Organização devem:

- Dimensionar as estruturas para o risco de sismo ;
- Implementar medidas construtivas antissísmicas adequadas;
- Respeitar a legislação em vigor e eventuais códigos internacionais para a tipologia da infraestrutura em causa, de modo a adequar as medidas construtivas e definir o dimensionamento.

No que respeita aos equipamentos e elementos não estruturais, uma vez que existem omissões na legislação técnica relativa à sua resistência sísmica, e tendo por base estudos já realizados , apresentam-se algumas medidas que as Organizações podem implementar para corrigir vulnerabilidades detetadas, sempre que aplicáveis:

- Melhorar a fixação dos transformadores elétricos, nomeadamente fixar às fundações para o caso dos transformadores poisados no solo, assim como reforçar ligações, postes e fundações, para o caso dos transformadores aéreos;
- Confinar baterias em estruturas fixas ao solo;
- Fixar armários, bastidores, equipamentos de controlo, computadores, écrans, etc.;
- Fixar maquinaria pesada;
- Fixar tetos falsos para resistir a movimentos horizontais;
- Melhorar o travamento transversal de condutas e tubagens;
- Adotar outras medidas em equipamentos ou estruturas individuais que possam ser tomadas, a analisar caso a caso.

A Organização deverá ainda considerar as seguintes recomendações de carácter geral:

- Incluir no seu planeamento de contingência o risco sísmico, identificando vulnerabilidades, sobretudo dos elementos mais críticos da infraestrutura, medidas de redução do risco e procedimentos para resposta em caso de cenário sísmico;
- Assegurar, quando disponíveis no território nacional, a ligação aos sistemas de alerta precoce, que permitam, sempre que aplicável, o fecho automático de sistemas e equipamentos (ou abrandamento do seu funcionamento), bem como avisar os utilizadores da infraestrutura alguns segundos antes do sismo para encontrarem abrigo e tomarem os procedimentos possíveis e adequados para a sua segurança e da infraestrutura;
- Assegurar redundâncias, como por exemplo, backups de informação, centros de controlo alternativos, etc., preferencialmente localizados em zonas do país com menor perigosidade sísmica;
- Ter em atenção situações potenciadoras de fragilidades, devidas às interdependências com outras infraestruturas e atividades;
- Coordenar a resposta com os serviços de emergência e outras entidades participantes no socorro, em caso de ocorrência sísmica;
- Proceder a formação e treino regular sobre a ocorrência de fenómenos sísmicos, destinada aos utilizadores mais frequentes do edifício ou infraestrutura, incorporando comportamentos de autoproteção adequados às características da mesma (rotas de evacuação ajustadas ao fenómeno em presença, pontos de encontro e de refúgio, entre outras medidas).

## 2.8. Proteção contra tsunamis

A Organização que se localizar numa zona suscetível de ser afetada por um tsunami, deverá ter em conta recomendações de minimização de efeitos deste fenómeno, quer para proteção das vidas humanas, que para proteção dos equipamentos.

No que respeita à proteção das vidas humanas, a Organização deve planear, implementar e treinar medidas para desencadear logo após um sismo que possa gerar um tsunami:

- Desenvolver procedimentos de proteção e evacuação prontos a ativar após eventual sinal sonoro, de modo a dirigir os colaboradores e outra população presente para área ou zona não suscetível de ser afetada por tsunami (não esquecer que o melhor aviso para o tsunami é o próprio sismo);
- Desenvolver planos de evacuação adequados, assinalando percursos de evacuação e pontos de encontro no exterior do edifício ou infraestrutura, situados a uma distância e altitude suficientes para que a onda não os atinja (têm que ser estudados antecipadamente);
- Proceder a formação e treino regular dos procedimentos anteriores destinada aos utilizadores mais frequentes do edifício ou infraestrutura;

No que respeita à proteção dos equipamentos, a Organização deve implementar medidas destinadas à minimização de danos, evitando que a água os atinja, tais como:

- Construir proteções para equipamentos importantes, como sejam barreiras, campânulas de proteção ou mesmo enterrar algumas estruturas, como tubagens e condutas;
- Desligar a energia a tudo o que for possível antes de abandonar o local em caso de ocorrência de um tsunami;
- Estudar e implementar outras medidas de forma detalhada e específica, dada a variedade de equipamentos.

Como informação complementar, as Organizações devem estar conscientes que:

- Existem regiões de Portugal Continental que são mais afetáveis por tsunamis, provocados por sismos gerados no mar, por norma a SW do Cabo de S. Vicente (Gorringe);
- As regiões mais afetáveis são o Algarve, Costa Alentejana e Área Metropolitana de Lisboa;
- Estudos existentes estimam os seguintes tempos de chegada para a onda, contados após o sismo:
  - 10-15 minutos no litoral do Algarve (Barlavento);
  - 20-30 minutos na litoral da Área Metropolitana de Lisboa.

## 2.9. Proteção contra intrusão

A Organização deverá providenciar a instalação de sistemas de segurança contra intrusão e roubo, através da implementação de meios humanos, mecânicos e/ou eletrónicos de modo a efetuar a gestão dos acessos, a garantir a segurança do perímetro e a preservar a propriedade privada, física e intelectual.

As Organizações devem ter:

- Um departamento central de segurança, independentemente da sua designação, chefiado por um diretor de segurança devidamente habilitado para o efeito, conforme Lei n.º 34/2013, de 16 de maio, e de um serviço de vigilância dotado de pessoal de segurança privada, devidamente habilitado;
- Regulamentos internos que especificam as medidas de proteção, políticas e operações relacionadas com os sistemas eletrónicos de segurança (modelo de segurança);
- Vigilância humana 24H/TDA (Todos os Dias do Ano) devidamente certificada (nos edifícios ou infraestruturas mais críticas) ou vigilância remota (nas restantes);
- Uma central de segurança ou posto de segurança que coordene a vigilância 24H/TDA;
- Facultativamente, uma redundância para a central de segurança ou posto de segurança;
- Um sistema automático de deteção de intrusão e roubo com capacidade de assegurar eficazmente um nível de proteção global, consoante a regulamentação aplicável, o grau de ameaça e os critérios de segurança exigidos pelos seus clientes, como sejam:
  - O equipamento central do sistema automático de deteção de intrusão e roubo, referido anteriormente, numa área controlada e protegida contra qualquer ataque ou adulterações;
  - O sistema automático de deteção de intrusão e roubo deve ter registo histórico de eventos;
  - O sistema automático de deteção de intrusão e roubo deve ter monitorização na central de segurança ou, em alternativa, ser controlado através de central recetora de alarmes de empresa da especialidade.
- Um sistema automático de controlo de acessos com capacidade de assegurar eficazmente um nível de proteção global das zonas de acesso controlado, limitado ou de proibição, consoante os graus de segurança pretendidos, a regulamentação aplicável, e o grau de ameaça e os critérios de segurança exigidos;
- O equipamento central (CPU) do sistema de controlo de acessos instalado numa área controlada e protegida contra qualquer ataque ou adulterações;
- Um sistema de controlo de acessos dotado obrigatoriamente de mecanismos ou meios que facilitem a saída de pessoas em qualquer situação de emergência;
- Um sistema de controlo de acessos com monitorização na central de segurança ou posto de segurança.



A Organização deve ainda ter:

- A gestão e atribuição dos acessos a residentes e visitantes efetuada por uma área de credenciação mediante critérios e políticas internas de segurança previamente definidas;
- Os acessos físicos aos edifícios ou infraestruturas classificadas de Acesso Interno equipados com mecanismos de autenticação e registo (por ex. receção/segurança, cartões de acesso, códigos de acesso, listas de autorização permanente), que permitam controlar e auditar os acessos efetuados;
- Os acessos físicos aos espaços classificados como Acesso Restrito obrigatoriamente controlados através de mecanismos de autenticação forte que garantam a identidade do utilizador assim como o registo individual dos utilizadores;
- Os restantes equipamentos de segurança instalados em locais dotados com monitorização e controlo de acessos;
- Um sistema de circuito fechado de televisão (CFTV), autorizado pela Comissão Nacional de Proteção de Dados (CNPD), com capacidade de assegurar eficazmente a monitorização e a gravação do perímetro exterior, dos pontos de acesso controlados no interior e todas as áreas protegidas ou críticas, e com monitorização/controlo na central de segurança ou posto de segurança;
- Os equipamentos de gravação do sistema de CFTV instalados numa área controlada e protegida contra qualquer ataque ou adulterações;
- Acautelada a proteção de documentação física sensível, classificada como confidencial ou secreta, num cofre ou casa forte com grau de resistência III, com referência às normas EN 1143-1 e EN 1300;
- Acautelada a guarda de numerário ou outros objetos de valor num cofre ou casa forte com um grau de resistência V, com referência às normas EN 1143-1 e EN 1300.

A Organização deve ainda:

- Atribuir um nível de classificação a cada infraestrutura/espço, de acordo com o respetivo grau de criticidade e propósito de utilização. Apresenta-se um exemplo de possíveis níveis e designações:
  - Acesso Público – O acesso é permitido a todos os utilizadores da infraestrutura e a entidades externas (clientes, visitantes, etc.). Exemplos de edifícios/áreas: receções, lojas, etc.;
  - Acesso Interno – O acesso é permitido à generalidade dos Colaboradores e aos Prestadores de Serviço autorizados. Exemplos de infraestruturas/espços: interior dos edifícios administrativos, áreas de trabalho, etc.;
  - Acesso Condicionado – O acesso só é permitido a Colaboradores e a Prestadores de Serviço autorizados, condicionado a um determinado conjunto de áreas ou funções e/ou à necessidade de acesso a este tipo de espaços. Exemplos de infraestruturas/espços: salas da Administração, salas específicas da atividade da

Organização, etc.;

- Acesso Restrito – O acesso deve ser restrito apenas aos Colaboradores e aos Prestadores de Serviço identificados individualmente numa lista de acessos autorizados para o espaço. Exemplos de infraestruturas/espços: Data Centers, Sala de Vigilância, etc.
- Mandar efetuar inspeções regulares (anuais) aos sistemas anteriormente referidos por empresa credenciada;
- Adotar medidas de proteção física e procedimentos de segurança que assegurem a salvaguarda dos bens contra um determinado quadro de ameaça aplicável;
- Ter barreiras de proteção que definam o limite físico das infraestruturas e formem um perímetro de segurança às áreas controladas, limitadas ou de exclusão;
- Garantir um grau de resistência dos materiais de construção (portas, paredes, teto, janelas), nas áreas consideradas críticas, de modo a ter um nível de proteção adequado face a uma potencial ameaça;
- Proteger com barreiras físicas e iluminação de segurança as portas ou as entradas do perímetro;
- Proteger com segurança humana (e cumulativamente com CFTV, controlo de acessos e barreiras físicas) as entradas do perímetro seguro;
- Ter um local adequado e meios eficazes para controlo da correspondência recebida, garantindo a confidencialidade da mesma;
- Implementar medidas para proteção dos seus sistemas de informação críticos mitigando a eventual ocorrência de ciberataques.

