

RELATÓRIO SOBRE OS SETORES DOS OPERADORES DE SERVIÇOS ESSENCIAIS

Caracterização, Regulamentação e Recomendações
no Âmbito do Observatório de Cibersegurança

Índice

Introdução	13
Contexto do relatório	15
Objetivos do relatório	16
Contexto Geral	17
Análise do questionário dirigido aos Reguladores de Serviços Essenciais	20
Resultados do questionário dirigido aos Operadores de Serviços Essenciais	52
Análise Setorial	172
1. Energia	172
1.1. Contextualização setorial	172
1.2. Ameaças	191
1.3. Capacitação	201
1.4. Investimento em cibersegurança	204
1.5. RJSC e legislação setorial	210
1.6. Standards e boas práticas aplicáveis	214
1.7. Desafios	217
1.8. Recomendações	221
2. Transportes	228
2.1. Contextualização setorial	228
2.2. Ameaças	259
2.3. Capacitação	275
2.4. Investimento em cibersegurança	279
2.5. RJSC e legislação setorial	286
2.6. Standards e boas práticas aplicáveis	293
2.7. Desafios	302
2.8. Recomendações	305
3. Bancário	319
3.1. Contextualização setorial	319

3.2. Ameaças	329
3.3. Capacitação	334
3.4. Investimento em cibersegurança.....	336
3.5. RJSC e legislação setorial.....	340
3.6. Standards e boas práticas aplicáveis	343
3.7. Desafios	347
3.8. Recomendações	350
4. Infraestruturas do mercado financeiro.....	360
4.1. Contextualização setorial	360
4.2. Ameaças	372
4.3. Capacitação	376
4.4. Investimento em cibersegurança.....	379
4.5. RJSC e legislação setorial.....	381
4.6. Standards e boas práticas aplicáveis	384
4.7. Desafios	386
4.8. Recomendações	387
5. Saúde	394
5.1. Contextualização setorial	394
5.2. Ameaças	409
5.3. Capacitação	414
5.4. Investimento em cibersegurança.....	417
5.5. RJSC e legislação setorial.....	421
5.6. Standards e boas práticas aplicáveis	423
5.7. Desafios	426
5.8. Recomendações	427
6. Fornecimento e distribuição de água potável.....	433
6.1. Contextualização setorial	433
6.2. Ameaças	444
6.3. Capacitação	452
6.4. Investimento em cibersegurança.....	454

6.5. RJSC e legislação setorial.....	458
6.6. Standards e boas práticas aplicáveis	460
6.7. Desafios	462
6.8. Recomendações	464
7. Infraestruturas digitais	472
7.1. Contextualização setorial	472
7.2. Ameaças	482
7.3. Capacitação	486
7.4. Investimento em cibersegurança.....	489
7.5. RJSC e legislação setorial.....	495
7.6. Standards e boas práticas aplicáveis	499
7.7. Desafios	500
7.8. Recomendações	502
Notas metodológicas.....	511
Bibliografia	512

Índice de Gráficos

Gráfico 1 - Reguladores que já comunicaram com os OSE sobre questões de cibersegurança...	21
Gráfico 2 - Origem da comunicação sobre questões de cibersegurança.....	21
Gráfico 3 - Formalidade da comunicação realizada.....	22
Gráfico 4 - Frequência da comunicação	23
Gráfico 5 - Impacto sentido na sua organização e nos OSE regulados	24
Gráfico 6 - Dificuldades sentidas relativamente à conformidade com a Diretiva NIS / Lei n.º 46/2018	25
Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSE em matéria de cibersegurança, em caso de atribuição da competência	26
Gráfico 8 - Recursos em falta para a capacidade de supervisão em matéria de cibersegurança .	27
Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores	28
Gráfico 10 - Medidas adotadas pelas entidades reguladoras para promover a maturidade em cibersegurança.....	29
Gráfico 11 - Perceção sobre o número de profissionais capacitados em matéria de cibersegurança na entidade reguladora	31
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados	31
Gráfico 13 - Perceção dos reguladores sobre o nível de cibersegurança estabelecido pela Diretiva NIS 1 / lei n.º 46/2018, de 13 de agosto, face aos desafios, perigos e ameaças existentes	32
Gráfico 14 - Reguladores que se encontram a fazer categorização de ameaças de cibersegurança	33
Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização.....	34
Gráfico 16 - Reguladores que orientam os OSE na digitalização de processos e na promoção de uma cultura digital	34
Gráfico 17 - Perceção sobre a necessidade de apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança nos setores regulados	35
Gráfico 18 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS.....	36
Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS.....	38
Gráfico 20 - Áreas através das quais o CNCS poderia prestar mais auxílio	40
Gráfico 21 - Standards e boas práticas recomendados aos OSE pelos reguladores.....	42

Gráfico 22 - Percentagem aproximada de OSE nos setores certificados em normas internacionais (como ISO/IEC 27001 ou ISO 22301) do conhecimento do regulador.....	45
Gráfico 23 - Reguladores com equipa de resposta a incidentes definida.....	47
Gráfico 24 - Reguladores que estão ou já estiveram em programas de formação e sensibilização para os riscos no ciberespaço promovidos pelo CNCS ou por outra entidade	48
Gráfico 25 - Reguladores recipientes de formação que partilharam os conhecimentos adquiridos com os OSE do setor	49
Gráfico 26 - Reguladores que frequentaram programas, e consideram que ter frequentado o programa robusteceu comportamentos relativos à cibersegurança dentro da organização.....	50
Gráfico 27 - Reguladores que, no âmbito dos programas, sentiram que a entidade formadora os sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto	50
Gráfico 28 - Reguladores pertencentes a estruturas de cooperação nacional/internacional de proteção do ciberespaço (ISACs - Centros de Análise e Partilha de Informação)	51
Gráfico 29 - Reguladores que recomendam a participação dos OSE em centros de partilha de informação como os ISACs	52
Gráfico 30 - Número de colaboradores na organização	52
Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores.....	54
Gráfico 32 - Implementação de apoios ou programas, próprios ou do Estado, para colaboradores que desejem formação na área de cibersegurança.....	55
Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança.....	55
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança.....	57
Gráfico 35 - Percentagem aproximada de trabalhadores do operador com certificações em cibersegurança.....	58
Gráfico 36 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (<i>helpdesk</i>), em matéria de cibersegurança e/ou tecnologias da informação.....	59
Gráfico 37 - Composição das equipas de <i>helpdesk</i>	62
Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores	63
Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa	64
Gráfico 40 - Caráter das formações disponibilizadas - formação interna ou externa	65
Gráfico 41 - Frequência média dos momentos de formação	65
Gráfico 42 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam	67
Gráfico 43 - Existência de cursos de atualização (“refresher courses”) para os colaboradores	69
Gráfico 44 - Perceção sobre a falta de profissionais em cibersegurança e áreas relacionadas....	69

Gráfico 45 - Vagas abertas para a área de cibersegurança	70
Gráfico 46 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança.....	71
Gráfico 47 - Motivos para a não abertura de vagas entre os OSE sem vagas abertas para a área de cibersegurança.....	72
Gráfico 48 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho	74
Gráfico 49 - Os OSE são responsáveis pelo funcionamento dos equipamentos necessários às funções dos colaboradores	76
Gráfico 50 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções	77
Gráfico 51 - Fornecimento de acesso remoto a sistemas (e-mail, aplicações ou documentos) dos OSE aos colaboradores	79
Gráfico 52 - Sistemas do OSE aos quais é dado acesso remoto aos colaboradores	79
Gráfico 53 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE.....	81
Gráfico 54 - OSE que utilizam Customer Relationship Management software (CRM)	84
Gráfico 55 - OSE que utilizam CRM para captar, armazenar e disponibilizar informação de clientes a outras funções do negócio	84
Gráfico 56 - OSE que adquiriram serviços de Computação Cloud (CC).....	85
Gráfico 57 - Finalidades dos serviços de Computação Cloud adquiridos	86
Gráfico 58 - Utilização de serviços de CC em conjunto com <i>Internet of Things (IoT)</i>	89
Gráfico 59 - Percentagem de sistemas core em <i>cloud</i>	90
Gráfico 60 - Percentagem de sistemas core <i>on-prem</i>	91
Gráfico 61 - Utilização de IoT pelos OSE	92
Gráfico 62 - Contextos de utilização de IoT	93
Gráfico 63 - Motivos pelos quais não utilizam IoT	95
Gráfico 64 - OSE que utilizam processos que recorrem a IA.....	98
Gráfico 65 - Funções para as quais utilizam IA (Geral)	99
Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança	103
Gráfico 67 - Divisão entre rede dos colaboradores e rede para <i>guests</i>	111
Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC	112
Gráfico 69 - Tipos de incidentes ocorridos	113
Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS.....	116
Gráfico 71 - Dificuldades no processo de notificação ao CNCS	117

Gráfico 72 - Dificuldades encontradas pelos OSE durante a notificação de incidentes ao CNCS	117
Gráfico 73 - Importância da intervenção do CNCS na resolução do incidente.....	118
Gráfico 74 - Avaliação da resposta dada pelo CNCS	118
Gráfico 75 - Motivos para a não notificação de incidentes de cibersegurança ao CNCS.....	120
Gráfico 76 - Seguro contra incidentes de cibersegurança	121
Gráfico 77 - Documentação/implementação de políticas e procedimentos de cibersegurança...	122
Gráfico 78 - Existência de Plano de Segurança que contemple a cibersegurança	123
Gráfico 79 - Políticas incluídas no Plano de Segurança	124
Gráfico 80 - Revisão do Plano de Segurança.....	127
Gráfico 81 - OSE que realizam procedimentos de deteção e gestão de vulnerabilidades	128
Gráfico 82 - OSE que dentro dos procedimentos de deteção e gestão de vulnerabilidades realizam análise de vulnerabilidades	128
Gráfico 83 - Frequência da análise de vulnerabilidades	129
Gráfico 84 - Realização de testes de intrusão	131
Gráfico 85 - Frequência de testes de intrusão.....	132
Gráfico 86 - Observação de requisitos mínimos e segurança por parte dos fornecedores em contexto de cadeia de abastecimento	134
Gráfico 87 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS	134
Gráfico 88 - Nomeação do contacto permanente que assegura os fluxos de informação de nível operacional e técnico com o CNCS.....	136
Gráfico 89 - Designação do contacto permanente.....	136
Gráfico 90 - Designação do responsável de segurança	137
Gráfico 91 - Critérios utilizados para a designação do responsável de segurança	137
Gráfico 92 - Formação específica de cibersegurança do responsável de segurança	140
Gráfico 93 - Tipo de formação específica em cibersegurança	141
Gráfico 94 - Motivos pelos quais o responsável de segurança não tem formação específica em cibersegurança.....	142
Gráfico 95 - Inventário de ativos essenciais elaborado e atualizado.....	145
Gráfico 96 - Submissão do inventário de ativos ao CNCS.....	145
Gráfico 97 - Elaboração do relatório anual previsto pelo decreto-lei n.º 65/2021, de 30 de julho	146
Gráfico 98 - Submissão do relatório anual ao CNCS.....	146

Gráfico 99 - Realização de análise de riscos anual no âmbito de cibersegurança.....	147
Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança.....	147
Gráfico 101 - Definição de calendário para cumprimento das obrigações decorrentes do decreto-lei n.º 65/2021, de 30 de julho.....	148
Gráfico 102 - Equipa de resposta a incidentes de cibersegurança	149
Gráfico 103 - Composição da equipa de resposta a incidentes de cibersegurança	149
Gráfico 104 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança	151
Gráfico 105 - Disponibilização aos colaboradores de canais rápidos para reporte de incidentes	153
Gráfico 106 - Acessibilidade e distribuição por todos os colaboradores dos contactos a utilizar em caso de incidente de cibersegurança	153
Gráfico 107 - Realização de exercícios de resposta a ciberataques.....	154
Gráfico 108 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança.....	155
Gráfico 109 - Orçamento específico para a área de cibersegurança.....	158
Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança	160
Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança.....	164
Gráfico 112 - Conhecimento de incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança.....	168
Gráfico 113 - Plano de Comunicação de Crises	169
Gráfico 114 - Secções definidas no Plano de Comunicação de Crises	169
Gráfico 115 - Motivos para a não definição de Plano de Comunicação de Crises	174

Índice de Figuras

Figura 1 - Número de incidentes no setor da Energia anualmente	194
Figura 2 - Número de incidentes no setor dos Transportes anualmente.....	259
Figura 3 - Investimento em SI de cada subsetor dos transportes	280
Figura 4 - Número de incidentes no setor Bancário anualmente	333
Figura 5 - Perda de controlo de informação no setor Bancário	348
Figura 6 - Número de incidentes no setor das Infraestruturas do Mercado Financeiro anualmente	375
Figura 7 - Número de incidentes no setor da Saúde anualmente	411
Figura 8 - Acesso ao Serviço	438
Figura 9 - Acesso ao Serviço de Saneamento de Águas Residuais Urbanas	439
Figura 10 - Qualidade da Água	440
Figura 11 - Cyber Kill Chain (CKC).....	445
Figura 12 - Modelo de ataque em espiral em redes onde convergem TI e TO	446
Figura 13 - Número de incidentes no setor da Água anualmente	450
Figura 14 - Velocidade de Internet	477
Figura 15 - Preço dos Cabazes.....	478
Figura 16 - Número de incidentes no setor das Infraestruturas Digitais anualmente	485

Índice de Tabelas

Tabela 1 - Setores, Subsetores e Tipos de Entidades.....	18
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança	46
Tabela 3 - Estimativa do total de entidades reguladas pelos reguladores por setor	53
Tabela 4 - Número estimado das entidades reguladas que são OSE.....	53
Tabela 5 - Agentes de ameaça mais prováveis (Eletricidade)	197
Tabela 6 - Agentes de ameaça mais prováveis (Petróleo)	198
Tabela 7 - Agentes de ameaça mais prováveis (Gás)	200
Tabela 8 - <i>Standards</i> e Boas Práticas (Subsetor Eletricidade)	214
Tabela 9 - <i>Standards</i> e Boas Práticas (Subsetor Petróleo)	215
Tabela 10 - <i>Standards</i> e Boas Práticas (Subsetor Gás)	216
Tabela 11 - Abordagem para identificação de OSE.....	217
Tabela 12 - Controlos de Segurança da CIS (Energia).....	228
Tabela 13 - Cenários de risco (Eletricidade).....	230
Tabela 14 - Cenários de risco (Petróleo).....	231
Tabela 15 - Cenários de risco (Gás).....	232
Tabela 16 - Variação e evolução dos indicadores financeiros e económicos (Transportes).....	242
Tabela 17 - Agentes de ameaça mais prováveis (Transporte Aéreo)	265
Tabela 18 - Principais ameaças (Transporte Marítimo)	266
Tabela 19 - Agentes de ameaça mais prováveis (Transporte Marítimo).....	268
Tabela 20 - Principais ameaças (Transporte Ferroviário)	269
Tabela 21 - Agentes de ameaça mais prováveis (Transporte Ferroviário).....	271
Tabela 22 - Principais ameaças (Transporte Rodoviário)	272
Tabela 23 - Agentes de ameaça mais prováveis (Transporte Rodoviário).....	274
Tabela 24 - <i>Standards</i> e Boas Práticas (Transportes Aéreo).....	293
Tabela 25 - <i>Standards</i> e Boas Práticas (Transportes Ferroviário)	295
Tabela 26 - <i>Standards</i> e Boas Práticas (Transporte Marítimo)	297
Tabela 27 - <i>Standards</i> e Boas Práticas (Transporte Rodoviário).....	300

Tabela 28 - Recomendações (Transportes)	306
Tabela 29 - Controlos de Segurança da CIS (Transportes)	309
Tabela 30 - Recomendações (Transporte Aéreo)	310
Tabela 31 - Cenários de risco (Transporte Aéreo)	311
Tabela 32 - Cenários de risco (Transporte Marítimo)	313
Tabela 33 - Cenários de risco (Transporte Ferroviário)	315
Tabela 34 - Recomendações (Transporte Rodoviário)	316
Tabela 35 - Medidas de segurança (Transporte Rodoviário)	317
Tabela 36 - Cenários de risco (Transporte Rodoviário)	318
Tabela 37 - Agentes de ameaça mais prováveis (Bancário)	333
Tabela 38 - Capacitação no setor Bancário	334
Tabela 39 - <i>Standards</i> e Boas Práticas (Bancário)	343
Tabela 40 - Cenários de risco (Bancário)	354
Tabela 41 - Controlos de Segurança da CIS (Bancário)	359
Tabela 42 - Agentes de ameaça mais prováveis (IMF)	375
Tabela 43 - <i>Standards</i> e Boas Práticas (Infraestruturas do Mercado Financeiro)	384
Tabela 44 - Cenários de risco (IMF)	387
Tabela 45 - Controlos de Segurança da CIS (IMF)	393
Tabela 46 - Agentes de ameaça mais prováveis (Saúde)	411
Tabela 47 - <i>Standards</i> e Boas Práticas (Saúde)	423
Tabela 48 - Cenários de risco (Saúde)	427
Tabela 49 - Controlos de Segurança da CIS (Saúde)	432
Tabela 50 - Agentes de ameaça mais prováveis (Fornecimento e distribuição de água potável)	450
Tabela 51 - <i>Standards</i> e Boas Práticas (Água)	460
Tabela 52 - Cenários de risco (Água)	465
Tabela 53 - Controlos de Segurança da CIS (Distr. Água Potável)	471
Tabela 54 - Velocidade de Internet	478
Tabela 55 - Agentes de ameaça mais prováveis (Infraestruturas Digitais)	485
Tabela 56 - Intervenções em Infraestruturas Digitais	490
Tabela 57 - <i>Standards</i> e Boas Práticas (Infraestruturas Digitais)	499

Tabela 58 - Cenários de risco (Infraestruturas Digitais)	503
Tabela 59 - Controlos de Segurança da CIS (Inf. Digitais)	510

Introdução

O atual cenário de cibersegurança encontra-se num contexto onde a amplitude, a frequência e o impacto dos incidentes de segurança estão a aumentar, constituindo uma séria ameaça ao funcionamento das redes e dos sistemas de informação. O risco de esses incidentes impedirem o exercício das atividades económicas, gerarem avultadas perdas financeiras, minarem a confiança dos utilizadores e causarem graves prejuízos à economia da União Europeia (UE) é real.

Foi neste contexto que surgiu a Diretiva NIS¹, derivada da necessidade formalizada pelo Parlamento Europeu e Conselho da UE da implementação e harmonização de medidas destinadas a garantir um elevado nível de segurança das redes e da informação em toda a UE. Esta necessidade advém, desde logo, da necessidade de garantir a fiabilidade, a segurança e a confiança nas atividades económicas e societárias e no mercado interno.

Assim, a Diretiva NIS tem por objetivo desenvolver as capacidades de cibersegurança em toda a União, mitigar os riscos associados às ameaças contra os sistemas de rede e informação utilizados para prestar serviços essenciais e garantir a continuidade de tais serviços perante incidentes. Pretende-se, portanto, contribuir para a segurança da União e para o eficaz funcionamento da sua economia e sociedade.

A Diretiva NIS estabelece, entre outros, requisitos de segurança e de notificação para os Operadores de Serviços Essenciais (OSE), categorizando-os em setores e subsetores. No contexto português, esta Diretiva foi transposta através da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC).

A lei portuguesa define um operador de um serviço essencial como: “uma entidade pública ou privada que presta um serviço essencial”², caracterizando um serviço essencial como “um serviço essencial para a manutenção de atividades societárias ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço”³.

Os setores considerados para efeitos da consideração como OSE são os seguintes: 1) Energia; 2) Transportes; 3) Bancário; 4) Infraestruturas do mercado financeiro; 5) Saúde; 6) Fornecimento e

¹ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148>.

² Lei n.º 46/2018, de 13 de agosto, artigo 3.º, alínea g), *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

³ Lei n.º 46/2018, artigo 3.º, alínea t).

distribuição de água potável; 7) Infraestruturas digitais. Cada um destes setores pode incluir subsetores a considerar, bem como tipos de entidades claramente identificados na lei. Estas considerações serão incluídas nos respetivos capítulos.

O presente relatório analisa, de um modo transversal, o estado da cibersegurança nos OSE, contém recomendações gerais para todos os OSE e recomendações específicas em função de cada um dos setores/subsetores, atendendo quer às boas práticas internacionais, quer às necessidades identificadas. As necessidades derivam das conclusões retiradas face ao investimento, capacitação, ameaças identificadas e de outros fatores indicados mediante os resultados de dois questionários - um dirigido às entidades reguladoras dos OSE, e outro dirigido aos próprios Operadores - realizados com o objetivo de compreender a realidade dos OSE em Portugal em matéria de cibersegurança.

Contexto do relatório

Atendendo à Lei n.º 46/2018 e considerando os termos da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC), aprovada em Conselho de Ministros, foi identificada a necessidade de reconhecer e analisar a realidade atual do estado de Cibersegurança nos setores relativos aos OSE.

Tal análise resultará na realização de um Relatório sobre os Setores dos Operadores de Serviços Essenciais (ROSE) que engloba a caracterização, regulamentação e recomendações no âmbito do Observatório de Cibersegurança.

O Observatório de Cibersegurança visa observar o fenómeno da cibersegurança em Portugal, nas suas mais variadas componentes, de modo a informar as partes interessadas e a apoiar a definição de políticas públicas. Tem, ainda, como missão, ser uma plataforma de análise e sistematização de conhecimento, bem como de debate, em torno de temas multidisciplinares da cibersegurança, identificando tendências com referências.

Os setores dos OSE sobre os quais foi desenvolvido o relatório e aplicados os questionários, são definidos pela Diretiva NIS: Energia, Transportes, Setor Bancário, Infraestruturas do Mercado Financeiro, Saúde, Infraestruturas Digitais e Fornecimento e Distribuição de Água Potável.

Objetivos do relatório

Este relatório teve como principais objetivos:

- Identificar e avaliar o estado da cibersegurança em Portugal, no que diz respeito aos diversos setores dos OSE, em vários domínios disciplinares e societais, com vista a acompanhar a execução e a avaliar o impacto desta mesma estratégia na sociedade;
- Compreender a situação concreta da Cibersegurança no país nas várias esferas em que incide a respetiva temática;
- Produzir um Relatório sobre os Setores dos OSE que engloba a caracterização, regulamentação e recomendações, no âmbito do Observatório de Cibersegurança, de modo a mensurar o estado da cibersegurança nacional no que diz respeito aos diversos setores dos OSE designados no RJSC;
- Criar um documento base aprofundado e tematicamente transversal e um caderno simplificado por cada setor suscetível de constituir um guia a entregar aos OSE.

O relatório elaborado atenderá aos seguintes pontos na análise setorial:

- Elementos de contexto:
 - Impacto socioeconómico;
 - Especificidades tecnológicas;
- Ameaças;
- Capacitação;
- Investimento em cibersegurança;
- RJSC e legislação setorial;
- Standards e boas práticas aplicáveis;
- Desafios;
- Recomendações.

Sublinha-se ainda que, no ponto relativo ao RJSC e legislação setorial, se inclui, em cada setor, uma breve análise sobre a nova Diretiva NIS 2, incidindo sobre as novas entidades abrangidas e sobre as novas obrigações face ao diploma.

Contexto Geral

Tal como já referido, um OSE é “uma entidade pública ou privada que presta um serviço essencial⁴ (...) para a manutenção de atividades societais ou económicas cruciais”⁵.

A estabilidade e eficiência da operação destes serviços impactam diretamente a qualidade de vida dos cidadãos e a competitividade do país. Por exemplo, no setor energético, a oferta confiável de eletricidade é essencial para as atividades dos operadores, para os serviços do Estado e para o quotidiano dos cidadãos, influenciando diretamente a produtividade e a atividade económica.

Além disso, os OSE desempenham um papel estratégico na implementação de políticas governamentais, tais como as relacionadas com a sustentabilidade ambiental e a inovação tecnológica. A segurança e resiliência digital destes operadores é, por isso, crucial para o crescimento sustentável de Portugal e da UE.

A Diretiva NIS indica que cada Estado-membro é responsável por determinar as entidades que preenchem os critérios da definição de OSE, indicando setores e subsetores a incluir, bem como realizando remissões para outras Diretivas de modo a caracterizar o tipo de entidades a considerar.

De um modo geral, a Diretiva NIS indica ainda que devem ser considerados os seguintes critérios para verificar se uma entidade é um OSE:

- A entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais;
- A prestação desse serviço depende de redes e sistemas de informação; e
- Um incidente pode ter efeitos perturbadores importantes na prestação desse serviço⁶.

Assim, segundo a Lei n.º 46/2018, foram explicitados os seguintes setores, subsetores e tipos de entidades:

⁴ Lei n.º 46/2018, artigo 3.º, alínea g).

⁵ Lei n.º 46/2018, artigo 3.º, alínea t).

⁶ Lei n.º 46/2018, artigo 3.º, alínea t).

Tabela 1 - Setores, Subsetores e Tipos de Entidades

Setor	Subsetor	Tipos de Entidades
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização
		Operadores da rede de distribuição
		Operadores da rede de transporte
	Petróleo	Operadores de oleodutos de petróleo
		Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
	Gás	Empresas de comercialização
		Operadores da rede de distribuição
		Operadores da rede de transporte
		Operadores do sistema de armazenamento
		Operadores da rede de gás natural em estado líquido (GNL)
		Empresas de gás natural
		Operadores de instalações de refinamento e tratamento de gás natural
Transportes	Transporte aéreo	Transportadoras aéreas
		Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos
		Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo
	Transporte ferroviário	Gestores de infraestruturas
		Empresas ferroviárias incluindo os operadores de instalações de serviço

	Transporte marítimo e por vias navegáveis interiores	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias
		Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos
		Operadores de serviços de tráfego marítimo
	Transporte rodoviário	Autoridades rodoviárias
		Operadores de sistemas de transporte inteligentes
Bancário		Instituições de crédito
Infraestruturas do mercado financeiro		Operadores de plataformas de negociação
		Contrapartes centrais (CCPs)
Saúde	Instalações de prestação de cuidados de saúde	Prestadores de cuidados de saúde
Fornecimento e distribuição de água potável	-	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais
Infraestruturas digitais		Pontos de troca de tráfego
		Prestadores de serviços de Sistema de Nomes de Domínio (<i>Domain Name Services, DNS</i>)
		Registos de nomes de domínio de topo

Análise do questionário dirigido aos Reguladores de Serviços Essenciais

No âmbito deste relatório, de modo a melhor reconhecer e analisar o atual estado de cibersegurança nos setores relativos aos Operadores de Serviços Essenciais (OSE), foram elaborados dois questionários para auxiliar essa análise. O primeiro relatório foi dirigido às entidades reguladoras dos setores em questão, e o segundo aos próprios Operadores de Serviços Essenciais desses setores.

Atendendo às diferenças entre as atividades de um Regulador e as atividades de um OSE, os questionários realizados são também distintos entre si, apesar de ambos incidirem sobre cibersegurança.

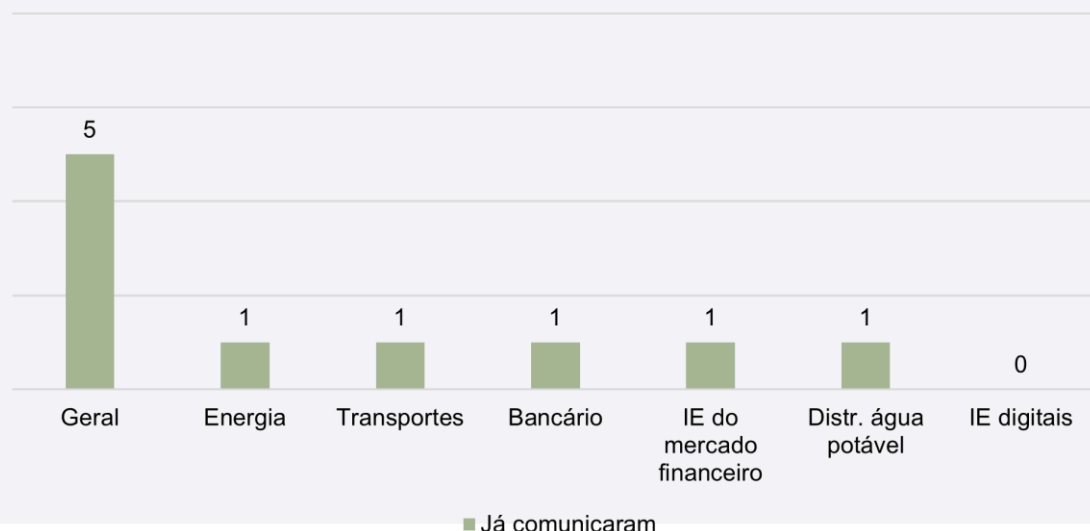
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez, é mais extenso, incidindo sobre as dimensões humanas, técnico-tecnológicas, processuais e de investimento ao nível da cibersegurança. As respostas a estes questionários foram recolhidas entre 11 e 29 de setembro de 2023.

O questionário aos reguladores foi partilhado com 11 entidades reguladoras. De entre estas 11, oito responderam ao questionário. Entre as oito entidades que responderam, contam-se uma entidade reguladora do setor da energia, três do setor dos transportes, uma do setor das infraestruturas do mercado financeiro (IMF), uma do setor bancário, uma do setor do fornecimento e distribuição de água potável e uma do setor das infraestruturas digitais. Nenhuma entidade reguladora do setor saúde respondeu ao questionário. Atendendo ao reduzido número de entidades reguladoras, os resultados são apresentados com números inteiros e não com percentagens.

O questionário destinado aos Operadores de Serviços Essenciais foi partilhado com 415 entidades - o número de entidades que reportaram ter responsável de segurança - tendo sido obtidas 200 respostas válidas. Destas 200 respostas, registaram-se oito do setor da energia, 26 do setor dos transportes, nove do setor bancário, 3 das infraestruturas do mercado financeiro (IMF), 40 do setor saúde, 89 do setor do fornecimento e distribuição de água potável e 25 do setor das infraestruturas digitais. Os resultados obtidos neste questionário são apresentados em percentagens.

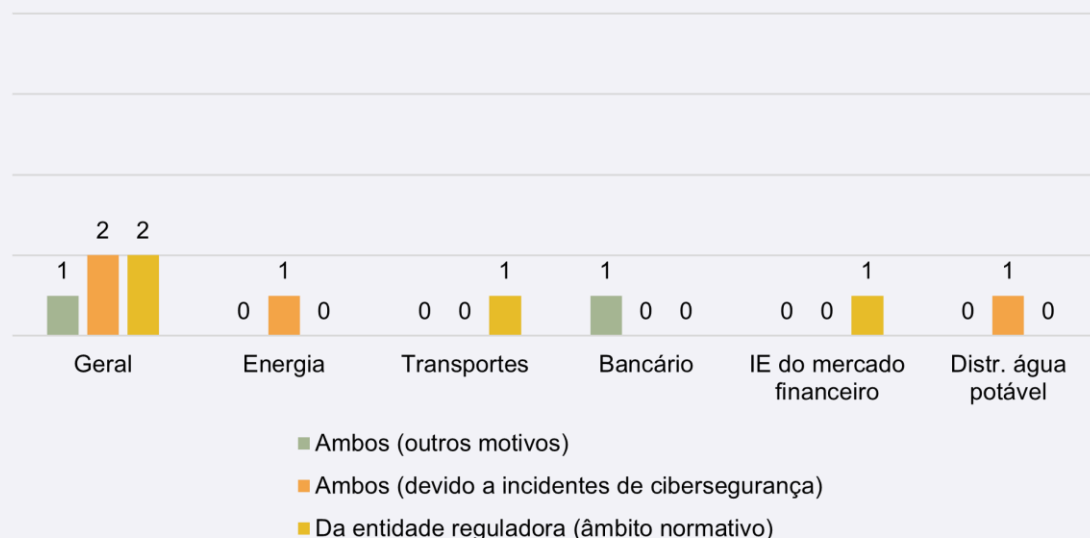
1. Comunicação entre OSE e respetivos Reguladores

Gráfico 1 - Reguladores que já comunicaram com os OSE sobre questões de cibersegurança



Entre os oito reguladores que responderam, cinco indicaram já ter comunicado com os OSE sobre questões de cibersegurança. Deve-se, no entanto, sublinhar que no setor dos transportes, registaram-se as respostas de três reguladores e que apenas um indicou já ter comunicado com os OSE sobre questões de cibersegurança. O regulador inquirido do setor das infraestruturas digitais também não indicou ter realizado qualquer comunicação sobre estas matérias aos OSE por si regulados.

Gráfico 2 - Origem da comunicação sobre questões de cibersegurança

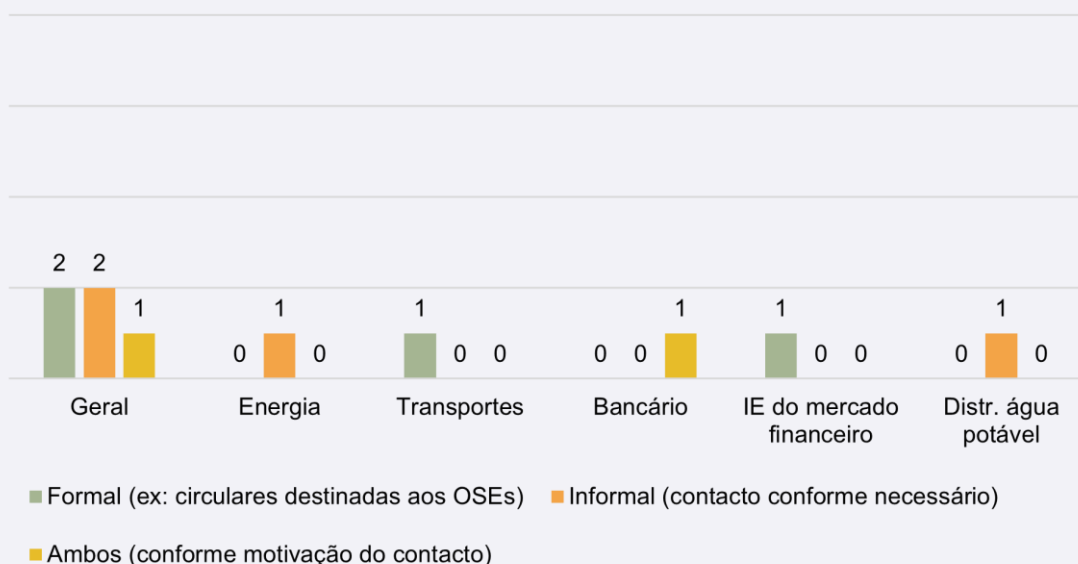


Relativamente à origem da comunicação sobre cibersegurança realizada por cinco dos reguladores, dois indicaram que a comunicação partiu dos próprios, em contexto de informação sobre normas do setor, outros dois responderam que houve comunicação que se gerou a partir dos dois lados,

devido à ocorrência de incidentes de cibersegurança e apenas um (o regulador do setor bancário) respondeu que houve comunicação sobre cibersegurança a ser realizada com os OSE devido a outros motivos. A questão não é aplicável ao setor das infraestruturas digitais pois o setor nunca efetuou qualquer comunicação.

O regulador do setor bancário foi bastante explícito sobre quais foram esses outros motivos. O mesmo indicou que existe uma interação normal de diálogo no âmbito da supervisão feita pelo regulador, como nas situações recorrentes de análise e avaliação ou de inspeções nas instalações dos OSE. Há também uma interação periódica que ocorre no seio da participação no Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO), fórum esse que inclui momentos específicos para a discussão sobre riscos e incidentes de cibersegurança. Para além destes, existe a comunicação espoletada pela ocorrência de incidentes, em que tanto pode haver a necessidade de o regulador informar os OSE sobre incidentes ocorridos, por exemplo, com o sistema SWIFT⁷, ou quando os próprios OSE comunicam detalhes sobre os incidentes que os afetaram a si. Por fim, há a comunicação realizada pontualmente através de instrumentos regulamentares emitidos pela entidade reguladora sobre matérias relevantes de forma transversal.

Gráfico 3 - Formalidade da comunicação realizada



Entre os mesmos cinco reguladores, mantendo a exclusão do setor das infraestruturas digitais, dois indicaram que a comunicação é geralmente feita de modo formal (setor dos transportes e setor das infraestruturas do mercado financeiro), através de, por exemplo, circulares; outros dois responderam que a comunicação é sobretudo informal, consoante a necessidade (setor da energia e setor da distribuição de água potável) e apenas o regulador do setor bancário indicou haver comunicação tanto de carácter formal como mais informal.

⁷ SWIFT é a sigla para "Society for Worldwide Interbank Financial Telecommunications". O sistema SWIFT é composto pelas várias entidades financeiras que são membros da SWIFT, às quais é atribuído um código SWIFT e que permite comunicações seguras entre essas mesmas entidades, incluindo transferências monetárias internacionais e a transmissão de instruções de pagamento, entre outras funcionalidades.

Gráfico 4 - Frequência da comunicação

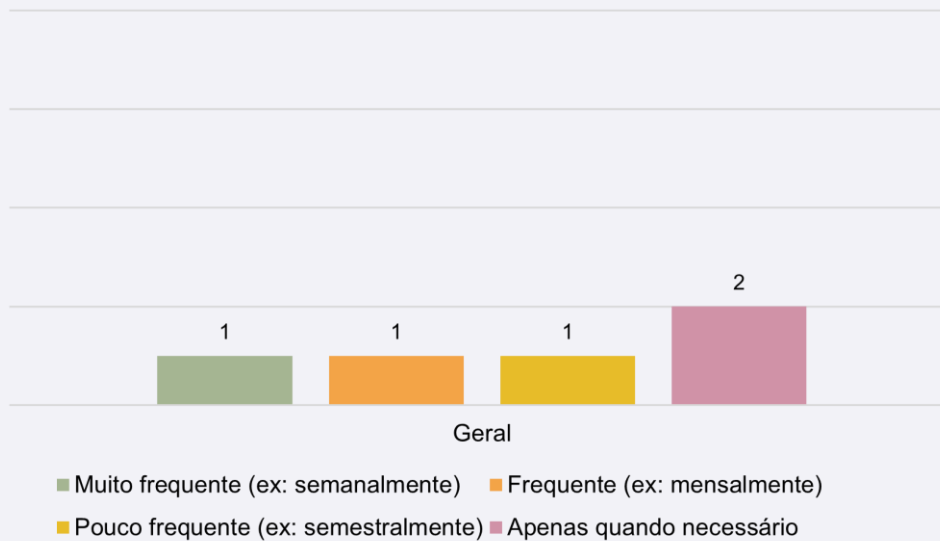
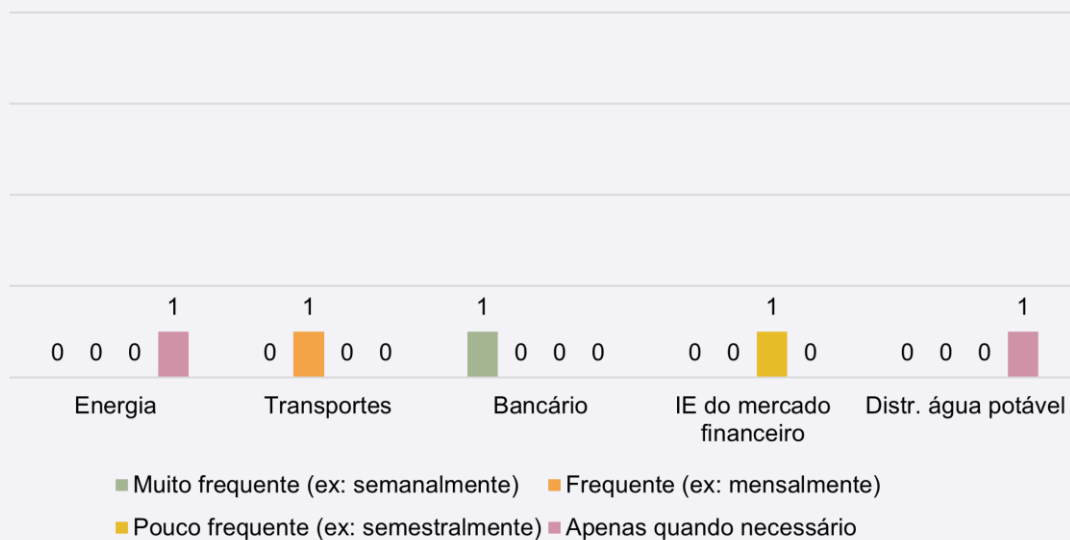


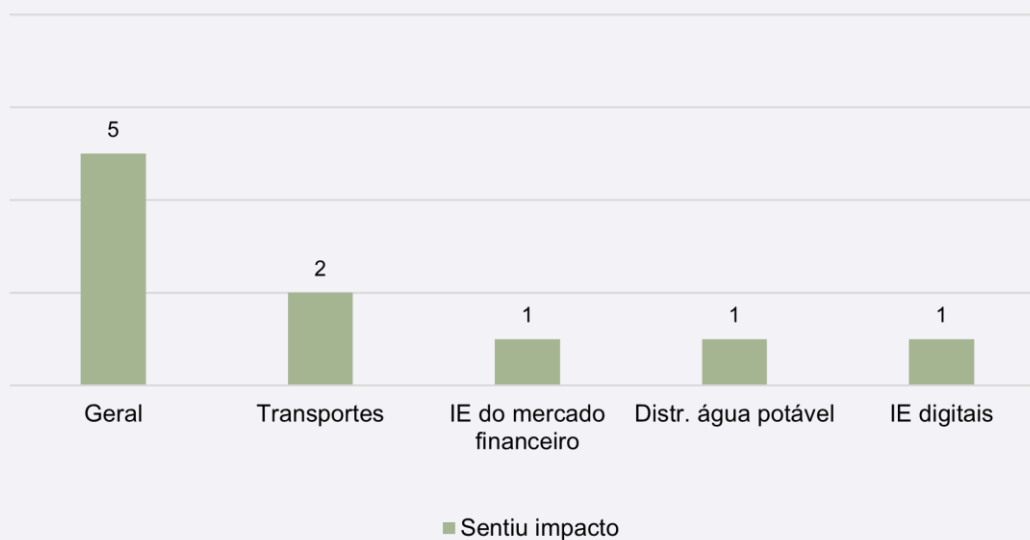
Gráfico 4.1 - Frequência da comunicação



No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. O regulador do setor bancário foi o único a indicar que a comunicação é realizada muito frequentemente, praticamente de forma semanal. Já o regulador dos transportes indicou comunicar com os OSE sobre cibersegurança com uma frequência mensal. Por sua vez, o regulador das IMF indicou que a frequência de comunicação com os OSE sobre questões de cibersegurança é pouco frequente, ocorrendo, por exemplo, semestralmente. Por fim, os setores da energia e da distribuição de água potável foram os que responderam que a comunicação é realizada apenas quando necessário, não havendo frequência ou periodicidade estimadas. Mantém-se a exclusão do setor das infraestruturas digitais.

2. Impacto da publicação da Diretiva NIS ou da transposição da mesma (publicação da Lei n.º 46/2018)

Gráfico 5 - Impacto sentido na sua organização e nos OSE regulados



Questionou-se aos reguladores se sentiram impacto nas suas organizações e nos OSE por si regulados pela publicação da Diretiva NIS. Entre os oito reguladores que responderam, cinco indicaram ter sentido esse impacto. Esse impacto ter-se-á então feito sentir no setor dos transportes, em que dois dos três reguladores inquiridos concordaram com a afirmação, no setor das infraestruturas do mercado financeiro, no setor da distribuição de água potável e no setor das infraestruturas digitais. Ver-se-á, de seguida, quais foram os impactos sentidos.

Gráfico 6 - Dificuldades sentidas relativamente à conformidade com a Diretiva NIS / Lei n.º 46/2018

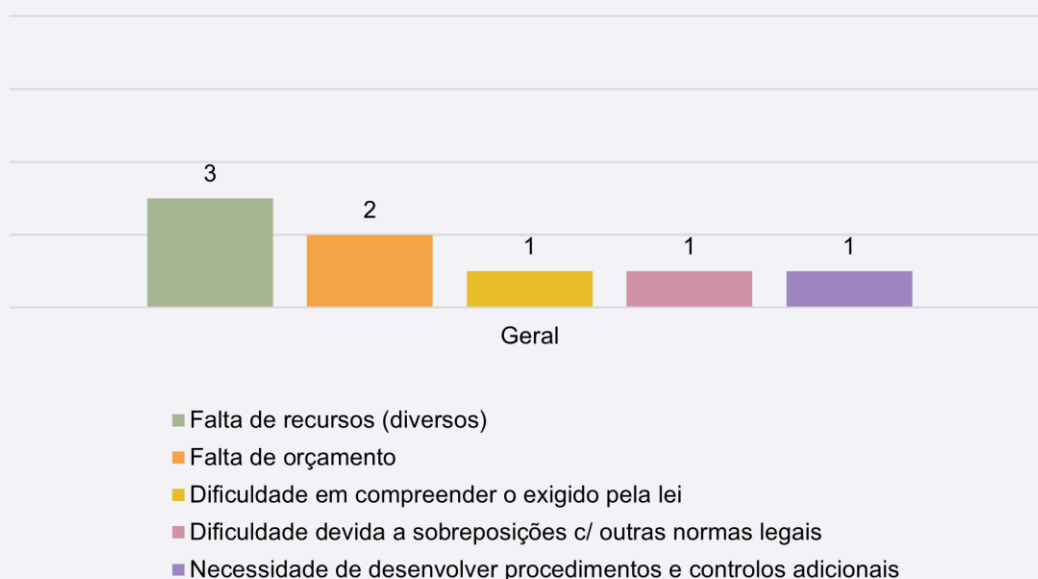
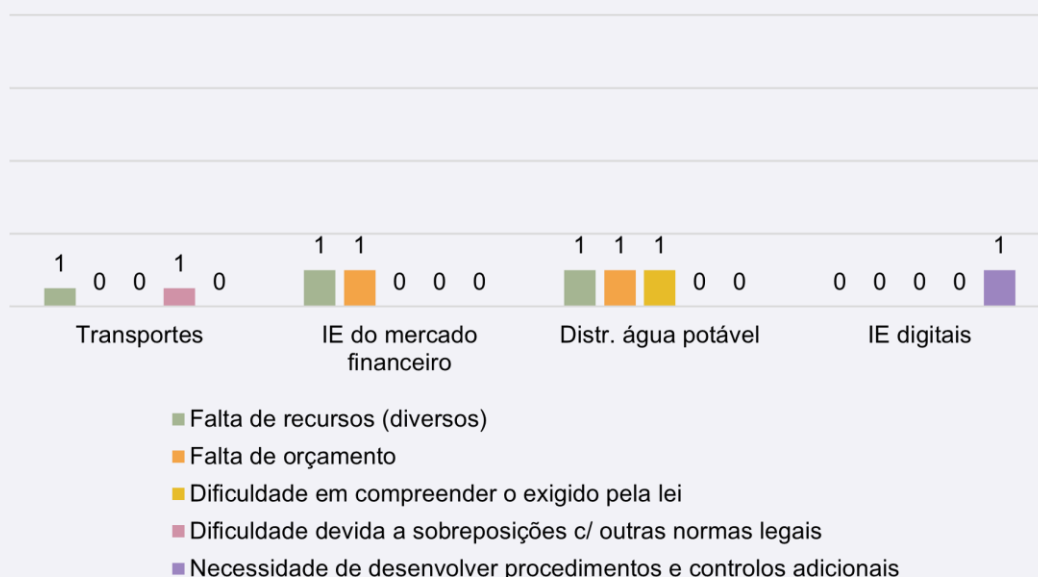


Gráfico 6.1 - Dificuldades sentidas relativamente à conformidade com a Diretiva NIS / Lei n.º 46/2018



Três dos cinco reguladores que indicaram ter sentido impacto na sua organização ou nos OSE por si regulados devido à publicação da Diretiva NIS afirmaram que uma das dificuldades encontradas foi a falta de recursos diversos para estar em conformidade com a mesma. Esta dificuldade foi indicada por um dos reguladores dos transportes, pelo regulador das IMF e pelo regulador do setor do fornecimento e distribuição de água potável.

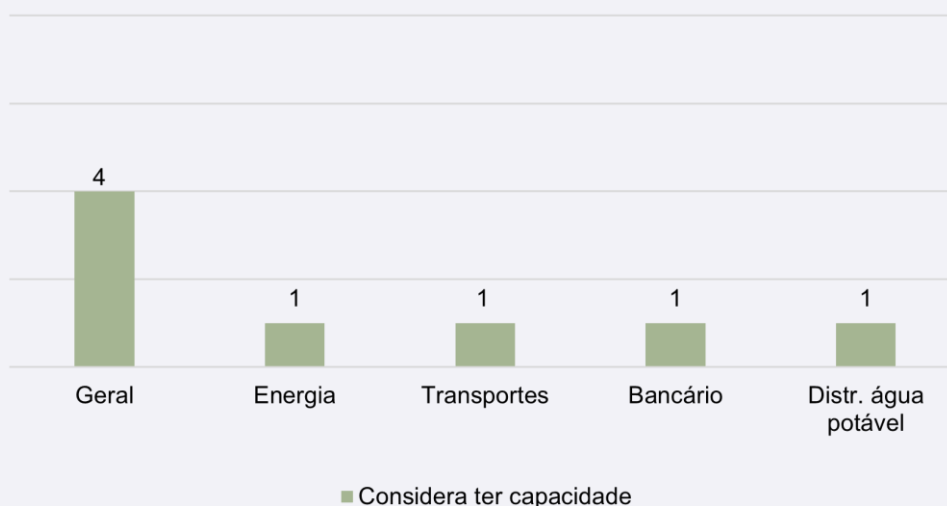
Os reguladores das IMF e o da distribuição de água potável indicaram também a falta de orçamento a conformidade com regime jurídico, como outra das dificuldades sentidas. Soma-se ainda, pelo

regulador do setor da distribuição de água, a dificuldade em compreender o que era exigido pela nova legislação, tendo este sido o único setor a apontar esta dificuldade. O setor da energia e o setor bancário não são abordados pois nenhum inquirido mencionou dificuldades. Dificuldades relativas à sobreposição com outras normas legais foram indicadas apenas por um dos reguladores do setor dos transportes. Já a necessidade de desenvolver procedimentos e controlos adicionais foi unicamente indicada pelo regulador do setor das infraestruturas digitais.

De acordo com um inquérito realizado pela ENISA, a implementação da diretiva NIS tem, normalmente, um efeito positivo nos OSE e provedores de serviços digitais. Este inquérito foi feito a 251 organizações (oriundas da França, Alemanha, Itália, Espanha e Polónia) e, destas, cerca de 58% já tinham estabelecido e completado a implementação da diretiva NIS. Cerca de 23% ainda estavam a implementar e 8% tinham planeado implementar a diretiva. Por outro lado, 10% não vão implementar a diretiva, mas vão usar a mesma como guia para o seu programa de segurança e só um referiu que não iria implementar a diretiva, nem seguir a mesma⁸.

3. Supervisão dos OSE em matéria legislativa de cibersegurança por parte dos Reguladores

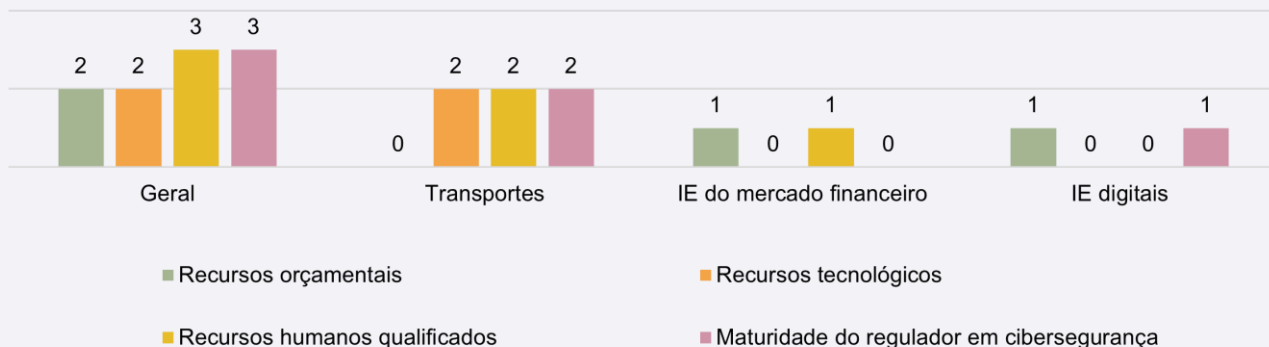
Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSE em matéria de cibersegurança, em caso de atribuição da competência



Foi questionado aos reguladores se teriam capacidade para realizar a supervisão dos operadores em matéria de cibersegurança. O número de respostas dividiu-se igualmente entre os que consideram ter a capacidade para realizar essa supervisão e os que não consideram tê-la (quatro reguladores consideram ter essa capacidade, outros quatro consideram não a ter). Posto isto, os reguladores inquiridos do setor da energia, bancário e da distribuição de água potável consideram ter a capacidade para realizar a supervisão dos operadores em matéria de cibersegurança. No setor dos transportes, apenas um dos três reguladores inquiridos considera ter a capacidade necessária para realizar essa supervisão em caso de atribuição da competência. Já os reguladores dos setores das infraestruturas do mercado financeiro e das infraestruturas digitais, indicaram não considerar ter essa capacidade.

⁸ ENISA, "NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist", 11 de dezembro de 2020, <https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist>.

Gráfico 8 - Recursos em falta para a capacidade de supervisão em matéria de cibersegurança



Entre os reguladores que consideram não ter essa capacidade, dois deles indicaram não ter suficientes recursos orçamentais, dois mencionaram suficientes recursos tecnológicos e três suficiente maturidade em cibersegurança. Além destes, três das entidades que consideram não ter a capacidade de realizar essa supervisão entendem não ter os recursos humanos suficientes para tal. Como os reguladores do setor da energia, bancário e distribuição de água potável referiram ter a capacidade necessária para realizar a supervisão, esta questão não se aplica.

No setor dos transportes, os dois reguladores que consideram não ter capacidade para realizar a supervisão dos operadores em matéria de cibersegurança indicaram não ter suficientes recursos tecnológicos, recursos humanos e suficiente maturidade em cibersegurança. Já nas infraestruturas do mercado financeiro, os principais recursos em falta para que essa supervisão possa ser realizada são recursos orçamentais e recursos humanos qualificados, já nas infraestruturas digitais, os principais recursos em falta indicados foram os recursos orçamentais e os recursos humanos qualificados.

A falta de recursos humanos qualificados em cibersegurança é um tema que surge repetidamente nas respostas tanto dos reguladores como dos OSE. Dados do Fórum Económico Mundial evidenciam uma escassez global de cerca 4 milhões de profissionais em cibersegurança⁹, escassez essa que coloca diversas dificuldades não só aos reguladores e aos OSE dos setores em análise, mas também noutras organizações e setores de atividade. Este tema é explorado em maior detalhe na análise do **Gráfico 44**.

⁹ World Bank, "Strategic Cybersecurity Talent Framework - White Paper", abril de 2024, 4, https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

4. Maturidade em cibersegurança no setor

Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores

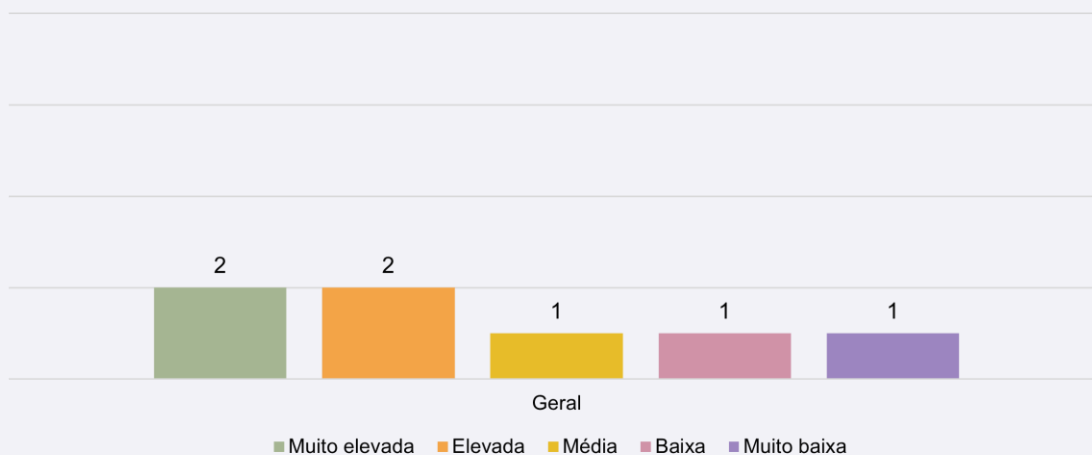
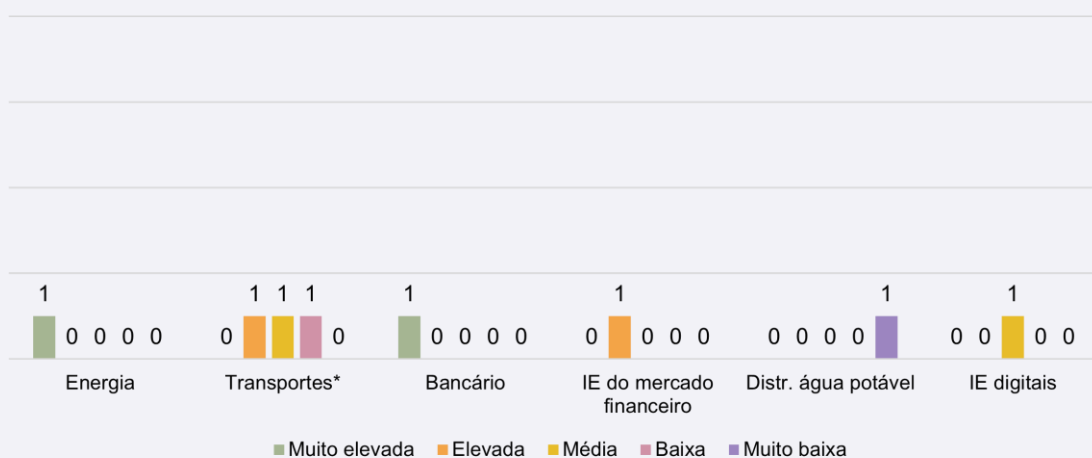


Gráfico 9.1 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores



A perceção dos reguladores sobre a maturidade em cibersegurança dos operadores varia entre os diversos reguladores dos diferentes setores. Entre os inquiridos, apenas dois dos oito reguladores consideram que a maturidade nos seus setores é muito elevada, sendo estes o da energia e o do setor bancário. No setor dos transportes, a perceção sobre o nível de maturidade varia entre os três reguladores inquiridos, com um destes a considerar que o nível é elevado, outro a considerar que é médio e o terceiro a considerar que a maturidade tem um nível baixo. O regulador das infraestruturas do mercado financeiro considera que a maturidade é elevada, o regulador do setor da distribuição de água potável é o único a considerar que a maturidade do seu setor é muito baixa e, por fim, o regulador do setor das infraestruturas digitais considera que a maturidade no setor é média.

Gráfico 10 - Medidas adotadas pelas entidades reguladoras para promover a maturidade em cibersegurança

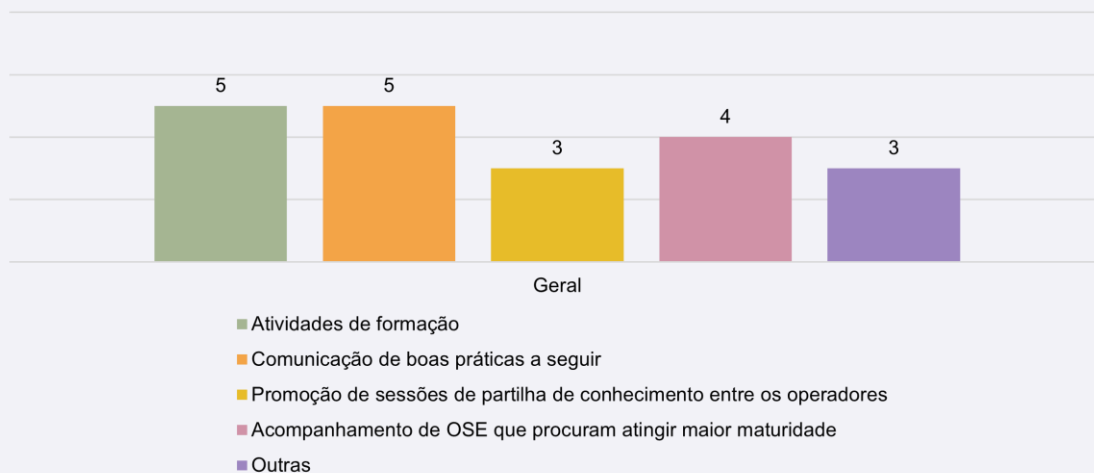


Gráfico 10.1 - Medidas adotadas pelas entidades reguladoras para promover a maturidade em cibersegurança

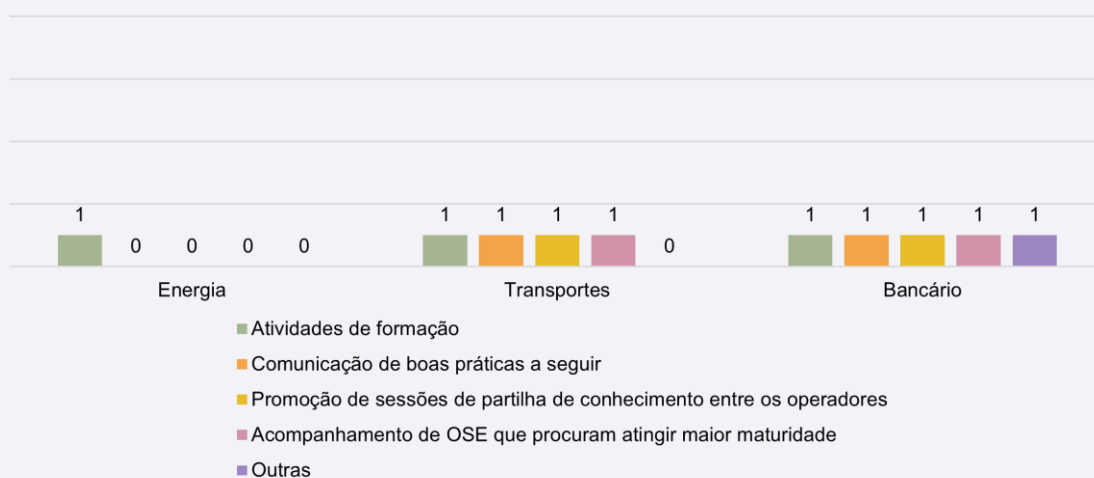
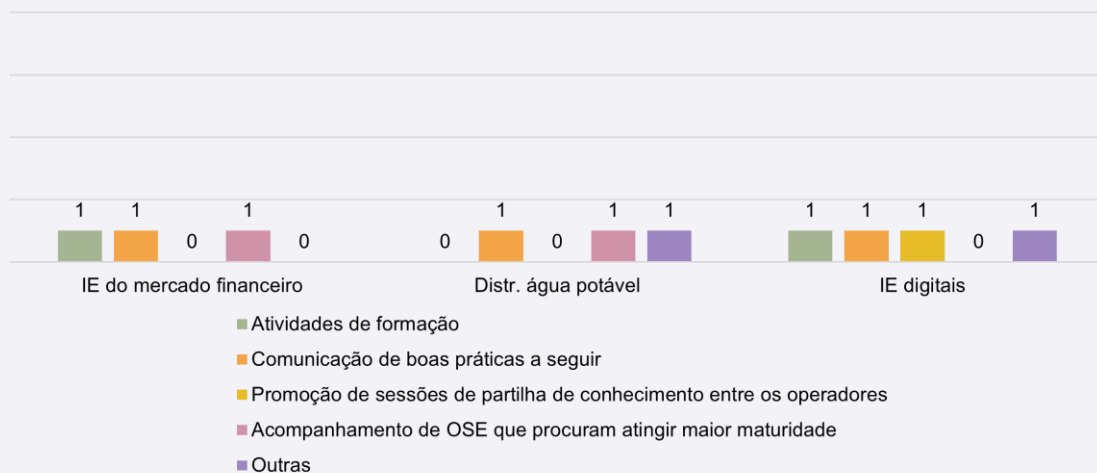


Gráfico 10.2 - Medidas adotadas pelas entidades reguladoras para promover a maturidade em cibersegurança



Os reguladores tentam promover a maturidade em cibersegurança nos seus respetivos setores através da adoção de diferentes medidas. Cinco dos reguladores inquiridos - regulador do setor da energia, um dos reguladores do setor dos transportes, o regulador do setor bancário, o das IMF e o das infraestruturas digitais - promovem atividades de formação num esforço para aumentar a maturidade no setor. Verifica-se o mesmo número de reguladores a recomendar boas práticas a seguir. O regulador do setor da energia não efetua comunicação de boas práticas a seguir já o setor o regulador do setor da distribuição de água potável embora não realize atividades de formação, realiza comunicações de boas práticas.

Relativamente à promoção de sessões de partilha de conhecimento, apenas três reguladores indicaram fazê-lo (regulador do setor dos transportes, do setor bancário e do setor das infraestruturas digitais). Quanto ao acompanhamento de OSE que procurem atingir maior maturidade em cibersegurança, quatro entidades referiram fazer esse acompanhamento, sendo estas uma das entidades reguladoras do setor dos transportes, o regulador do setor bancário, o regulador das IMF, e o regulador do setor da distribuição de água potável.

Gráfico 11 - Perceção sobre o número de profissionais capacitados em matéria de cibersegurança na entidade reguladora

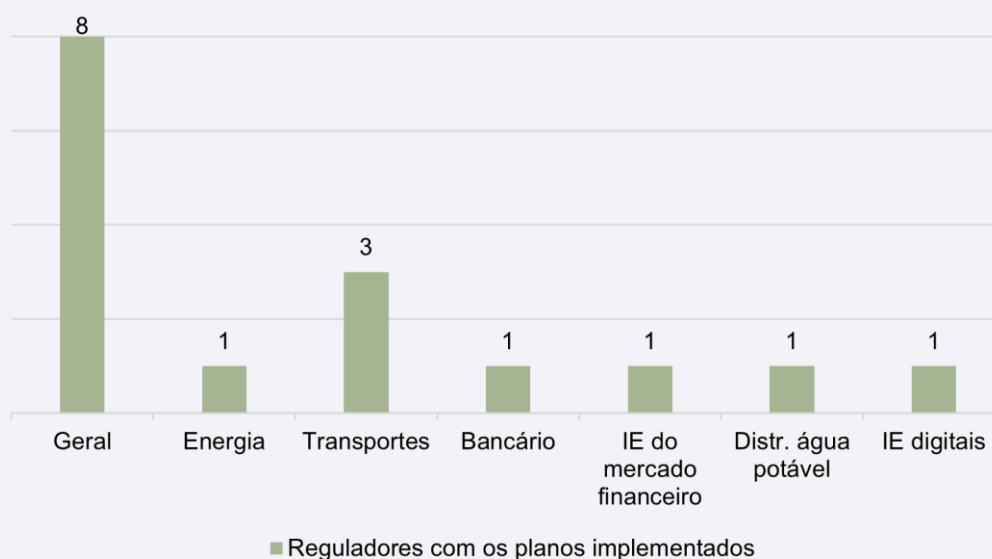


Apenas duas das entidades reguladoras inquiridas, nomeadamente do setor bancário e do setor das infraestruturas digitais, consideram ter suficientes profissionais capacitados em matéria de cibersegurança, enquanto os restantes seis (regulador do setor da energia, três reguladores do setor dos transportes e o regulador das IMF e o da distribuição de água potável) não consideram ter suficientes profissionais capacitados na área.

Novamente, estes resultados prender-se-ão com a escassez global de profissionais em cibersegurança já referida no

Gráfico 8 e que é analisada em detalhe no **Gráfico 44**.

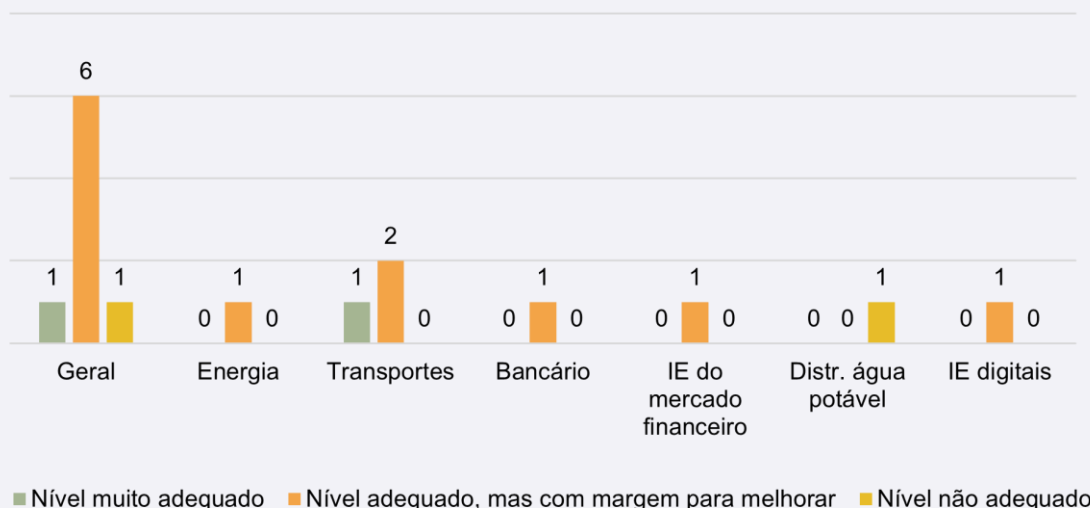
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados



Todas as entidades reguladoras inquiridas referiram ter os planos de segurança e de resposta a incidentes implementados.

5. Nível de segurança estabelecido pela legislação em vigor

Gráfico 13 - Perceção dos reguladores sobre o nível de cibersegurança estabelecido pela Diretiva NIS 1 / lei n.º 46/2018, de 13 de agosto, face aos desafios, perigos e ameaças existentes



Na generalidade, a maioria dos reguladores dos OSE, nomeadamente seis, consideram que a Diretiva NIS procura estabelecer um nível adequado de cibersegurança entre os OSE, mas com margem para melhorar, face aos atuais desafios, perigos e ameaças nesta matéria. Apenas um regulador considera que o nível de cibersegurança que a Diretiva NIS procura estabelecer é muito adequado, e outro regulador do setor da distribuição de água potável considera que a Diretiva não leva os operadores a estabelecerem um nível adequado de cibersegurança face aos atuais perigos, desafios e ameaças. No setor da energia, o regulador inquirido considera que o nível de cibersegurança estabelecido pela Diretiva NIS é adequado, mas com margem para melhorar, tal como o setor bancário, setor das infraestruturas do mercado financeiro e infraestruturas digitais.

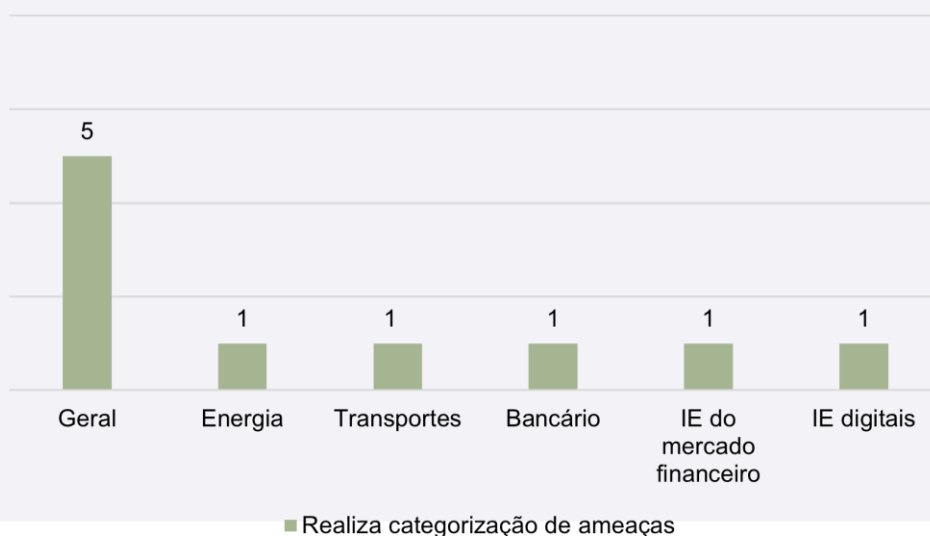
No setor dos transportes, um dos três reguladores considera que o nível de cibersegurança estabelecido pela Diretiva NIS é muito adequado e os outros dois reguladores consideram que o nível estabelecido é adequado, mas que tem margem para melhorar enquanto o regulador inquirido do setor da água considera que o nível de cibersegurança que a Diretiva NIS procura estabelecer não é adequado face aos perigos e ameaças vigentes. Uma questão semelhante foi colocada, em 2021, não aos reguladores, mas a diversos OSE na União Europeia, no âmbito do relatório *NIS Investments 2021*. As respostas recolhidas indicam que quase 50% (48,9%) dos operadores de serviços essenciais consideram que a Diretiva NIS teve um impacto positivo nas suas organizações e na União, aumentando o nível de cibersegurança das organizações, ao fortalecer as suas capacidades de deteção e de recuperação de incidentes¹⁰.

¹⁰ ENISA, "NIS Investments", novembro de 2021, 5, <https://www.enisa.europa.eu/publications/nis-investments-2021>.

Importa sublinhar que a Diretiva NIS tem já cerca de oito anos, e a sua transposição, cerca de seis anos. Face à rápida evolução dos cenários das ciberameaças e ao tempo que a implementação de novas diretivas costuma levar, é expectável que rapidamente se comecem a identificar pontos que poderiam ser melhorados. É também por esse motivo que as instituições europeias têm continuado o seu trabalho num esforço de melhorar o nível de cibersegurança da União, através de novas diretivas, como a NIS 2, que abrange novos setores, e através de novos regulamentos, como o *Digital Operational Resilience Act* (DORA), destinado ao setor financeiro, e o *Cyber Resilience Act* (CRA) que estabelece novos requisitos de cibersegurança para produtos com elementos digitais.

6. Categorização de ameaças

Gráfico 14 - Reguladores que se encontram a fazer categorização de ameaças de cibersegurança



Cinco dos oito reguladores inquiridos - o do setor da energia, um dos três reguladores no setor dos transportes, o do setor bancário, o das infraestruturas do mercado financeiro e o do setor das infraestruturas digitais realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores do setor dos transportes e o regulador do setor do fornecimento e distribuição de água potável.

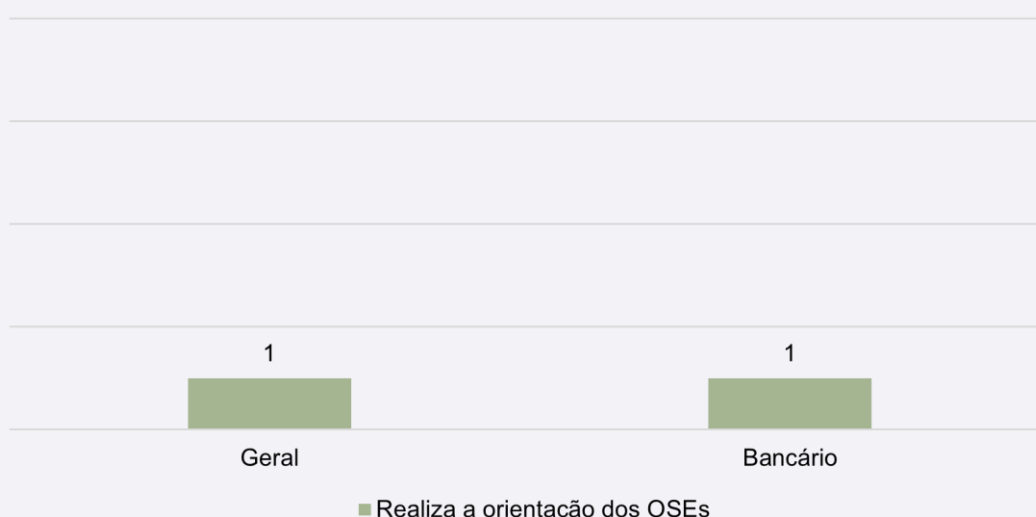
Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização



Dos cinco reguladores que realizam categorização de ameaças, apenas dois partilham informação relativa às ameaças com os OSE, sendo estes o regulador do setor dos transportes e o regulador do setor bancário. Os restantes setores não efetuam a partilha de informação, nomeadamente o setor da energia, infraestruturas do mercado financeiro e infraestruturas digitais. No caso do setor de distribuição de água potável a questão não se aplica.

7. Orientação dos OSE por parte da entidade reguladora

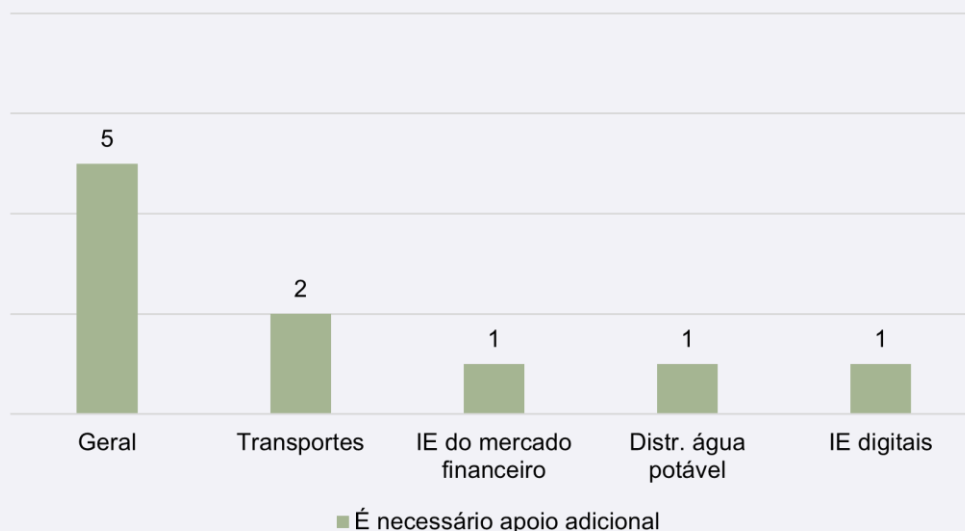
Gráfico 16 - Reguladores que orientam os OSE na digitalização de processos e na promoção de uma cultura digital



Apenas um dos reguladores (o do setor bancário) indicou fornecer orientação aos OSE na digitalização de processos e na promoção de uma cultura digital, enquanto os restantes sete reguladores indicaram não fazer esse tipo de orientação.

8. Apoio por parte do CNCS

Gráfico 17 - Perceção sobre a necessidade de apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança nos setores regulados



Entre os reguladores inquiridos, cinco (dois dos reguladores do setor dos transportes, o regulador das IMF, o regulador do setor do fornecimento e distribuição de água potável e o regulador das infraestruturas digitais) têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional, sendo estes o regulador do setor da energia, o regulador do setor bancário e um dos reguladores dos transportes.

Gráfico 18 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS

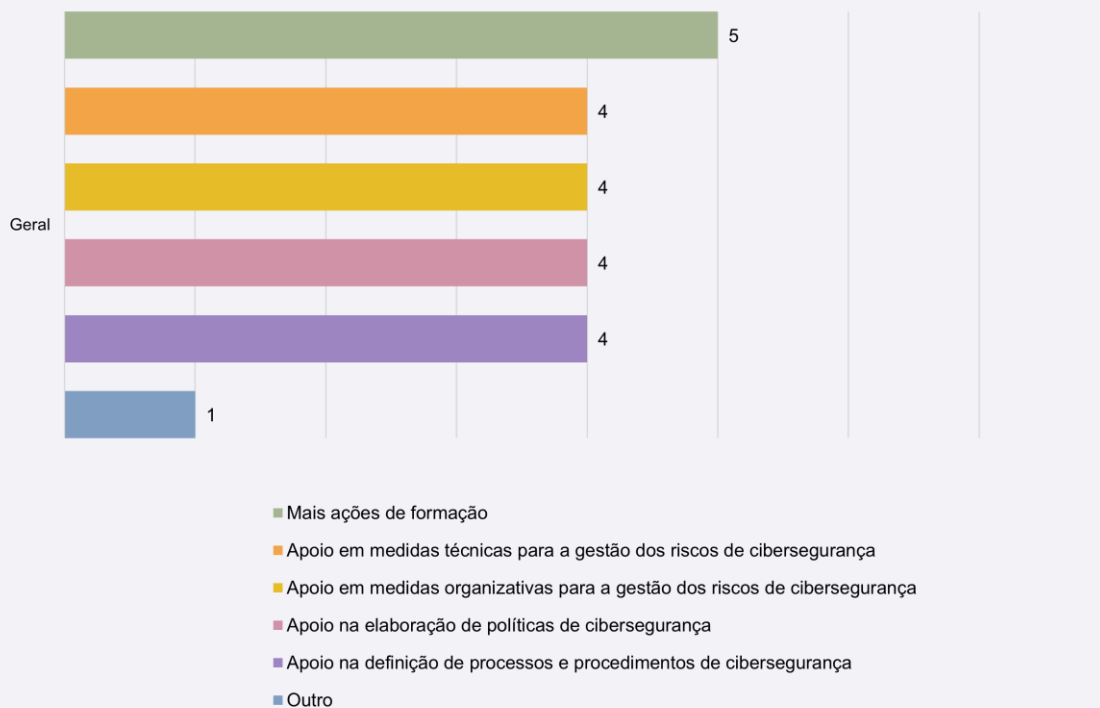


Gráfico 18.1 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS



Gráfico 18.2 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS



Entre os reguladores que consideram necessário apoio adicional do CNCS para que sejam atingidos níveis de maturidade em cibersegurança mais elevados nos vários setores, todos gostariam de ver mais ações de formação realizadas. Além destas, quatro destes reguladores gostariam que houvesse também mais apoio por parte do CNCS relativamente a medidas técnicas e organizativas para a gestão de riscos de cibersegurança, apoio na elaboração de políticas de cibersegurança e ainda apoio na definição de processos e procedimentos de cibersegurança. Dos cinco que consideram necessário apoio adicional, um dos setores gostaria ainda de ver outros apoios, como exercícios conjuntos de cibersegurança e gestão de crises, cocriação, nomeadamente gostariam de ver documentos/orientações/guias para o setor feitos em cooperação com as entidades do setor e o próprio CNCS, avaliação de soluções de confiança, recomendações e casos setoriais, referindo-se a haver também recomendações para os OSE com base em casos concretos ocorridos no setor como por exemplo um ataque a uma infraestrutura e como proteger.