## 2.10. Formação e exercícios

A Organização deve proporcionar aos seus colaboradores:

- Formação obrigatória em utilização dos equipamentos de combate a incêndios (extintores e mangueiras de combate a incêndios);
- Formação obrigatória em evacuação dos edifícios ou infraestruturas, de modo a saírem de forma organizada em caso de evacuação;
- Informação sobre comportamentos seguros e resilientes, medidas de autoproteção e procedimentos adequados a ter para diferentes situações de acidente grave ou catástrofes;
- Outras informações e/ou formações complementares na área da segurança em ambiente profissional e/ou doméstico, como por exemplo sensibilização em primeiros socorros e suporte básico de vida, medidas de autoproteção contra sismos e tsunamis, acidentes geomorfológicos ou incêndios.

A Organização deve promover:

- Exercícios de evacuação (por ex. anuais) onde se possa aferir a formação dada;
- Exercícios para testar os procedimentos de coordenação e execução previstos nos seus planos de emergência internos, quer ao nível da estrutura interna da





Simulacro – CGD

Organização, quer na articulação com entidades externas intervenientes na resposta em termos de proteção e socorro;

- Testes e verificações regulares (por ex. mensais), pela própria Organização ou por entidade subcontratada, do estado de conservação/operacionalidade dos equipamentos e sistemas de segurança existentes;
- Auditorias/inspeções regulares (por ex. anuais), por entidade independente e devidamente credenciada, aos equipamentos e sistemas de segurança anteriormente referidos;
- A manutenção dos registos e evidências da execução dos programas de manutenção e de testes;
- Participar em exercícios com a proteção civil e promover a realização de exercícios envolvendo os principais Fornecedores e/ou com os Prestadores de Serviço chave para a atividade.

### 3. GESTÃO DA CONTINUIDADE DE NEGÓCIO

O(s) plano(s) de continuidade de negócio e de gestão de crise devem conter medidas eficazes para garantir a continuidade das atividades/serviços críticos da Organização e para proteger as pessoas, ativos físicos, valor financeiro, reputação e capital social da Organização.

A Organização deve ter:

- Uma política de gestão de crise e de continuidade de negócio que define a responsabilidade de liderança e a linha organizacional em caso de emergência, de modo a torná-la mais resiliente;
- Um plano de gestão de crise e de continuidade de negócio fiável que lhe permita continuar a desenvolver a sua atividade em caso de crise;
- Planos para lidar com a rutura e com a capacidade de responder a acontecimentos imprevistos;
- A capacidade de se adaptar com sucesso quando o(s) plano(s) existente(s) não se enquadra(m) nos acontecimentos que estão a ocorrer;
- Mecanismos eficazes que identifiquem os riscos atuais e futuros, e que permitem desenvolver uma estratégia e os planos necessários aos riscos identificados;
- Uma estrutura interna que se dedique à avaliação, gestão e controlo de riscos de forma sistémica;
- Responsáveis pela implementação da resiliência organizacional com acesso direto para comunicar com a gestão de topo da Organização;
- Um planeamento para atuação em crise, com normas, procedimentos e regras claras que definem exatamente as atribuições de cada membro envolvido;
- Um (ou vários) local alternativo para poder continuar a operar, após uma situação de crise ter inviabilizado as suas infraestruturas;
- Um plano de transporte para os locais alternativos dos seus colaboradores chave;
- Um plano de comunicação que permita o contacto com os seus colaboradores-chave em caso de crise;
- Os seus dados críticos, e os dos seus clientes, disponíveis para serem utilizados em situação de crise, através de backups ou de outras soluções de resiliência;
- A existência de meios de comunicação alternativos (voz, internet, etc.);
- Identificados os fornecedores de serviços críticos e garantir que estes têm a capacidade de continuar a cumprir contratos de fornecimento de bens e serviços mesmo em situação de crise.

A Organização deve ainda assegurar que:

- Possui processos de Gestão da Continuidade de Negócio alinhados com as melhores práticas e normas internacionais (por ex. a norma ISO 22301 – Business Continuity Management);
- Possui técnicos devidamente formados na estrutura

interna que se dedica à avaliação, gestão e controlo dos riscos de Continuidade;

- Os procedimentos que tornam a Organização mais resiliente estão alinhados e são eficazes e eficientes para o(s) tipo(s) de risco que se pretende anular/minimizar;
- A abordagem à resiliência da Organização satisfaz, é coerente e está integrada no planeamento operacional interno;
- Os colaboradores possuem a formação e o treino sobre preparação e resposta a acidentes graves e catástrofes;
- Testa frequentemente os seus planos de gestão de crise;
- Audita as suas capacidades de resiliência.

## 4. GESTÃO DE SEGUROS

### 4.1. Tipos de seguros

TIPOS DE SEGUROS	EXEMPLOS	COBERTURAS DE RISCOS
<b>Património</b>	<b>(danos próprios)</b>	<b>Aplicável a danos físicos ou destruição</b>
<b>Geral</b>	<b>Edifícios/infraestruturas (bens imóveis)</b>	<ul style="list-style-type: none"> <li>– Deve cobrir riscos tais como incêndio/explosão, inundação, atos da natureza, sismo, quedas/quebras, furto/roubo, vandalismo/sabotagem, tumultos, privação de uso local arrendado, avarias mecânicas de máquinas, etc. ;</li> <li>– Em bens próprios, arrendados, leasing;</li> <li>– Em bens de terceiros confiados (só cobre quando declarados).</li> </ul>
	<b>Equipamentos (bens móveis)</b>	
	<b>Existências</b>	
<b>Específicas</b>	<b>Equipamento eletrónico</b>	<ul style="list-style-type: none"> <li>– Permite franquias menores;</li> <li>– Permite cobrir danos em equipamentos de terceiros em edifícios ou infraestruturas da Organização;</li> <li>– Permite cobrir equipamentos em locais específicos (por ex. em stands móveis).</li> </ul>
	<b>Roubo</b>	<ul style="list-style-type: none"> <li>– Permite franquias menores;</li> <li>– Permite incluir coberturas específicas com por ex. roubo de valores (dinheiro, cheques, etc.) ou roubo de equipamentos expostos numa loja.</li> </ul>
	<b>Multirriscos comerciais</b>	<ul style="list-style-type: none"> <li>– Permite franquias menores;</li> <li>– Permite incluir coberturas específicas com por ex. infraestruturas, equipamentos e existências em lojas ou determinadas localizações da Organização.</li> </ul>
	<b>Existências logística</b>	<ul style="list-style-type: none"> <li>– Permite incluir coberturas específicas com por ex. equipamentos e existências das Organização que estejam armazenados em edifícios ou infraestruturas de um operador logístico.</li> </ul>
	<b>Terrorismo</b>	<ul style="list-style-type: none"> <li>– Permite incluir a cobertura de terrorismo que habitualmente está excluída da apólice de património geral;</li> <li>– Este seguro é cada vez mais relevante para Organizações com infraestruturas críticas e/ou grande projeção nacional.</li> </ul>
<b>Perdas de Exploração</b>	<b>(danos próprios)</b>	–
<b>Lucros Cessantes</b>	–	<ul style="list-style-type: none"> <li>– Aplicável a causas físicas associadas a património (por ex. incêndio);</li> <li>– Cobre a margem bruta perdida durante o período de interrupção de atividade da Organização;</li> <li>– Cobre apenas danos próprios, não cobre danos em clientes;</li> <li>– A franquia é habitualmente definida em nº horas de interrupção (por ex. 4h, 24h, 48h);</li> <li>– É fundamental que a Organização adeque a franquia ao património afetado.</li> </ul>
<b>Interrupção de Negócio</b>	–	<ul style="list-style-type: none"> <li>– Aplicável a causas físicas (por ex. incêndio) e não físicas (por ex. falha de tecnologia ou de fornecimento de utilities);</li> <li>– Cobre a margem perdida durante o período de interrupção e deve cobrir, idealmente, a margem perdida futura (por ex. resultante da perda de clientes e respetiva receita futura);</li> <li>– Cobre danos próprios por interrupção de negócio e perdas catastróficas, não cobre danos em clientes;</li> <li>– É uma apólice pouco usual e cujas condições são difíceis de definir, pelo que as Organizações devem explorar a viabilidade deste seguro com seguradoras.</li> </ul>