Como o regulador do setor da energia entende não haver necessidade de apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, não é considerado nesta questão. No setor da energia e no setor bancário a questão não se aplica, pois, ambos os setores mencionam não necessitar de apoio adicional.

No setor dos transportes, dois dos três reguladores inquiridos consideram necessário apoio adicional por parte do CNCS, gostariam de ver esse apoio prestada na forma de mais ações de formação, apoio em medidas técnicas e em medidas organizativas para a gestão dos riscos de cibersegurança, na elaboração de políticas de cibersegurança e apoio na definição de processos e procedimentos de cibersegurança bem como outros apoios. Já no setor de infraestruturas do mercado financeiro e no setor da distribuição de água potável, os reguladores inquiridos gostariam de ver esse apoio adicional traduzido em mais ações de formação, apoio em medidas técnicas e organizativas para a gestão dos riscos de cibersegurança, apoio na elaboração de políticas de cibersegurança e apoio na definição de processos e procedimentos de cibersegurança.

Quanto ao regulador inquirido no setor das infraestruturas digitais, este gostaria de ver mais ações de formação e outras medidas como exercícios conjuntos de cibersegurança e gestão de crises, cocriação, avaliação de soluções de confiança, recomendações e casos setoriais.

Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS

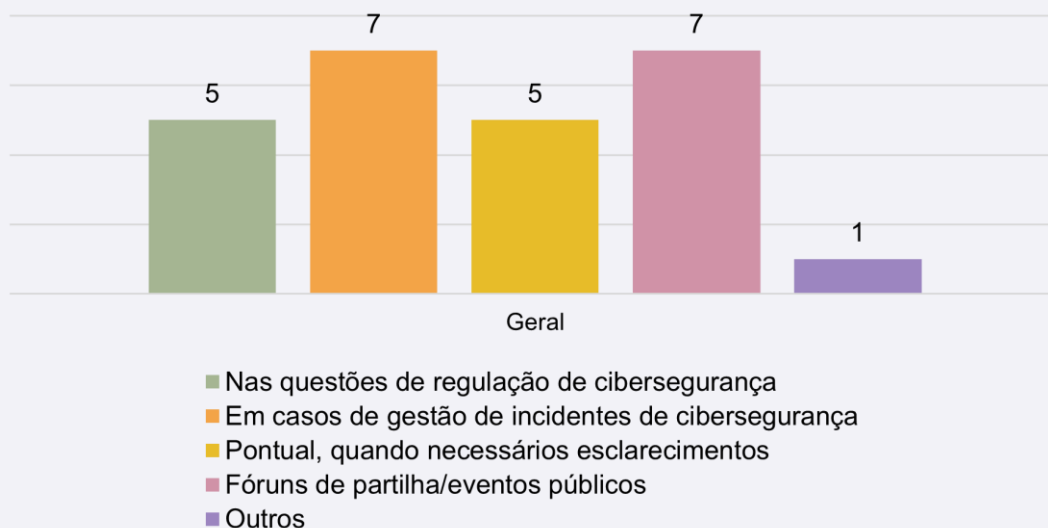


Gráfico 19.1 - Tipos de interação existentes entre reguladores e CNCS

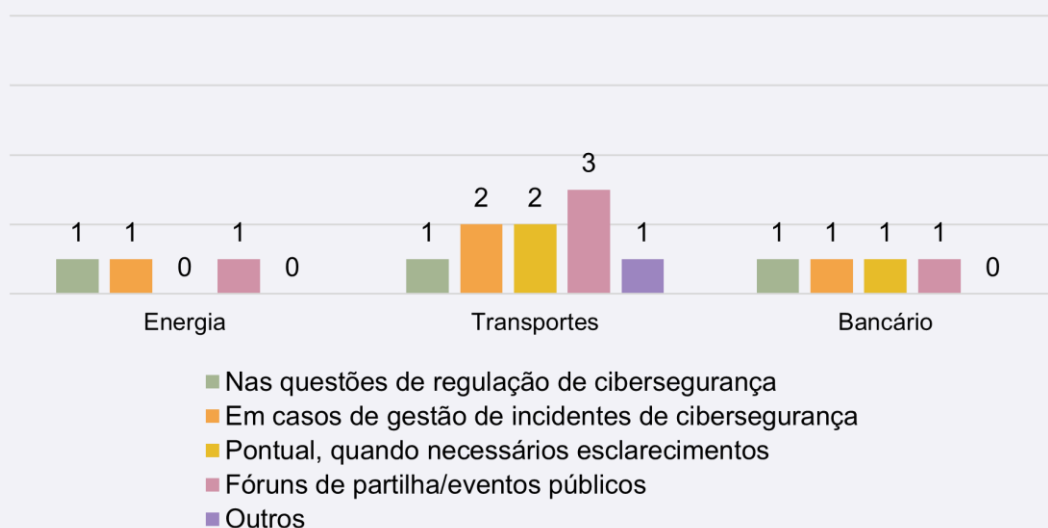
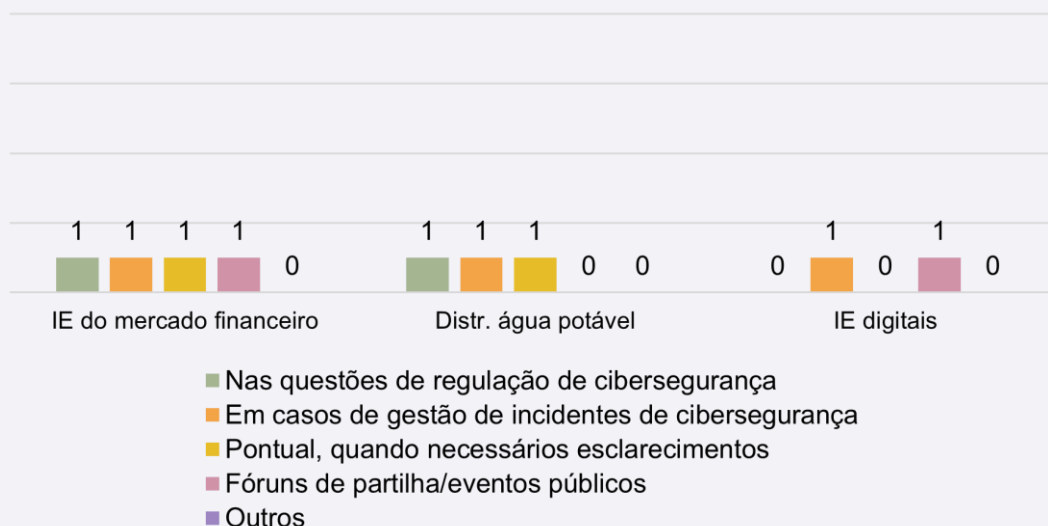


Gráfico 19.2 - Tipos de interação existentes entre reguladores e CNCS



Relativamente às interações entre os reguladores e o CNCS, sete dos reguladores interagem com o Centro no contexto de incidentes de cibersegurança ou em fóruns de partilha/eventos públicos. Já menos reguladores, cinco, interagem com o CNCS devido a questões relacionadas com regulação de cibersegurança ou de forma pontual quando necessita de esclarecimentos em matéria de cibersegurança. Apenas um refere interagir noutros contextos, como na definição de limiares de reporte incidentes.

No setor da energia, bancário, infraestruturas do mercado financeiro e distribuição de água potável, existe um equilíbrio, ambos indicam por norma interagem com o CNCS no âmbito de questões relacionadas com a cibersegurança, em situação de gestão de incidentes de cibersegurança e em fóruns de partilha e eventos públicos. bem como em casos pontuais quando necessário. Quanto ao setor dos transportes, um dos três reguladores referiu haver interação no âmbito de questões de regulação de cibersegurança, dois indicaram haver interação em casos de gestão de incidentes de cibersegurança e de forma pontual, quando são necessários esclarecimentos, todos referiram interagir com o CNCS em fóruns de partilha e eventos públicos. Apenas um dos reguladores referiu outro tipo de interação, relativo à definição de limites de reporte de incidentes.

Gráfico 20 - Áreas através das quais o CNCS poderia prestar mais auxílio

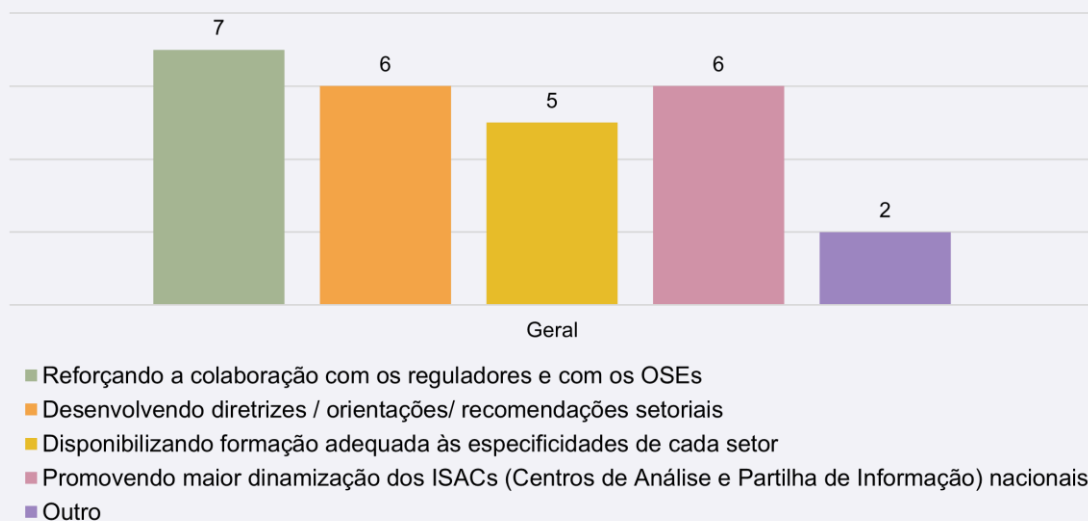


Gráfico 20.1 - Áreas através das quais o CNCS poderia prestar mais auxílio

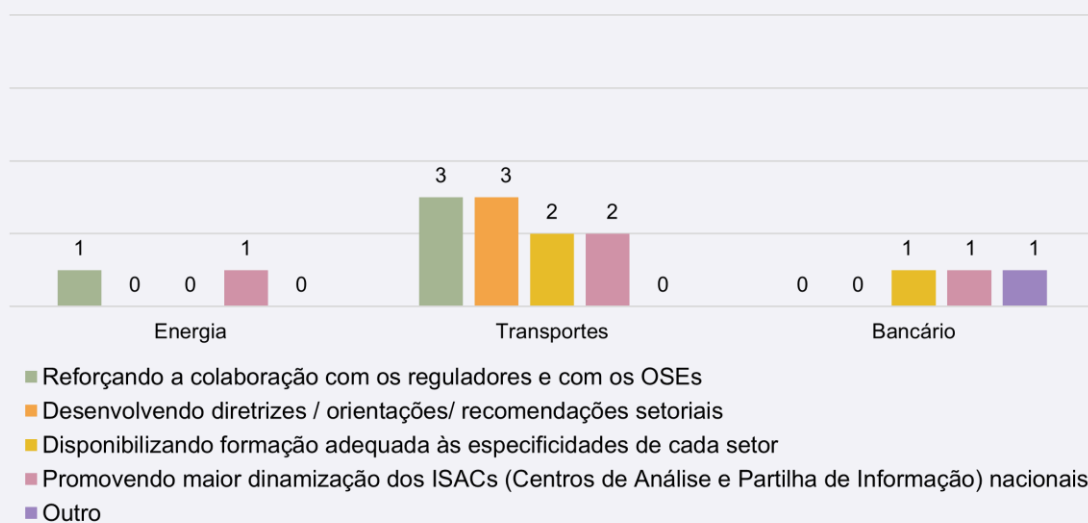
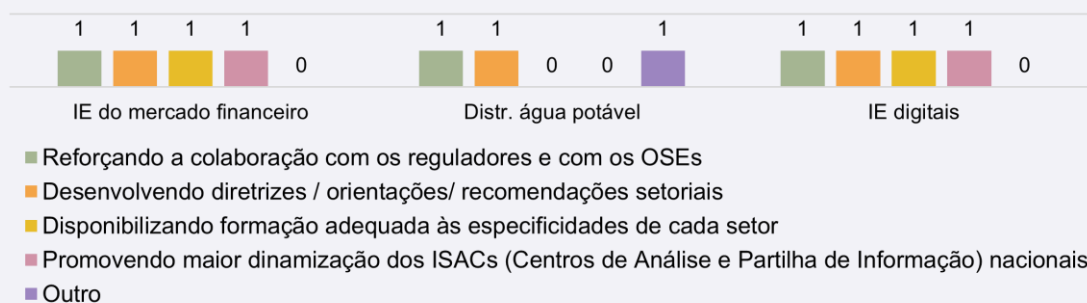


Gráfico 20.2 - Áreas através das quais o CNCS poderia prestar mais auxílio



Relativamente às áreas através das quais o CNCS poderia prestar mais auxílio, sete dos reguladores (excetua-se o regulador do setor bancário) indicaram que este poderia reforçar a colaboração realizada com os reguladores e com os OSE, as áreas de desenvolvimento de diretrizes/orientações/recomendações setoriais e promover mais a dinamização dos Centros de Análise e Partilha de Informação (ISACs) nacionais foram referidas por seis reguladores. De todos os reguladores, cinco indicaram que este poderia prestar mais auxílio através da disponibilização de formação adequada às especificidades de cada setor, enquanto dois referem apoio ao nível do desenvolvimento dos ISACs em alinhamento com os reguladores setoriais.

Tanto no setor bancário como no setor da energia, os reguladores inquiridos consideram que o CNCS poderia promover maior dinamização dos ISACs nacionais, no setor da energia também indicaram que poderiam reforçar a sua colaboração com os reguladores e com os OSE. Já o setor bancário referiu que o CNCS poderia prestar mais auxílio através da disponibilização de formação adequada às especificidades de cada setor, através da alimentação destes com informação.

No setor dos transportes, os três reguladores inquiridos indicam que gostariam de ver o reforço da colaboração do CNCS com os reguladores e operadores, bem como o desenvolvimento de diretrizes, orientações ou recomendações setoriais. Dois dos três reguladores inquiridos referiram ainda que o CNCS poderia prestar mais auxílio através da disponibilização de formação adequada às especificidades de cada setor e promover uma maior dinamização dos ISACs.

Nas infraestruturas do mercado financeiro e nas infraestruturas digitais, os reguladores inquiridos indicaram que gostariam de ver mais auxílio prestado ao nível do reforço da colaboração do CNCS com os reguladores e operadores, ao nível do desenvolvimento de diretrizes, orientações ou recomendações setoriais, da disponibilização de formação adequada às especificidades do setor e de maior dinamização dos ISACs.

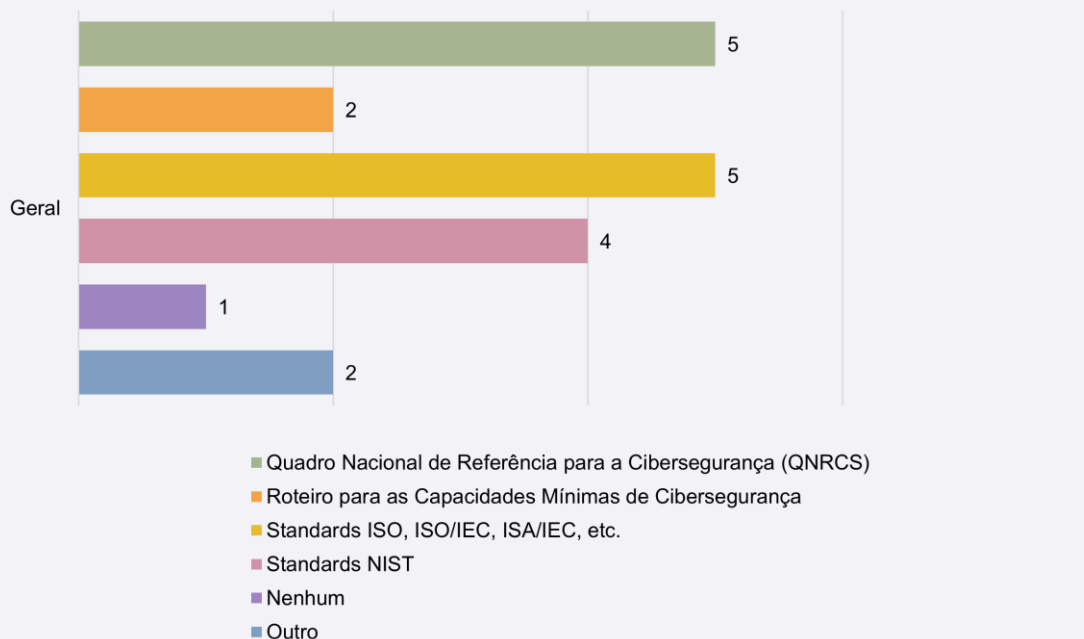
No caso do regulador do setor da distribuição de água potável, este respondeu que gostaria de ver o reforço da colaboração entre CNCS e entidades reguladoras e operadores, e o desenvolvimento de diretrizes/orientações/recomendações setoriais.

O Centro Nacional de Cibersegurança lançou um desafio denominado por “Compromisso C-Academy” que consiste em fornecer um programa de formação avançada em cibersegurança para

a administração pública e o setor privado. As organizações poderão escolher, pelo menos, três formações até ao final de 2025. Alguns dos principais benefícios incluem - “Reforço da cibersegurança da organização, setor ou região, aumento da resiliência e da capacidade de resposta a ataques” e “Acesso a conteúdos formativos de elevada qualidade”¹¹.

9. Standards e boas práticas recomendadas

Gráfico 21 - Standards e boas práticas recomendados aos OSE pelos reguladores



¹¹ CNCS, “Compromisso C-Academy”, <https://www.cncs.gov.pt/pt/c-academy-compromisso/>.

Gráfico 21.1 - Standards e boas práticas recomendados aos OSE pelos reguladores



Gráfico 21.2 - Standards e boas práticas recomendados aos OSE pelos reguladores

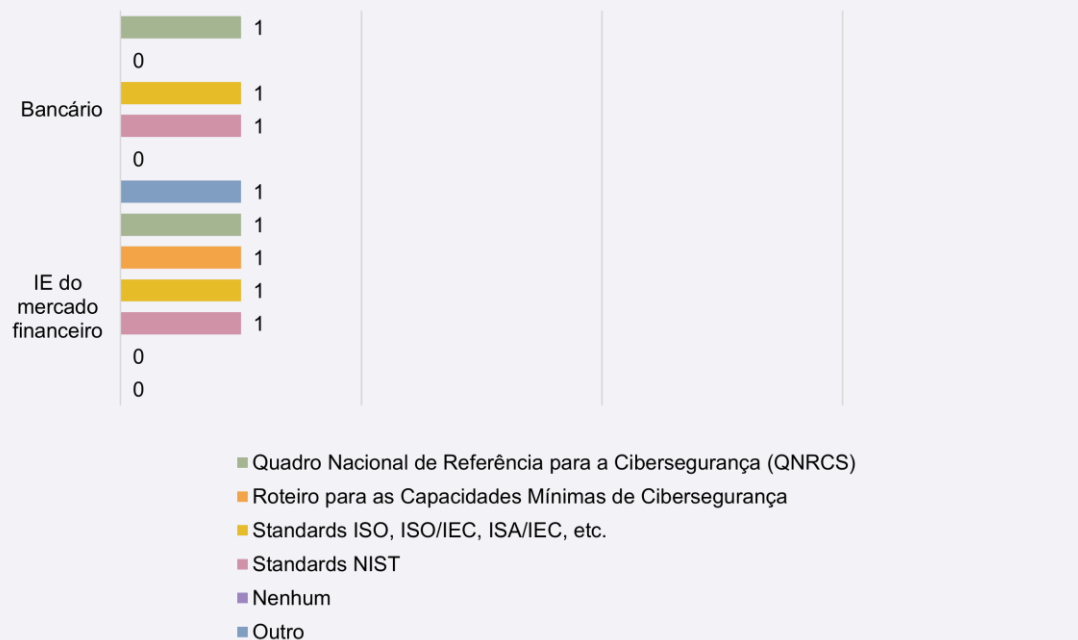


Gráfico 21.3 - Standards e boas práticas recomendados aos OSE pelos reguladores



A nível geral, os principais *standards* e boas práticas recomendados pelos reguladores aos OSE são o Quadro Nacional de Referência para a Cibersegurança (QNRCS) e *standards* internacionais como os da *International Organization for Standardization* (ISO), recomendados por cinco dos reguladores, seguidos dos *standards* do *National Institute of Standards and Technology* (NIST), recomendados por quatro dos reguladores. Quanto ao Roteiro para as Capacidades Mínimas, este é apenas recomendado por três dos reguladores. Dois dos reguladores recomendam ainda outros *standards*/boas práticas e o restante não faz qualquer tipo de recomendação.

Na opção “outros”, foram referidos *standards* da *International Civil Aviation Organization* (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain Keys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting and Conformance*).

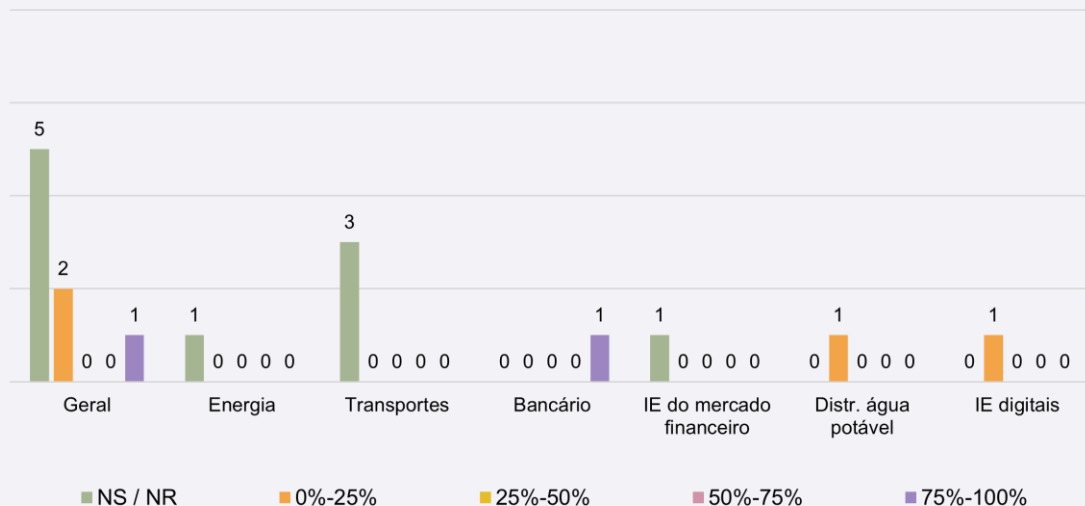
No setor da energia, o regulador inquirido recomenda aos operadores a adoção do QNRCS, *standards* ISO e *standards* NIST. No setor dos transportes, apenas um dos três reguladores refere recomendar aos operadores o QNRCS e o Roteiro para as Capacidades Mínimas, e outro refere recomendar *standards* NIST e outros *standards* como os do ICAO e o último indica não fazer qualquer recomendação.

No setor bancário, o regulador refere recomendar o QNRCS, *standards* ISO, *standards* NIST e ainda outras recomendações setoriais, como a EBA/GL/2019/04, da Autoridade Bancária Europeia (EBA, no inglês). O regulador do setor das infraestruturas do mercado financeiro recomenda aos operadores o QNRCS, o Roteiro para as Capacidades Mínimas, *standards* ISO e *standards* NIST.

Os reguladores do setor da distribuição de água potável e do setor das infraestruturas digitais indicaram recomendar aos operadores *standards* ISO, sendo que este último também indicou boas práticas como a utilização de DNSSEC, DKIM e DMARC.

De acordo com um estudo realizado em 2023 pelo Departamento de Ciência, Tecnologia e Inovação do Governo do Reino Unido, o uso de boas práticas de cibersegurança diminuiu de 2021 para 2023. Nesta diminuição podem ser nomeados o decréscimo no uso de políticas de palavras-passe, onde se verificou uma redução de utilização pelos inquiridos de 79% para 70%, enquanto no uso de *Firewalls* se registou uma diminuição de 78% para 66%¹².

Gráfico 22 - Percentagem aproximada de OSE nos setores certificados em normas internacionais (como ISO/IEC 27001 ou ISO 22301) do conhecimento do regulador



A maioria dos operadores, cinco, não conhece a percentagem aproximada de OSE certificados em normas internacionais como a ISO/IEC (*International Electrotechnical Commission*) 27001 (sobre Sistemas de Gestão de Segurança da Informação) e ISO 22301 (sobre Continuidade de Negócio). Já dois informam que existem entre 0%-25% de operadores certificados em normas internacionais ISO ou similares. Um regulador informa haver 75%-100% de operadores certificados em normas internacionais do tipo.

Tanto no setor da energia como no de infraestruturas do mercado financeiro indicaram não conhecer a percentagem aproximada de operadores no setor certificados em normas internacionais do tipo referido.

Os três reguladores inquiridos no setor dos transportes referiram também não conhecer a percentagem de operadores certificados em normas internacionais como a ISO 27001 e ISO 22301 ou outras. No setor bancário, o regulador indicou que 75%-100% dos OSE são certificados em normas internacionais dos tipos referidos. Nos setores do fornecimento e distribuição de água potável e infraestruturas digitais, os reguladores identificam entre 0%-25% de operadores certificados em normas internacionais ISO ou semelhantes.

¹² Department for Science, Innovation & Technology, "Cyber security breaches survey 2023", 19 de abril de 2023, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>

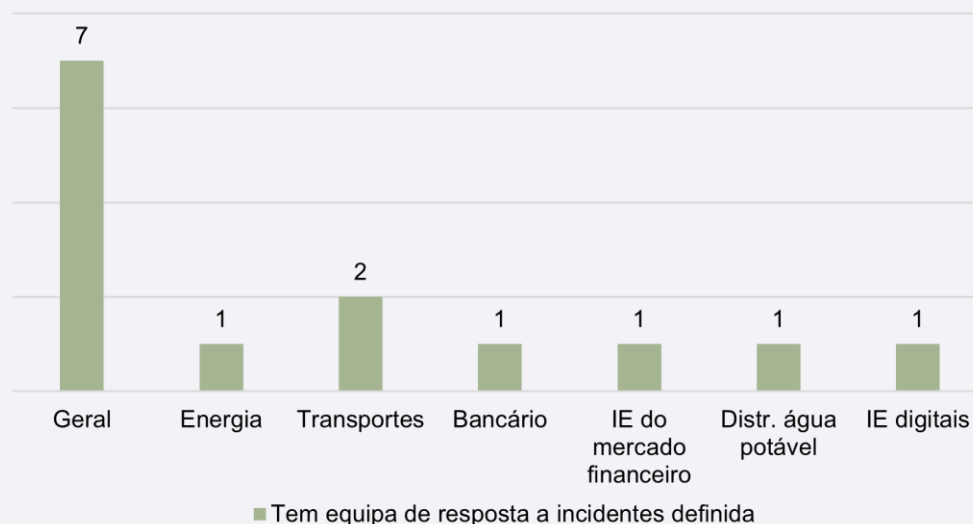
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança

Setores	Normativos
Energia	<i>Network Code on Cybersecurity (publicação pendente)</i>
Transporte	<i>Transport Cybersecurity Toolkit (CE)</i> ; Regulamento UE 2019/1583
Bancário	EBA/GL/2019/04; Instrução n.º 4/2021 do Banco de Portugal (BdP); EBA/GL/2017/05; EBA/GL/2019/02; EBA/GL/2021/05; Instrução n.º 21/2019; Regulamento UE 2022/2554
Infraestruturas do Mercado Financeiro	Lei de Resiliência Operacional Digital (<i>Digital Operation Resilience Act - DORA</i>)
Distribuição de Água Potável	N/A
Infraestruturas Digitais	Lei n.º 46/2018 de 13 de agosto

Foi também questionado aos reguladores que normativos setoriais específicos nacionais ou europeus em matéria de cibersegurança estavam em vigor nos respetivos setores. Partindo das suas respostas, obteve-se a **Tabela 2**.

10. Definição de equipa de resposta a incidentes de cibersegurança

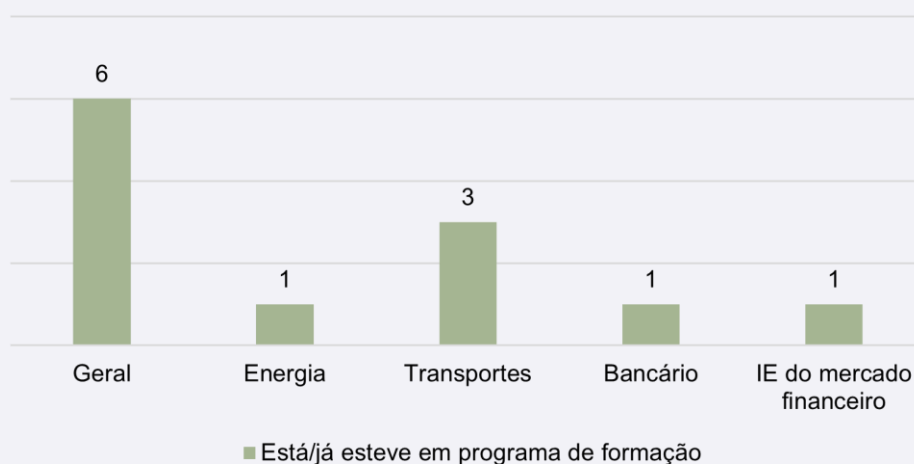
Gráfico 23 - Reguladores com equipa de resposta a incidentes definida



Relativamente à definição de equipas de resposta a incidentes, a grande maioria dos reguladores inquiridos (sete) tem uma equipa definida. No setor dos transportes, dois dos três reguladores inquiridos indicaram ter equipa de resposta a incidentes definida, enquanto o terceiro indicou não ter equipa definida, mas tem suficientes profissionais para formar essa equipa. No setor bancário, da energia, infraestruturas do mercado financeiro, distribuição de água potável e infraestruturas digitais, os reguladores inquiridos informaram ter definido a equipa de resposta a incidentes.

11. Sensibilização e consciencialização

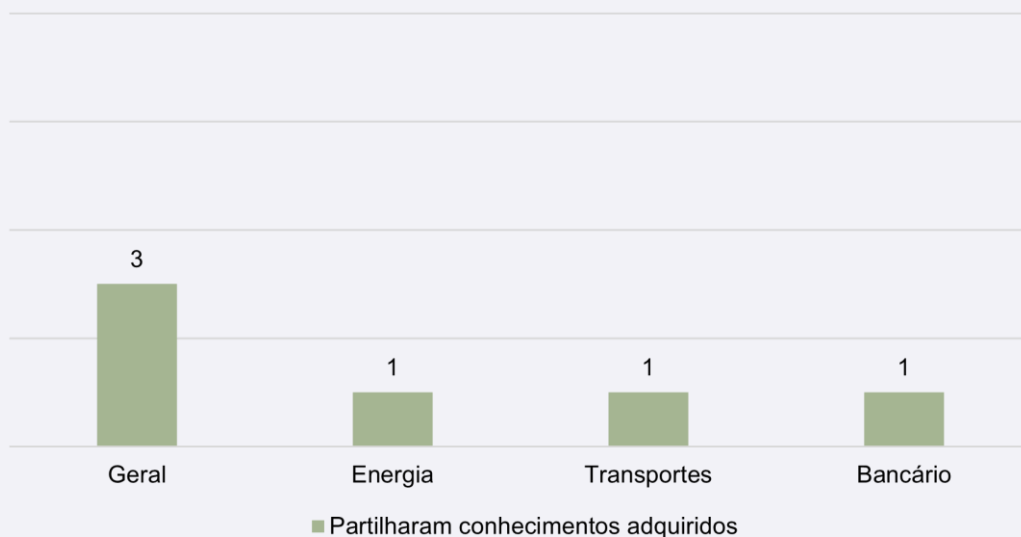
Gráfico 24 - Reguladores que estão ou já estiveram em programas de formação e sensibilização para os riscos no ciberespaço promovidos pelo CNCS ou por outra entidade



Relativamente à participação em programas de formação e sensibilização para os riscos no ciberespaço, seis dos reguladores inquiridos, indicaram que participam ou já participaram em programas do género promovidos pelo CNCS ou outra entidade, enquanto dois, o regulador do setor do fornecimento e distribuição de água potável e o regulador das infraestruturas digitais, nunca participaram em tais programas.

Os reguladores inquiridos do setor da energia, bancário e infraestruturas do mercado financeiro informaram estar ou já ter estado em programas de formação e sensibilização para os riscos no ciberespaço. No setor dos transportes, os três reguladores inquiridos indicaram estarem ou já terem estado em programas de formação e sensibilização sobre as matérias referidas. Os reguladores do setor do fornecimento e distribuição de água potável e infraestruturas digitais inserem-se no grupo dos 25%, tendo indicado que nunca participaram em programas do tipo.

Gráfico 25 - Reguladores recipientes de formação que partilharam os conhecimentos adquiridos com os OSE do setor

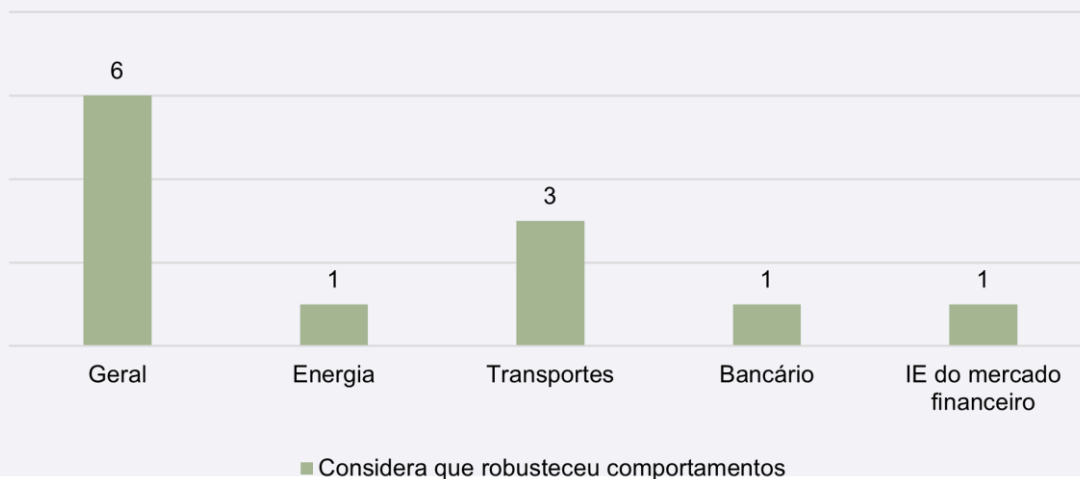


No seguimento da participação nos programas de formação e sensibilização para os riscos no ciberespaço, questionou-se se os conhecimentos adquiridos nesses programas foram partilhados com os OSE do setor. Os setores que fizeram essa partilha e os que não fizeram dividem-se igualmente.

No global, metade dos inquiridos partilharam os conhecimentos adquiridos com os operadores do setor, enquanto os restantes não partilharam qualquer conhecimento adquirido com os operadores do setor.

Os reguladores do setor energia e bancário referem ter partilhado os conhecimentos adquiridos com os operadores do seu setor. Relativamente ao setor dos transportes, apenas um dos três reguladores referiu ter partilhado os conhecimentos adquiridos na formação com os operadores, enquanto os outros dois reguladores não indicam ter feito essa partilha. Nas infraestruturas do mercado financeiro, distribuição de água potável e no setor das infraestruturas digitais, o regulador não terá feito essa partilha com os operadores.

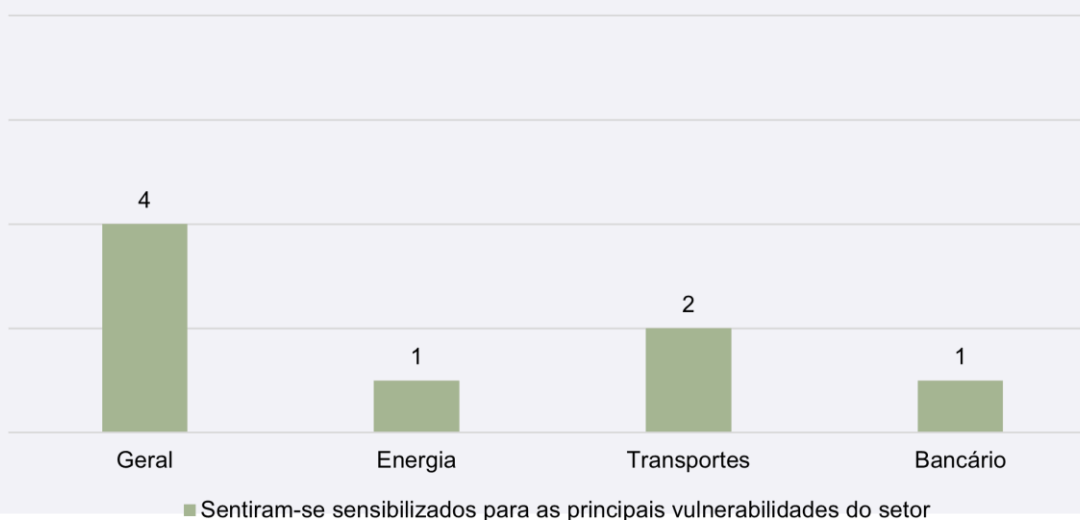
Gráfico 26 - Reguladores que frequentaram programas, e consideram que ter frequentado o programa robusteceu comportamentos relativos à cibersegurança dentro da organização



Entre os reguladores que frequentaram os programas de formação e sensibilização, todos consideram que ter frequentado os programas robusteceu os comportamentos relativos à cibersegurança dentro da sua organização.

Como indicado no gráfico anterior, esta questão também não se aplica ao regulador do setor da distribuição de água potável ou ao do setor das infraestruturas digitais, que não participaram em programas do género.

Gráfico 27 - Reguladores que, no âmbito dos programas, sentiram que a entidade formadora os sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto



Ainda no âmbito da participação nos programas de formação e sensibilização, foi questionado aos reguladores se sentiram que a entidade formadora os sensibilizou para as principais vulnerabilidades a que o seu setor está ou esteve exposto. Quatro dos que participaram nesses

programas consideraram que essa sensibilização foi feita e dois consideraram que não ficaram sensibilizados sobre as principais vulnerabilidades do setor.

No setor da energia e no setor bancário, o regulador inquirido considerou que a entidade formadora o sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto. Nos transportes, dois dos três reguladores inquiridos consideraram que a entidade formadora os sensibilizou para essas vulnerabilidades. O terceiro regulador discorda sobre ter sido sensibilizado acerca das mesmas. Quanto ao regulador inquirido do setor das infraestruturas do mercado financeiro, este considera que a entidade formadora não o sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto. Quanto ao setor de distribuição de água potável e ao setor das infraestruturas digitais a situação aplicável é a mesma que a anterior.