TIPOS DE SEGUROS	EXEMPLOS	COBERTURAS DE RISCOS
<b>Responsabilidade Civil</b>	<b>(danos em terceiros)</b>	<b>Aplicável apenas a danos com causas físicas</b>
<b>Geral</b>	<b>Responsabilidade Civil Exploração</b>	<ul style="list-style-type: none"> <li>– Aplicável a atos, erros ou omissões no exercício da atividade empresarial com danos físicos causados a terceiros (pessoas, bens e edifícios);</li> <li>– Responsabilidade por situações de acidente ou negligência (sem dolo) de atos praticados por colaboradores/subcontratados;</li> <li>– Cobre as atividades de exploração da Organização (não cobre todas as necessidades de empresas de serviços);</li> <li>– Pode cobrir danos físicos em bens públicos ou privados durante construções/installações de infraestruturas (por ex. condutas, cabos, etc.) e cobrir danos pessoais ou patrimoniais em clientes (por ex. provocados por equipamentos);</li> <li>– No caso de atividades subcontratadas, esta responsabilidade e a obrigatoriedade de efetuar o seguro devem preferencialmente ser exigidas ao fornecedor/parceiro via contrato de serviços.</li> </ul>
<b>Específicas</b>	<b>Responsabilidade Civil Produto</b>	<ul style="list-style-type: none"> <li>– Cobre “produtos físicos” produzidos pela Organização (por ex. equipamentos de marca própria);</li> <li>– Pode cobrir custos de recolha e/ou desmontagem dos produtos.</li> </ul>
	<b>Responsabilidade Civil Ambiental</b>	<ul style="list-style-type: none"> <li>– Cobre riscos de impacto ambiental (danos ambientais) no solo, na água e na biodiversidade, de forma a cumprir com a legislação aplicável;</li> <li>– Pode cobrir derrames de combustíveis em depósitos e outras substâncias perigosas, provenientes de geradores, baterias e de armazenamento de outros produtos químicos;</li> <li>– É uma cobertura específica, habitualmente não incluída por defeito na apólice de Responsabilidade Civil Geral;</li> <li>– Para além de garantir os danos provocados no património de terceiros pelos riscos de poluição súbita e acidental (imprevista), poderá ser necessário um seguro (ou garantia bancária) para cobrir também o custo de medidas de prevenção e reparação das consequências da poluição.</li> </ul>
<b>Responsabilidade Civil Profissional</b>	<b>(danos em terceiros)</b>	<ul style="list-style-type: none"> <li>• <b>Inclui causas não físicas: atos intelectuais, conceção e arquitetura, gestão de serviços, etc.;</b></li> <li>• <b>Relacionado com as atividades soft das Organizações, sendo mais adequado para os setores de serviços.</b></li> </ul>
<b>Responsabilidade Geral</b>	–	<ul style="list-style-type: none"> <li>– Aplicável a atos, erros ou omissões no exercício da atividade empresarial com danos para terceiros;</li> <li>– Responsabilidade por situações de acidente ou negligência (sem dolo) de atos praticados por colaboradores/subcontratados;</li> <li>– Tem de existir uma reclamação escrita de cliente/terceiro;</li> <li>– A responsabilidade é derivada da relação contratual (por ex. vender um serviço a um cliente ou comprar um fornecimento a um terceiro);</li> <li>– Deve cobrir o atraso na entrega de bens/serviços ou não cumprimento de requisitos que pode provocar perdas de exploração em clientes (por incumprimento do contrato);</li> <li>– Pode cobrir violações de privacidade por perda, roubo ou uso indevido de informação de clientes causadas pela Organização ou por terceiros (por ex. por um hacker);</li> <li>– No caso de atividades subcontratadas, esta responsabilidade e a obrigatoriedade de efetuar o seguro devem preferencialmente ser exigidas para o fornecedor/parceiro via contrato de prestação de serviços.</li> </ul>
<b>Proteção Específica</b>	<b>(danos em terceiros e danos próprios)</b>	<ul style="list-style-type: none"> <li>– Aplicável a atos, erros ou omissões no exercício da atividade empresarial;</li> <li>– Pode ser composto por vários módulos específicos: Módulo de Responsabilidade por Subcontratação que é relevante para Organizações que prestam Managed Services para clientes empresariais; Módulo de Proteção da Informação que cobre danos próprios e é relevante para Organizações de setores tecnológicos ou de outros setores que tratam muitos dados pessoais de clientes; Módulo de Cibersegurança que cobre danos próprios e que é relevante para empresas tecnológicas.</li> </ul>

TIPOS DE SEGUROS	EXEMPLOS	COBERTURAS DE RISCOS
Crime	(danos próprios)	Aplicável apenas a danos com causas físicas
<b>Fraude em Serviços</b>	–	<ul style="list-style-type: none"> <li>– Aplicável a atos praticados por clientes ou terceiros (fraudsters)</li> <li>– Pode cobrir danos decorrentes da utilização fraudulenta ou abusiva de serviços prestados pela Organização (por ex. cliente pratica fraude) ou de sistemas de informação da Organização (por ex. fraudulento aproveita potenciais vulnerabilidades dos standards tecnológicos)</li> <li>– Cobre impactos financeiros e operacionais (por ex. custos operacionais, custos a pagar a outras Organizações, etc.).</li> </ul>
<b>Fraude/ Infidelidade de Colaboradores</b>	–	<ul style="list-style-type: none"> <li>– Aplicável a atos intencionais de colaborador/subcontratado que prejudicam a Organização (pressupõe dolo)</li> <li>– Pode cobrir contrafação, furto, fraude na transferência de fundos; dano, destruição ou desaparecimento de dinheiro/títulos; uso impróprio, ou não autorizado, de recursos da Organização por parte de um funcionário.</li> </ul>
<b>Proteção da Informação (roubo ou uso indevido)</b>	–	<ul style="list-style-type: none"> <li>– Aplicável a atos praticados por terceiros (não são colaboradores nem subcontratados da Organização);</li> <li>– Cobre danos decorrentes do roubo ou uso indevido de informação de negócio ou de clientes;</li> <li>– Pode cobrir perda de informação nos sistemas, quebra de confidencialidade/privacidade; roubo ou fuga de informação; informação de negócio ou de clientes (por ex. registos de transações, dados de clientes, nº cartões crédito, etc.);</li> <li>– É uma apólice pouco usual, pelo que as Organizações devem explorar a viabilidade deste seguro com seguradoras.</li> </ul>

#### 4.2. Boas práticas

A Organização deve ainda assegurar boas práticas nos seus processos de gestão de seguros, tais como:

- Uniformizar o portfólio de seguros e apólices entre as diversas subsidiárias ou localizações da Organização, beneficiando do melhor conhecimento das apólices que uma uniformização permite;
- Otimizar o mix de coberturas, de capitais e de franquias, sem contudo fazer aumentar os custos das apólices;
- Ajustar os valores dos capitais cobertos e/ou das franquias, tendo em conta, por exemplo:
  - no seguro de património, rever proactivamente e periodicamente o património a segurar e os respetivos critérios de valorização (de edifícios, equipamentos, etc.), de modo a assegurar a existência de um "custo de reposição em novo" que seja realista e adequado à substituição do património em caso de sinistro com perda total ou quase total;
  - no seguro de património, declarar obras e benfeitorias, mas não declarar equipamentos que estejam obsoletos ou que estejam à consignação;
  - no seguro de património, efetuar uma análise aprofundada do património declarado por cada subsidiária e por cada local de risco, de modo a evitar declarar itens que fiquem abaixo das franquias;
  - no seguro para Perdas de Exploração, rever os critérios de cálculo dos lucros cessantes e negociá-los com a seguradora.

- Contratar seguros adequados à "grandeza do risco", tendo em conta, por exemplo:
  - que os limites de cobertura contratados podem não ser suficientes para cobrir "riscos catastróficos" que afetem uma determinada zona (por ex. sismo que afete vários edifícios numa zona suscetível de sismos), devendo os limites ser aumentados para esses riscos em particular;
  - que as coberturas contratadas podem ser adequadas para cobrir "riscos maiores" em localizações independentes (por ex. incêndio ou explosão num determinado edifício), desde que os sinistros sejam independentes e não ocorram no mesmo período temporal;
  - que uma apólice de património geral pode não ser adequada para cobrir "riscos menores" em determinadas localizações de risco (por ex. roubo em loja), podendo ser mais adequado uma apólice específica (por ex. seguro multiriscos ou seguro de roubo).
- Avaliar a pertinência de informar as seguradoras acerca das alterações ao perfil de risco, ainda que temporárias, de modo a evitar recusas de indemnização em caso de sinistro. No caso de algum equipamento de proteção e segurança ficar impedido de funcionamento, mesmo que temporariamente, esse risco deverá ser identificado. Para tal, a Organização deve implementar um procedimento que é habitualmente conhecido pelas seguradoras como "Procedure for Impairments to Protective Systems".





# **PARTE III**

## **Aplicação de Boas Práticas de Resiliência**

Edifício da Siemens

A implementação das boas práticas referenciadas na Parte I e na Parte II deste Manual são concretizáveis de diferentes formas, sendo, no entanto, a maioria de aplicabilidade transversal aos diversos setores dos operadores de infraestruturas críticas.

Nesta Parte são apresentados casos reais de iniciativas levadas a cabo por diferentes Organizações, que são um exemplo prático do aumento da resiliência.

## PROGRAMA CAIXA SEGURA

O Programa Caixa Segura da Caixa Geral de Depósitos tem como visão dotar todos os empregados do grupo CGD do conhecimento e treino de segurança que potencie as boas práticas e que conduza a uma cultura de segurança global, minimizando assim o risco. Está alicerçado em espaços físicos de formação, sensibilização e informação sobre questões de segurança, nos edifícios centrais de Lisboa e Porto.

Nestes espaços, elementos do Gabinete de Prevenção e Segurança (GPS) e profissionais do setor da segurança privada pertencentes ao Grupo de Intervenção para Emergências (GIE), com formação avançada em socorrismo e extinção de incêndios ministram formação aos residentes do(s) edifício(s) (Colaboradores diretos e contratados) no primeiro dia de trabalho no edifício (Visita Segura), inseridos no processo de acolhimento e credenciação. Este programa proporciona também aos colaboradores e respetivos familiares formação em extinção de incêndios, socorrismo, evacuação de edifícios, riscos e medidas preventivas em situações de acidente grave ou catástrofe natural ou antropogénica, num total de mais de vinte riscos diferentes.

É também neste local que se formam e gerem os elementos dos Grupos de Primeira Intervenção (GPI) e de Equipas de Resposta a Emergência (ERE) – Colaboradores com formação diferenciada nas áreas do socorrismo e combate a incêndios – que atuam no primeiro alarme em caso de acidente grave ou catástrofe.

Conta-se também com parcerias com o Regimento de Sapadores Bombeiros (RSB) e Serviço Municipal de Proteção Civil (SMPC) de Lisboa que complementam a formação teórica com aulas práticas sobre as medidas de autoproteção relativas aos riscos identificados.

Para mais informação:  
José Manuel Gonçalves  
[gps.secretariado@cgd.pt](mailto:gps.secretariado@cgd.pt)  
[www.cgd.pt](http://www.cgd.pt)



Diagrama do Programa Caixa Segura.



Local onde são ministradas as formações no Edifício Sede da CGD.

## RISCO

O GPS consciente dos riscos coletivos a que os residentes da CGD estão expostos, sentiu a necessidade de transmitir aos Colaboradores e residentes dos edifícios centrais, formação relativa a comportamentos seguros e respetivas medidas de autoproteção inerentes a situações de acidente grave ou catástrofe, de como atenuar os seus efeitos e como proteger as pessoas e outros ativos quando ocorram situações de perigo.

## AÇÃO

O Conceito Caixa Segura levou à criação de um Programa adequado à formação, desenvolvimento de conteúdos formativos que expusessem os riscos e as medidas de autoproteção adequadas. Envolveram-se os meios humanos internos, credenciados para a realização das ações de formação, complementados por formadores externos do RSB e SMPC de Lisboa, com o objetivo de ampliar a cultura de segurança na Caixa Geral de Depósitos.

## IMPACTO

A consciencialização coletiva ao grau de exposição ao risco a que as pessoas da organização se encontram expostas e, as medidas de autoproteção preconizadas, criam maior confiança na reação a catástrofes, evitando assim o pânico. Utilizou-se ainda a capacidade de formação instalada para ministrar ações de formação específicas aos descendentes dos Colaboradores da CGD (férias escolares). Na Rede Comercial, a formação de cariz safety foi complementada com medidas de prevenção de cariz security.

## RESULTADO

Aumento da cultura de segurança no Universo CGD, que se propaga para as famílias dos Colaboradores. Melhor desempenho nos simulacros organizados pelo GPS, e que envolvem os agentes de Proteção Civil (APC). O sucesso do Programa Caixa Segura levou a CGD a expandir o programa a um agrupamento escolar vizinho.

## LIÇÕES APRENDIDAS

A formação em prevenção contra catástrofes naturais ou antropogénicas aos Colaboradores, aliada à instalação de dispositivos de segurança adequados, deverá ser sempre considerada um investimento que auxilia as empresas a tornarem-se mais resilientes e preparadas para enfrentar uma qualquer situação catastrófica.

## CASO DE NEGÓCIO

A formação em medidas de prevenção contra catástrofes naturais ou antropogénicas são determinantes para a resiliência dos Colaboradores da CGD, dado que lhes permitirá ultrapassar, devidamente organizados, um evento catastrófico, e tendo como principal objetivo a salvaguarda da vida humana, ajudando também a cumprir os designios da Caixa Geral de Depósitos, manter o negócio, mesmo em face de situações adversas.

## OPORTUNIDADES DE REPLICAÇÃO

Para as empresas que pretendam implantar uma cultura de segurança, formando os seus Colaboradores em medidas de prevenção contra catástrofes naturais ou antropogénicas, o Programa Caixa Segura da Caixa Geral de Depósitos poderá constituir um guia para a sua implementação, e caso assim o pretendam, a CGD poderá partilhar o seu conhecimento, nestas matérias, com os interessados.

## COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

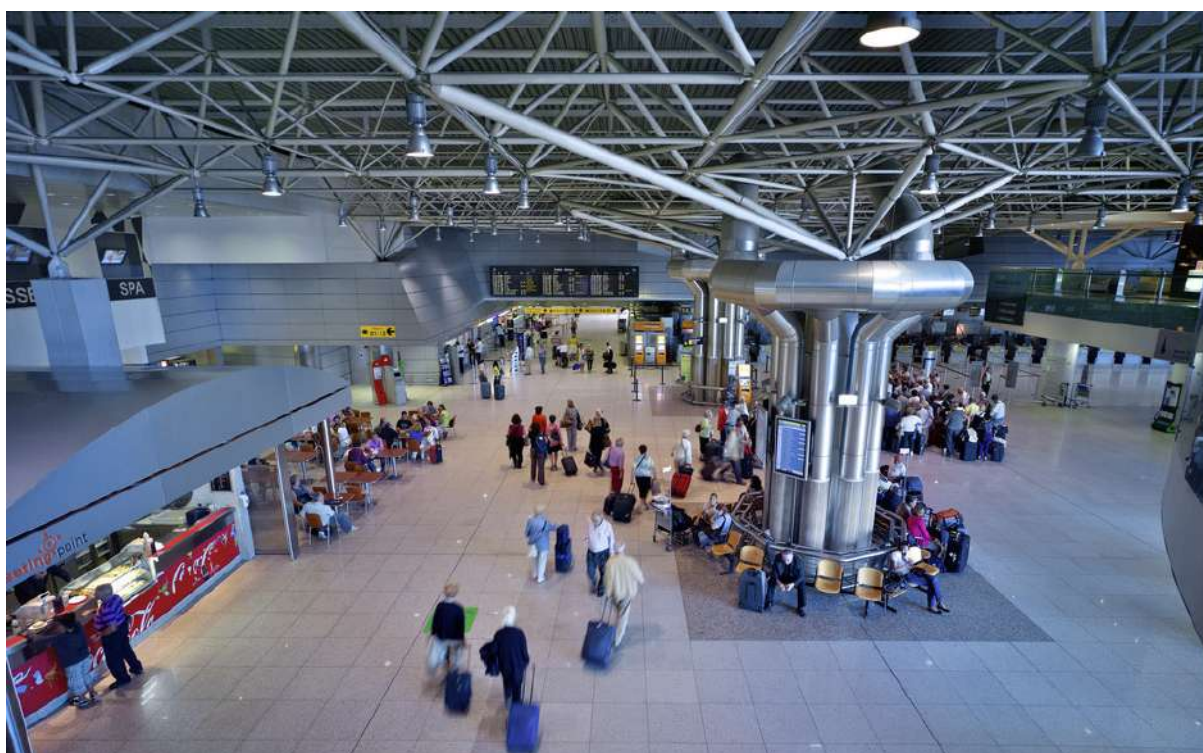
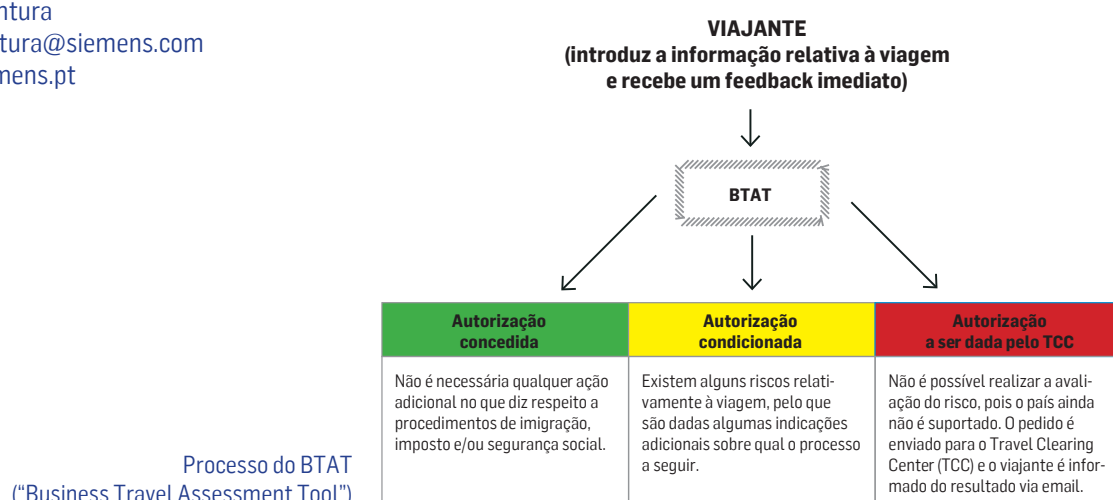
1	Redução da mortalidade induzida por desastre até 2030		A transmissão de conhecimentos relativos a medidas de autoproteção contra catástrofes naturais ou antropogénicas aos Colaboradores da CGD e outros residentes cria um efeito de cascata permitindo que estes conhecimentos sejam aplicados não só nas horas de serviço normais, mas também nos períodos de ausência, com as respetivas famílias e amigos. Com esta formação específica ministrada pela "Caixa Segura" pretende-se que os Colaboradores da CGD, face a situações de emergência, consigam ultrapassar comportamentos de pânico e assumam comportamentos organizados e treinados, reduzindo assim o número de potenciais vítimas.
2	Reduzir o número de pessoas afetadas até 2030	X	
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a disrupção de serviços básicos até 2030	X	
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		



## SISTEMA DE APOIO AO COLABORADOR EM VIAGEM

Na atualidade, a atividade comercial das organizações determina deslocações frequentes dos seus colaboradores tanto no território nacional, como internacional, sendo que, no caso de viagens para outros países, estas devem ser realizadas atendendo à especificidade e regulamentos desses locais, com o objetivo de proteger os colaboradores dos riscos relacionados quer com as viagens, mas também durante a permanência e/ou o trabalho no dia-a-dia quando deslocados. Deste modo devem ser estabelecidas medidas que passem pela definição, criação e implementação de processos, aplicáveis a toda a empresa, necessários para atingir convergência entre unidades no que toca à segurança.

Para mais informação:  
Jorge Ventura  
jorge.ventura@siemens.com  
www.siemens.pt



Aeroporto Humberto Delgado – Lisboa



RISCO	AÇÃO	IMPACTO	RESULTADO
Ao viajar, as pessoas podem ficar expostas a riscos maiores do que os existentes no seu local de origem, mas também a novos riscos. Para além das condições diferentes em termos de clima, fuso horário e altitude, os colaboradores devem atender a todos os outros aspetos legais e culturais dos locais para onde viajam, uma vez que os mesmos contribuem para a exposição ao risco e vulnerabilidade dos colaboradores, o que poderá condicionar ou mesmo inibir a persecução das atividades comerciais e consequentemente dos negócios.	De forma a assegurar a segurança dos viajantes, foram implementados regulamentos de viagem obrigatórios aplicáveis a determinados países, devido à situação atual do mesmo ou ao tipo do país. Para implementação dos regulamentos, avaliação de risco, verificação e adoção de ações adequadas, o processo é suportado em diversas ferramentas de controlo e registo. O módulo "Travel Security" inclui informações sobre cada país, o "procede à avaliação de risco e a ferramenta ADLER permite a avaliação do risco.	Na eventualidade de acontecimento de alguma situação crítica que altere as condições locais e que exponha os colaboradores a situações extremas (que coloquem em causa a sua saúde e/ou segurança), é necessário possuir, para além de informação em tempo real sobre a localização dos colaboradores, meios disponíveis e acessíveis que permitam retirar as pessoas para locais seguros.	Nos casos de: Autorização Concedida Não é necessária qualquer ação adicional no que diz a procedimentos de imigração, imposto e/ou segurança social; Autorização Condicionada Existem alguns riscos relativamente à viagem, pelo que são dadas algumas indicações adicionais sobre qual o processo a seguir; Autorização a ser dada pelo TCC Não é possível realizar a avaliação do risco, pois o país ainda não é suportado. O pedido é enviado para o Travel Clearing Center (TCC) e o viajante é informado do resultado via eMail.