12. Cooperação nacional/internacional de proteção do ciberespaço

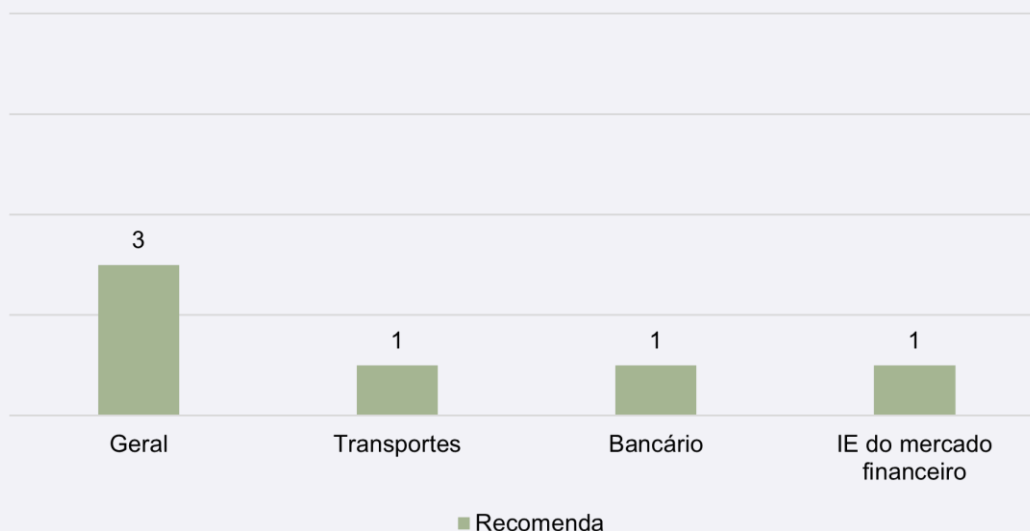
Gráfico 28 - Reguladores pertencentes a estruturas de cooperação nacional/internacional de proteção do ciberespaço (ISACs - Centros de Análise e Partilha de Informação)



Relativamente à pertença a estruturas de cooperação nacional ou internacional de proteção do ciberespaço, como os Centros de Análise e Partilha de Informação, apenas dois dos reguladores indicaram fazer parte de alguma dessas estruturas, enquanto os restantes seis indicaram não pertencer a qualquer estrutura do tipo.

Os reguladores dos setores da energia, infraestruturas do mercado financeiro, distribuição de água potável e infraestruturas digitais insere-se no grupo da maioria, não fazendo parte de nenhuma estrutura do tipo. No setor dos transportes, apenas um dos três reguladores inquiridos indicou pertencer a uma estrutura de cooperação nacional ou internacional como um ISAC, enquanto os restantes dois reguladores indicaram não pertencer a nenhuma estrutura do género. No caso do regulador inquirido do setor bancário, este também indicou pertencer a estruturas do tipo referido.

Gráfico 29 - Reguladores que recomendam a participação dos OSE em centros de partilha de informação como os ISACs



Relativamente à pertença a estruturas de cooperação nacional ou internacional de proteção do ciberespaço, como os Centros de Análise e Partilha de Informação, apenas três dos reguladores indicaram fazer parte de alguma dessas estruturas, enquanto os restantes cinco indicaram não pertencer a qualquer estrutura do tipo.

No caso dos reguladores inquiridos do setor da energia, distribuição de água potável e infraestruturas digitais, estes não recomendam aos operadores a participação em centros de partilha de informação. No setor dos transportes, apenas um dos três reguladores inquiridos recomenda aos operadores do setor a participação em centros de partilha de informação ou ISACs. Os outros dois reguladores não fazem essa recomendação. No setor bancário e no sector das infraestruturas do mercado financeiro, o regulador inquirido recomenda a participação em centros de partilha e análise de informação aos OSE.

13. Regulação de entidades e OSE

Por fim, questionou-se aos reguladores dos setores em análise qual o número de entidades por si reguladas e quantas destas eram OSE. Das respostas obtidas foram criadas as **Tabelas 3 e 4**.

Tabela 3 - Estimativa do total de entidades reguladas pelos reguladores por setor

Setores	Estimativa
Energia	32
Transportes	> 19 000
Bancário	120
Infraestruturas do Mercado Financeiro	> 1 000
Distribuição de Água Potável	350
Infraestruturas Digitais	100

Tabela 4 - Número estimado das entidades reguladas que são OSE

Setores	Número estimado de entidades reguladas
Energia	9
Transportes	760
Bancário	10
Infraestruturas do mercado financeiro	4
Fornecimento e distribuição de água potável	240
Infraestruturas digitais	30

Resultados do questionário dirigido aos Operadores de Serviços Essenciais

Gráfico 30 - Número de colaboradores na organização

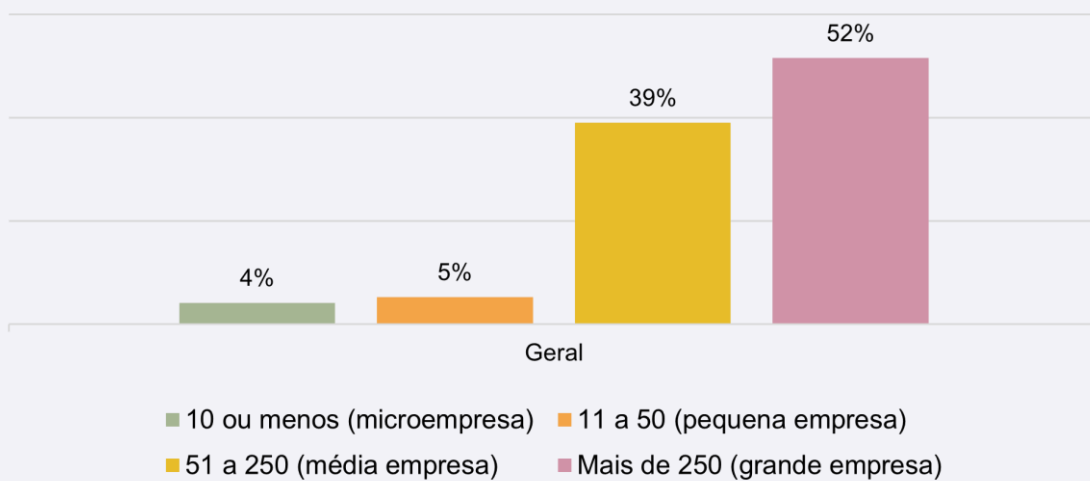


Gráfico 30.1 - Número de colaboradores na organização

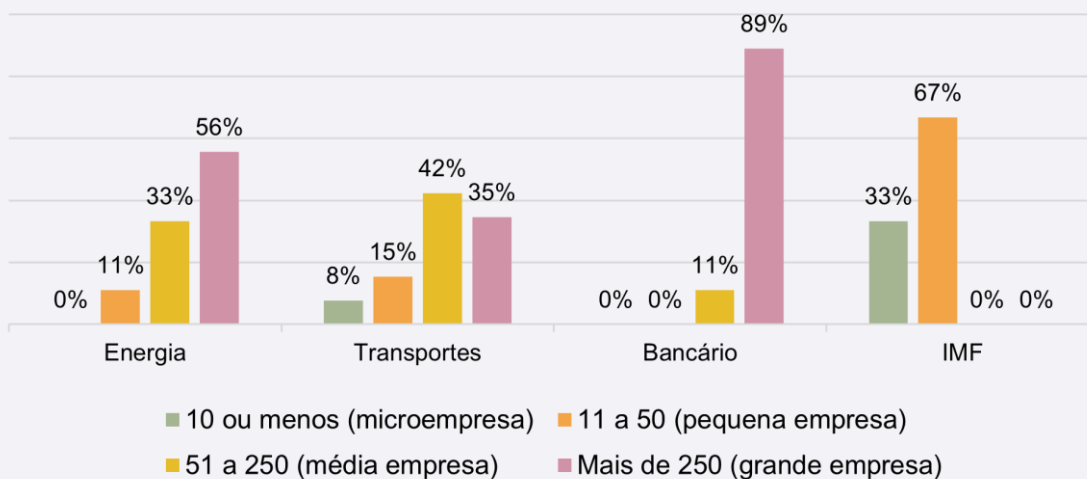
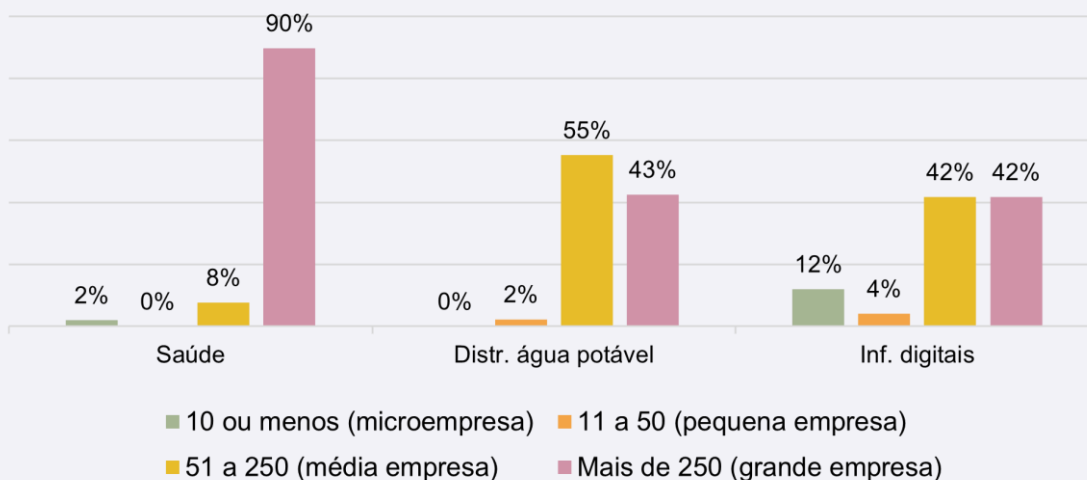


Gráfico 30.2 - Número de colaboradores na organização

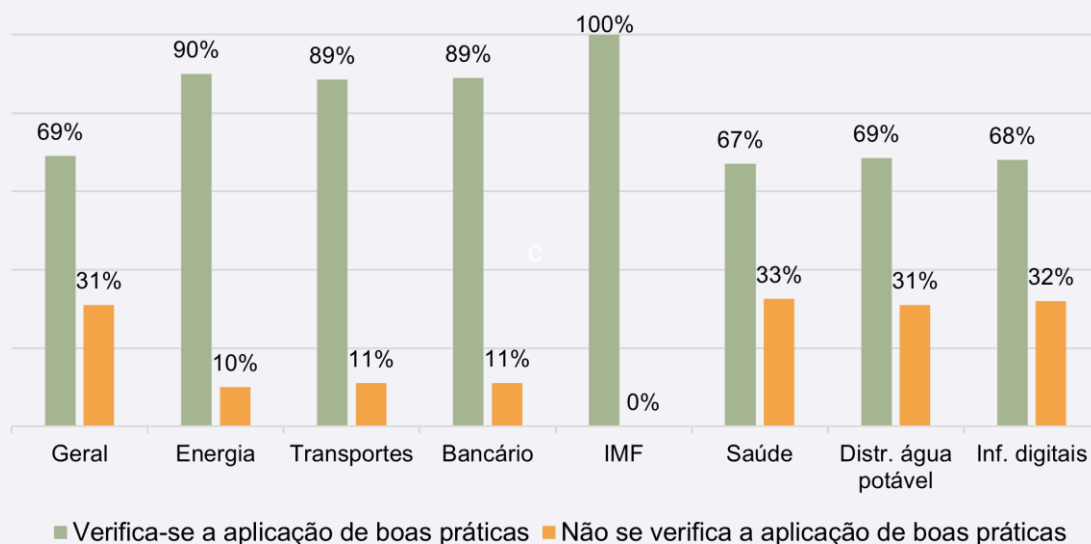


O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSE. As médias empresas representam 39% dos OSE, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas (4% e 5%, respetivamente).

Destacam-se os setores da energia, o setor bancário e o setor saúde, em que as grandes empresas são mais comuns. Contrariamente, nos setores dos transportes e no setor do fornecimento e distribuição de água potável, são mais comuns as médias empresas. Já no setor das infraestruturas digitais observa-se uma igual distribuição entre médias empresas e grandes empresas (42% cada). O setor das infraestruturas do mercado financeiro surge como o único a apresentar apenas micro e pequenas empresas.

A composição do tecido empresarial dos OSE difere grandemente daquele que é o tecido empresarial geral das empresas portuguesas. Enquanto entre os OSE mais de 50% destes são grandes empresas, 99,9% das demais empresas em Portugal são, segundo dados de 2022 da PORDATA, pequenas e médias empresas, com apenas 0,1% sendo grandes empresas¹³.

Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores



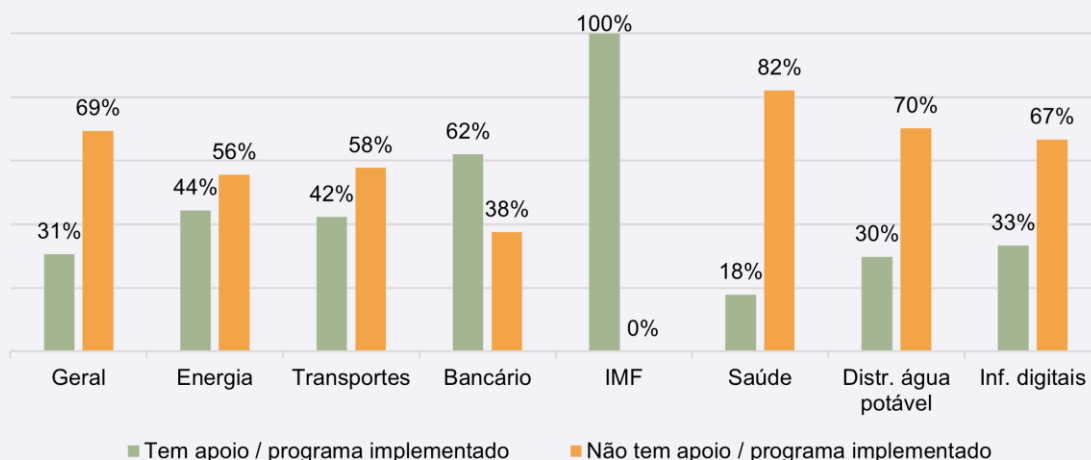
De um modo geral, os operadores percecionam a adoção de boas práticas de cibersegurança por parte dos seus colaboradores. Alguns exemplos dessas boas práticas são a não partilha de palavras-passe, o bloqueio do computador durante momentos de ausência da estação de trabalho, o cuidado com a informação confidencial do operador ou a denúncia de *e-mails* suspeitos/tentativas de *phishing*, entre outras. Na generalidade, dois terços dos operadores consideram que há uma efetiva adoção dessas boas práticas pelos seus colaboradores.

Os setores da energia, dos transportes, o setor bancário e o das infraestruturas do mercado financeiro destacam-se por serem setores nos quais mais de 80% dos operadores consideram que boas práticas de cibersegurança são aplicadas pelos seus colaboradores. No setor das infraestruturas do mercado financeiro, todos os inquiridos percecionam a aplicação dessas boas práticas.

Nos setores da saúde, distribuição de água potável e infraestruturas digitais, a perceção de que estas boas práticas são aplicadas varia entre 68% e 69%.

¹³ PORDATA, "Empresas: total e por dimensão", dados de 2022, <https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857>.

Gráfico 32 - Implementação de apoios ou programas, próprios ou do Estado, para colaboradores que desejem formação na área de cibersegurança



À data de realização do questionário, apenas um terço dos operadores tinham apoios ou programas próprios ou do Estado para colaboradores interessados em formação na área de cibersegurança. Os setores bancário e das infraestruturas do mercado financeiro destacam-se dos restantes setores em estudo, uma vez que, no setor bancário, a maioria dos operadores (63%) tem maneira de fornecer esse apoio ou programa formativo aos colaboradores, e que no setor das infraestruturas do mercado financeiro todos os operadores disponibilizam esses apoios ou programas.

Na saúde, no fornecimento e distribuição de água potável e nas infraestruturas digitais, mais de dois terços dos operadores não têm apoios ou programas próprios ou do Estado para colaboradores que desejem formação em cibersegurança.

Importa sublinhar, que estas respostas não significam que não seja dada formação em cibersegurança aos colaboradores. O que acontece é que muita da formação disponibilizada pelos operadores aos colaboradores não está inserida num programa de formação específico, ou então não existem apoios para colaboradores que procurem formações ministradas fora da organização, tal como se poderá verificar no **Gráfico 38**.

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança

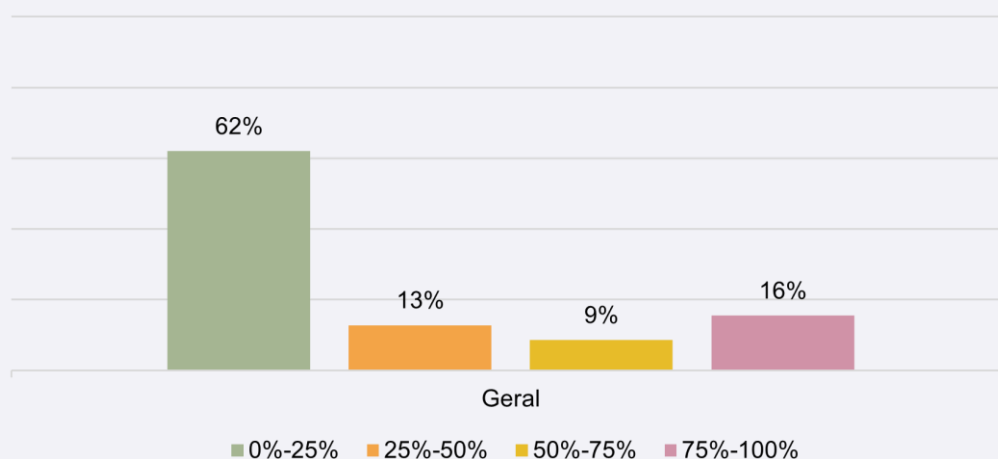


Gráfico 33.1 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança

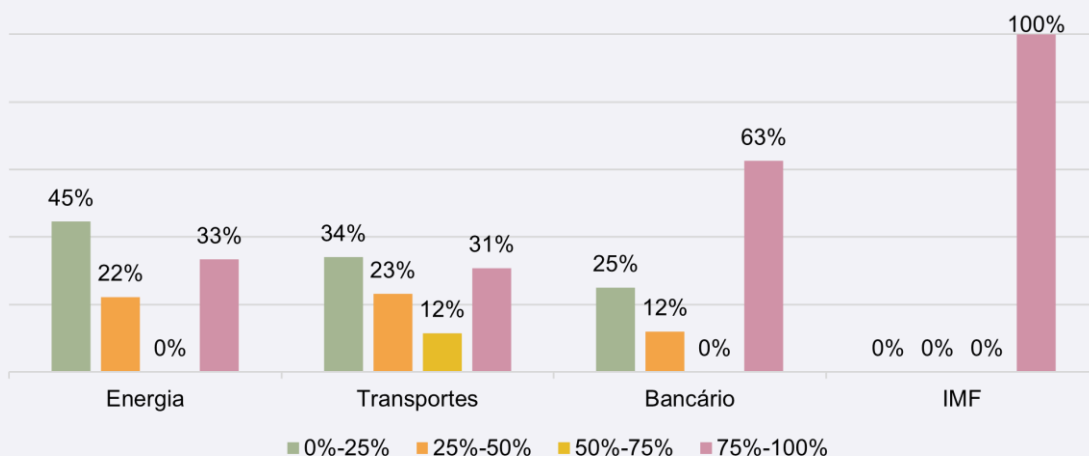
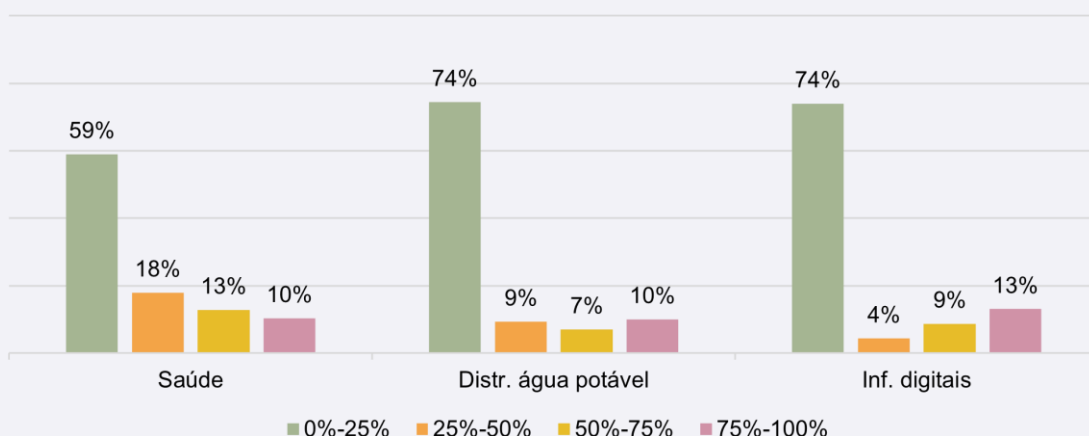


Gráfico 33.2 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Na maioria dos OSE (62%), a percentagem de colaboradores com formação básica em cibersegurança não ultrapassa os 25%.

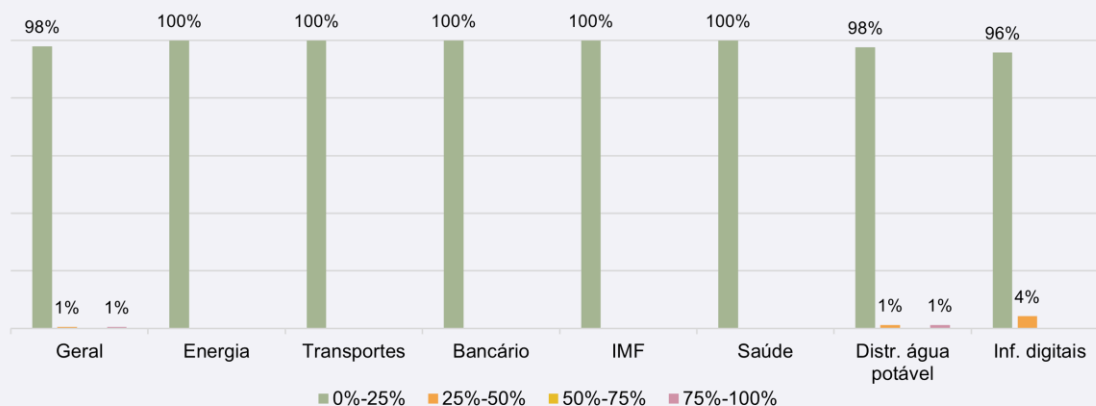
O setor das infraestruturas do mercado financeiro surge em destaque, uma vez que todos os operadores do setor indicaram ter entre 75%-100% de colaboradores com formação básica em cibersegurança, sendo este o setor que apresenta a mais elevada percentagem de colaboradores com formação nesta matéria.

O setor bancário apresenta também resultados positivos, dado que 63% dos operadores inquiridos indicam que a percentagem de colaboradores com formação básica na área se situa no intervalo 75%-100%.

Nos setores da energia e dos transportes, embora predominem os operadores onde a quantidade de colaboradores com este tipo de formação não ultrapassa os 25%, há mais dos 30% de operadores com percentagens de colaboradores com formação básica em cibersegurança no intervalo 75%-100%.

Nos setores da saúde, do fornecimento e distribuição de água potável, e no setor das infraestruturas digitais, a percentagem de operadores onde três quartos dos colaboradores ou mais têm formação básica em cibersegurança é relativamente baixa, nunca ultrapassando os 13%.

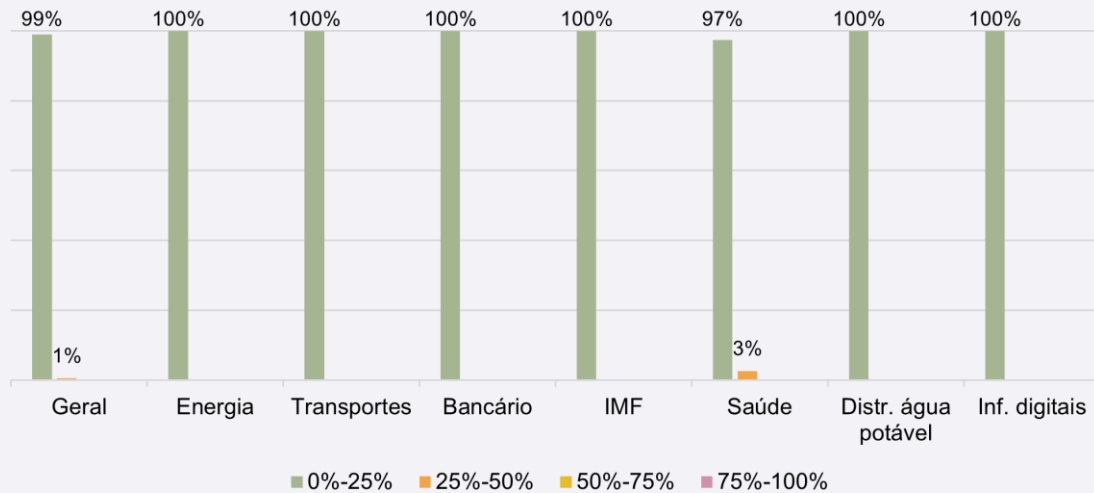
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



Face aos resultados obtidos na questão anterior, é de esperar que a percentagem de colaboradores com formação superior em cibersegurança seja diminuta. É também de esperar que o seja, dado que cada OSE congrega várias áreas profissionais, como os recursos humanos, as finanças e a cibersegurança, não sendo composta apenas por profissionais da área em análise neste relatório.

Em termos gerais, a percentagem de trabalhadores dos operadores com formação superior em cibersegurança situa-se predominantemente na faixa entre 0%-25% em todos os operadores de todos os setores. Existe um número reduzido de colaboradores dos operadores inquiridos, com formação superior em cibersegurança. Destacam-se os setores do fornecimento e distribuição de água potável e das infraestruturas digitais, nos quais se registam operadores com percentagens de colaboradores com formação superior em cibersegurança nas faixas acima dos 25%. No setor da água, 1% dos OSE indicaram haver entre 25%-50% de colaboradores com essa formação superior e outros 1% indicaram serem entre 75%-100% dos colaboradores. No setor das infraestruturas digitais, registam-se 4% dos OSE a atingirem a faixa 25%-50% de colaboradores com essa valência.

Gráfico 35 - Percentagem aproximada de trabalhadores do operador com certificações em cibersegurança



A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. Contudo, há que destacar o setor da saúde, onde 3% dos operadores indicaram haver 25%-50% de colaboradores com certificações em cibersegurança. Novamente, o resultado geral é um resultado expectável, uma vez que não se espera que colaboradores de outras áreas sejam certificados em cibersegurança.

De acordo com os dados disponíveis no relatório *NIS Investments* 2021, da ENISA, apenas 7,5% dos OSE na UE indicavam ter uma preocupação em certificar os colaboradores da própria organização. A nível setorial, no mesmo relatório, em nenhum dos setores se superava os 11% de OSE a certificar os seus próprios colaboradores¹⁴.

¹⁴ ENISA, "NIS Investments", novembro de 2021, 73.

Gráfico 36 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (*helpdesk*), em matéria de cibersegurança e/ou tecnologias da informação

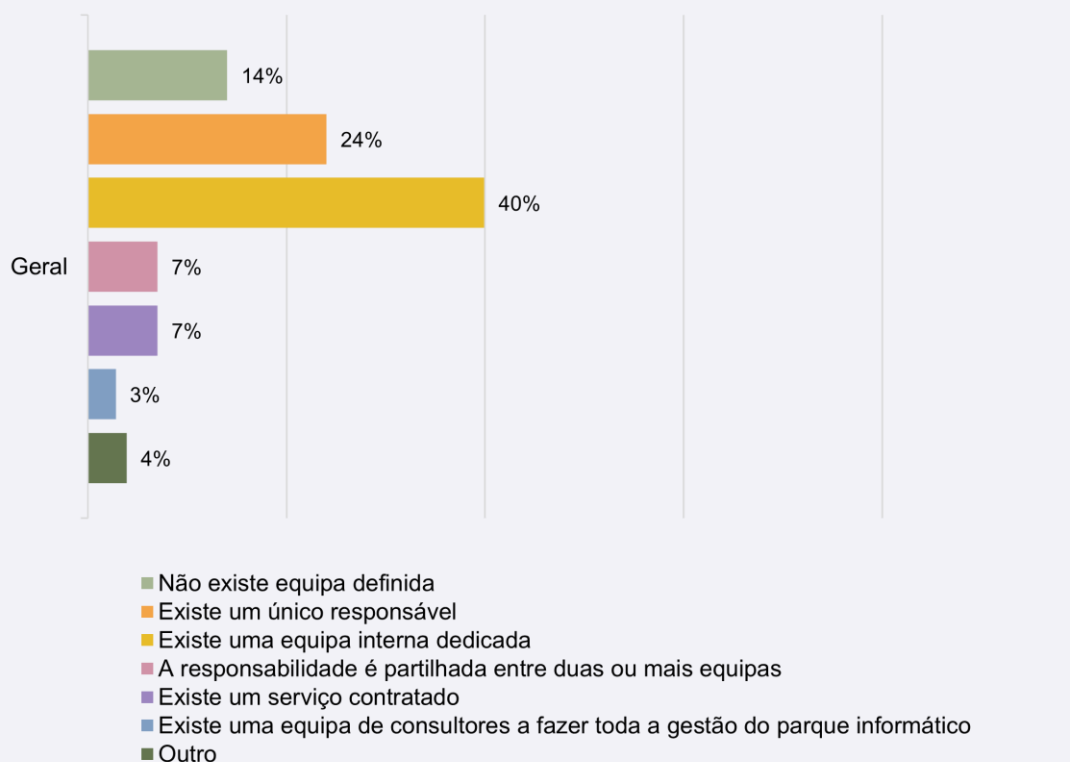


Gráfico 36.1 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (*helpdesk*), em matéria de cibersegurança e/ou tecnologias da informação

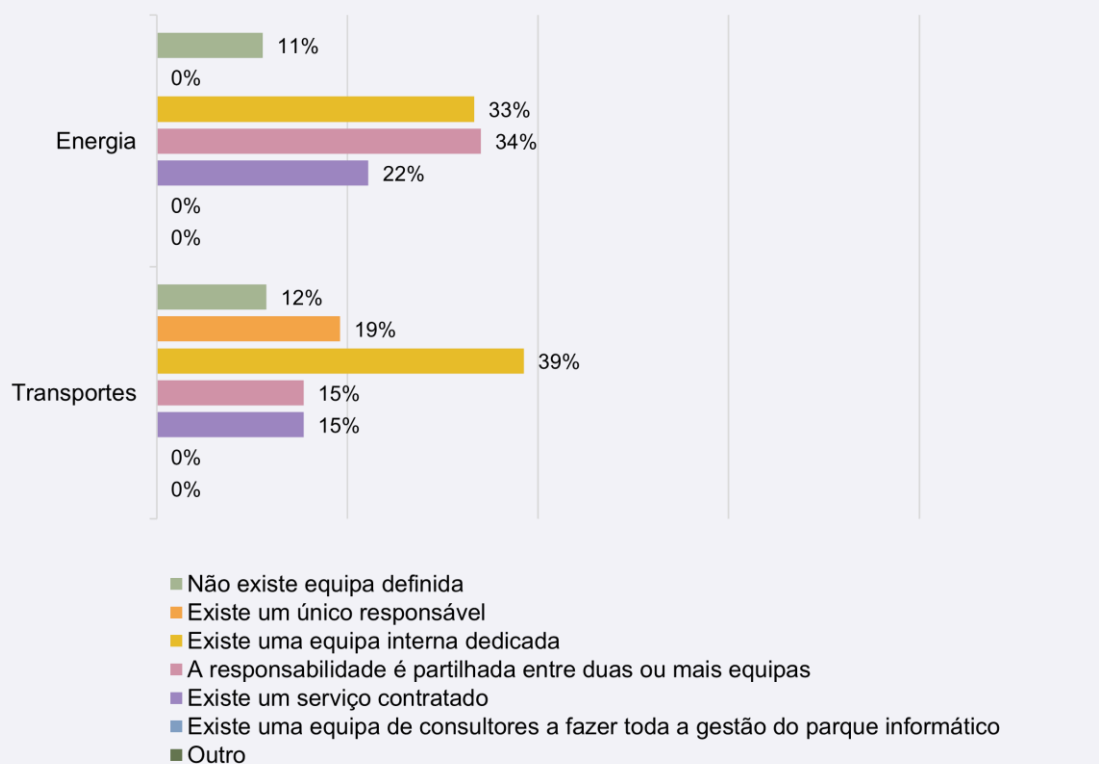


Gráfico 36.2 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (*helpdesk*), em matéria de cibersegurança e/ou tecnologias da informação

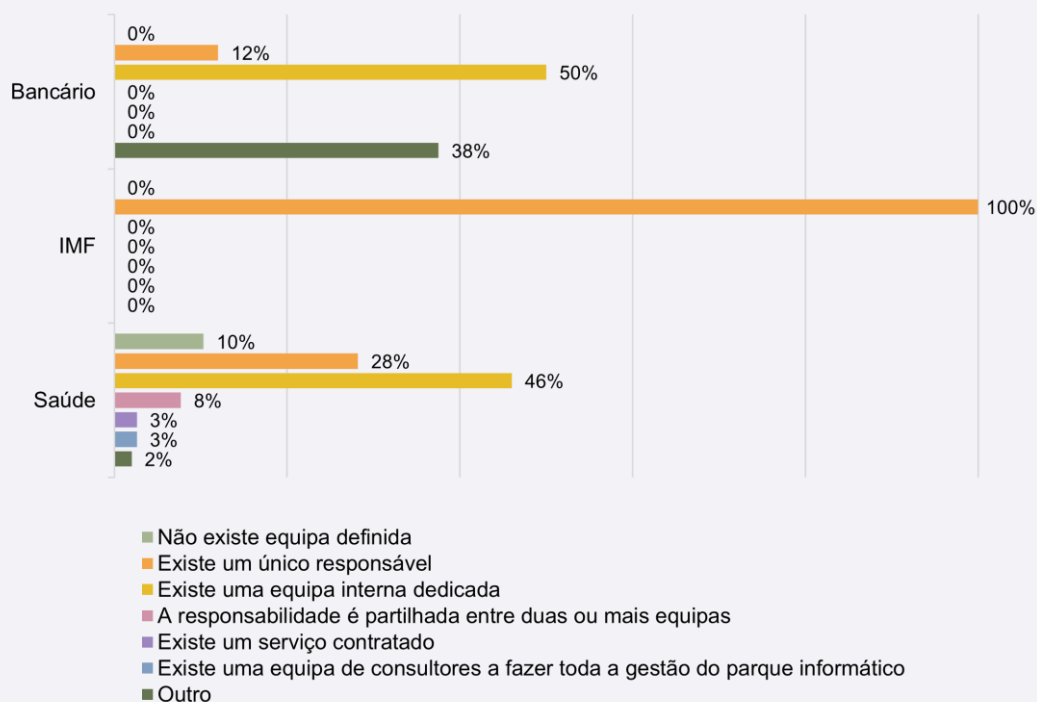
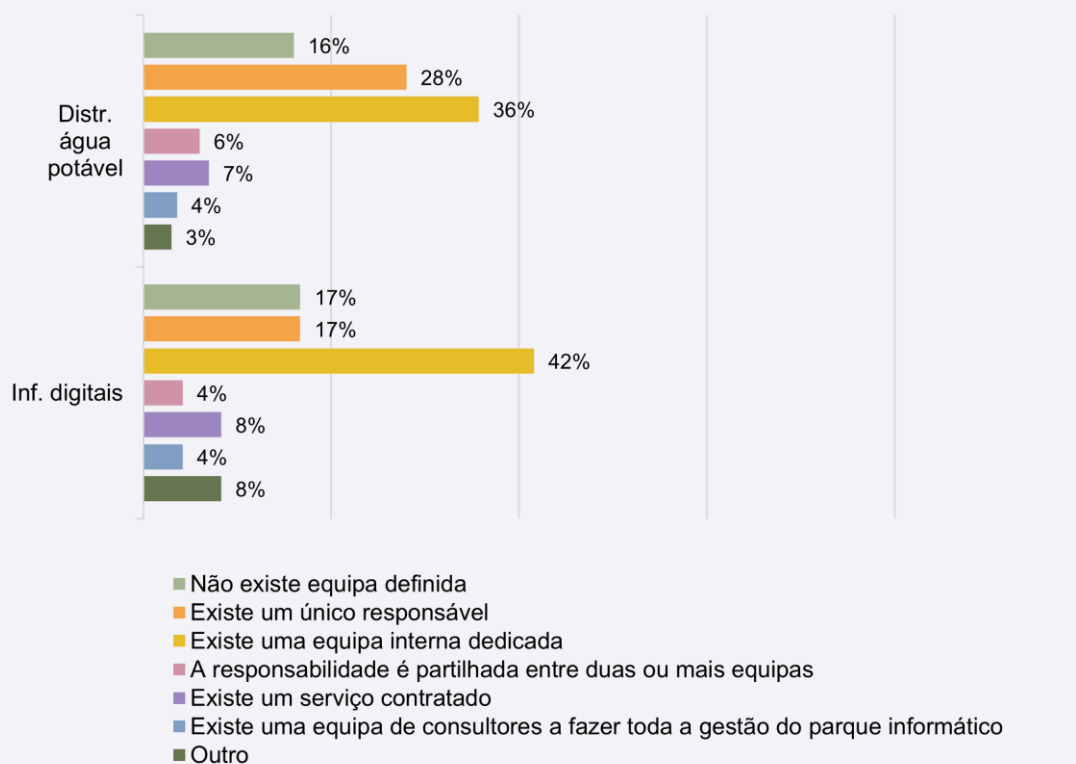


Gráfico 36.3 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (*helpdesk*), em matéria de cibersegurança e/ou tecnologias da informação



De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (25% dos casos).

Verificam-se ainda outras situações, como a não existência de equipa definida (em 14% dos operadores inquiridos), a partilha de a responsabilidade entre duas ou mais equipas (7%), a existência um serviço contratado (7%), aquelas onde uma equipa de consultores faz toda a gestão do parque informático (3%). Entre os que responderam “outro”, as principais soluções indicadas foram a existência de Security Operation Center (SOC) ou haver uma equipa de uma entidade tutelar a prestar o serviço de *helpdesk*, como no caso dos serviços municipalizados na distribuição de água potável, em que a equipa responsável pertence, por exemplo, à comunidade intermunicipal.

Os operadores do setor energético contam, maioritariamente, com uma ou mais equipas dedicadas (34%) ou com uma única equipa dedicada (33%), verificando-se também o recurso à contratação externa do serviço de *helpdesk* em 22% dos casos. Já nos setores dos transportes, da banca, da saúde, da distribuição de água e das infraestruturas digitais, prevalece a presença de uma equipa interna dedicada, com pelo menos 36% dos OSE a optarem por esta solução no setor dos transportes, e chegando aos 50% de OSE no setor bancário. Por sua vez, no setor infraestruturas do mercado financeiro, a responsabilidade é maioritariamente atribuída a um único responsável.

Gráfico 37 - Composição das equipas de *helpdesk*

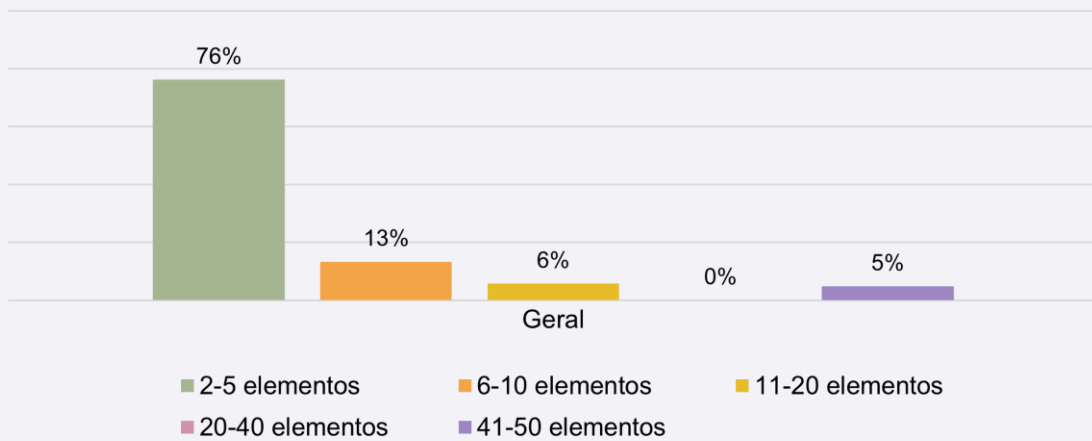


Gráfico 37.1 - Composição das equipas de *helpdesk*

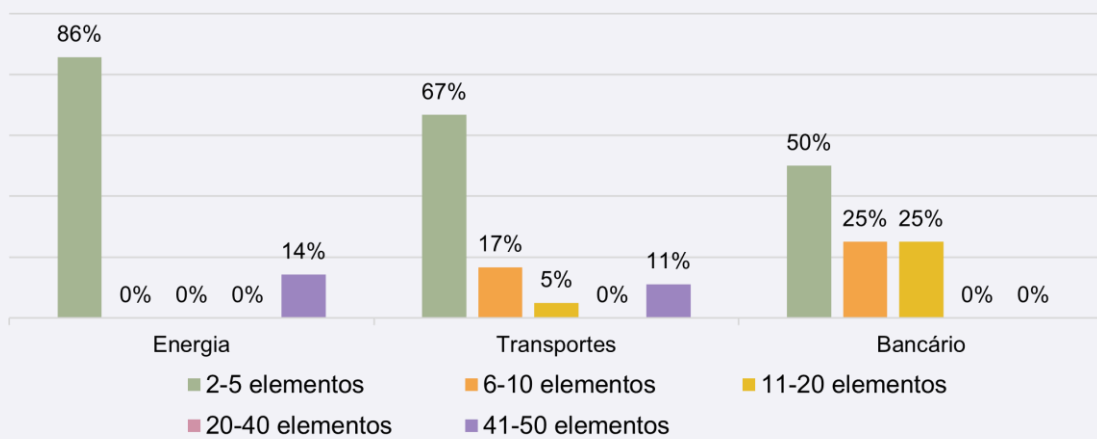
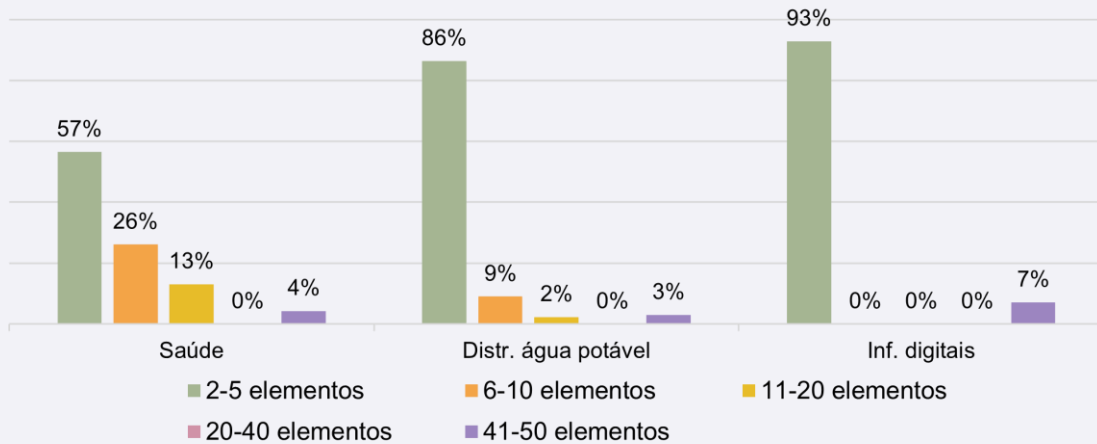
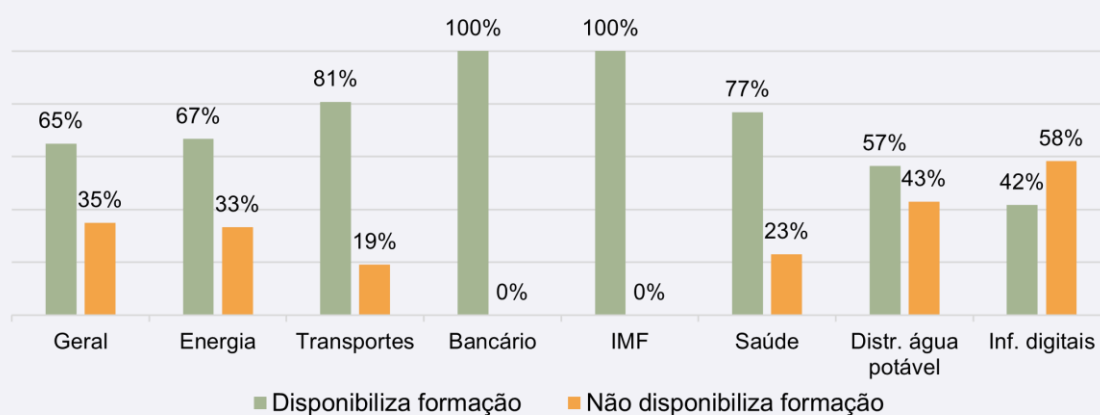


Gráfico 37.2 - Composição das equipas de *helpdesk*



Na sua larga maioria, as equipas de *helpdesk* são compostas por 2-5 elementos. Entre os OSE com equipas de *helpdesk*, 76% apresentam equipas com esta composição. Esta composição foi a mais indicada em todos os setores, correspondendo em qualquer um destes à realidade de pelo menos 50% dos OSE com equipas de *helpdesk*. Verificam-se também outras composições, com equipas mais vastas, nas organizações de maior dimensão. No entanto, enquanto é evidente que apenas grandes empresas têm equipas de *helpdesk* com mais de 41 elementos, nem todas as grandes empresas têm equipas tão vastas. Resulta assim que há grandes empresas em que as funções de *helpdesk* são asseguradas por equipas mais reduzidas, até um máximo de 20 elementos. Concomitantemente, nenhum dos inquiridos indicou ter uma equipa de 20-40 elementos. A questão não é aplicável ao setor das infraestruturas do mercado financeiro.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

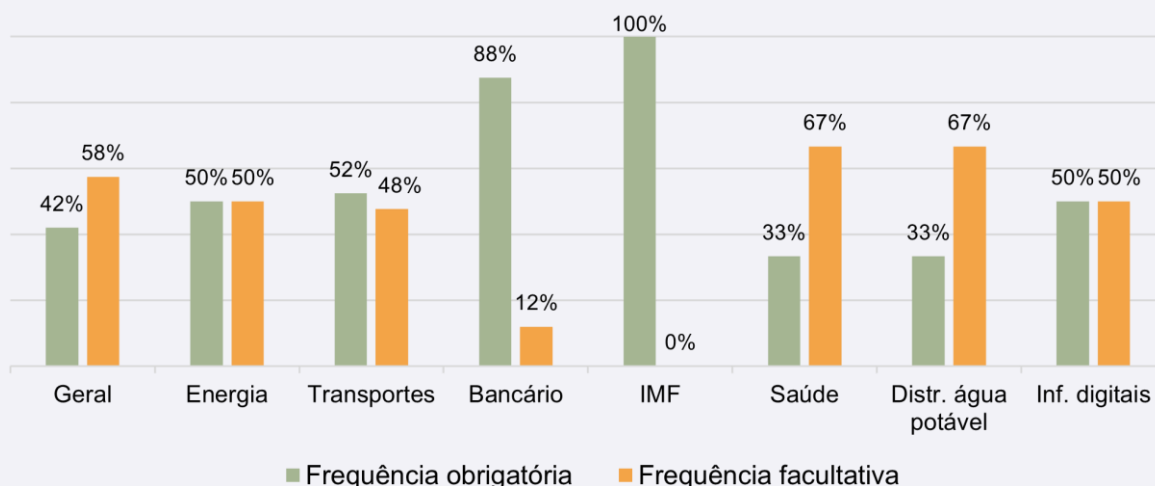


Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. As exceções a esta realidade verificam-se no setor do fornecimento de água potável, no qual 57% dos OSE indicam disponibilizar formação aos colaboradores, ficando assim 8 p.p. abaixo da percentagem geral, bem como no setor das infraestruturas digitais, no qual menos de metade dos inquiridos (42%) indica disponibilizar formação aos colaboradores. Notavelmente, nos setores da banca e das infraestruturas do mercado financeiro, todos os OSE indicaram disponibilizar formação em cibersegurança aos seus colaboradores.

Comparando com dados do Inquérito à Utilização das TIC nas Empresas (IUTICE) de 2022, realizado pelo Instituto Nacional de Estatística (INE), 63,3% das empresas em Portugal procuraram consciencializar os seus colaboradores sobre cibersegurança durante o ano de 2021¹⁵. Já um outro estudo, realizado pela Microsoft Portugal em setembro de 2023, intitulado “Estado da Cibersegurança em Portugal”, indica que 84% das empresas portuguesas ministram formação de sensibilização para a cibersegurança. A discrepância nestes resultados poder-se-á dever à composição das amostras de cada estudo. Embora seja expectável que cada vez mais empresas disponibilizem formação em cibersegurança aos seus colaboradores, um crescimento de 20% em dois anos das entidades que disponibilizam formação em cibersegurança aos seus colaboradores é improvável.

¹⁵ INE, “Inquérito à Utilização das TIC nas Empresas”, 2022, 18, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=585250024&att_display=n&att_download=y

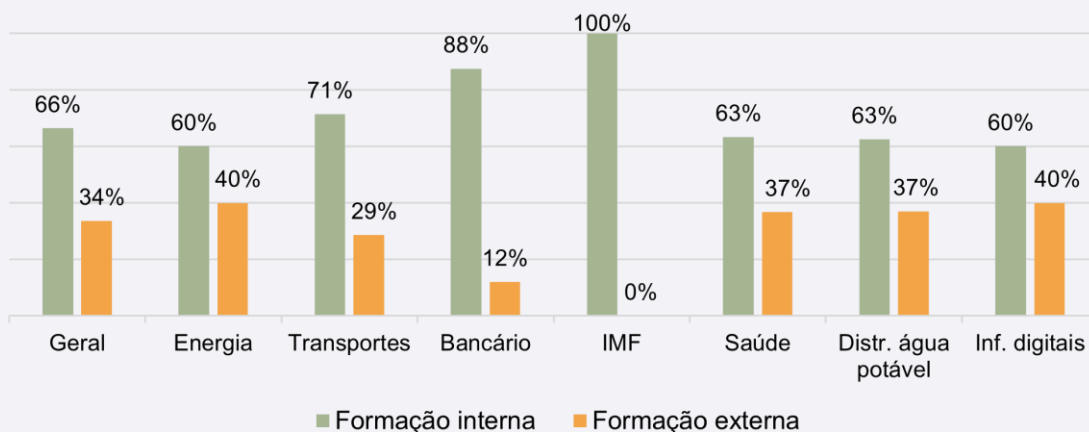
Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais esta tendência não se verifica. Por exemplo, no setor da energia e no setor das infraestruturas digitais, há tantos OSE onde a formação é obrigatória como onde é facultativa, e em setores como o dos transportes, da banca, e das infraestruturas do mercado financeiro, são mais os OSE nos quais a formação tem caráter obrigatório em vez de facultativo. Destacam-se as elevadas percentagens de OSE nos quais a frequência das formações é obrigatória nos setores da banca (88%) e das infraestruturas do mercado financeiro (100%). Já nos setores da saúde e da distribuição de água potável, apenas um terço dos inquiridos (33%) indicou que a formação em cibersegurança era de frequência obrigatória. Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre OSE e demais empresas em Portugal. Enquanto em 42% dos OSE que disponibilizam formação, esta é de caráter obrigatório, apenas em 19,2% das empresas portuguesas há formações obrigatórias. Já ao nível das de caráter facultativo (ou voluntário, nos termos do IUTICE), os resultados são mais similares aos do questionário realizado pelo CNCS, uma vez que estas se verificam em 58% dos OSE que disponibilizam formação e em 56,2% das empresas participantes no inquérito¹⁶.

¹⁶ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 19.

Gráfico 40 - Caráter das formações disponibilizadas - formação interna ou externa



Neste gráfico, fica evidenciado o maior recurso à formação interna do que externa entre os OSE. A maioria dos inquiridos (66%) recorre aos meios internos para fins de formação aos colaboradores. Surgem em destaque os setores bancário e das infraestruturas do mercado financeiro, com as maiores percentagens de OSE a darem formação interna (88% e 100%, respetivamente). Contudo, cerca de um terço dos OSE (34%) recorre a entidades externas para formar os seus colaboradores. Os setores onde mais se recorre a entidades externas para ministrar formação são o da energia e o das infraestruturas digitais, ambos com 40% de OSE a optarem por esse método, embora se continue a registar uma maioria de operadores que recorrem aos meios internos para dar formação.

Gráfico 41 - Frequência média dos momentos de formação

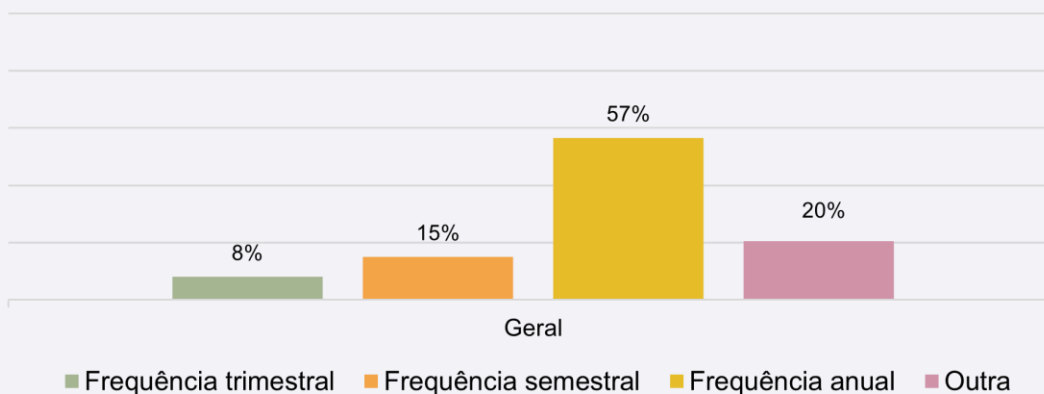


Gráfico 41.1 - Frequência média dos momentos de formação

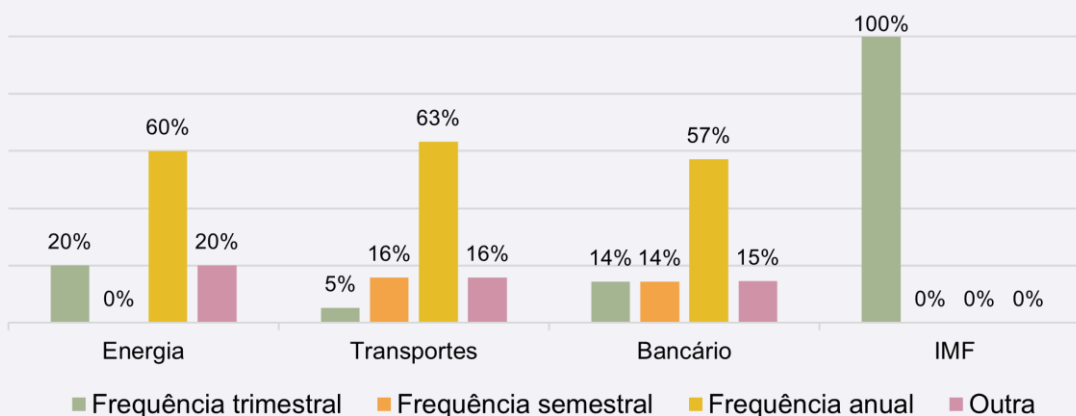
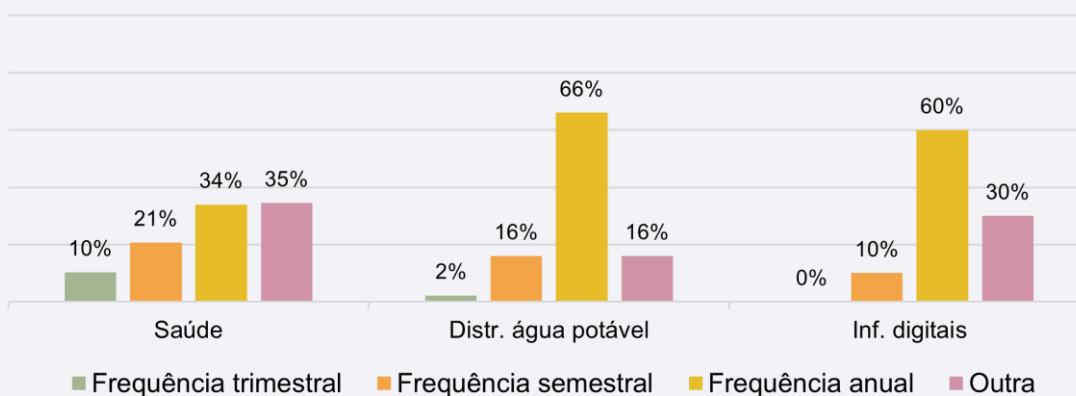


Gráfico 41.2 - Frequência média dos momentos de formação



Em termos gerais, a maioria dos OSE que disponibiliza formação (57%) indica que a frequência média dos momentos de formação é anual. Contudo, no setor das infraestruturas do mercado financeiro, todos os inquiridos indicaram que a frequência dos momentos de formação é trimestral. Por sua vez, o setor da saúde é o que apresenta uma distribuição mais variada da frequência média dos momentos de formação.

Entre os OSE que indicaram “Outra” frequência, tanto se registam frequências superiores à trimestral, chegando os momentos de formação a ser mensais ou mesmo semanais, como frequências inferiores à anual, onde não existe uma periodicidade definida e os momentos de formação sucedem de modo *ad hoc*. Por exemplo, tanto no setor da saúde como no das infraestruturas digitais, que são os que apresentam percentagens mais elevadas na opção “Outra”, tanto se registaram respostas indicando momentos de formação semanais ou mesmo diários, como respostas que indicavam que não se realizaram momentos de formação em cibersegurança em mais de um ano.

Gráfico 42 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam

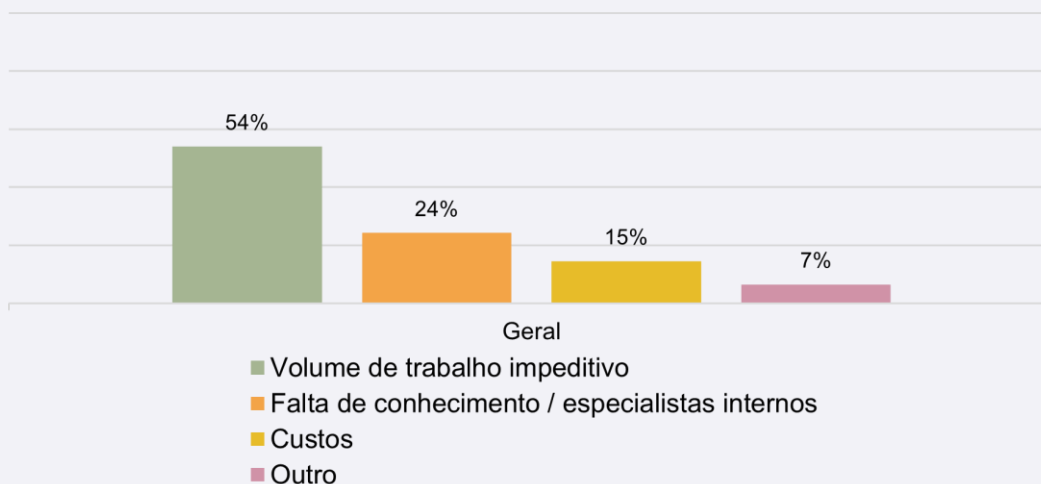


Gráfico 42.1 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam

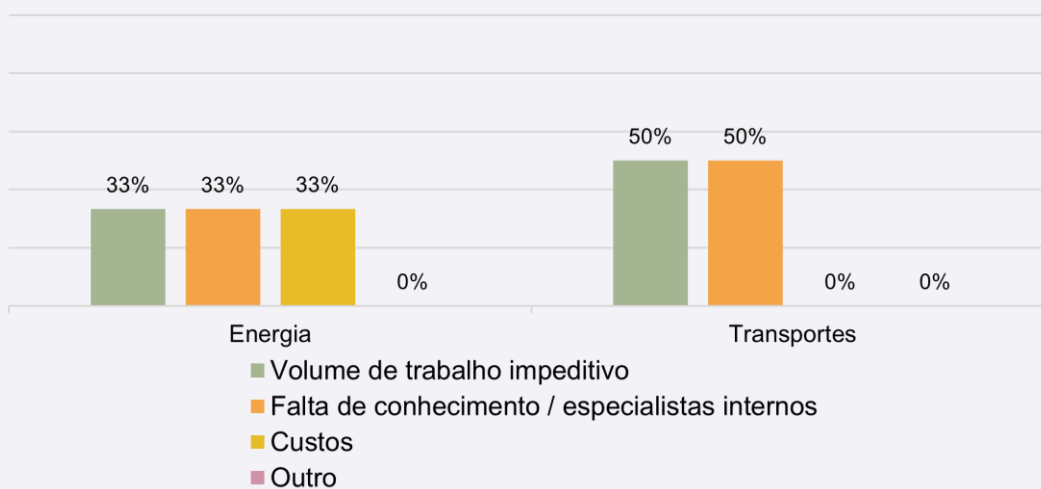
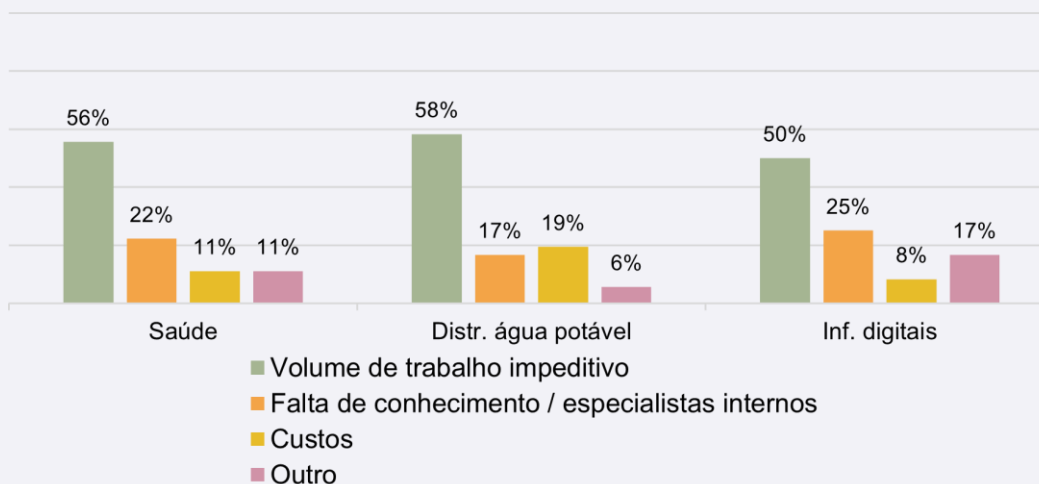


Gráfico 42.2 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam

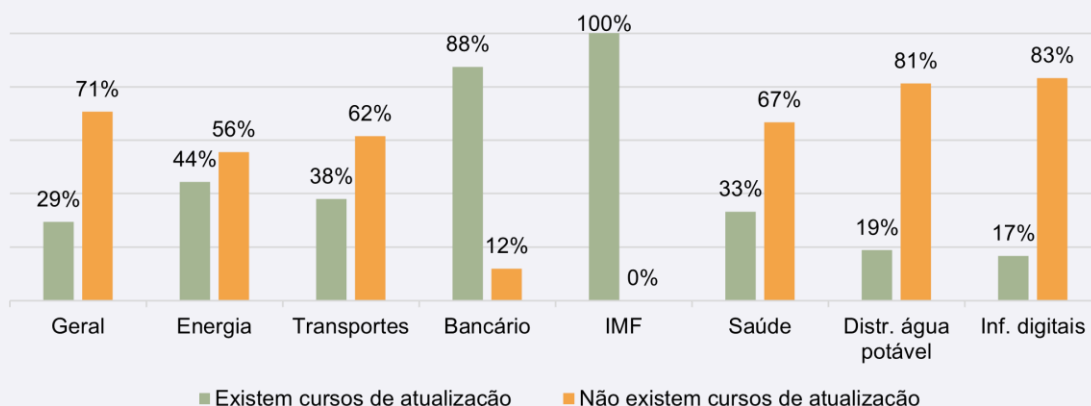


Os motivos para a não disponibilização de formação são na sua maioria atribuídos ao volume de trabalho impeditivo, tendo este motivo sido indicado por 54% dos OSE que afirmaram não disponibilizar formação em cibersegurança aos seus colaboradores. No setor da energia, os motivos para a não disponibilização de formação estão igualmente distribuídos entre volume de trabalho impeditivo, falta de conhecimento ou de especialistas internos, e custo. Cada um destes motivos foi apresentado por um terço (33%) dos OSE que não disponibilizam formação.

No caso do setor dos transportes, as razões para não disponibilizar formação distribuem-se igualmente pelo volume de trabalho impeditivo e pela falta de conhecimento/especialistas internos, com 50% dos OSE que não disponibilizam formação a indicarem estes motivos.

Nos restantes setores, saúde, distribuição de água potável e infraestruturas digitais, o principal motivo indicado continua a ser o volume de trabalho impeditivo, indicado por 50% a 58% dos OSE que não disponibilizam formação. Estes três setores são também os únicos a indicar “Outros” motivos para a falta de formação. Esses outros motivos passam, segundo os OSE, pela falta de planos de formação dentro das organizações e pela alocação de recursos financeiros a formação noutras áreas que não a cibersegurança.

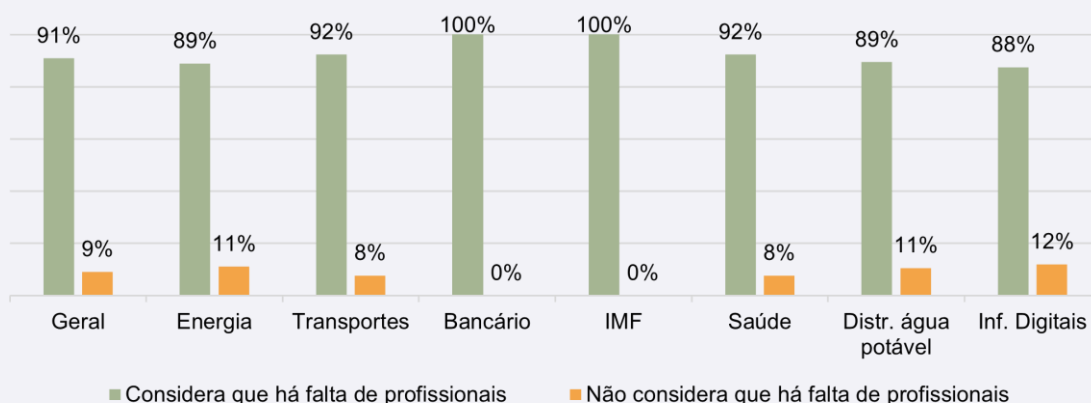
Gráfico 43 - Existência de cursos de atualização (“refresher courses”) para os colaboradores



A oferta de cursos ou formações de atualização em cibersegurança para os colaboradores é escassa na generalidade, com apenas 29% dos OSE inquiridos a indicarem a existência destes cursos. Contudo, os setores bancário e das infraestruturas do mercado financeiro contrariam essa tendência geral, com quase 90% dos inquiridos no setor bancário a indicarem que disponibilizam cursos de atualização e a totalidade dos inquiridos no setor das infraestruturas do mercado financeiro a indicarem o mesmo.

Por sua vez, os setores da distribuição de água potável e das infraestruturas digitais superam a percentagem geral, com mais de 80% dos OSE de cada um destes setores a não disponibilizarem este tipo de cursos ou formações.

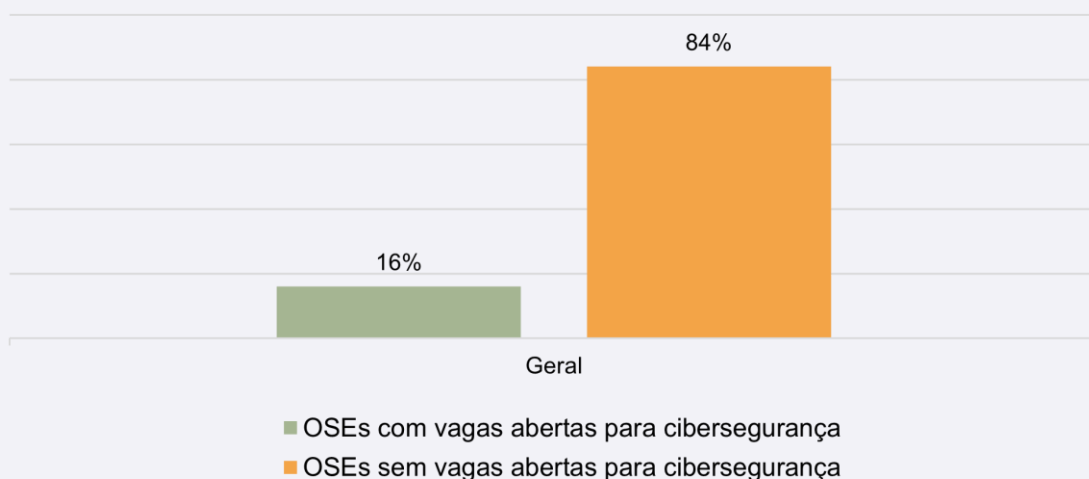
Gráfico 44 - Perceção sobre a falta de profissionais em cibersegurança e áreas relacionadas



A vasta maioria dos OSE inquiridos (91%) considera haver um cenário de escassez de profissionais de cibersegurança e áreas relacionadas no mercado de trabalho. Especificamente, nos setores da banca e das infraestruturas do mercado financeiro, todos os OSE inquiridos consideram que há falta de profissionais na área. O setor onde menor percentagem de OSE considerou haver falta de profissionais de cibersegurança foi o das infraestruturas digitais e, mesmo assim, 88% concordam com a escassez de profissionais na área.

A escassez de profissionais em cibersegurança é um problema que persiste há largos anos, devido à discrepância entre a velocidade a que a tecnologia evolui e o tempo que leva a formar os profissionais. Segundo o Fórum Económico Mundial, a atual escassez global de profissionais em cibersegurança é de cerca de 4 milhões de profissionais¹⁷ e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia¹⁸. Esta falta de profissionais coloca aos empregadores na área desafios como conseguir pessoal qualificado, conseguir desenvolver equipas que possuam as capacidades técnicas desejadas e conseguir manter os bons profissionais encontrados¹⁹. De modo a combater esta escassez, organizações como o Fórum Económico Mundial e a ENISA têm feito diversas recomendações, que passam pela contratação de profissionais vindos de outras áreas de formação que não apenas as das TIC, engenharia e matemática, pela admissão de colaboradores menos experientes, ou mesmo sem experiência (sendo esta adquirida ao longo do desempenho das funções pretendidas), a admissão de colaboradores em trabalho totalmente remoto, e pela valorização dos profissionais, não só a nível salarial, mas também a nível das perspetivas de progressão de carreira e até mesmo do respeito pelos profissionais no local de trabalho^{20 21}.

Gráfico 45 - Vagas abertas para a área de cibersegurança



¹⁷ Banco Mundial, "Strategic Cybersecurity Talent Framework", 5.

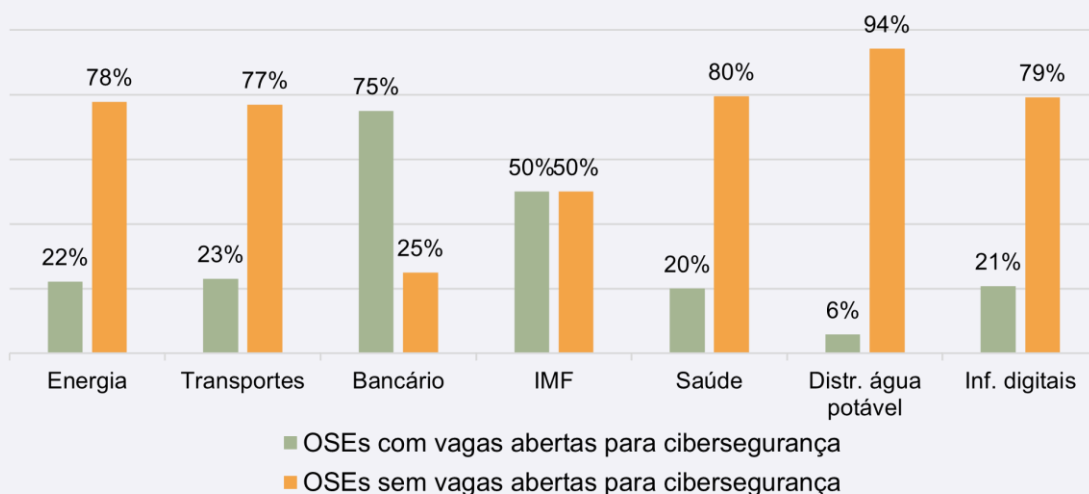
¹⁸ ENISA, "Cybersecurity Skills Conference: Strengthening human capital in the EU", <https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu>.

¹⁹ ENISA, "NIS Investments", 2022, 16, <https://www.enisa.europa.eu/publications/nis-investments-2022>.

²⁰ ENISA, "NIS Investments", 2022, 16-17.

²¹ Banco Mundial, "Strategic Cybersecurity Talent Framework", 22-25.

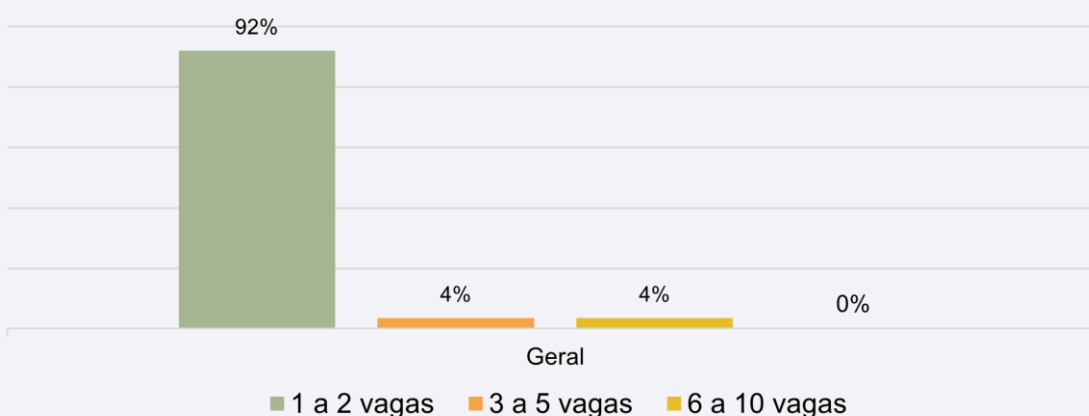
Gráfico 45.1 - Vagas abertas para a área de cibersegurança



À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. Sectorialmente, registaram-se duas exceções: o setor bancário e o setor das infraestruturas do mercado financeiro, com 75% dos OSE da banca a indicarem ter vagas em aberto, e 50% das IMF a terem também vagas em aberto. Contrastando, o setor da distribuição de água potável foi o que registou a percentagem mais baixa de OSE com vagas abertas para cibersegurança, atingindo apenas os 6%.

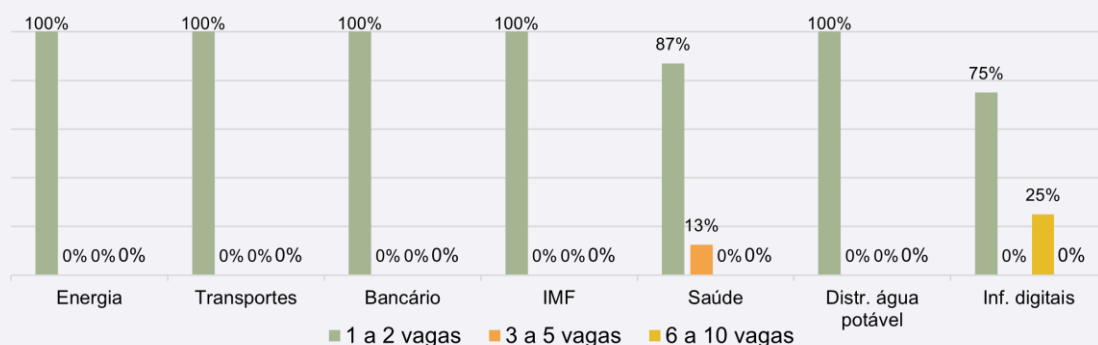
Embora não se possa fazer uma associação direta entre vagas para cibersegurança e para pessoal especialista em TIC, os dados do IUTICE de 2022 mostram que, nesse ano, apenas 6,2% das empresas portuguesas tentaram recrutar pessoal especialista em TIC²².

Gráfico 46 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança



²² INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 15.

Gráfico 46.1 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança



Entre os 16% de OSE que tinham vagas abertas na área de cibersegurança, a maioria destes (92%) tinha 1 a 2 vagas por preencher. Tal era o caso para todos os OSE com vagas em aberto nos setores da energia, dos transportes, da banca e das infraestruturas do mercado financeiro. Apenas no setor da saúde se registaram OSE com 3 a 5 vagas em aberto e só no das infraestruturas digitais houve indicação de haver entre 6 e 10 vagas em aberto.