### LIÇÕES APRENDIDAS

O registo sobre situações ocorridas, a partilha com as outras unidades da organização e a observação em tempo real das condições existentes em cada localização, devem ser utilizados como critérios de identificação dos riscos e consequentemente da definição de medidas preventivas que assegurem a segurança das pessoas em viagem e quando deslocadas.

### CASO DE NEGÓCIO

A avaliação das condições a obedecer noutras geografias, bem como a respetiva avaliação dos riscos da deslocação, determinam as medidas adequadas a respeitar em caso de viagem. Deste modo, reúnem-se as melhores condições de deslocação e estadia, permitindo realizar as atividades de negócio em perfeito conhecimento das necessidades locais e com os colaboradores em segurança. A adoção de medidas preventivas adequadas a cada necessidade, previne e evita a ocorrência de danos, sendo que a não ocorrência dos mesmos constitui benefícios imediatos e duradouros.

### OPORTUNIDADES DE REPLICAÇÃO

A implementação deste processo teve início nos serviços centrais da sede internacional da organização, tendo sido gradualmente replicada em todas as unidades locais, entenda-se países. O cariz internacional da organização e a participação e intercâmbio continuado de todas as unidades, permite reproduzir rapidamente os processos e introduzir melhorias constantes e em tempo real que melhor respondem aos requisitos, porém idêntico conceito e processos podem ser implementados em qualquer tipo e dimensão organizacional.

### COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

1	Redução da mortalidade induzida por desastre até 2030		As pessoas são um bem de valor incalculável, pelo que assegurar a sua proteção, segurança e até conforto, em todas as circunstâncias, é crucial para que estas possam realizar as suas atividades em condições adequadas, de modo a acrescentar valor a clientes, parceiros e à sociedade em geral.
2	Reduzir o número de pessoas afetadas até 2030	X	
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a interrupção de serviços básicos até 2030		
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		

## INSTALAÇÃO DE SISTEMAS DE ALERTA E FECHO AUTOMÁTICO DE CÉLULAS DE RESERVATÓRIOS DE ÁGUA

Em Portugal Continental as regiões classificadas com suscetibilidade elevada a sismos distribuem-se maioritariamente nos distritos de Lisboa, Setúbal, Santarém, Beja e Faro. A ocorrência de um evento de elevado impacto representa, para a sociedade, perdas económicas e humanas consideráveis e consequentemente danos significativos nos principais elementos estruturais expostos à ameaça. A EPAL é responsável pela distribuição de água potável à cidade de Lisboa através de uma infraestrutura de distribuição de água com mais de 1400 km de extensão. As origens da água encontram-se a dezenas de quilómetros da cidade, situando-se a principal, Castelo do Bode, a cerca de 100 km. Sendo o abastecimento de água essencial à sociedade, e sendo impossível determinar num evento desta natureza, as infraestruturas afetadas, dimensão e impacto, o projeto tem como objetivo cativar o maior volume de água na cidade, junto da população abastecida, permitindo garantir de forma racionada a distribuição de água enquanto as infraestruturas afetadas não são reabilitadas. Assim, o projeto define 3 modos de isolamento de células de reservatórios previamente identificadas cujo fecho intempestivo não coloca o sistema em perigo. Através de "botão de pânico", acionar à distância o fecho simultâneo de todas as células; acionamento de todas as células através da deteção simultânea de dois sismógrafos e isolamento individualizado de cada célula por comando do autómato local por nível mínimo.

Para mais informação:  
[responsavel.seguranca.epal@adp.pt](mailto:responsavel.seguranca.epal@adp.pt)  
[www.epal.pt](http://www.epal.pt)



Em cima à esquerda: Cobertura de reservatório;  
Em cima à direita: Interior de reservatório;  
Em baixo à esquerda: Equipamento de deteção sísmica;  
Em baixo à direita: Válvulas elétricas para fecho automático de célula do reservatório para retenção de reserva de água.

## RISCO

A vulnerabilidade sísmica está relacionada com a capacidade que um determinado elemento tem, para resistir ou para ser afetado pelo perigo sísmico, e com a severidade da ação do sismo. Qualquer infraestrutura de abastecimento de água está sujeita a este risco, desde a captação, tratamento, transporte, elevação, reserva e distribuição, não sendo possível prever as zonas mais afetadas por um sismo, dada a imprevisibilidade associada a este tipo de fenómeno.

## AÇÃO

Perante a imprevisibilidade do impacto de um sismo, há que desenvolver ações que permitam armazenar o máximo de água junto dos locais de consumo para garantir o abastecimento de água durante o período de reabilitação das infraestruturas afetadas. Perante a gravidade dos danos causados, proceder-se-á à racionalização da água a distribuir com o apoio das entidades competentes. A maximização da reserva de água está condicionada pela segurança do próprio sistema de abastecimento, não sendo possível fechar todas as células dos reservatórios sem que antes sejam tomadas várias medidas de paragem do sistema, que possui uma enorme inércia e importa acautelar para evitar males maiores. Assim, foram criados automatismos onde há um compromisso entre o volume de reserva e a segurança do sistema. Os automatismos procuram responder a várias dificuldades que surjam ao nível de falhas de comunicações e de energia elétrica.

## IMPACTO

A perda de reservas de água por não fecho oportuno dos reservatórios, associado a uma falha grave do sistema adutor, resulta na interrupção do fornecimento de água à população e órgãos vitais da sociedade, que pode durar várias horas ou dias. Numa ocorrência sísmica, com incidência em várias instalações em simultâneo, na cidade de Lisboa, os tempos de reposição de água poderão ser amplamente ultrapassados, pelo que é essencial a adoção de medidas preventivas que minimizem o impacto causado e de retenção de reservas estratégicas.

Com a aplicação desta medida (sistemas de alerta para fecho automático na ocorrência de eventos sísmicos) pretende-se maximizar as reservas nos sistemas de abastecimento que possam vir a sofrer quando sujeitos a eventos de elevado impacto.

## RESULTADO

Nas zonas sísmicas de maior criticidade e de maior concentração populacional, identificadas como prioridade, pretende-se maximizar a reserva disponível em todos os reservatórios. O estabelecimento de novas medidas terá em consideração o risco sísmico, garantia do máximo de reservas de água, e prevenção de componentes críticas no sistema de abastecimento de água de forma a permitir a manutenção e reposição célere do abastecimento de água numa situação pós-sismo.

## LIÇÕES APRENDIDAS

O histórico e a investigação científica efetuada sobre eventos de elevado impacto devem ser utilizados como critérios de identificação de prioridades de intervenção que permitam a proteção de ativos críticos na disponibilização de serviços críticos para a sociedade.

## CASO DE NEGÓCIO

A identificação e seleção das células dos reservatórios abrangidos foi feita, numa primeira fase, nas zonas de risco sísmico mais elevado e consequentemente mais expostas, tendo por objetivo maximizar as reservas de água nos reservatórios, em situação de sismo.

## OPORTUNIDADES DE REPLICAÇÃO

O projeto foi executado numa primeira fase nas zonas sísmicas de maior criticidade. A nível nacional esta medida poderia ser uma boa prática recomendável para aplicar em reservatórios que abasteçam grandes aglomerados populacionais de modo a maximizar o nível de reservas de água. Será também uma mais-valia para empresas congéneres noutros países sujeitos ao risco sísmico.

## COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

1	Redução da mortalidade induzida por desastre até 2030		A proteção das infraestruturas críticas assume, hoje em dia, uma envolvente cada vez mais significativa e a proteção dos ativos críticos demonstra não só uma preocupação das empresas mas também com a sociedade, minimizando os efeitos causados com a ocorrência de um evento disruptivo de elevados impactos
2	Reduzir o número de pessoas afetadas até 2030	X	
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a disrupção de serviços básicos até 2030	X	
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		Torna-se necessário o investimento, quer a nível dos programas de investigação, ao nível de ações conjuntas de planeamento e de emergência ou de reforço das edificações, assim como no investimento em capacitar a comunidade para uma recuperação efetiva.
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		

## SISTEMA ANTI-SÍSMICO EM TRANSFORMADORES DE POTÊNCIA

Em Portugal Continental as regiões classificadas com suscetibilidade elevada a sismos distribuem-se maioritariamente nos distritos de Lisboa, Setúbal, Santarém, Beja e Faro. A ocorrência de um evento de elevado impacto representa, para a sociedade, perdas económicas e humanas consideráveis e consequentemente danos significativos nos principais elementos estruturais expostos à ameaça. Sendo o abastecimento de energia elétrica essencial ao funcionamento da sociedade, considera-se que os Transformadores de Potência (TP) das Subestações (SE), como elementos críticos da rede de distribuição, devem ser dotados de sistemas que os salvaguardem perante a ocorrência de um evento desta natureza.

Para mais informação:

Carlos Silva Neto

[carlos.silvaneto@edp.pt](mailto:carlos.silvaneto@edp.pt)

[www.edpdistribuicao.pt](http://www.edpdistribuicao.pt)

[www.edpdistribuicao.pt/pt/rede/SE%20Tipo/SE\\_Tipo.html](http://www.edpdistribuicao.pt/pt/rede/SE%20Tipo/SE_Tipo.html)



Fixação de Transformadores de Potência com rodas em carris sobrelevados.



## RISCO

A vulnerabilidade sísmica está relacionada com a capacidade que um determinado elemento tem, para resistir ou para ser afetado pelo perigo sísmico, e com a severidade da ação do sismo. O risco sísmico exprime a probabilidade de se igualar, ou exceder, um determinado valor de perdas, num dado local e intervalo de tempo. O risco sísmico a que está sujeito o território nacional varia consoante a região, e depende de diversos fatores entre os quais, a existência de elementos vulneráveis expostos a determinados níveis de perigosidade sísmica. Entre os diversos elementos da rede elétrica (linhas AT e MT, apoios, postos de transformação e subestações), são os equipamentos existentes nas subestações que apresentam maior vulnerabilidade em situações de sismo. Nas SE's os TP's são os componentes mais críticos, dada a sua importância no sistema elétrico e o risco associado à sua destruição (ex. quebra, derrames de óleo, incêndio, rotura de travessias).