Gráfico 47 - Motivos para a não abertura de vagas entre os OSE sem vagas abertas para a área de cibersegurança

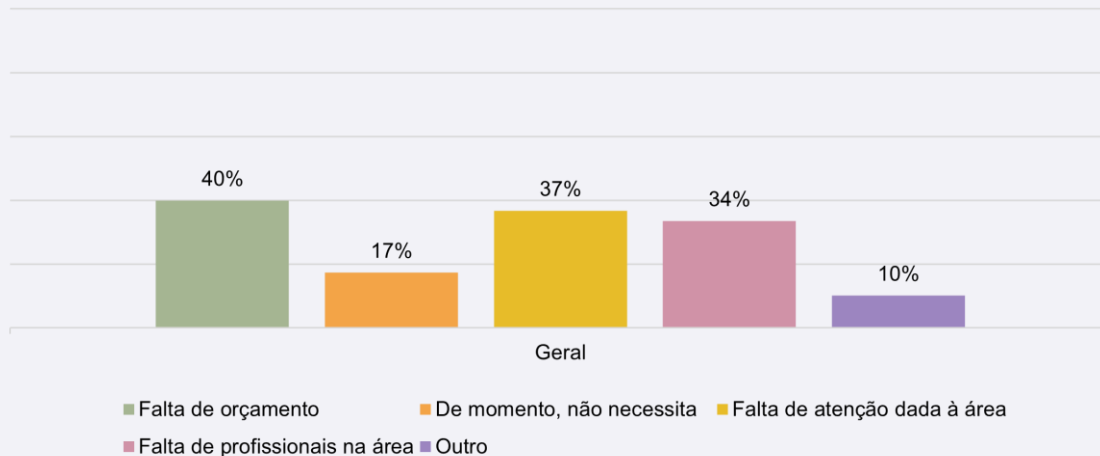


Gráfico 47.1 - Motivos para a não abertura de vagas entre os OSE sem vagas abertas para a área de cibersegurança

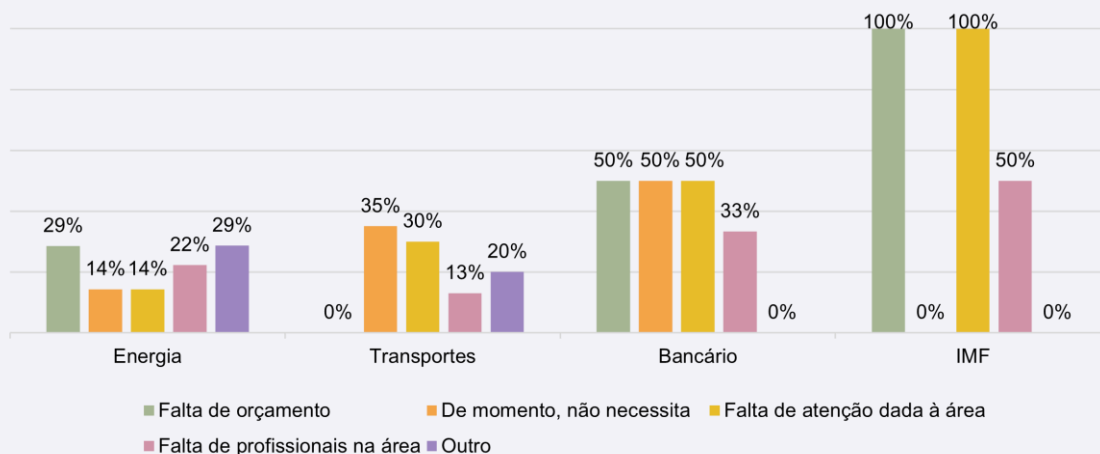
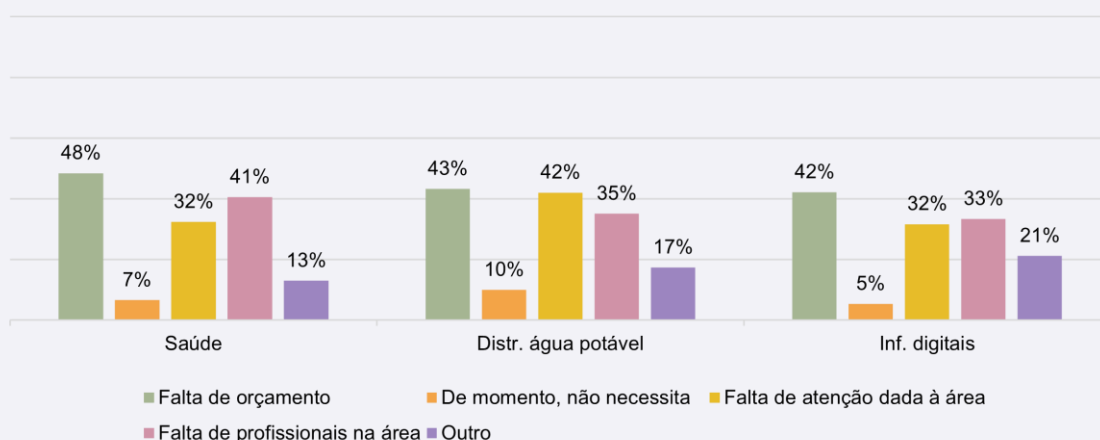


Gráfico 47.2 - Motivos para a não abertura de vagas entre os OSE sem vagas abertas para a área de cibersegurança



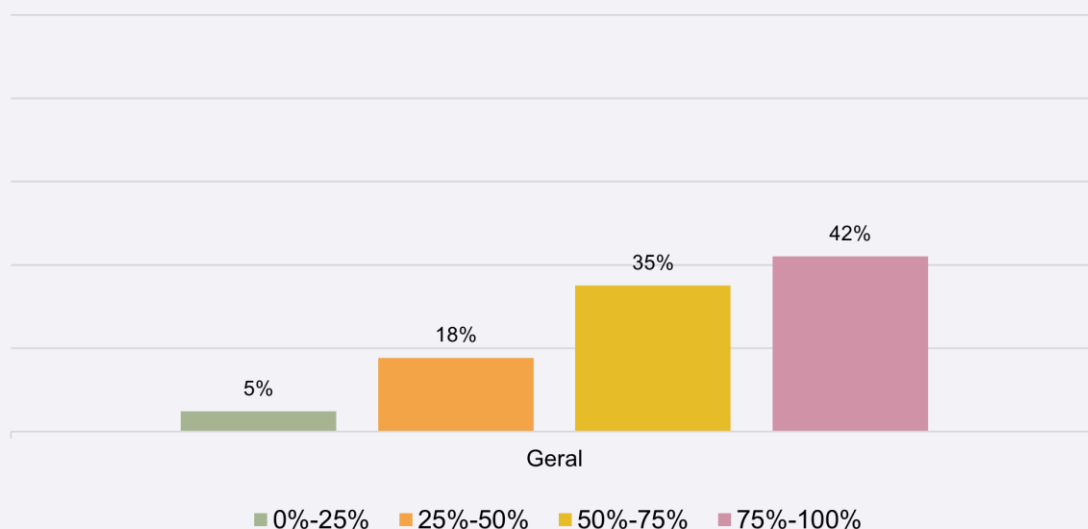
No seguimento das questões sobre vagas em aberto para a área de cibersegurança, questionou-se também os motivos pelos quais os OSE não teriam tais vagas disponíveis.

A resposta mais comum foi a falta de orçamento, indicada por 40% dos OSE sem vagas em aberto, seguida da falta de atenção dada à área (37%) e da falta de profissionais de cibersegurança (34%). Apenas em 17% dos casos foi indicado que não havia vagas em aberto por se considerar que de momento não eram necessários mais profissionais. Os 10% de OSE que indicaram “outros” motivos mencionaram motivos como o facto de existirem poucos conhecimentos/noção da gravidade de um ataque informático, haver questões legais que impedem a contratação de mais recursos.

De acordo com os dados do IUTICE de 2022, 61,4% das empresas portuguesas sentiram dificuldades no recrutamento. Entre estas, 82,1% apontaram a falta de candidaturas como um problema, cerca de 57% mencionaram a falta de qualificações ou de experiência relevante dos candidatos como outra dificuldade e 91,9% indicaram que as expectativas de remuneração dos candidatos eram demasiado elevadas²³.

Voltando aos dados obtidos através do questionário realizado, a “falta de atenção dada à área” indicada por 37% dos OSE sem vagas em aberto é um dos aspetos mais preocupantes que surgem na análise. Um dos Objetivos Estratégicos (Objetivo 3) da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 passa por gerar e “garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço”²⁴, objetivo esse que não pode ser cumprido quando há falta de atenção dada à área. Tratando-se de Operadores de Serviços Essenciais, esta lacuna torna-se ainda mais grave. Recorda-se, também, que é uma boa prática constante de normativos internacionais, como a ISO/IEC 27001, que a direção/administração das organizações demonstre o seu compromisso para com segurança da informação e que esta assegure a alocação dos recursos necessários para cumprir esse desígnio²⁵.

Gráfico 48 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho

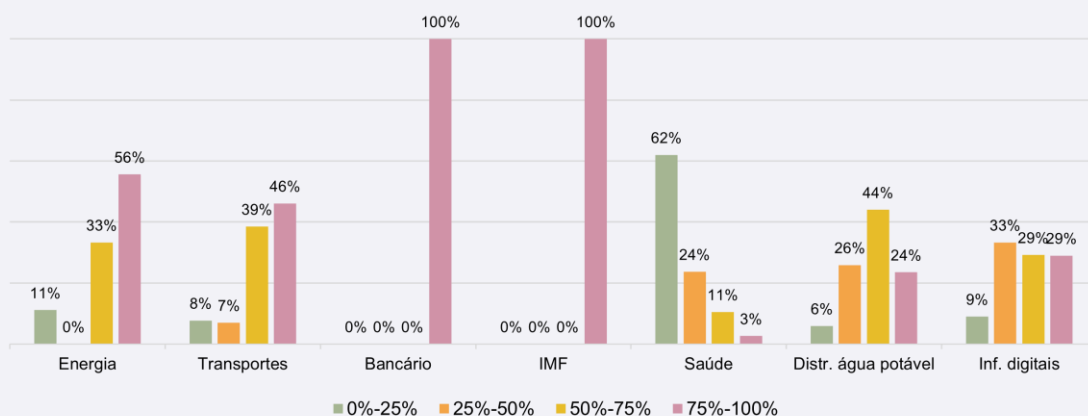


²³ INE, “Inquérito à Utilização das TIC nas Empresas”, 2022, 15-17.

²⁴ CNCS, “Estratégia Nacional de Segurança do Ciberespaço 2019-2023”, 11, <https://www.cncs.gov.pt/docs/cnsc-ensc-2019-2023.pdf>.

²⁵ International Organization for Standardization, “International Standard ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, 2.

Gráfico 48.1 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho



Apesar de predominar entre os OSE o intervalo 75%-100% de colaboradores com acesso a equipamentos digitais (indicado por 42% dos OSE), é visível que, com exceção dos setores bancário e das infraestruturas do mercado financeiro, há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos. O setor da saúde é o mais evidente, no qual mais de 60% dos operadores indicam uma percentagem de até 25% dos colaboradores com acesso a equipamentos digitais na realização do seu trabalho.

Outro setor curioso é o das infraestruturas digitais, onde os intervalos predominantes são o intervalo 25%-50% e o intervalo 50%-75% de operadores com acesso a equipamentos digitais.

Também no setor do fornecimento e distribuição de água potável se verifica que o intervalo mais recorrente é o intervalo 50%-75% de colaboradores com acessos a esses equipamentos. Já nos setores da energia e dos transportes é acompanhada a tendência geral de ter entre 75% a 100% dos colaboradores com acesso a equipamentos digitais.

Segundo dados do IUTICE de 2022, em 2021, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais (+17,2 p.p. face a 2021), abrangendo 28,1% do pessoal ao serviço (+4,2 p.p. que em 2021). Neste ano, 74,7% das empresas tinham pessoal ao serviço com acesso remoto ao sistema de correio eletrónico da empresa²⁶.

²⁶ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 4-5.

Gráfico 49 - Os OSE são responsáveis pelo funcionamento dos equipamentos necessários às funções dos colaboradores

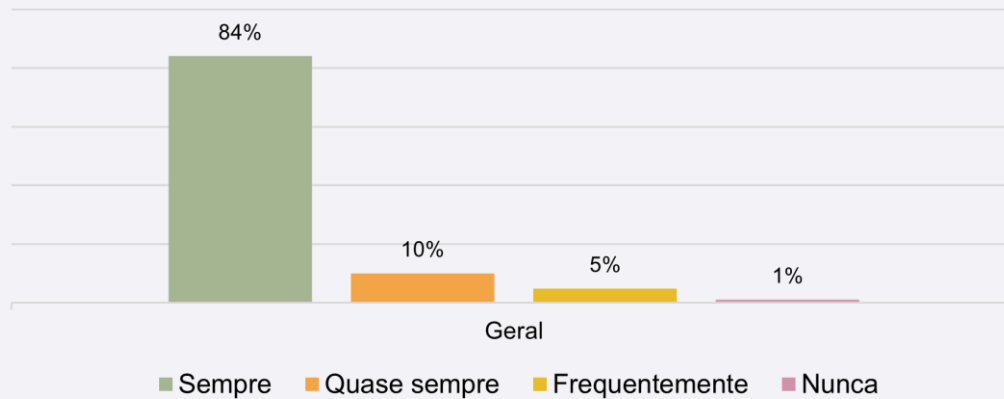


Gráfico 49.1 - Os OSE são responsáveis pelo funcionamento dos equipamentos necessários às funções dos colaboradores

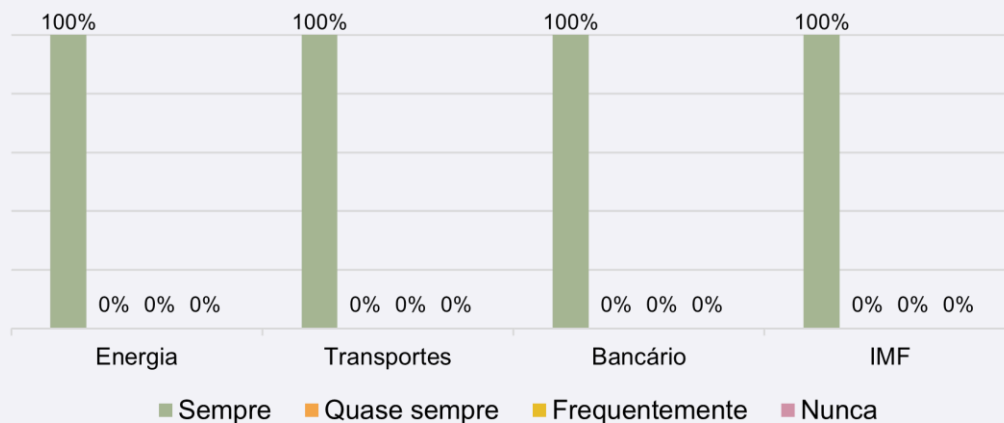
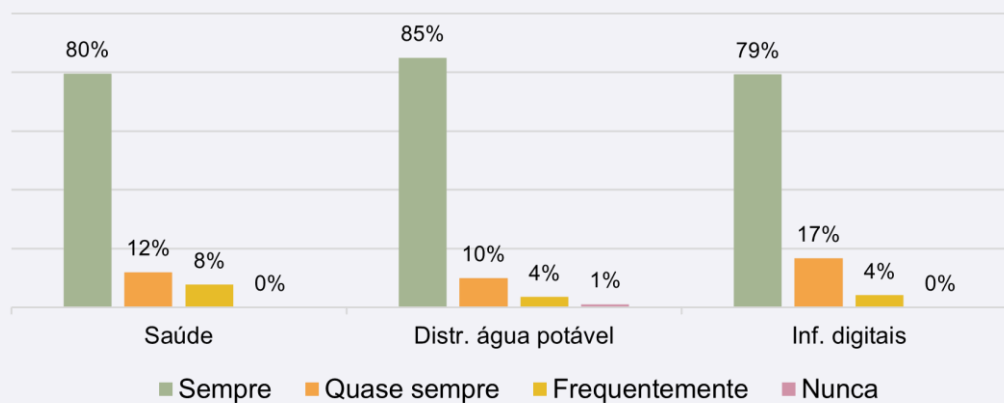


Gráfico 49.2 - Os OSE são responsáveis pelo funcionamento dos equipamentos necessários às funções dos colaboradores



Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. Todos os operadores inquiridos nos setores da energia, dos transportes, da banca e das infraestruturas do mercado financeiro indicaram ser os próprios a fornecer sempre os equipamentos necessários aos colaboradores.

Contrastando, nos setores da saúde, do fornecimento e distribuição de água potável e das infraestruturas digitais, registam-se alguns OSE onde nem sempre o fornecimento dos equipamentos necessários é feito pelo OSE em questão. No setor da saúde, houve 80% de OSE a indicar que eram sempre responsáveis pelo fornecimento dos equipamentos, no da distribuição de água potável, 85%, e no das infraestruturas digitais, 79%. Ressalva-se ainda que não se registaram situações em que os operadores nunca fornecem os equipamentos, impondo esse encargo aos colaboradores.

Novamente, sublinha-se que segundo o IUTICE de 2022, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais, abrangendo 28,1% do pessoal ao serviço²⁷.

Gráfico 50 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções

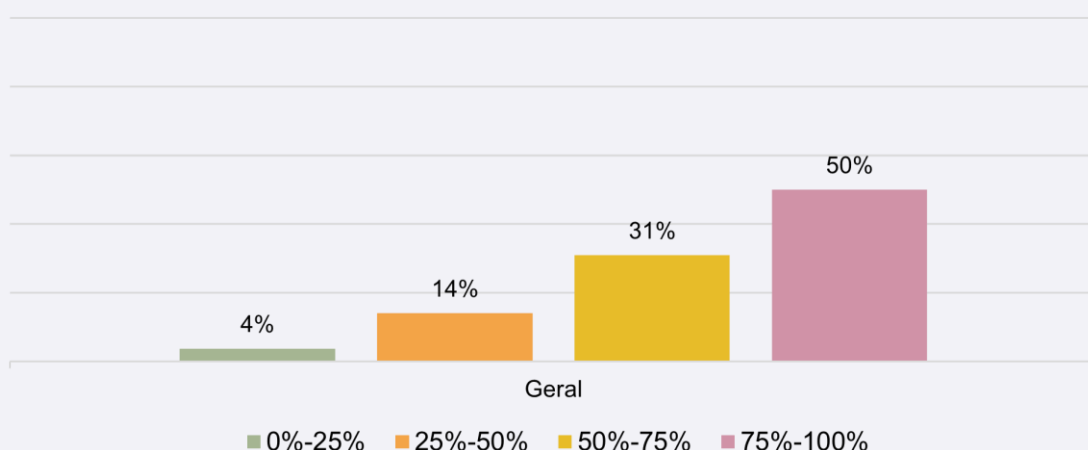
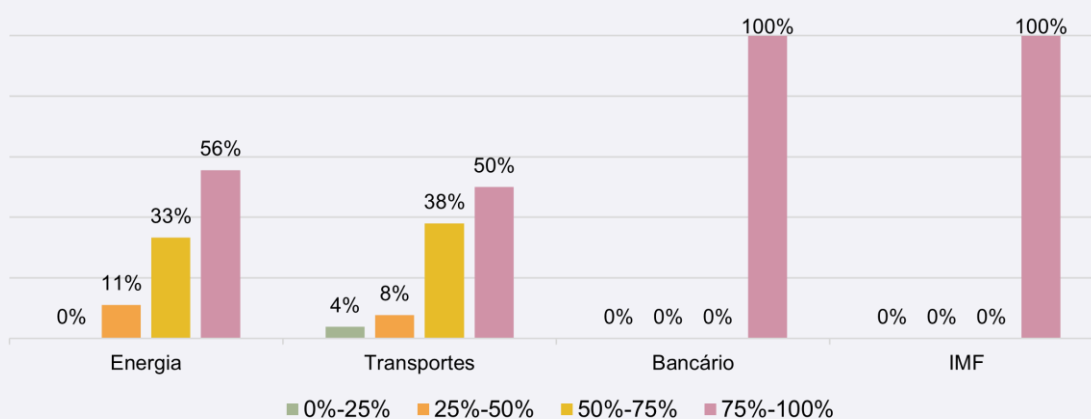
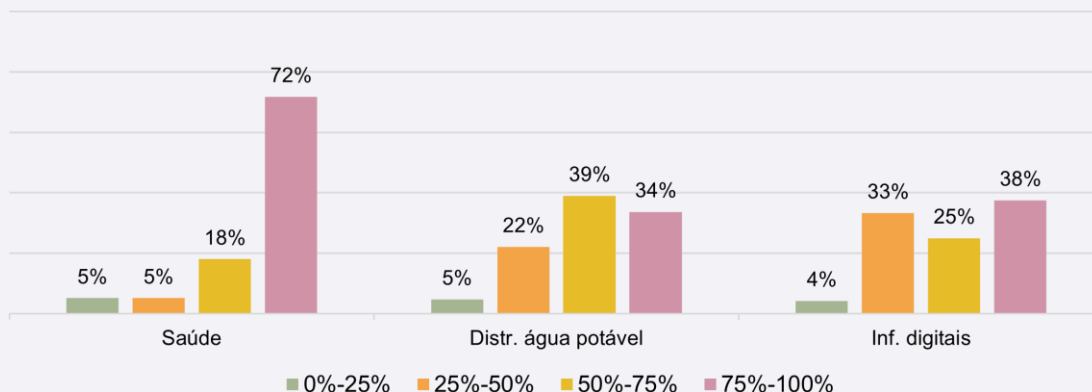


Gráfico 50.1 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções



²⁷ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 4-5.

Gráfico 50.2 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções



A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.

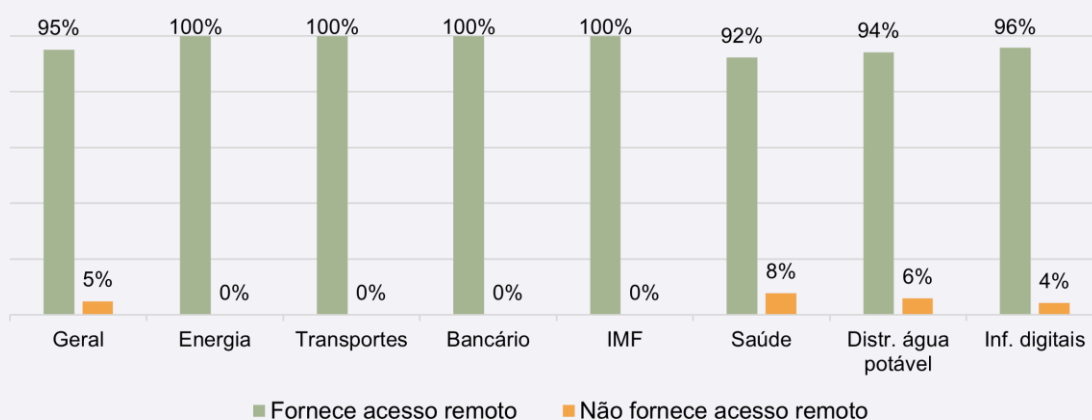
Nos setores bancário e das IMF, verifica-se que todos os operadores fornecem esse acesso a pelo menos 75% dos colaboradores. Nos restantes setores, com exceção do setor do fornecimento e distribuição de água potável, a faixa predominante continua a ser aquela em que 75%-100% dos colaboradores tem acesso à Internet no desempenho das suas funções, embora se registem operadores nos quais a percentagem de trabalhadores com acesso à Internet é menor.

No setor do fornecimento e distribuição de água potável, verifica-se que a situação mais comum entre os OSE é haver 50%-75% dos colaboradores com acesso à Internet, contrariando a tendência geral.

Voltando a comparar com dados do IUTICE, mas agora com o de 2023, verifica-se que há mais colaboradores com acesso à Internet no contexto específico dos OSE do que das várias empresas portuguesas. Juntando os dois intervalos onde mais de 50% dos colaboradores têm acesso à Internet, obtém-se 81% de OSE onde 50% dos colaboradores acedem à Internet no desempenho das suas funções. No contexto empresarial português, apenas 48,9% dos colaboradores têm acesso à Internet para fins de trabalho. Mesmo comparando sectorialmente onde possível, como nos setores da energia e dos transportes, os OSE continuam a apresentar mais colaboradores com acesso à Internet: segundo o IUTICE, no setor da energia, há 39,8% de colaboradores com acesso à Internet, enquanto o questionário realizado demonstra que em 89% dos OSE desse setor, 50% dos colaboradores ou mais têm acesso à Internet; e no setor dos transportes, 56,6% dos colaboradores têm acesso à Internet no contexto empresarial português, enquanto no contexto dos OSE 88% indicam haver 50% ou mais colaboradores com acesso à Internet para fins de trabalho²⁸.

²⁸ INE, "Inquérito à Utilização das TIC nas Empresas", 2023, 3.

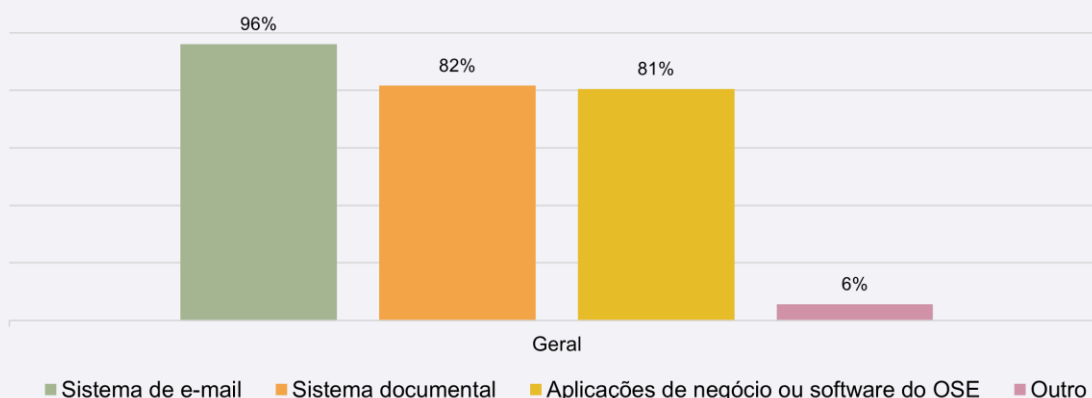
Gráfico 51 - Fornecimento de acesso remoto a sistemas (e-mail, aplicações ou documentos) dos OSE aos colaboradores



O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSE aos colaboradores é uma realidade em praticamente todos os OSE inquiridos (95%). No setor da energia, no dos transportes, no da banca e no das IMF, todos os OSE indicaram permitir o acesso remoto a esses sistemas por parte dos seus colaboradores. Apenas nos setores da saúde, da distribuição de água potável e das infraestruturas digitais se registaram exceções. Ainda assim, pelo menos 92% dos operadores nestes setores fornecem acesso remoto a esses sistemas aos seus colaboradores.

Voltando a comparar com os dados do IUTICE de 2022, há uma maior percentagem de Operadores de Serviços Essenciais a fornecer acesso remoto ao sistema de e-mail do que na generalidade das empresas em Portugal. Enquanto 95% dos OSE indicaram dar esse acesso remoto, no contexto empresarial geral apenas 74,7% das empresas fornecem acesso remoto ao sistema de e-mail²⁹.

Gráfico 52 - Sistemas do OSE aos quais é dado acesso remoto aos colaboradores



²⁹ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 6-7.

Gráfico 52.1 - Sistemas do OSE aos quais é dado acesso remoto aos colaboradores

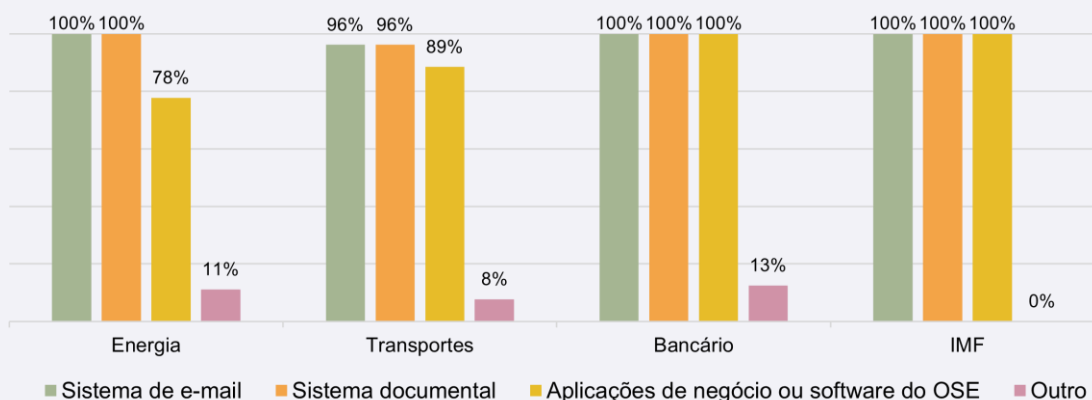
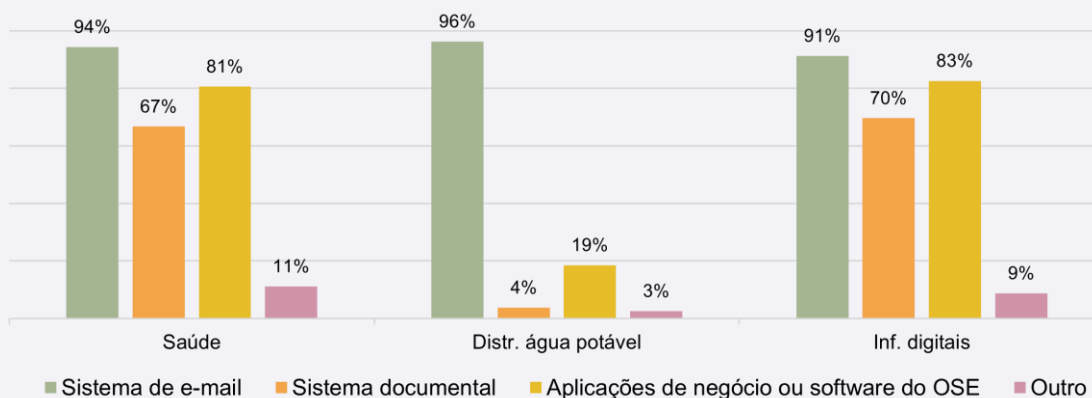


Gráfico 52.2 - Sistemas do OSE aos quais é dado acesso remoto aos colaboradores



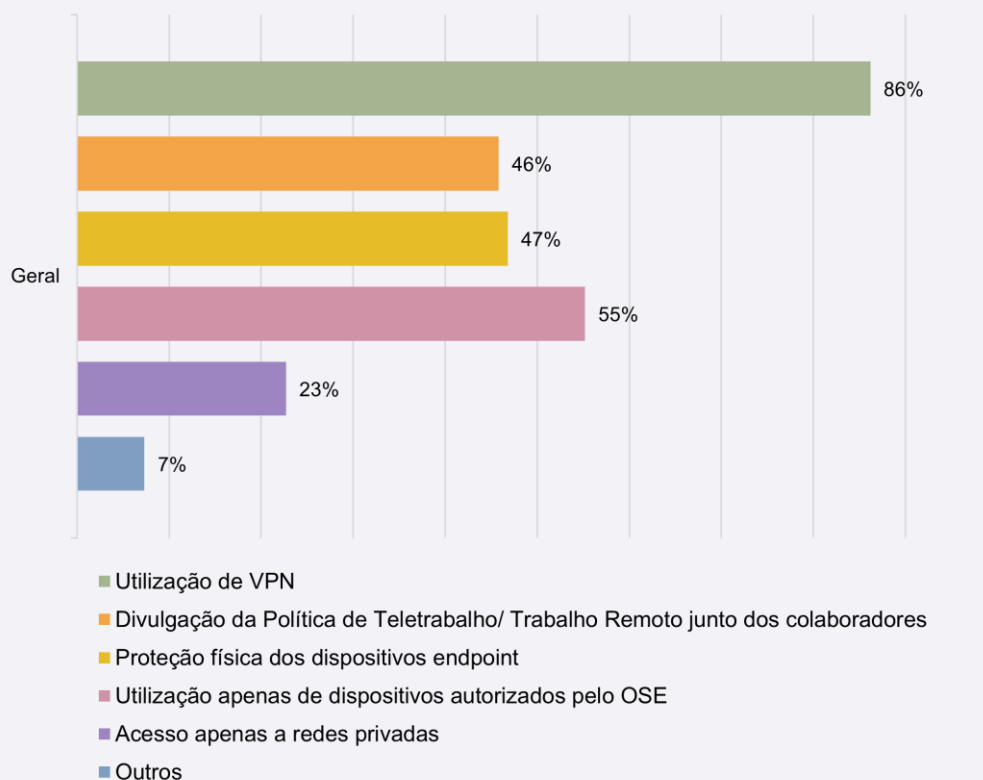
Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no a aplicações de negócio ou a *software* do operador. 6% refere conceder acesso remoto a outros tipos de sistemas, sem especificar quais.

Nos setores bancário e das IMF, os sistemas de e-mail, documentais e aplicações de negócio podem ser acedidos remotamente por todos os colaboradores. Já no setor do fornecimento e distribuição de água potável, é notório que o principal sistema ao qual é dado acesso remoto é somente o de *e-mail* (96%), havendo muito menos OSE nesse setor nos quais é dado acesso remoto ao sistema documental (4%) ou a aplicações de negócio ou a *software* do OSE (19%).

Comparando novamente com dados do IUTICE de 2022, os OSE continuam a fornecer mais acesso remoto a diferentes sistemas do que a generalidade das empresas portuguesas. Tinha já sido vista a diferença na disponibilização geral de acesso remoto por parte dos colaboradores a sistemas entre OSE (95% a disponibilizar) e empresas (74,7% a disponibilizar).

Revisitando essa comparação entre cada sistema, é visível que há mais OSE a dar acesso remoto aos documentos da organização do que empresas em geral (82% de OSE contra 65% de empresas) e também mais OSE a dar acesso remoto a aplicações ou *software* de negócio (81%) do que empresas (63,9%)³⁰.

Gráfico 53 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE



³⁰ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 6-7.

Gráfico 53.1 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE

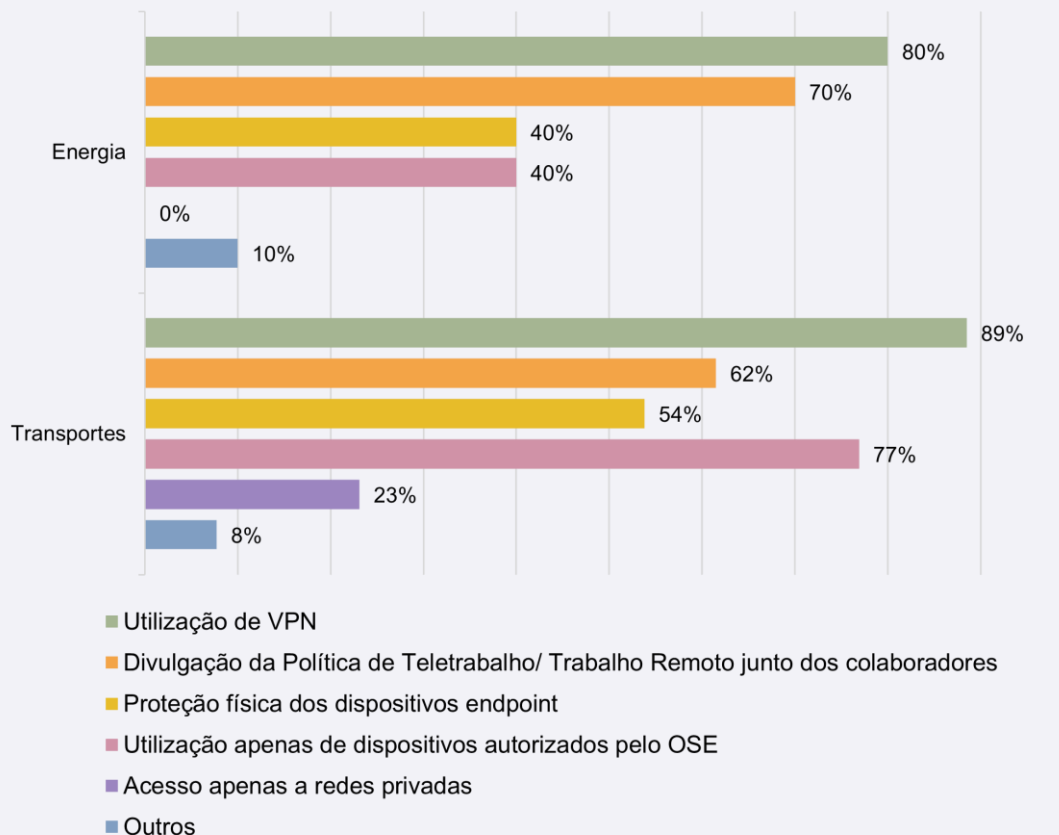


Gráfico 53.2 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE

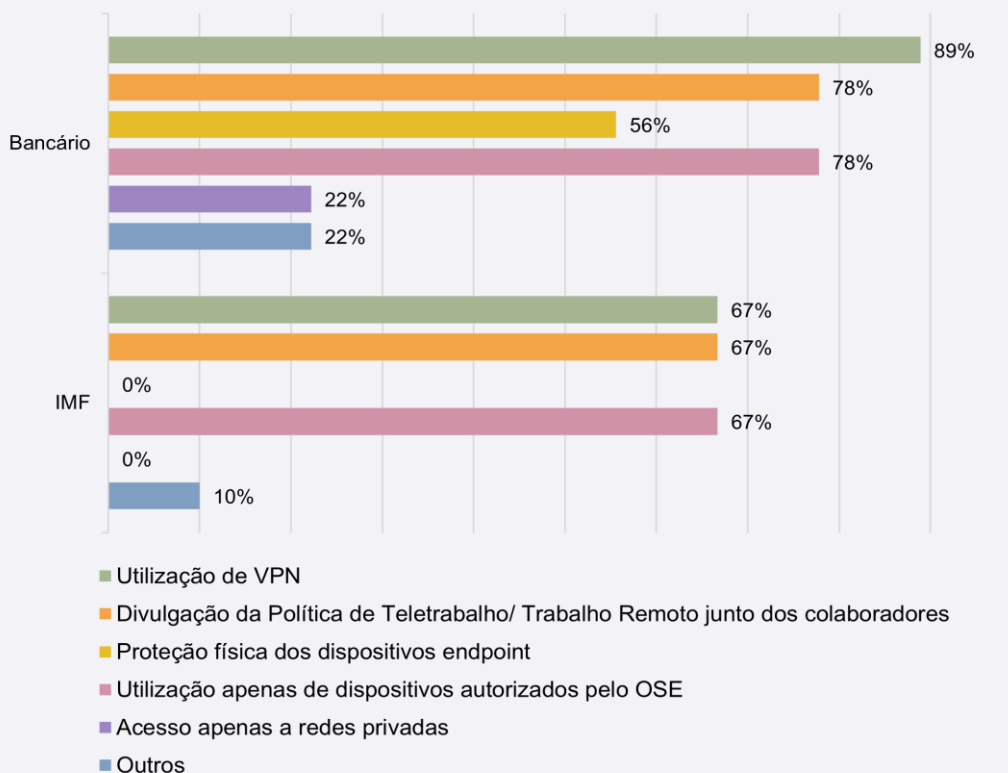
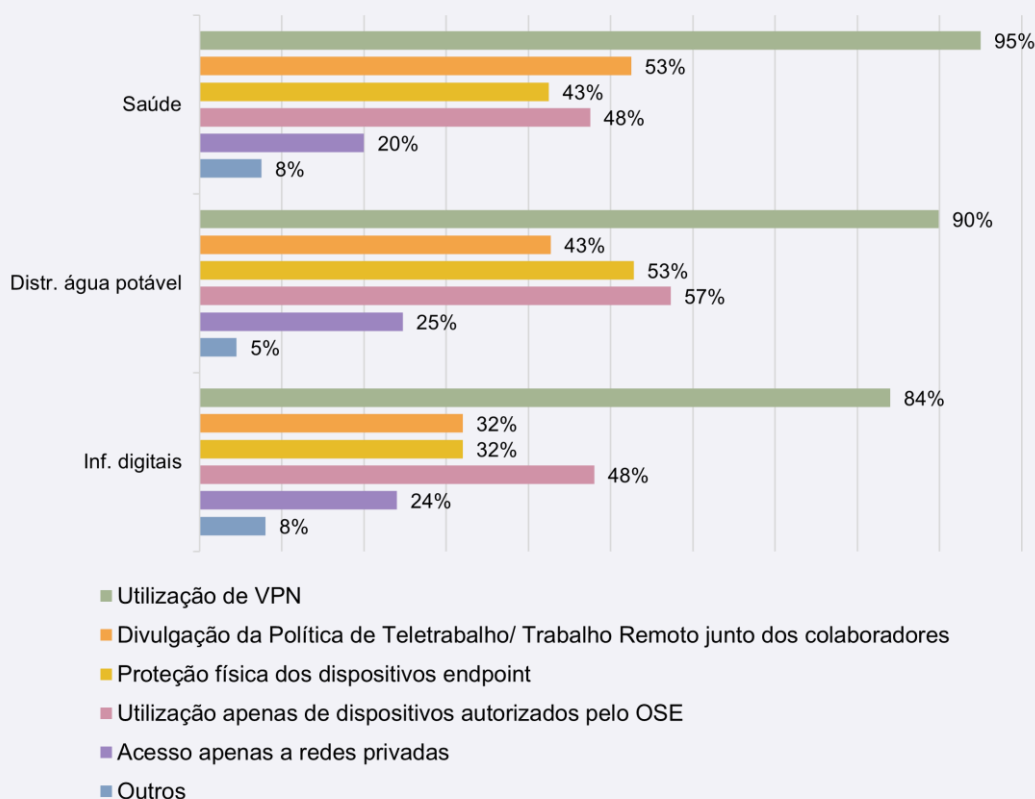


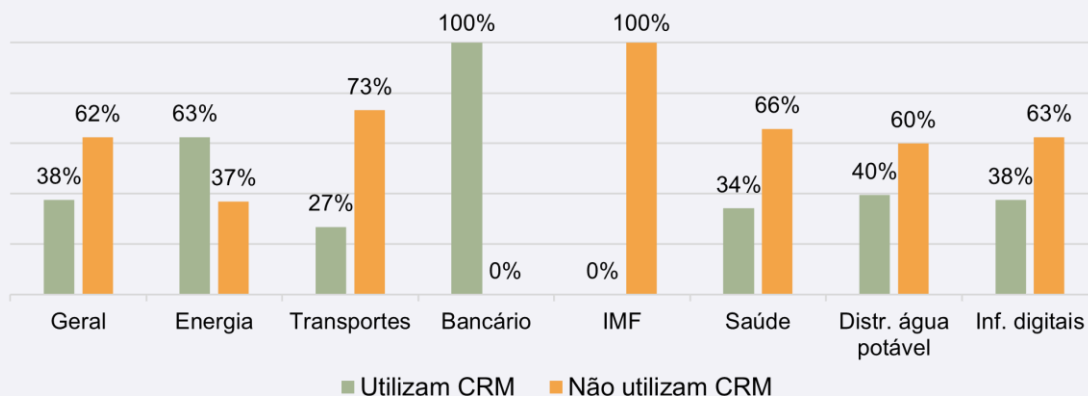
Gráfico 53.3 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE



No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança para acesso remoto menos utilizada pelos OSE. No entanto, esta pode ser uma medida de segurança adicional, mesmo quando se utiliza VPN.

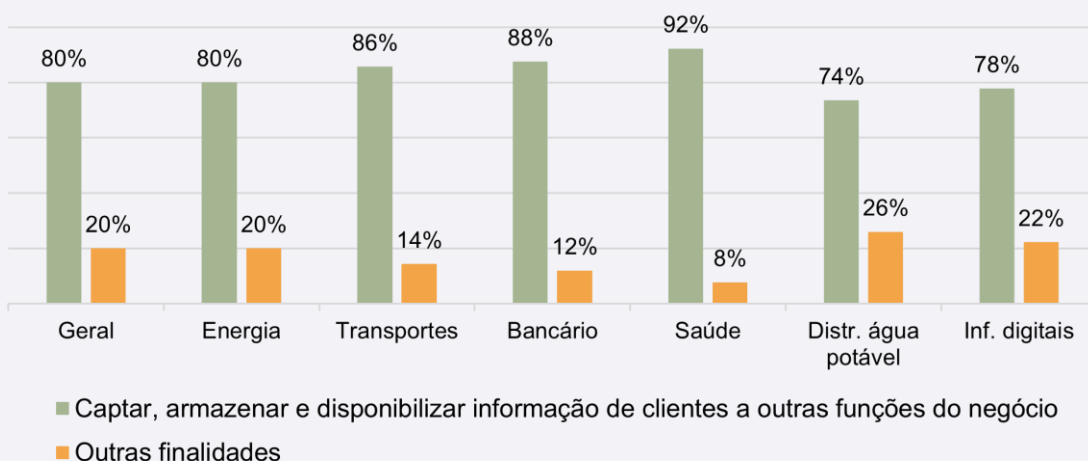
A segunda boa prática mais aplicada é a utilização de dispositivos autorizados pelos OSE, mas com uma prevalência bem mais reduzida (verificada apenas em 55% dos casos). Medidas como a divulgação da Política de Teletrabalho/Trabalho Remoto, proteção física dos dispositivos *endpoint* e acesso apenas através de redes privadas verificam-se em menos de 50% dos operadores inquiridos. Os operadores que indicaram outras boas práticas mencionaram a utilização de autenticação multifator, máquinas virtuais a operar nos servidores do operador (VDI's: *Virtual Desktop Infrastructure*) e gestão de acessos privilegiados (PAM: *Privileged Access Management*). O IUTICE questiona também quais as medidas de segurança aplicadas pelas empresas, embora não enquadre a questão no caso específico do acesso remoto. Apesar de se verificar uma elevada percentagem de empresas a utilizar medidas como palavras-passe seguras (84%) e backups em local distinto (73,7%), apenas 44,2% indicaram utilizar VPN, contrastando com os 86% de OSE que recorrem a esta medida.

Gráfico 54 - OSE que utilizam Customer Relationship Management software (CRM)



São mais os operadores que não utilizam *software* de *Customer Relationship Management* (CRM)³¹ - 62% - do que aqueles que utilizam - 38%. Curiosamente, nos dois setores da área financeira (bancário e IMF) observa-se um grande contraste já que de todos os OSE do setor bancário utilizarem CRM e nenhum dos OSE das IMF utilizar este tipo de *software*. Quanto aos setores dos transportes, saúde, fornecimento e distribuição de água potável e das infraestruturas digitais, predominam os operadores que não utilizam CRM, ao passo que, no setor de energia, a maioria dos operadores (63%) já utiliza esse tipo de *software*.

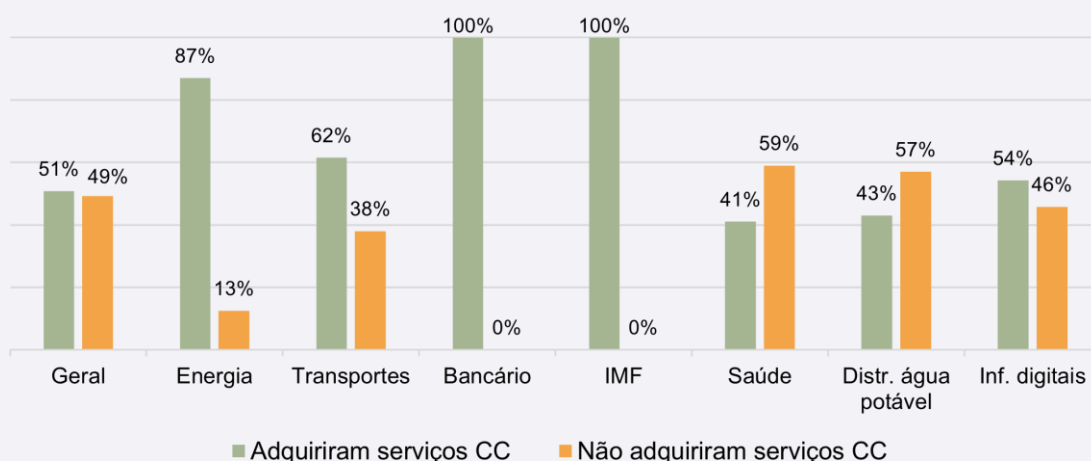
Gráfico 55 - OSE que utilizam CRM para captar, armazenar e disponibilizar informação de clientes a outras funções do negócio



Entre os operadores que utilizam CRM, a maioria utiliza-o para captar, armazenar e disponibilizar informações de clientes a outras funções do negócio (80%). Os restantes 20% utilizam CRM para outros fins não especificados. O setor em que mais OSE utilizam CRM para as funções especificadas é o da saúde, com 92%, e o setor onde menos OSE indicam utilizar CRM para as funções descritas é o do fornecimento e distribuição de água potável (74%). Como o setor das infraestruturas do mercado financeiro mencionou não utilizar CRM, a questão não se aplica.

³¹ *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos e na maximização de lucros.

Gráfico 56 - OSE que adquiriram serviços de Computação Cloud (CC)



À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização.

Os setores que mais procuraram este tipo de serviços foram os setores bancário, o das infraestruturas do mercado financeiro (em ambos, todos os inquiridos adquiriram este tipo de serviços), o da energia (com 87%), o dos transportes (62%) e o das infraestruturas digitais (54%). Os setores onde menos de 50% dos OSE inquiridos adquiriram serviços *cloud* foram o da saúde e o do fornecimento e distribuição de água potável.

O relatório *NIS Investments* de 2022 demonstra que a procura por serviços *cloud* aumentou grandemente devido aos efeitos da pandemia, tendo sido uma prioridade de investimento nesse ano - cerca de 45% dos OSE colocaram o investimento em serviços *cloud* como um dos principais objetivos de 2021³². Em 2023, este tipo de serviços continuou a ser uma das áreas onde os OSE mais aumentaram o seu investimento (49% dos OSE inquiridos pela ENISA em 2023 indicaram ter aumentado os seus investimentos em plataformas *cloud*)³³. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*³⁴.

³² ENISA, "NIS Investments", 2022, 11.

³³ ENISA, "NIS Investments", 2023, 10.

³⁴ INE, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 57 - Finalidades dos serviços de Computação Cloud adquiridos

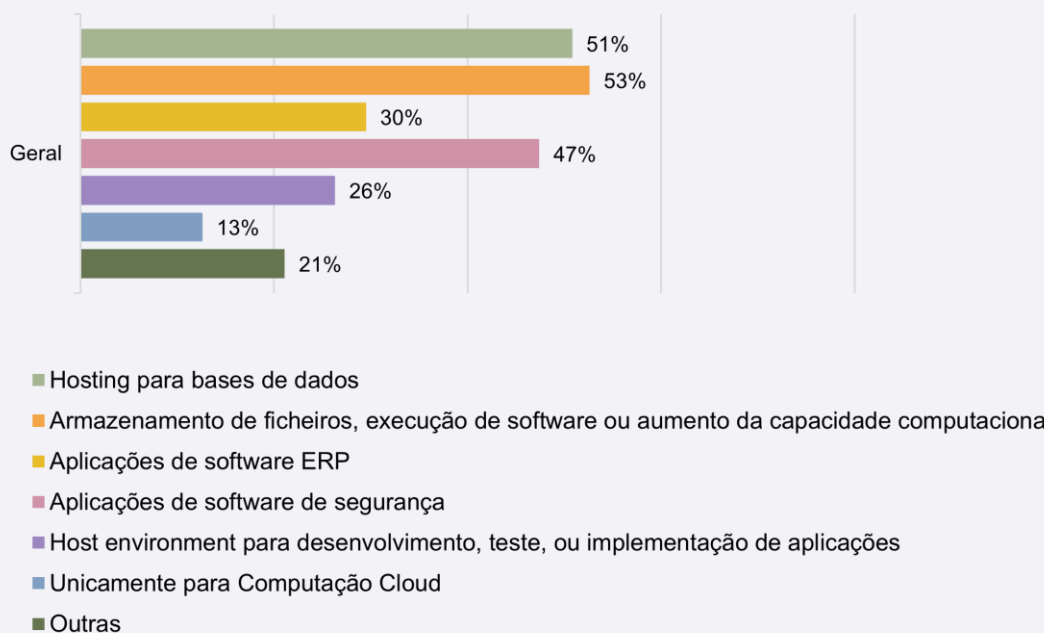


Gráfico 57.1 - Finalidades dos serviços de Computação Cloud adquiridos

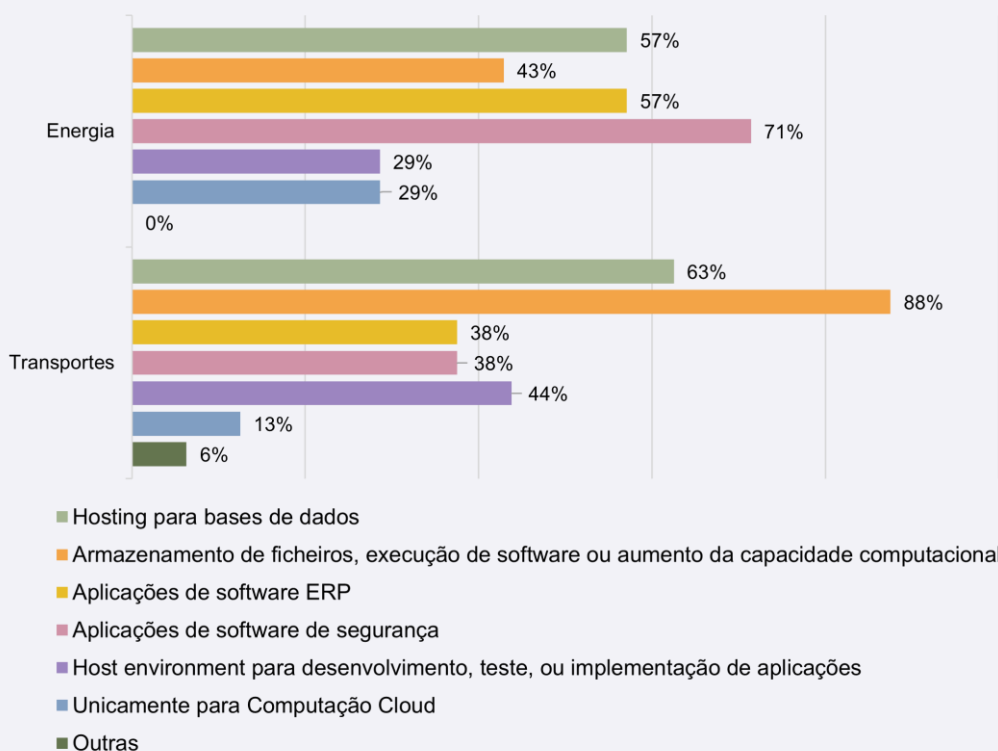


Gráfico 57.2 - Finalidades dos serviços de Computação Cloud adquiridos

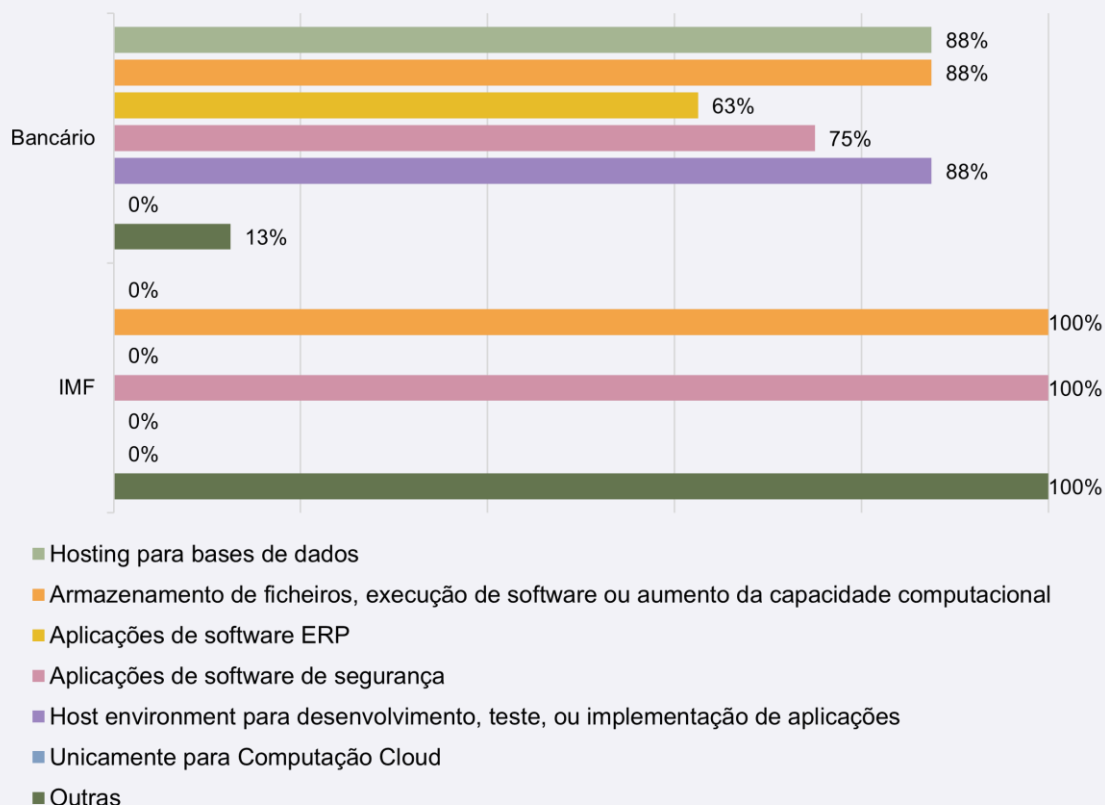


Gráfico 57.3 - Finalidades dos serviços de Computação Cloud adquiridos

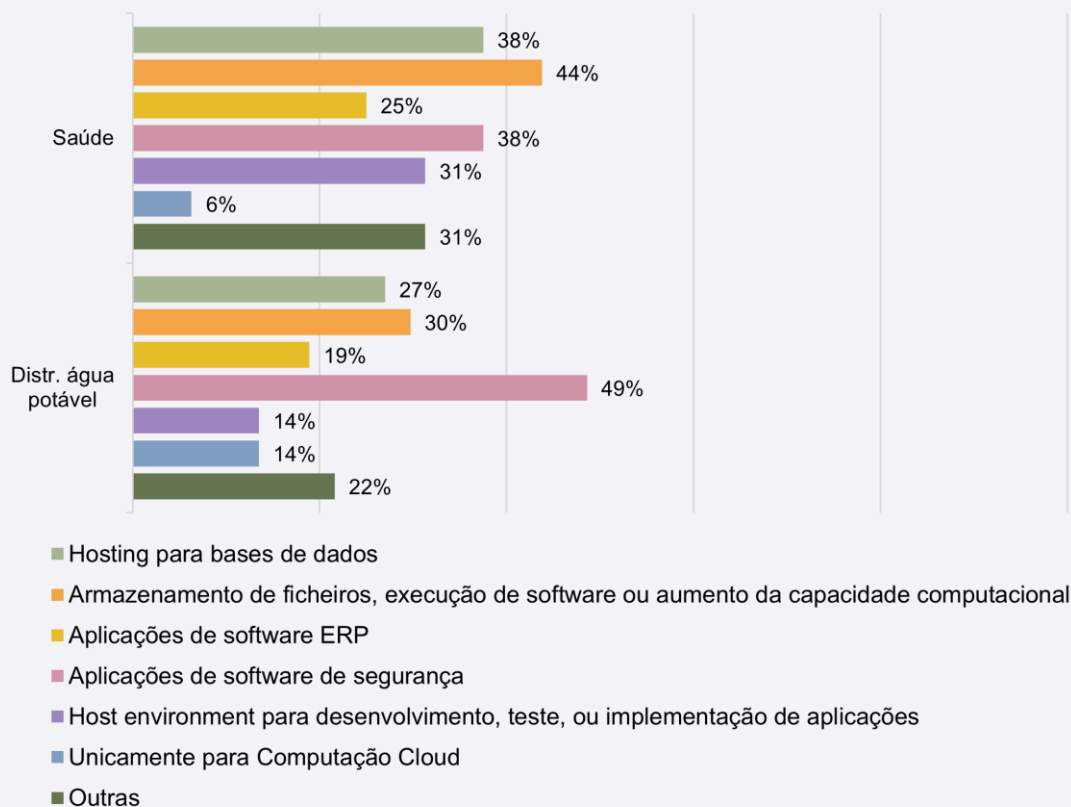
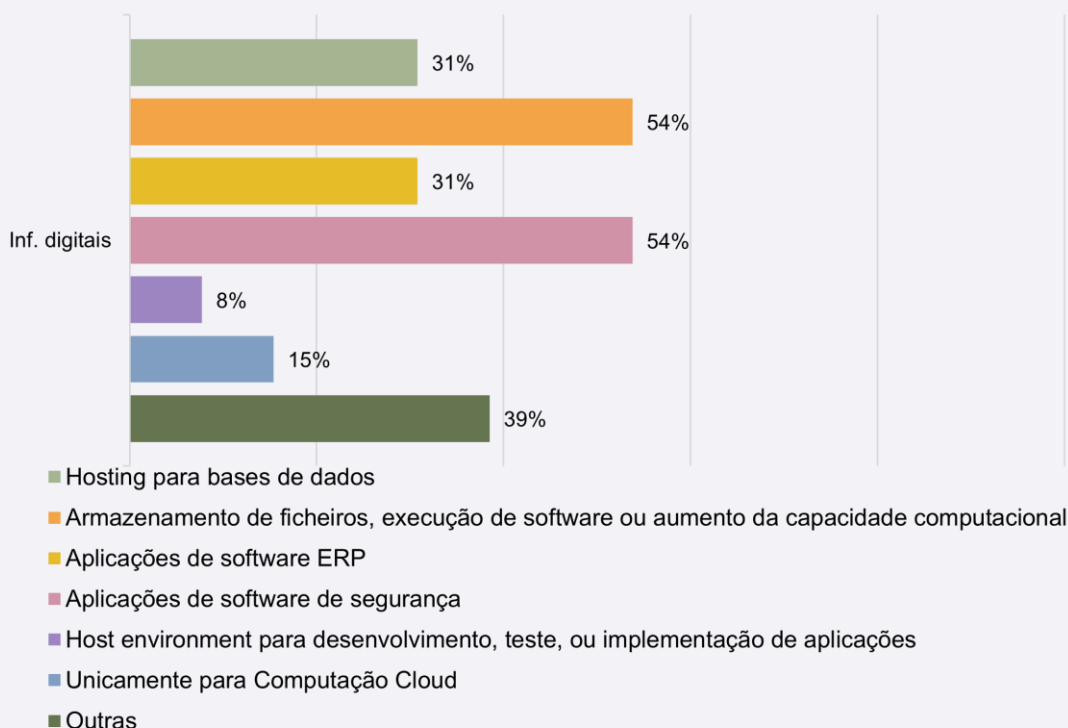


Gráfico 57.4 - Finalidades dos serviços de Computação Cloud adquiridos



As finalidades dos serviços de Computação Cloud são múltiplas, variando entre *hosting* para bases de dados; armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional; aplicações de *software* ERP³⁵ aplicações de *software* de segurança; *host environment* para desenvolvimento, teste ou implementação de aplicações; e, por fim, exclusivamente para Computação Cloud.

De forma geral, é mais comum os operadores terem como finalidade *hosting* para bases de dados, armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional e aplicações de *software* de segurança.

No setor bancário, uma das aplicações com grande destaque é a utilização de Computação Cloud para *host environment* para desenvolvimento, para além do *hosting* para base de dados e do armazenamento de ficheiros.

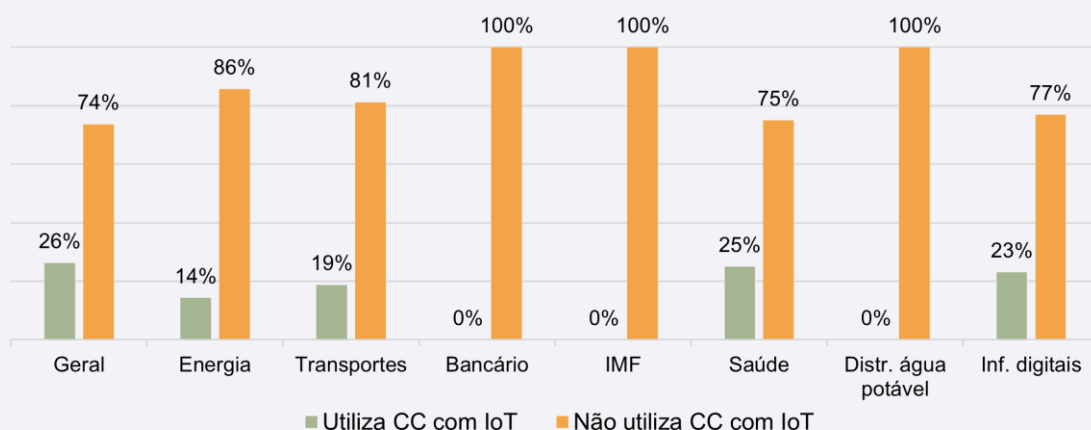
No setor das infraestruturas do mercado financeiro destacou-se a opção “Outras”, que no caso deste setor contempla a utilização de Computação Cloud para suportar sistemas de e-mail e servidores DNS.

³⁵ ERP (Enterprise Resource Planning) refere-se a um tipo de *software* que as organizações utilizam para gerir os seus recursos e atividades do dia-a-dia, passando pela gestão de projetos, de recursos humanos e logística, entre outras áreas fundamentais para o funcionamento de uma organização. Uma solução ERP completa permitirá também planejar, orçamentar e prever questões do foro financeiro de uma organização.

A nível setorial, torna-se evidente que o armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional é uma das finalidades mais comuns nos setores dos transportes, da banca e das infraestruturas do mercado financeiro, tendo sido indicada por pelo menos 88% dos OSE destes setores. A utilização de serviços *cloud* para a utilização de *software* ou de aplicações de segurança é também uma das finalidades mais recorrentes entre estes setores, tendo sido indicada por pelo menos 71% dos OSE dos mesmos. Já nos setores da saúde, distribuição de água potável e infraestruturas digitais, menos finalidades foram indicadas por uma maioria significativa dos OSE. Nesses setores, as duas finalidades indicadas (armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional e utilização de *software* ou de aplicações de segurança) apenas no setor das infraestruturas digitais foram indicadas por mais de 50% dos inquiridos (54%). As restantes finalidades foram indicadas nestes setores por cerca de 30% ou menos dos OSE inquiridos.

Comparando com dados do IUTICE de 2023, os serviços de *cloud computing* foram adquiridos pelas empresas em Portugal tendo em vista o funcionamento do serviço de correio eletrónico (91,1%), o armazenamento de ficheiros (73,7%), o funcionamento de *software* de aplicações de segurança (67,2%) e *software* de escritório (66,1%)³⁶.

Gráfico 58 - Utilização de serviços de CC em conjunto com *Internet of Things* (IoT)



De modo geral, não é frequente, entre os OSE, a utilização de serviços de Computação Cloud (CC) em conjunto com a *Internet of Things* (IoT), embora alguns operadores o façam (26%). Especificamente, nos setores bancário, das infraestruturas do mercado financeiro e do fornecimento e distribuição de água potável, nenhum operador utiliza CC com IoT.

Os setores da saúde e das infraestruturas digitais são os setores em estudo onde os operadores mais utilizam os serviços CC em conjunto com *Internet of Things*, ambos ultrapassando os 20% de utilização. Os setores da energia e dos transportes ficam aquém desse limiar de 20%.

³⁶ INE, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 59 - Percentagem de sistemas core em *cloud*

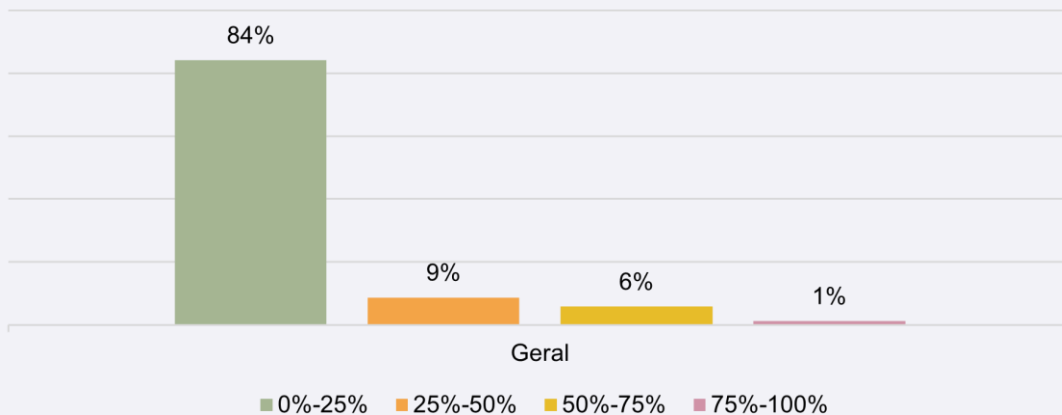


Gráfico 59.1 - Percentagem de sistemas core em *cloud*

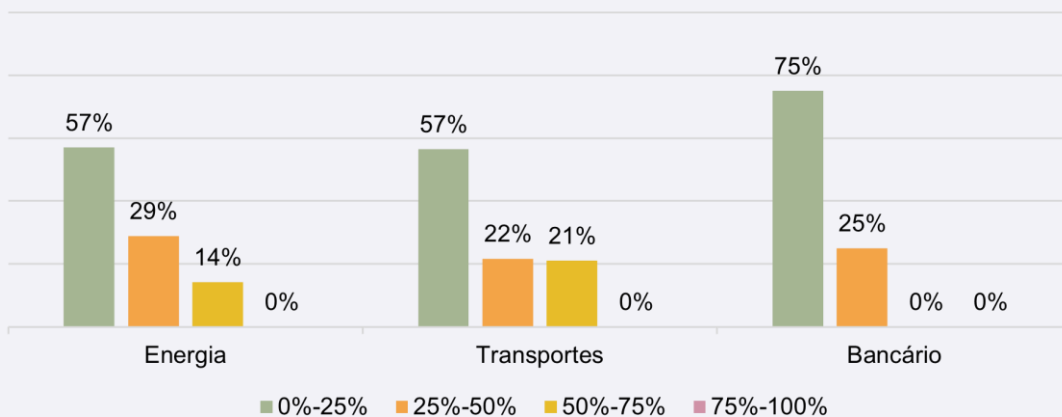
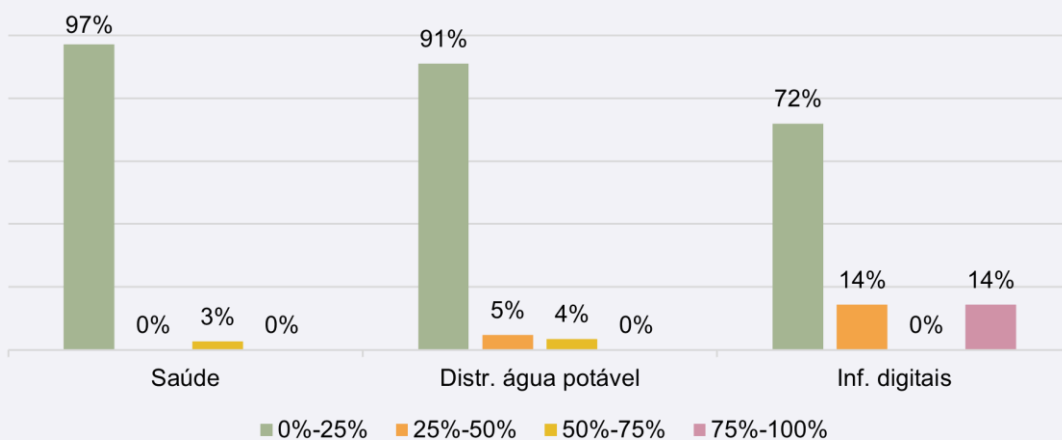


Gráfico 59.2 - Percentagem de sistemas core em *cloud*



Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos.

Há, no entanto, exceções. Por exemplo, nos setores da energia, dos transportes, e da saúde, registam-se OSE cuja percentagem de sistemas *core* em *cloud* se encontra no intervalo de 50%-75% e, no setor das infraestruturas digitais, foi possível identificar operadores onde essa percentagem está já no último intervalo, de 75%-100%. No setor das infraestruturas do mercado financeiro, foi encontrado um erro nos dados obtidos, pelo que os mesmos tiveram de ser invalidados.

Gráfico 60 - Percentagem de sistemas core on-prem

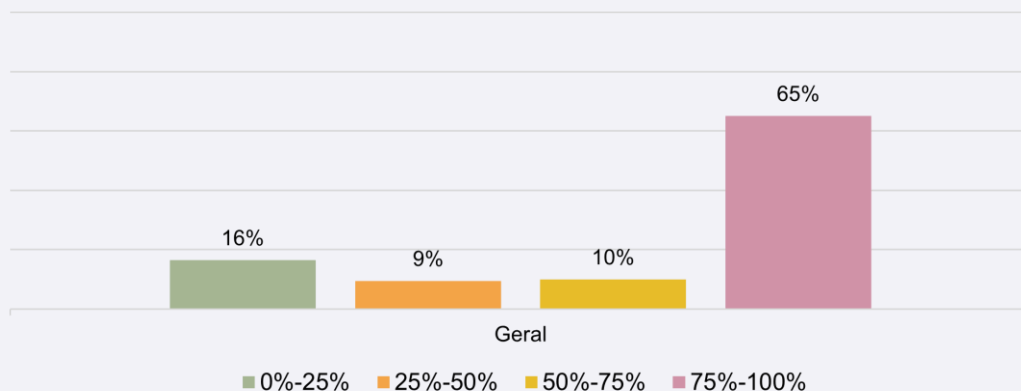


Gráfico 60.1 - Percentagem de sistemas core on-prem

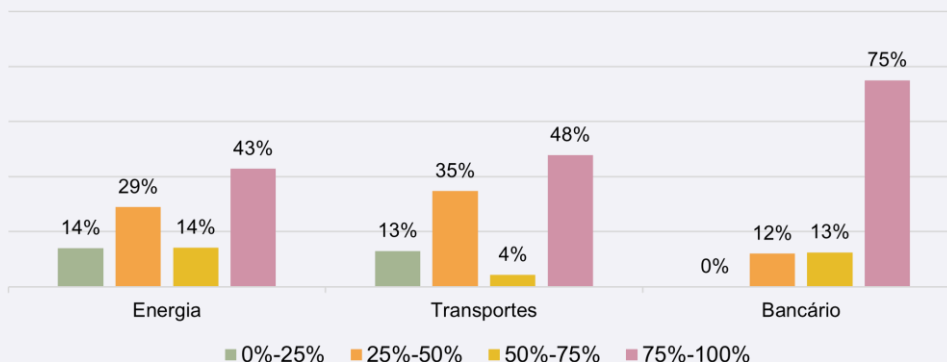
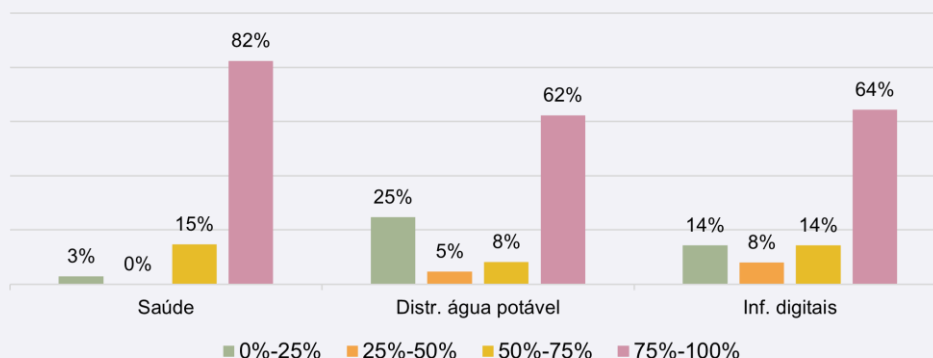
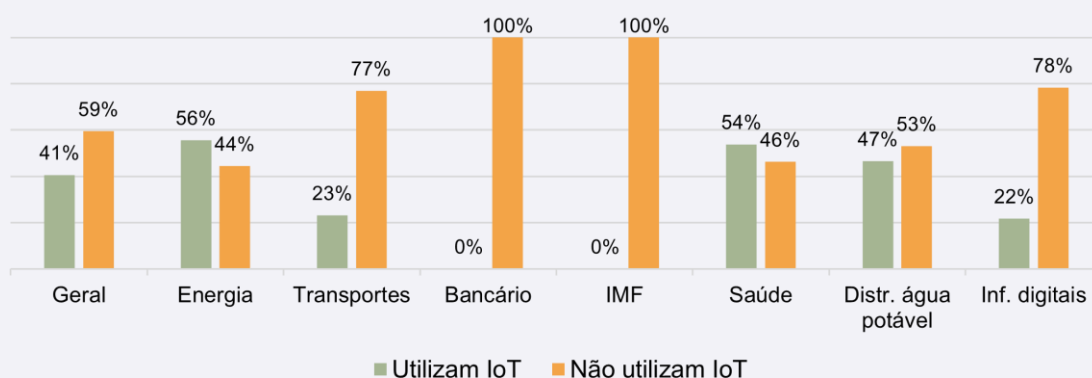


Gráfico 60.2 - Percentagem de sistemas core on-prem



Contrastando com o gráfico anterior, aqui se mostra a tendência dos operadores em manter os seus sistemas core no próprio ambiente da organização (on-prem) e não na cloud. De um modo geral, cerca de 60% dos operadores inquiridos referem que mantêm entre 75% a 100% de sistemas principais dentro do ambiente de TI da sua organização. No setor das infraestruturas do mercado financeiro, foi encontrado um erro nos dados obtidos, pelo que os mesmos tiveram de ser invalidados. Nas infraestruturas digitais a maioria dos operadores tem entre 0 a 25% de sistemas principais. Nos restantes setores, prevalece a faixa de 75 a 100%. Nos setores de energia e transportes, as percentagens são bastante distribuídas, apresentando pouca diferença percentual entre as diferentes faixas.

Gráfico 61 - Utilização de IoT pelos OSE



A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT. Destacam-se os setores bancário e das IMF, onde a totalidade dos inquiridos respondeu não utilizar de todo IoT.

Em contraste, nos setores de energia e saúde, são mais os operadores que utilizam IoT do que aqueles que não utilizam, embora essa seja uma maioria ligeira, pouco acima dos 50%. No caso do fornecimento e distribuição de água potável, as diferenças percentuais são também ténues, mas são mais os operadores que não utilizam IoT. Nos restantes setores, infraestruturas digitais e transportes, prevalece a não utilização de IoT.

De acordo com dados da ANACOM, no mercado empresarial, em 2021, aproximadamente 23% das empresas portuguesas com dez ou mais funcionários utilizaram dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente pela Internet, um aumento de 10 pontos percentuais em relação ao ano anterior. Portugal estava 6 p.p. abaixo da média da UE27, tendo ainda assim subido do 19.º para o 16.º lugar neste *ranking*. A utilização desses dispositivos tende a ser maior à medida que aumenta o tamanho da empresa, estando acima da média nas médias empresas (35%) e nas grandes empresas (46%). A estrutura do tecido produtivo português pode, portanto, explicar uma utilização relativamente menor dessas tecnologias em comparação com outros países. Por setor de atividade, a utilização de dispositivos interconectados monitorizados ou controlados remotamente pela Internet nos setores da eletricidade e da água foi de 41%³⁷.

³⁷ ANACOM, "Utilização da Internet das Coisas (IoT - Internet of Things)", 2022, pp. 5 e 16-20, https://www.anacom.pt/streaming/relatorioInternet_dasCoisas_IoT2022.pdf?contentId=1737940&field=ATTACHED_FILE.

Gráfico 62 - Contextos de utilização de IoT

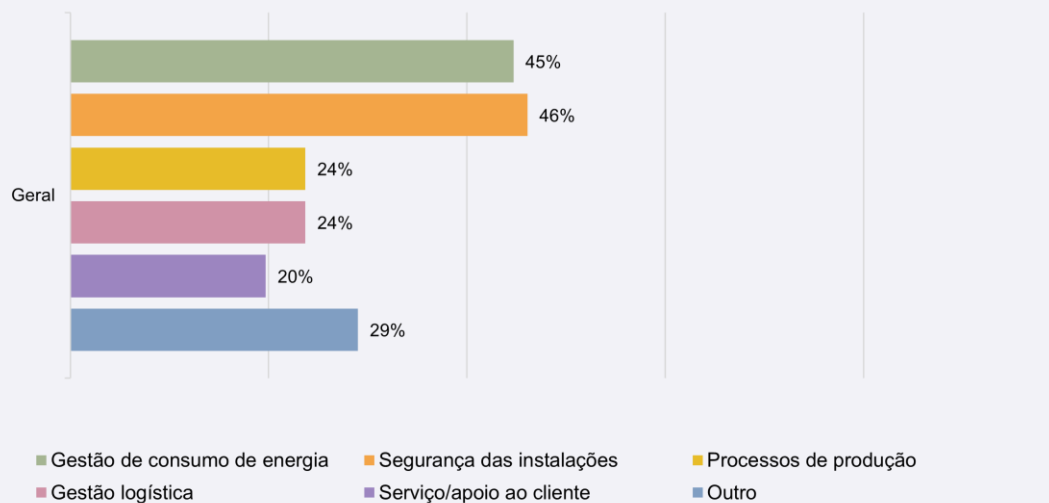


Gráfico 62. 1 - Contextos de utilização de IoT

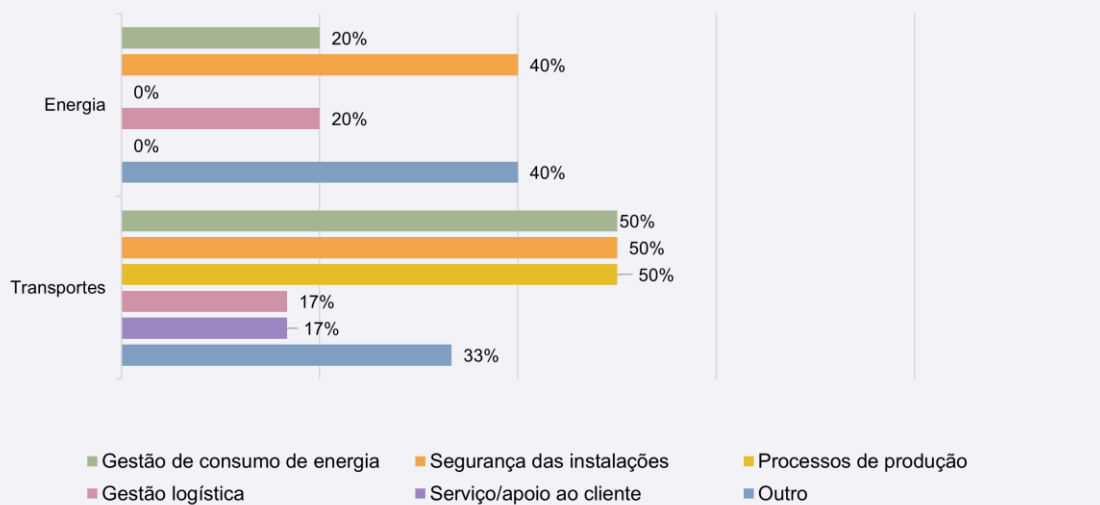
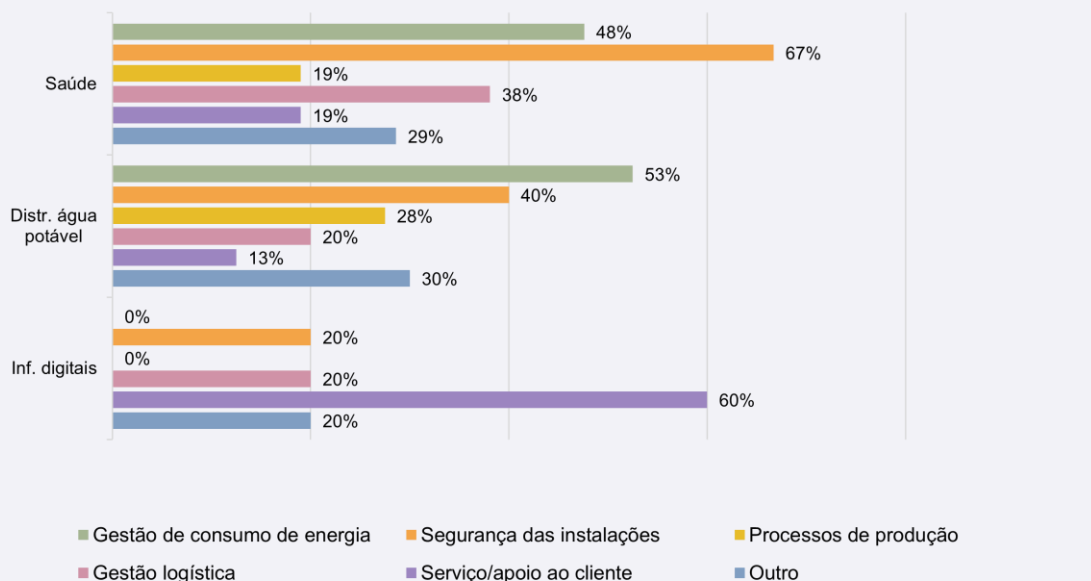


Gráfico 62.2 - Contextos de utilização de IoT



Dado que os setores bancário e infraestruturas do mercado financeiro não possuem operadores que utilizem IoT, não há dados relativos aos contextos da sua utilização nestes setores. De maneira geral, a utilização de IoT é mais comum nos contextos de gestão do consumo de energia e de segurança das instalações, respondido por cerca de 45% dos inquiridos, ao contrário da utilização de IoT para serviço/apoio ao cliente, que tem menos expressividade, cerca de 20%. Contudo, no setor da energia, o uso de IoT para a segurança das instalações. Neste setor, a opção “Outro” contempla a utilização de IoT para fins de manutenção preditiva e de telemetria. No setor dos transportes, o mesmo número de operadores (50%) indicou utilizar IoT para a gestão do consumo de energia, para a segurança das instalações e para processos de produção. No setor da saúde, a utilização de IoT é mais frequente no contexto de segurança das instalações. No fornecimento e distribuição de água potável, destaca-se a gestão de consumo de energia, e nas infraestruturas digitais, em contraste com todos os outros setores, o âmbito principal é o serviço/apoio ao cliente.