## AÇÃO

Para instalação de sistemas antissísmicos nos TP's foram utilizados como critérios (\*) de seleção a identificação de 3 zonas consideradas de risco sísmico mais elevado, ou seja, zona sísmica de maior criticidade (prioridade 1), zona sísmica de criticidade elevada (prioridade 2), zona sísmica de criticidade moderada (prioridade 3) e ainda as características de cada TP. Assim, identificaram-se cerca de 125 SE em exploração nas 3 zonas de risco sísmico referenciadas, perfazendo um total de 221 TP's a analisar. Posteriormente, será efetuada, uma análise mais detalhada aos TP's considerando a especificidade de cada instalação, para determinar a solução antissísmica mais adequada a aplicar (fixação ao solo com ou sem rodados).

(\*) Com base num estudo "Avaliação de Sustentabilidade Sísmica de Subestações" solicitado pela EDP Distribuição à Faculdade de Ciência e Tecnologia da Universidade de Coimbra (Departamento de Engenharia Civil) de Maio de 2010

## IMPACTO

A perda de um ou mais TP's numa subestação resulta na interrupção do fornecimento de energia que pode durar várias horas. Segundo os dados estatísticos, o estudo desenvolvido, permite concluir que a taxa de avarias em TP AT/MT entre os anos 2006 e 2013 é de 1,2% (relativamente ao total de TP existentes na EDP Distribuição), sendo o tempo de reparação de 12h. Numa ocorrência sísmica, com incidência em várias instalações em simultâneo, os tempos de reposição de energia poderão ser amplamente ultrapassados, pelo que é essencial a adoção de medidas preventivas que minimizem o impacto causado. Com a aplicação desta medida (sistemas antissísmicos) pretende-se minimizar o impacto que os TP's possam vir a sofrer quando sujeitos a eventos de elevado impacto.

## RESULTADO

Nas zonas sísmicas de maior criticidade, identificadas como prioridade 1 e 2, a garantia total de alimentação das redes MT é alcançada mediante a instalação de sistemas antissísmicos em apenas 20 TP's, ou seja apenas 18% do total de TP's. O número ascenderá a 111 TP's se se incluir todas as zonas de prioridade.

O estabelecimento de novas subestações terá em consideração o risco sísmico, e em particular, a aplicação de sistemas antissísmicos nos TP's, dada a sua importância no abastecimento de energia elétrica e a dificuldade de reparação ou substituição numa situação pós-sismo.

## LIÇÕES APRENDIDAS

O histórico e a investigação científica efetuada sobre eventos de elevado impacto devem ser utilizados como critérios de identificação de prioridades de intervenção que permitam a proteção de ativos críticos na disponibilização de serviços críticos para a sociedade.

## CASO DE NEGÓCIO

A identificação e seleção das subestações, instaladas nas zonas de risco sísmico mais elevado e consequentemente dos Transformadores de Potência mais expostos, têm por objetivo otimizar os custos de intervenção. Assim, mediante a otimização da rede afeta a diferentes subestações, garante-se a totalidade da alimentação das redes afetadas pela perda de um ou dois Transformadores de Potência em determinada subestação.

## OPORTUNIDADES DE REPLICAÇÃO

O projeto será executado em duas fases sendo a prioridade a zona sísmica de maior criticidade (prioridade 1) e a zona sísmica de criticidade elevada (prioridade 2). Numa segunda fase será também replicado nas zonas de risco moderado (prioridade 3). Adicionalmente, e sem ter em conta as zonas de vulnerabilidade sísmica, todas as subestações novas incluem a aplicação destes sistemas antissísmicos. A nível nacional este estudo poderia ser uma boa prática recomendável aplicar nos TP's de clientes e também uma mais-valia para empresas congéneres noutros países sujeitos ao risco sísmico.

## COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

1	Redução da mortalidade induzida por desastre até 2030		A proteção das infraestruturas críticas assume, hoje em dia, uma envolvente cada vez mais significativa e a proteção dos ativos críticos demonstra não só uma preocupação das empresas mas também com a sociedade, minimizando os efeitos causados com a ocorrência de um evento disruptivo de elevados impactos
2	Reduzir o número de pessoas afetadas até 2030	X	
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a disrupção de serviços básicos até 2030	X	
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		Torna-se necessário o investimento, quer a nível dos programas de investigação, ao nível de ações conjuntas de planeamento e de emergência ou de reforço das edificações, assim como no investimento em capacitar a comunidade para uma recuperação efetiva.
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		

## **CENTRO DE COMANDO OPERACIONAL – CCO**

O Gestor da Infraestrutura Ferroviária, no âmbito da implementação de uma estratégia global de modernização da rede ferroviária, envolvendo investimentos em via, catenária, sinalização, telecomunicações e outros sistemas (sinalização e de controlo automático de velocidade), implementou, no início de 2000, uma nova fase de exploração ferroviária.

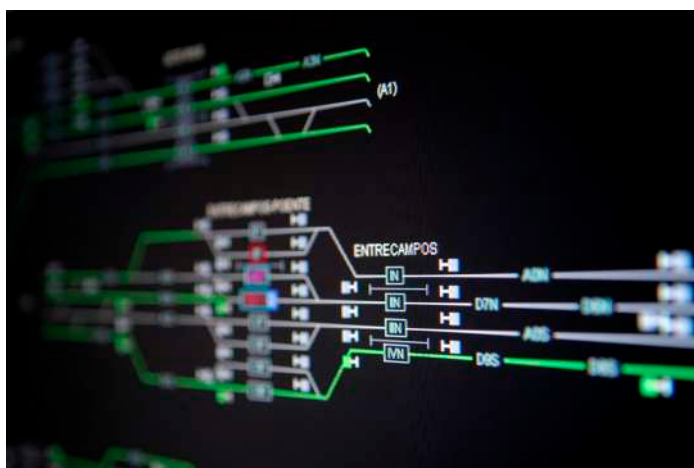
Estes novos sistemas, de elevada fiabilidade, foram concentrados nos Centros de Comando Operacional, possibilitando uma gestão indiferenciada da circulação em ambos os sentidos e vias férreas, permitindo densidades de tráfego bastante mais elevadas. Estes sistemas permitiram aumentar a qualidade do serviço com uma redução dos custos operacionais.

Para mais informação:

Rui Nunes da Silva

[rui.nsilva@infraestruturasdeportugal.pt](mailto:rui.nsilva@infraestruturasdeportugal.pt)

[www.infraestruturasdeportugal.pt](http://www.infraestruturasdeportugal.pt)



Centro de Comando Operacional  
e diagrama do CCO.



## RISCO

A infraestrutura ferroviária apresenta diversos pontos críticos (obras de arte, salas equipamentos técnicos), assim como infraestruturas críticas ao abrigo do atual enquadramento legal, que obrigam a uma constante monitorização.

A gestão não integrada dos sistemas de suporte à exploração ferroviária apresentava limitação várias, tais como: fragmentação da informação associada à exploração, não partilha de informação, operacionais com funções rotineiras (desmotivação), desaproveitamento de sinergias entre sistemas/bases de dados.

## AÇÃO

Foi implementada uma evolução de 6 Centros de Tráfego Centralizados (CTC) e Estações de Concentração, de âmbito regional bastante restrito, para um modelo de gestão mais abrangente assente em três CCO agregando diversas competências operacionais, tais como:

- Chefia do CCO, que assegura um comando funcional único ao qual se subordinam os vários agentes que coabitam na sala de comando;
- Supervisão da circulação, que assegura as ações de gestão e comando da circulação na sua área de atuação;
- Operação/Regulação de circulação, que operacionaliza o comando e controlo da circulação, ao nível da segurança, pontualidade e regularidade;
- Supervisão/Operação PGI, que centraliza toda a informação sobre o fornecimento de energia elétrica à catenária, e monitoriza os sistemas de registo de funcionamento dos equipamentos complementares para a segurança da circulação.

## IMPACTO

Os CCO representam uma evolução técnica e funcional, fundamentalmente na coordenação e supervisão de todas as funções e atividades ligadas aos processos operacionais da exploração ferroviária. Permitem a otimização da exploração da rede, maximizando a sua capacidade disponível, e a melhoria da qualidade do serviço ao nível das melhores práticas europeias, com padrões elevados de fiabilidade, eficiência e segurança.

Maior eficiência operacional, permitindo a interligação coerente dos diversos sistemas, facilitando o controlo pelo utilizador. Os sistemas integrados incluem sistemas de visualização ("Vídeo Wall"), transmissão, comunicações de voz, comunicações rádio-solo comboio (RSC), gravação de voz e dados, CCTV, SCADA, áudio e videoconferência.

## RESULTADO

Os CCO proporcionam à IP um controlo transparente de todas as operações ferroviárias através de interfaces gráficas com módulos para programação de serviço, disposição da infraestrutura, planeamento de horário, controlo, registo de dados, estatísticas, gestão de tráfego e disponibilização de informação. Permitem, também, em caso de falha, o funcionamento em modo degradado, através da articulação com as estações aí inseridas.

## LIÇÕES APRENDIDAS

A criação de centros multidisciplinares que permitem congregar, de forma sustentada, os serviços "core" de uma organização, podem constituir-se como uma vantagem, quer ao nível competitivo, quer ao nível organizacional.

Esta evolução permite, também, criar rotinas na avaliação de risco e aumentar a capacidade de resiliência da organização.

## CASO DE NEGÓCIO

A implementação destes sistemas/centros que têm como principal função a gestão da circulação ferroviária, permitem conhecer em cada momento o estado da infraestrutura, da circulação, assim como das ocorrências podem potenciar alguma ameaça para a empresa. Apresentam vantagens como: poupança significativa de custos através de ganhos de eficiência, qualidade no serviço ao utilizador final, redução de encargos operacionais, interoperacionalidade, sistemas integrados.

## OPORTUNIDADES DE REPLICAÇÃO

Este conceito poderá ser replicado em empresas de gestão de infraestruturas.

## COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

1	Redução da mortalidade induzida por desastre até 2030		O transporte ferroviário, especialmente se comparado com outros modos de transporte, caracteriza-se pela dificuldade de alternativa ao canal disponibilizado para circulação. Pela ausência de alternativa por modo ferroviário e pela insuficiência da alternativa de outros modos de transporte, grande parte da rede ferroviária apresenta elevado índice de criticidade. Estes factos sublinham a necessidade da existência de planeamento específico para a proteção de infraestruturas consideradas críticas, assim como para a criação de centros/estruturas que executem esse planeamento.
2	Reduzir o número de pessoas afetadas até 2030	X	
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a disrupção de serviços básicos até 2030	X	
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		





## RISCO

Um incidente com impacto significativo na disponibilização de serviços aos clientes ou na execução das mission critical activities da empresa causado, por exemplo, pela falha total ou parcial de uma infraestrutura crítica, pode ter consequências negativas em termos de reputação, imagem e receita. Os clientes dos serviços de comunicações estão habituados a ter serviços disponíveis em qualquer lugar e a qualquer momento pelo que são pouco tolerantes a interrupções. O elevado mediatismo do setor das comunicações – com vários meios de comunicação especializados – e a capacidade dos clientes amplificarem o seu descontentamento através das redes sociais implicam que mesmo falhas de curta duração tenham potencial para impacto elevado na empresa.

## AÇÃO

Implementação de um Plano de Gestão de Crise que defina regras, procedimentos e instrumentos que devem ser usados para a avaliação, escalamento, notificação e preparação da comunicação no âmbito de um incidente com impacto significativo. O Plano deve ter estrutura modular, de forma a poder ser instanciado em vários tipos de incidentes e deve prever a definição de um Kit de Instrumentos de Gestão de Crise (KIGC) que disponibilize à equipa de gestão de crise a informação e ferramentas essenciais para a execução das respetivas atividades no âmbito de uma crise. Deve também prever-se a formação teórica e prática dos elementos da Equipa de Gestão de Crise.

## IMPACTO

Os principais objetivos da implementação do Plano de Gestão de Crise são a minimização do impacto no negócio decorrente de um incidente com impacto significativo, garantia de uma atuação alinhada entre várias áreas da organização e a gestão adequada e atempada da comunicação com os stakeholders relevantes. O Kit de Instrumentos de Gestão de Crise, em particular, deve garantir que os elementos da equipa de gestão de crise sabem que atividades devem ser executadas e fornecer a informação ou suportes necessários. A formação da Equipa de Gestão de Crise deve promover a aceitação e aprovação do Plano na organização e dotar os vários elementos da equipa com conhecimentos para a aplicação prática do Plano numa situação de crise.

## RESULTADO

Foi implementado um Plano de Gestão de Crise NOS para o cenário de Falha de Serviço de Comunicações, tendo sido já replicado para outros cenários. O Plano define, em detalhe, as regras, procedimentos e instrumentos que devem ser usados em Crise, ao mesmo tempo que, em paralelo, se realizam as atividades de recuperação e restauro. O Kit implementado inclui os Organigramas de Crise; a Matriz de Avaliação que permite classificar o nível de gravidade de uma Crise; um cartão SIM de contingência que pode ser usado no caso de falha da rede de comunicações da NOS; um Crisis Pocket Guide que inclui os contactos principais e alternativos de todos os elementos da equipa de Gestão de Crise; uma Checklist que descreve as atividades que cada elemento da Equipa de Gestão de Crise deve executar. O Plano de Gestão de Crise e Kit permitiram melhorar a capacidade de resposta da NOS a incidentes com impacto significativo, afinando a capacidade de articulação entre áreas e a preparação da comunicação em crise com os stakeholders relevantes.

## LIÇÕES APRENDIDAS

Apesar das regras, procedimentos e instrumentos do Plano de Gestão de Crise deverem estar descritas com detalhe e devidamente fundamentadas, não se deve comprometer a agilidade da atuação quando a crise acontece. A solução para este problema pode passar pela definição de um Kit de Instrumentos de Gestão de Crise com a informação essencial, mantendo-se o Plano completo para efeitos formativos e informativos. A formação da Equipa de Gestão de Crise, com componente teórica e casos práticos, é essencial à aceitação e utilização bem sucedida do Plano.

## CASO DE NEGÓCIO

O Plano de Gestão de Crise da NOS permitiu melhorar a resposta da empresa a incidentes com impacto significativo, garantindo o envolvimento e alinhamento das áreas necessárias e a gestão adequada e atempada dos stakeholders relevantes. O Plano permite mitigar as consequências de um incidente, em particular nas vertentes de reputação, imagem e perda de receita.

## OPORTUNIDADES DE REPLICAÇÃO

Internamente, a NOS já replicou o Plano de Gestão de Crise e o respetivo Kit a cenários denominados como "Crowd Events" (eventos com concentração elevada de pessoas e forte associação à marca NOS, e.g., NOS Alive). O plano foi adaptado aos tipos de cenários de crise mais relevantes e ao perfil da equipa de crise no terreno para promover a agilidade de aplicação. O Plano de Gestão de Crise, no formato desenvolvido na NOS, é aplicável a qualquer organização que possa ser afetada por um incidente significativo. Será particularmente relevante em organizações com grande visibilidade pública, onde é necessária uma gestão adequada e atempada dos stakeholders relevantes. Cada organização pode desenvolver várias instâncias de um Plano de Gestão de Crise para dar resposta a diferentes tipos de incidentes com impacto significativo.

## COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

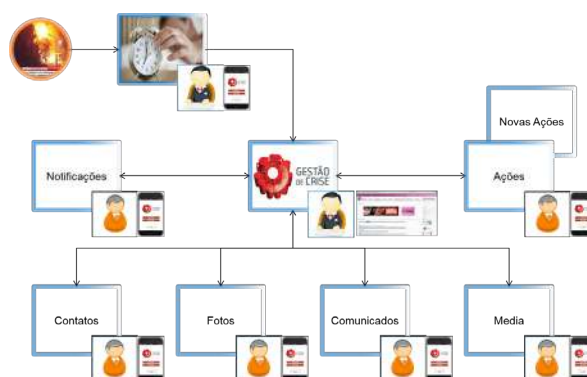
1	Redução da mortalidade induzida por desastre até 2030		As comunicações eletrónicas são, hoje em dia, essenciais tanto para os cidadãos individuais como para as empresas. Estes serviços suportam as comunicações entre pessoas, entre máquinas, o acesso a informação, aos serviços públicos (cada vez mais digitais) aos serviços de emergência, segurança e proteção. Torna-se assim necessário que os operadores de comunicações eletrónicas implementem mecanismos que, em paralelo com os processos de recuperação e restauro de serviços, contribuam para o alinhamento e articulação das várias áreas da organização e para a gestão dos stakeholders relevantes, obtendo benefícios ao nível da redução das pessoas afetadas, das perdas económicas e da disrupção de serviços básicos.
2	Reduzir o número de pessoas afetadas até 2030	X	
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a disrupção de serviços básicos até 2030	X	
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		



## APLICAÇÃO PARA GESTÃO DE CRISES

A Sonae Investimentos é uma multinacional que gere um portefólio de negócios no sector do retalho alimentar e não alimentar, com presença maioritária em Portugal, possuindo estabelecimentos de venda ao público em vários locais distribuídos de norte a sul do país. A ocorrência de um evento de elevado impacto que se transforme numa situação de crise, pode representar um risco para a sua imagem, para a capacidade de continuar as suas operações, para a retenção de clientes, para a capacidade de servir a comunidade e ainda para a forma como é avaliada no mercado financeiro e pelos seus parceiros. Reconhecendo a importância da resiliência dos negócios, a Sonae Investimentos foi desenvolvendo ao longo dos tempos Manuais de Gestão de Crise e de Continuidade do Negócio, para fazer face a eventuais interrupções que pudessem ocorrer nos principais ativos e processos da empresa. Para garantir a operacionalização destes manuais, que muitas vezes se tornam obsoletos como consequência da elevada dinâmica dos negócios, foi desenvolvido um aplicativo para automatização das várias fases do ciclo de gestão de crises, dotando as equipas de ferramentas que funcionam em tempo real, contribuindo para a eficácia da resposta, a contenção dos impactos e a redução dos tempos de recuperação.

Para mais informação:  
 José Luis Amorim  
[jamorim@sonae.pt](mailto:jamorim@sonae.pt)  
[www.sonae.pt](http://www.sonae.pt)



## RISCO

Existem hoje, várias ameaças que podem, uma vez materializadas, configurar situações de crise, nomeadamente vagas de calor, vagas de frio e de granizo, temporais, chuvas intensas e súbitas, sismos, maremotos, furacões e tornados. No negócio do retalho, que é caracterizado pelo elevado número de interações com clientes, a indisponibilidade de produtos, dos sistemas de informação e das instalações (edifícios centrais, entrepostos, centros de fabrico e lojas), assume particular relevância, pode pôr em causa a capacidade de manter em funcionamento as operações ou processos críticos, com consequências diretas para o serviço ao cliente, a rentabilidade dos negócios e a imagem das empresas. Para reduzir o impacto do risco de interrupção do negócio, foram sendo desenvolvidos ao longo dos tempos manuais de Gestão de Crise em formato papel, que descrevem os cenários de crise, a equipa de gestão de crise e respetivos contactos, modelo de escalada e as ações de contingência. Da aplicação prática desses manuais, observou-se que eram pouco acionáveis, encontravam-se normalmente desatualizados, eram de difícil acesso e pouco ágeis para serem utilizados em situações reais e não garantiam o registo histórico nem a partilha das aprendizagens.

## AÇÃO

Para operacionalizar os manuais de Gestão de Crise que foram elaborados para os ativos imobiliários e negócios considerados mais relevantes, foi realizado um projeto interno na Sonae para desenvolvimento de um aplicativo cujos principais objetivos foram:

- Automatizar o processo de comunicação e gestão em tempo real das ações de contingência em situação de crise;
- Automatizar o processo de consulta dos Manuais de Gestão de Crise, a partir de qualquer lugar e através de qualquer dispositivo (smartphones, tablets, computadores pessoais);
- Centralizar informação e garantir fácil acesso;
- Gerir centralmente os processos de resposta à crise;
- Garantir a atualização automática das equipas e contactos de gestão de crise e respetivas ações de contingência;
- Facilitar e automatizar o processo de revisão dos manuais;
- Garantir a existência de um histórico e das lições aprendidas em cada crise;
- Criar versão digital dos manuais de Gestão de Crise.

## IMPACTO

A perda temporária ou definitiva, de um ativo imobiliário, nomeadamente entrepostos e lojas, pode provocar a interrupção do negócio, durante vários dias, semanas ou até meses, dependendo da sua severidade, o que se poderá traduzir em perdas de exploração na ordem dos milhares de euros e na indisponibilidade dos produtos para os clientes. Por outro lado, há que ter em conta a ocorrência de eventos com abrangência numa determinada região, como é o caso dos sismos. Nestas situações as consequências poderão ainda ser mais gravosas, uma vez que poderão afetar vários ativos imobiliários em simultâneo. Neste cenário os tempos de reposição de operação poderão ser amplamente ultrapassados, pelo que é essencial a adoção de procedimentos de gestão de crise que minimizem o impacto causado.

## RESULTADO

A solução adotada visou garantir a disponibilidade deste serviço em qualquer momento e a partir de qualquer dispositivo, complementada com requisitos de fácil usabilidade e ergonomia.

A implementação desta nova ferramenta, contribui para uma gestão proactiva de situações de crise, com redução dos impactos e tempos de recuperação mais rápidos e com consequente credibilização da imagem da empresa junto dos seus stakeholders e minimização dos impactos junto das populações.

## LIÇÕES APRENDIDAS

A utilização dos sistemas de informação, de ferramentas colaborativas e dos dispositivos móveis (ex: smartphones), são aceleradores em processos vitais, como a gestão de crises, contribuindo para uma maior dinâmica e alinhamento da equipa de gestão de crise, com repercussão direta na contenção dos impactos e na redução dos tempos de indisponibilidade.

## CASO DE NEGÓCIO

O desenvolvimento da aplicação para Gestão de Crises, teve por objetivos minimizar os potenciais impactos decorrentes de acidentes e situações de catástrofe, reduzir o tempo de indisponibilidade do serviço ao cliente e consequentemente o impacto nas vendas.

## OPORTUNIDADES DE REPLICAÇÃO

A aplicação desenvolvida para gestão de crises, poderá no futuro evoluir para uma lógica de prevenção de crises. A título de exemplo, está-se a estudar a possibilidade de esta passar a recolher informações publicadas pelo Instituto Português do Mar e da Atmosfera para que preventivamente as equipas responsáveis pela proteção física das instalações possam por em prática ações que evitem ou limitem os danos que possam decorrer de situações climáticas extremas.

## COMO É QUE O PROJETO CONTRIBUIU PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

1	Redução da mortalidade induzida por desastre até 2030		O World Economic Forum, no seu reporte anual sobre os principais riscos globais que podem afetar em 2017 as organizações, considerou o risco associado aos eventos climáticos extremos como sendo o principal risco a ter em atenção. No setor do retalho, o sourcing faz-se cada vez mais em países mais expostos a catástrofes naturais. Tendo em conta esta realidade, torna-se imperioso que as organizações lancem iniciativas que protejam os seus principais ativos imobiliários e assegurem a continuidade dos seus negócios. São inúmeras as ferramentas que podem contribuir para a previsão de situações de risco potencial e assegurar a gestão eficaz de situações de crise. Desmaterialização dos processos, mobilidade, conectividade e eficiência operacional são também drivers para aumentar a resiliência dos negócios.
2	Reduzir o número de pessoas afetadas até 2030		
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a disrupção de serviços básicos até 2030		
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		
6	Aumentar a cooperação internacional com países em desenvolvimento		
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030	X	

## **ASSISTÊNCIA HUMANA – CARE TEAM E ASSISTANCE TEAM**

A TAP Portugal aposta na humanização da resposta a emergências e ocorrências operacionais. Há largos anos que possui equipas de intervenção voluntária devidamente formadas e treinadas, constituídas por trabalhadores do Grupo TAP, que são ativadas em situações de crise. Ambas as equipas desempenham, no terreno, um papel fundamental na assistência a passageiros e familiares quer seja em consequência de um acidente ou incidente aéreo através do Care Team ou em situações de disrupção operacional através do Assistance Team. A sua intervenção é crítica para manter ou recuperar a confiança dos passageiros na Empresa que, nestas situações, é sempre afetada. As duas equipas contam com mais de 600 voluntários.

Para mais informação:  
Maria João Calha  
[mcalha@tap.pt](mailto:mcalha@tap.pt)  
[www.flytap.com](http://www.flytap.com)





## RISCO

A indústria da aviação em geral, e a TAP em particular, desenvolvem a sua atividade num contexto exigente, sujeito a grande diversidade de riscos que potencialmente podem comprometer a viabilidade do negócio. Destes riscos, destacam-se obviamente acidentes e incidentes aéreos, com enorme impacto na vida dos passageiros e da Empresa. Ocorrências operacionais que originem situações de fluxo anormal de tráfego – greves, crises políticas – e fenómenos naturais (erupções vulcânicas) podem por em causa a atividade da TAP.

## AÇÃO

Numa situação de incidente ou acidente aéreo a assistência prática e emocional dada pelo Care Team da TAP tem-se revelado essencial. A missão desde grupo de voluntários em específico é acompanhar e apoiar sobreviventes e familiares das vítimas, assistindo a necessidades básicas e estabelecendo um elo de comunicação entre eles e a Empresa. Estando a TAP integrada na Star Alliance, o Care Team atua em rede e em articulação com várias entidades e nacionalidades. O grupo de voluntários da TAP pode ser ativado num incidente ou acidente que envolva uma companhia aérea parceira.

## IMPACTO

A atuação destas equipas permite que a TAP esteja junto das pessoas – passageiros e familiares afetados por uma situação de emergência ou major disruption operacional – dando uma resposta imediata, competente e coordenada, que salvguarde os interesses da Empresa. A sua atuação permite a continuidade da operação com o mínimo impacto (continuidade do negócio).

## RESULTADO

A história comprova que um acidente aéreo, bem como, uma major disruption operacional, pode causar danos irreparáveis à reputação de uma companhia aérea, conduzindo muitas vezes à ruína do negócio. O trabalho desenvolvido pelas equipas de intervenção voluntária da TAP permite que seja transmitida uma mensagem consistente e autêntica aos passageiros e familiares afetados por uma situação de emergência ou ocorrência operacional, recuperando a confiança que na maioria dos casos foi perdida.

## LIÇÕES APRENDIDAS

As situações reais que levaram à ativação das equipas de intervenção voluntária TAP (exemplos: acidente Spanair, acidente Germanwings, nuvens vulcânicas) são evidências claras de que a assistência humana tem um papel fundamental e insubstituível. As experiências e testemunhos dos elementos que participaram nestas situações são incluídos em módulos formativos, para treino de todos os voluntários. Acima de tudo a missão destas equipas é fazer o que está certo, salvaguardando os interesses da TAP, no que diz respeito a passageiros, staff e familiares. Um acidente que conduza à perda de vidas é devastador!

## CASO DE NEGÓCIO

A aposta feita pela TAP na humanização da resposta a emergências e ocorrências operacionais tem permitido manter e reforçar a credibilidade da Empresa junto dos clientes, para além de assegurar a continuidade do negócio com o mínimo impacto financeiro e operacional, nas situações em que as equipas são ativadas. No caso de uma companhia aérea, a constituição de uma equipa formada e treinada para dar apoio às vítimas e famílias no caso de um acidente aéreo (Care Team na TAP), é um requisito obrigatório para obtenção de certificação IATA Operational Safety Audit, internacionalmente reconhecida como standard de referência para as companhias aéreas.

## OPORTUNIDADES DE REPLICAÇÃO

A existência destas equipas pode obviamente ser replicada em empresas cuja natureza da atividade implique a existência de riscos com impacto em pessoas – vítimas, familiares, staff. Estas equipas são o complemento humano de outras entidades que no terreno, têm uma ação direcionada para a resolução do incidente ou ocorrência operacional, e que não estão obviamente focadas na assistência solidária e emocional ao indivíduo afetado.

## COMO É QUE O PROJETO CONTRIBUI PARA A IMPLEMENTAÇÃO DOS OBJETIVOS DO QUADRO DE SENDAI?

1	Redução da mortalidade induzida por desastre até 2030		A ação das equipas de intervenção voluntária é fundamental na transição da situação de emergência/ major disruption operacional para a normal atividade da Empresa. O curto tempo de resposta da sua atuação minimiza o impacto que situações extremas podem ter na atividade de transporte aéreo. A atual articulação com várias entidades e nacionalidades, fruto da inclusão numa aliança constituída por várias empresas – Star Alliance – mas também a forte ligação da TAP aos Países Africanos de Língua Oficial Portuguesa, contribui para a cooperação internacional de Portugal junto de países em desenvolvimento.
2	Reduzir o número de pessoas afetadas até 2030		
3	Reduzir as perdas económicas até 2030	X	
4	Reduzir as infraestruturas críticas afetadas e a interrupção de serviços básicos até 2030		
5	Aumentar os países com estratégias nacionais e locais de RRC até 2020		
6	Aumentar a cooperação internacional com países em desenvolvimento	X	
7	Aumentar a disponibilidade e acesso a Sistemas de Alerta Precoce e a informação de Risco de Desastre às comunidades até 2030		



## AGRADECIMENTOS

As entidades integrantes do Grupo de Trabalho 4 – Triénio 2015-2017 da Plataforma Nacional para a Redução do Risco de Catástrofes agradecem todos os contributos recebidos para a elaboração, revisão e edição do presente manual, designadamente:

- CGD – José Carlos Bragança, João Paulo Estrela e João Sales Belchior
- ANPC – Alexandra Santos, Bárbara Lopes Dias, Carlos Mendes, Francelino Silva, Inês Lamim, Luis Sá, Patrícia Pires
- EDP Distribuição – Carlos Bexiga Filipe, Carlos Silva Neto, Nuno Ferreira
- EPAL – Joaquim Sereno
- GALP – Fernando Machado
- IP – Pedro António
- NOS – Pedro Gaspar Moreira
- SIEMENS – Jorge Ventura
- SONAE – Pedro Cupertino de Miranda
- TAP – Helder Batista, Luis Miguel Falcão, Tiago Delfino, Marta Almeida

## PROMOÇÃO



## COORDENAÇÃO



## REDAÇÃO



## PARTICIPAÇÃO