O mesmo estudo da ANACOM mencionado no gráfico anterior indica que “os equipamentos IoT foram sobretudo utilizados para segurança das instalações (86%), gestão do consumo de energia (32%), gestão logística (21%), processos de produção (19%), monitorização das necessidades de manutenção (18%) e serviço ao cliente (13%)”³⁸.

³⁸ ANACOM, “Utilização da Internet das Coisas (IoT - *Internet of Things*)”, 2022, 17.

Gráfico 63 - Motivos pelos quais não utilizam IoT

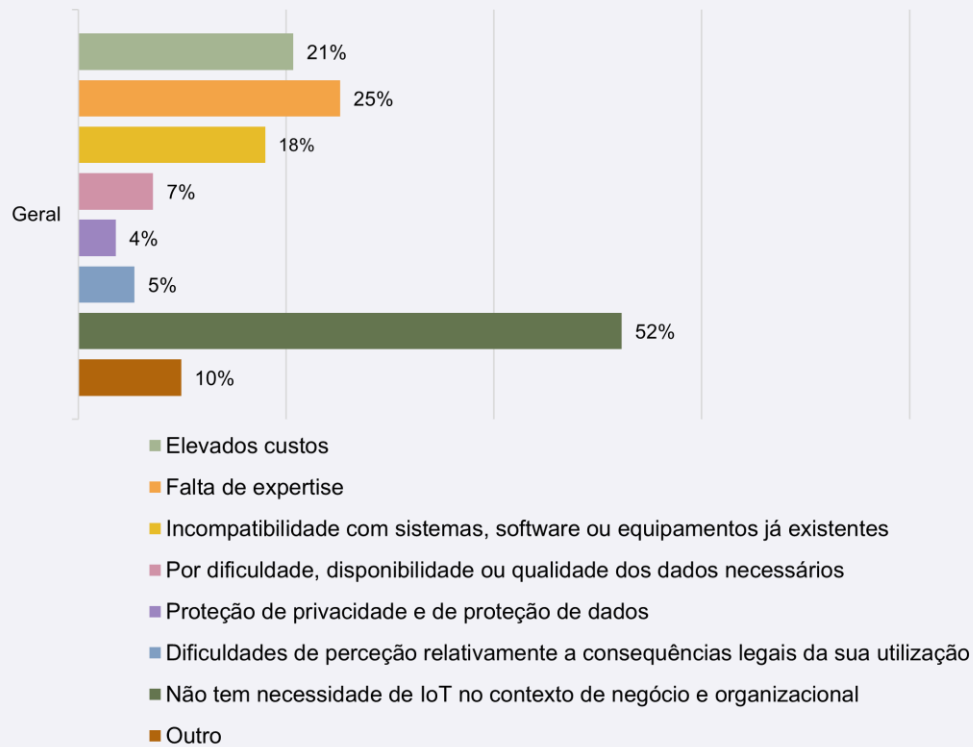


Gráfico 63.1 - Motivos pelos quais não utilizam IoT

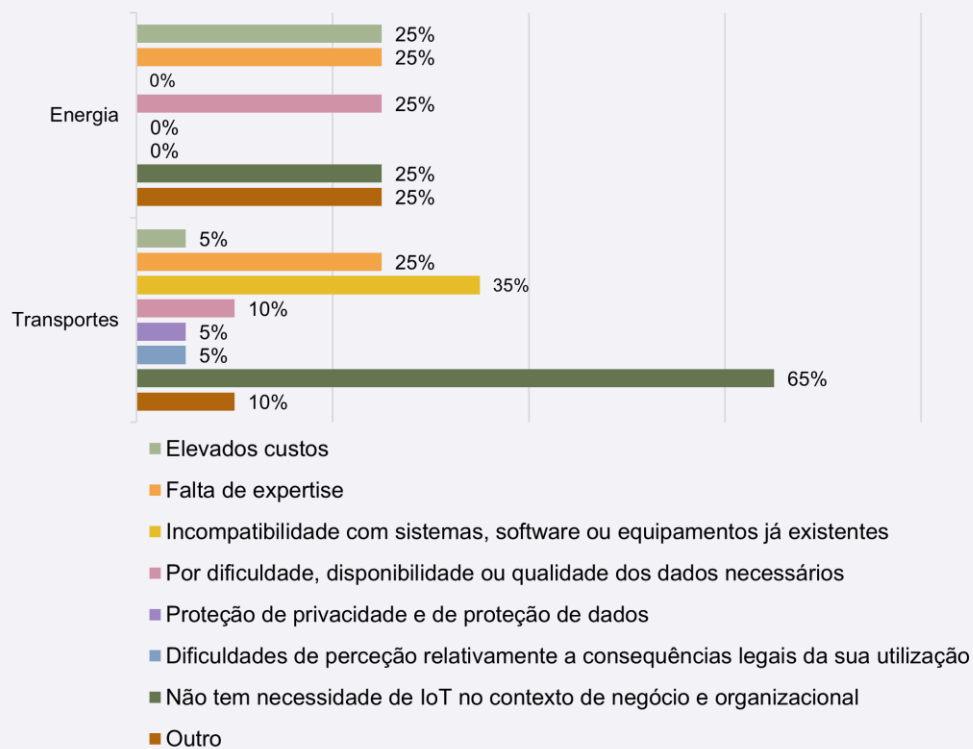


Gráfico 63.2 - Motivos pelos quais não utilizam IoT

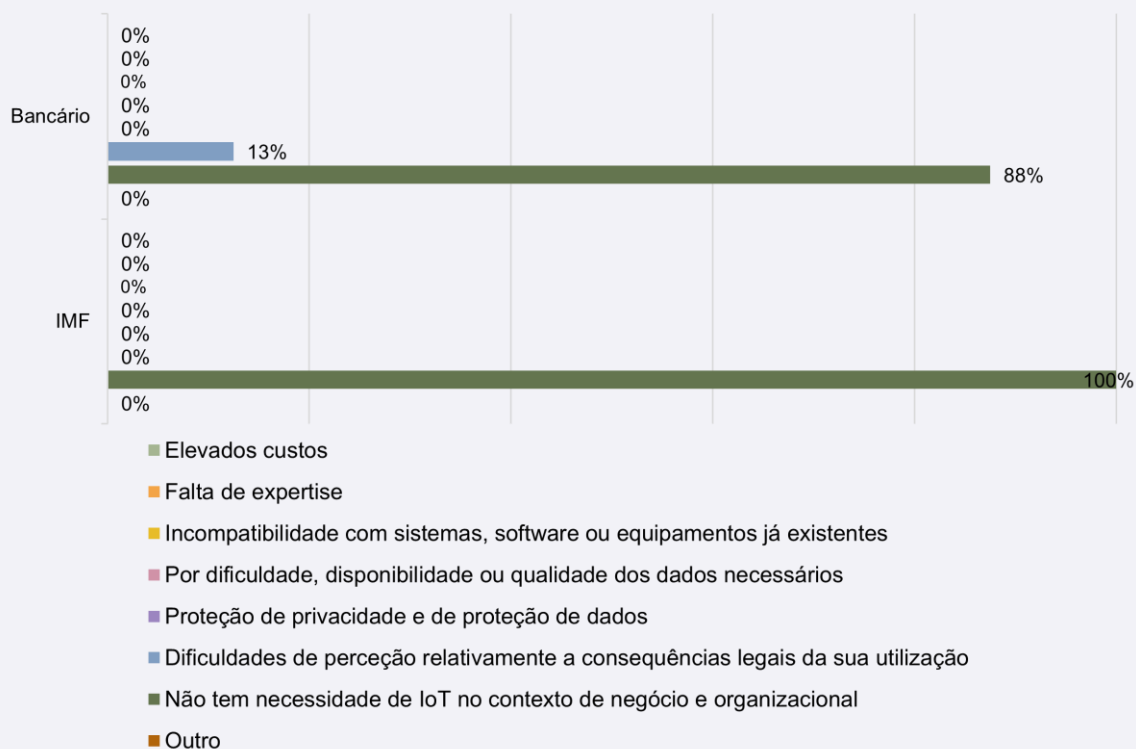


Gráfico 63.3 - Motivos pelos quais não utilizam IoT

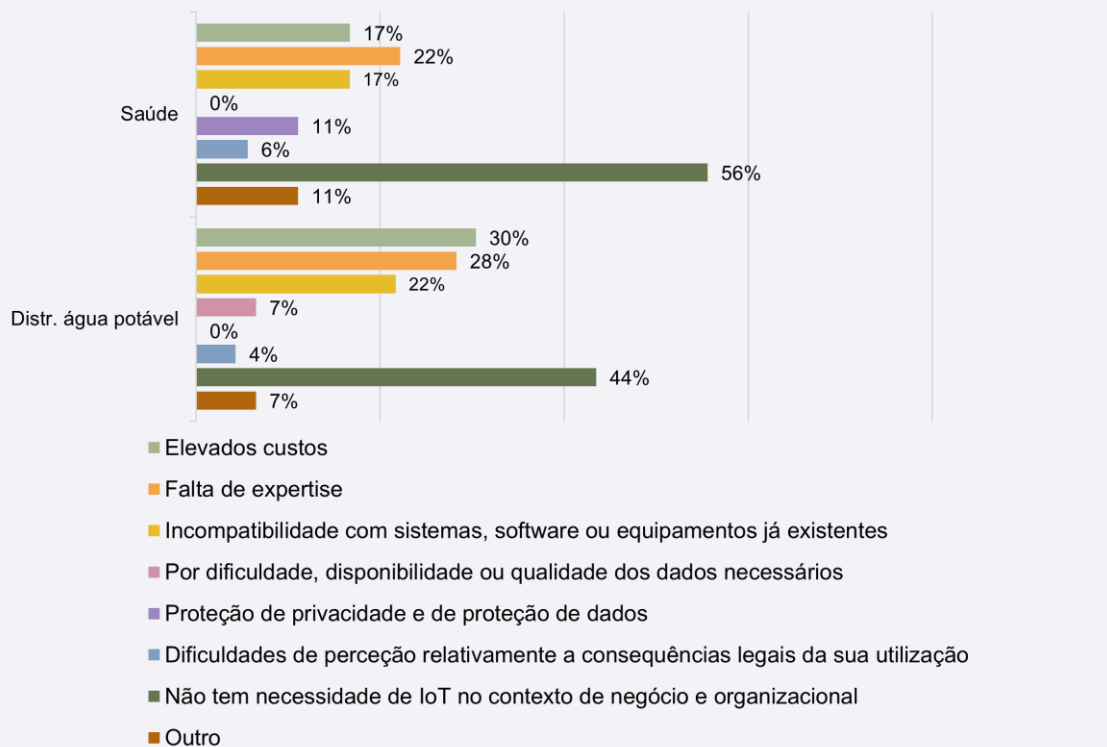
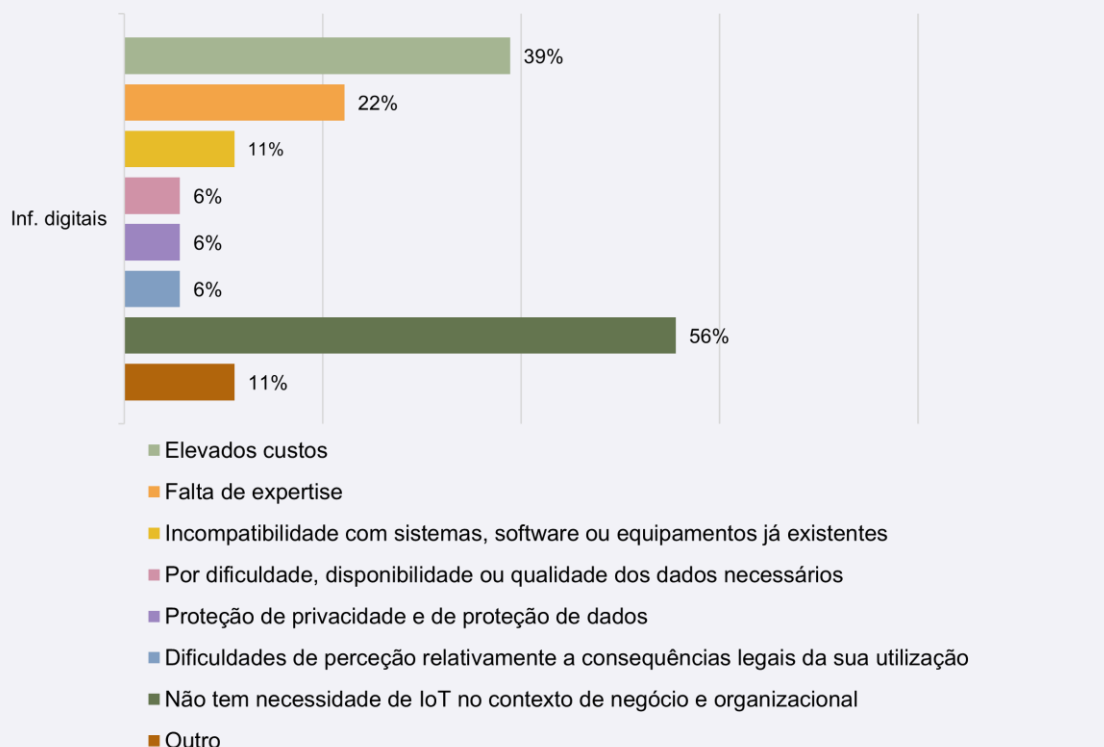


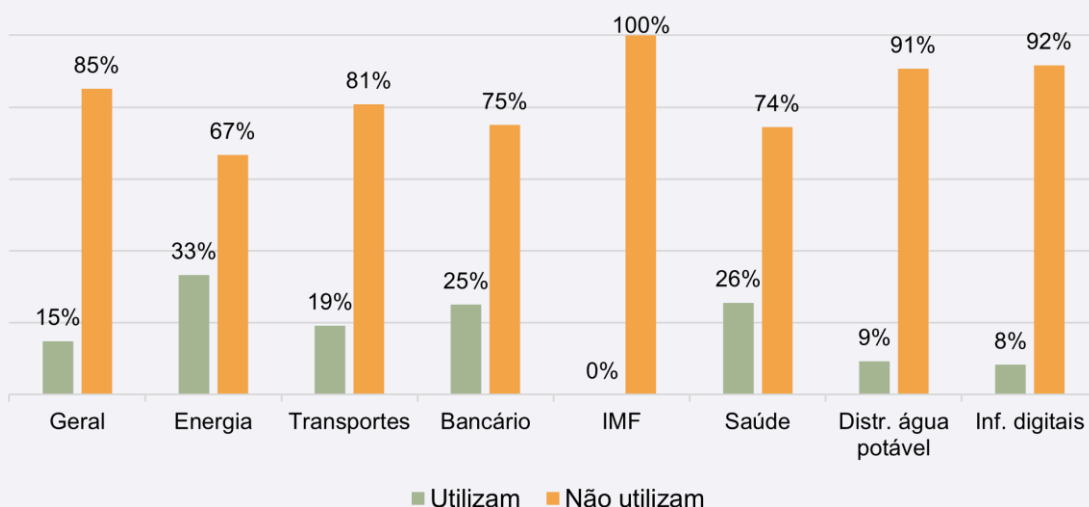
Gráfico 63.4 - Motivos pelos quais não utilizam IoT



São vários os motivos que fazem com que os operadores não utilizem IoT, desde os custos associados à incompatibilidade com sistemas em utilização, passando por vários outros. No entanto, o motivo mais evidente para a não utilização de IoT é não haver necessidade para tal no contexto de negócio ou organizacional (52%). Com exceção do setor da energia, no qual se verifica uma distribuição mais uniforme entre os motivos indicados para a não utilização de IoT, a falta de necessidade de IoT é o motivo mais indicado pelos operadores dos restantes setores. Apenas no setor do fornecimento e distribuição de água potável houve menos de 50% dos operadores a indicarem esse motivo.

Na opção “Outros”, foi sobretudo indicado que se estava a preparar a implementação de IoT na organização para os anos de 2024 e 2025.

Gráfico 64 - OSE que utilizam processos que recorrem a IA



A utilização ou o recurso à IA é ainda reduzido entre os OSE. Apenas 15% dos inquiridos referem já utilizar ou recorrer a IA dentro das suas organizações.

Por norma, há pouca utilização de processos com recurso a Inteligência Artificial (IA) por parte dos operadores. Tal é verificável em todos os setores. Contudo, é de salientar os setores da energia, bancário e da saúde, nos quais já se registam mais de 25% dos operadores a recorrer a Inteligência Artificial. No caso da energia, a quantidade de operadores a utilizar IA já ultrapassa os 30%. Apenas no setor das infraestruturas do mercado financeiro não se registaram operadores a recorrer a Inteligência Artificial.

Comparando com dados do IUTICE de 2023, conclui-se que no universo dos Operadores de Serviços Essenciais há uma maior percentagem de empresas a já recorrer a Inteligência Artificial do que se se olhar para o panorama empresarial geral português. Enquanto 15% dos OSE indicaram já utilizar IA, apenas 7,9% das empresas declararam fazê-lo. Ainda no âmbito do IUTICE, o setor da indústria e energia continua a ser um dos que mais utiliza IA (8,8%), mas fica atrás de outros como o da informação e comunicação (29,8%)³⁹, quando no questionário do CNCS o setor da energia surge como aquele onde mais OSE utilizam Inteligência Artificial (33%). O IUTICE identifica também uma relação entre a dimensão das empresas e a utilização de IA - se separarem as empresas por dimensão (número de colaboradores), é possível constatar que são sobretudo as grandes empresas que já recorrem a IA (35,4%), e que essa utilização decresce quando se analisam PMEs: 16,4% das médias empresas utilizam IA e, no caso das pequenas empresas, esta percentagem é de apenas 5,8%⁴⁰.

³⁹ INE, "Inquérito à Utilização das TIC nas Empresas", 2023, 16-17.

⁴⁰ INE, "Inquérito à Utilização das TIC nas Empresas", 2023, 16-17.

Gráfico 65 - Funções para as quais utilizam IA (Geral)

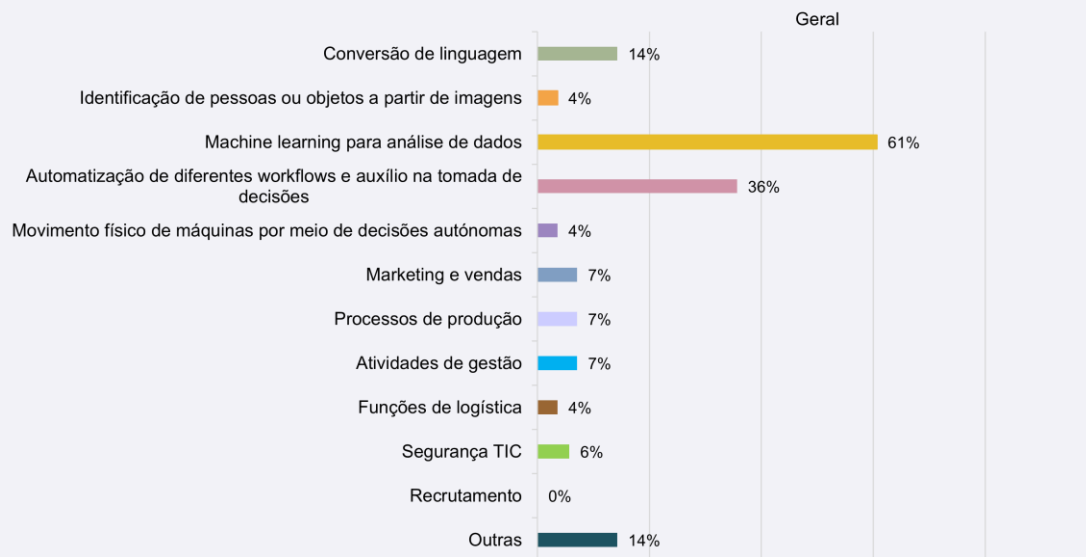


Gráfico 65.1 - Funções para as quais utilizam IA (Energia)

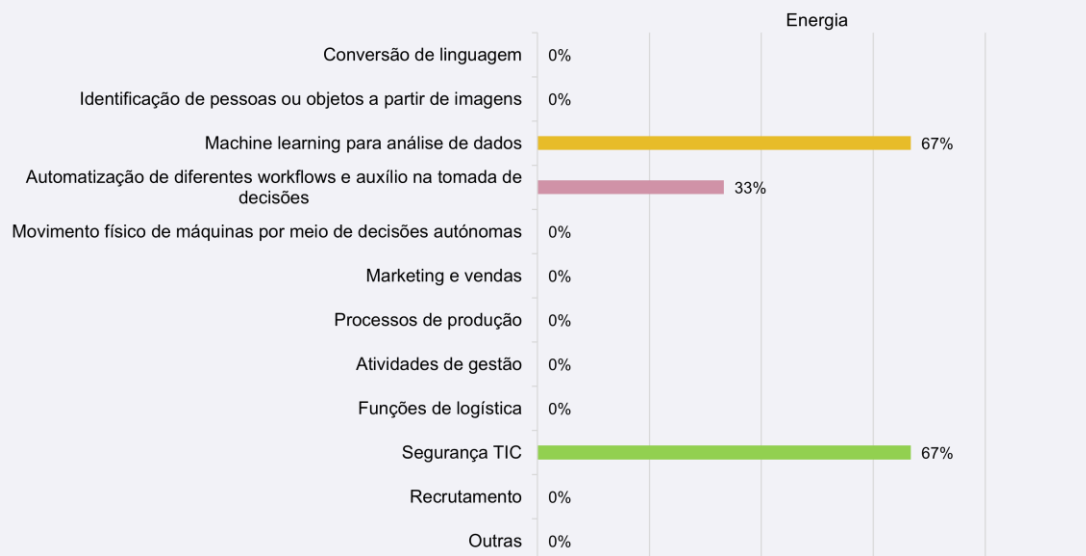


Gráfico 65.2 - Funções para as quais utilizam IA (Transportes)

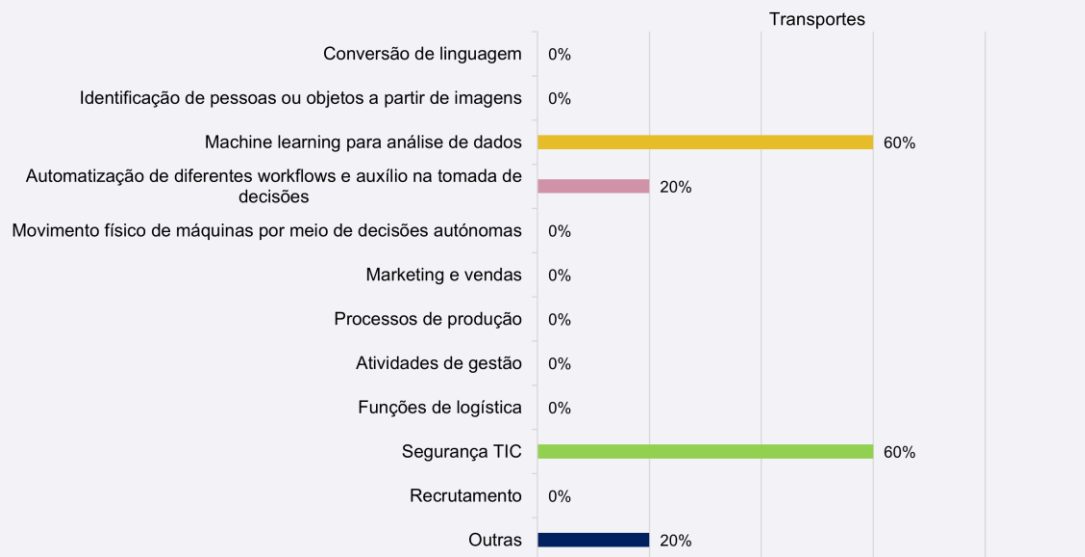


Gráfico 65.3 - Funções para as quais utilizam IA (Bancário)

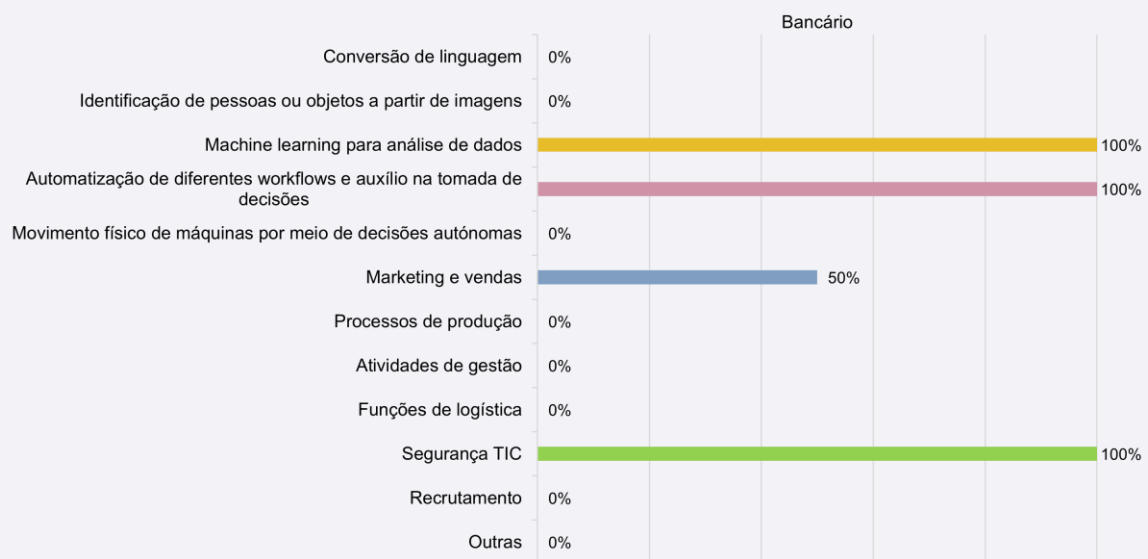


Gráfico 65.4 - Funções para as quais utilizam IA (Saúde)

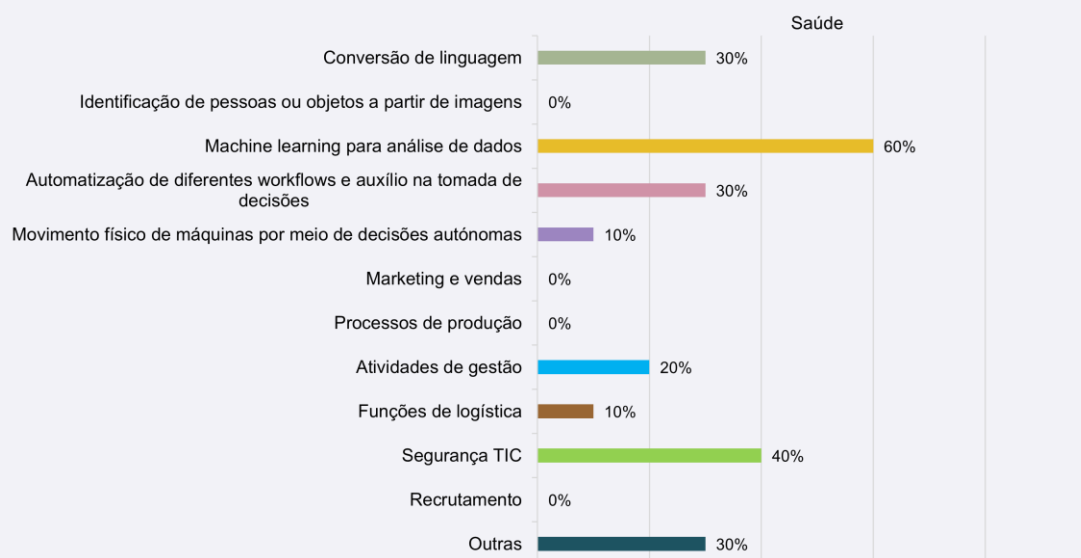


Gráfico 65.5 - Funções para as quais utilizam IA (Distribuição de Água Potável)

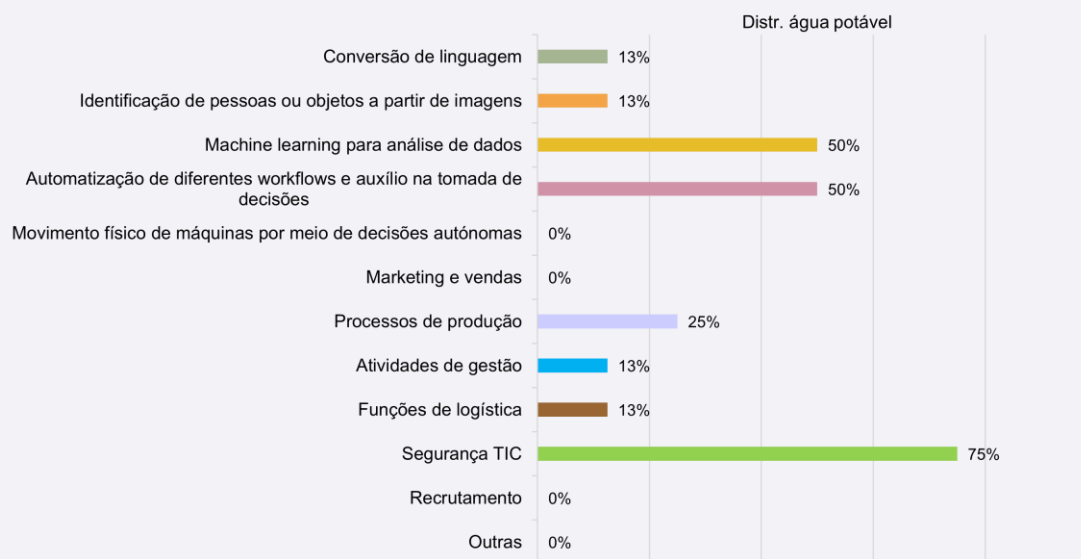
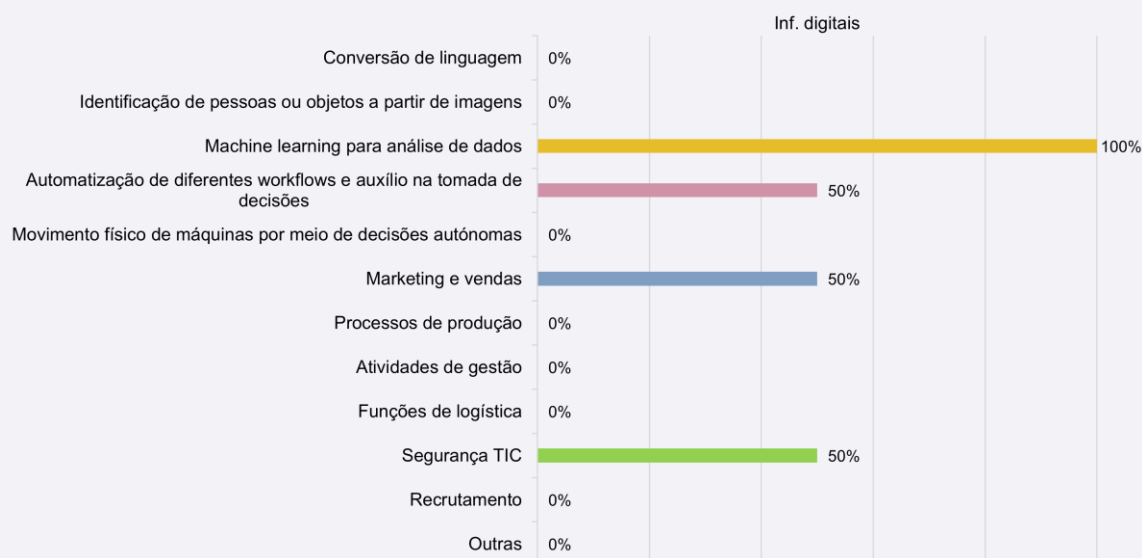


Gráfico 65.6 - Funções para as quais utilizam IA (Infraestruturas Digitais)



Os operadores que já recorrem a Inteligência Artificial utilizam-na para diversas funções. As principais funções incluem: conversão de linguagem, identificação de pessoas ou objetos a partir de imagens, *machine learning* para análise de dados, automatização de fluxos de trabalho e auxílio na tomada de decisões, movimento físico de máquinas por meio de decisões autónomas, marketing e vendas, processos de produção, atividades de gestão e segurança TIC. A utilização de IA para *machine learning* e análise de dados sobressai entre as demais, tendo esta sido indicada por 60% dos operadores que recorrem a Inteligência Artificial. Destaca-se também a utilização de IA para a automatização de fluxos de trabalho e auxílio na tomada de decisões, indicada por 35% dos OSE que fazem uso de IA. As restantes funções surgem de forma mais residual, sendo indicadas por apenas 15% ou menos dos OSE que já recorrem a IA. Curiosamente, não se registou o recurso a Inteligência Artificial em processos de recrutamento entre os OSE inquiridos.

Como os inquiridos do setor das infraestruturas do mercado financeiro afirmam não utilizar IA, esta questão não é aplicável.

De acordo com os dados do IUTICE de 2023, entre as empresas que utilizam tecnologia de IA, 44,7% delas utilizam-na para identificar objetos ou pessoas através de imagens. Em seguida, 40,8% das empresas utilizam tecnologias que automatizam fluxos de trabalho ou auxiliam na tomada de decisão. Tecnologias para análise de linguagem escrita são utilizadas por 35% das empresas, apresentando um ligeiro. Já as tecnologias de aprendizagem automática para análise de dados, incluindo *deep learning*, são adotadas por 26,2% das empresas. A tecnologia de IA menos utilizada pelas empresas é a que permite a movimentação física de máquinas através de decisões autónomas baseadas na observação do meio ambiente, com apenas 8,3% de adoção. No entanto, no setor da Indústria e Energia, essa tecnologia é mais prevalente, sendo utilizada por 15,3% das empresas que empregam IA⁴¹.

⁴¹ INE, "Inquérito à Utilização das TIC nas Empresas", 2023, 17-18.

Segundo o estudo já referido da Microsoft sobre o estado da cibersegurança em Portugal, “embora a IA possa desempenhar um papel absolutamente estratégico na evolução da cibersegurança, a sua integração nos processos de segurança é ainda uma realidade longínqua para a maioria das organizações”⁴². Nesse estudo, 54% dos inquiridos auscultados afirmam não utilizar soluções de segurança com recurso a IA. As organizações que já o fazem – 21% – recorrem a competências de reporte de incidentes de segurança 66%, *cyber intelligence* e a exposição a ameaças 61%, sistemas preditivos de ataque 49% e resposta a incidentes 46%⁴³.

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança



⁴² Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024, 9, https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.

⁴³ Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024, 9.

Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança



Gráfico 66.2 - Medidas de proteção contra ameaças de cibersegurança



Gráfico 66.3 - Medidas de proteção contra ameaças de cibersegurança

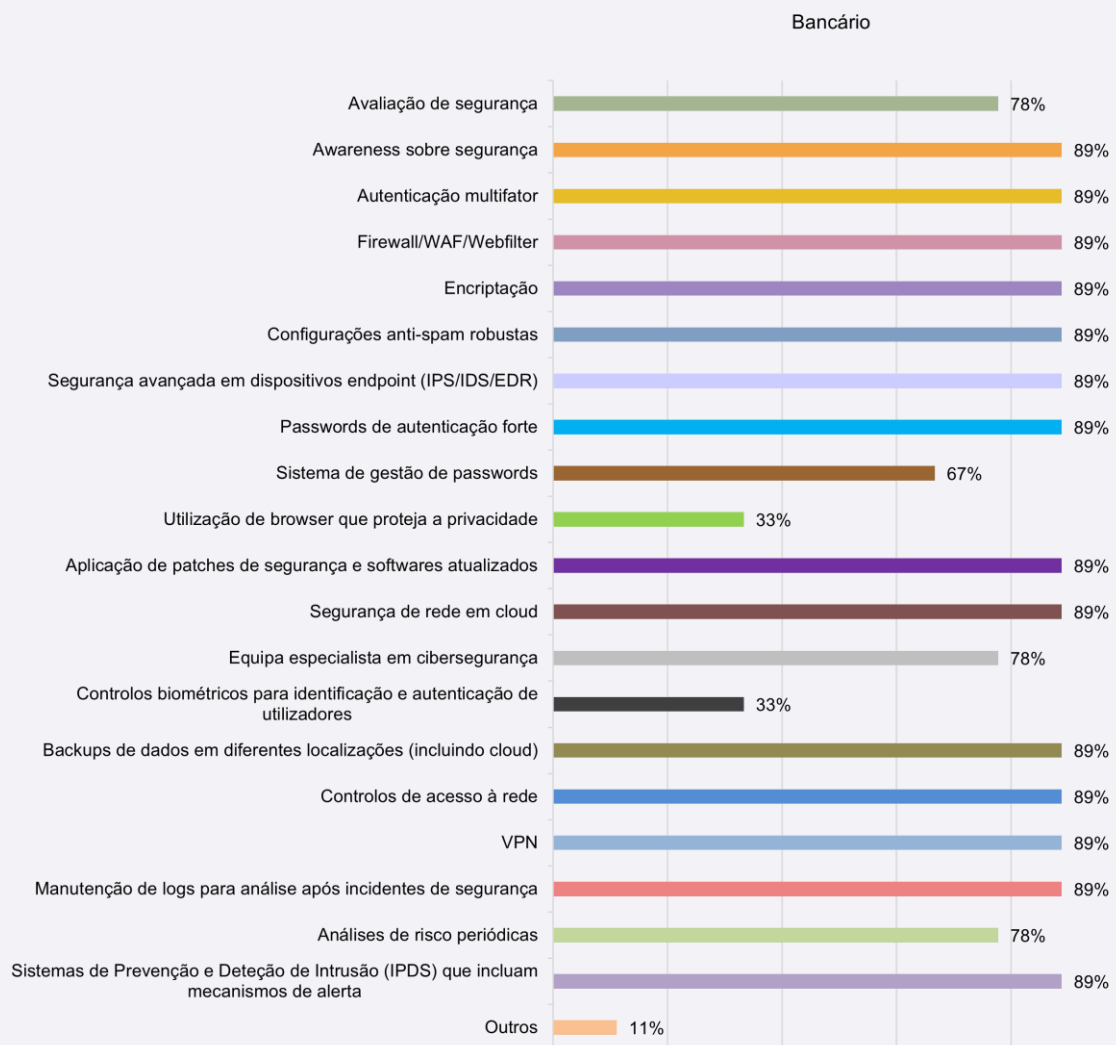


Gráfico 66.4 - Medidas de proteção contra ameaças de cibersegurança

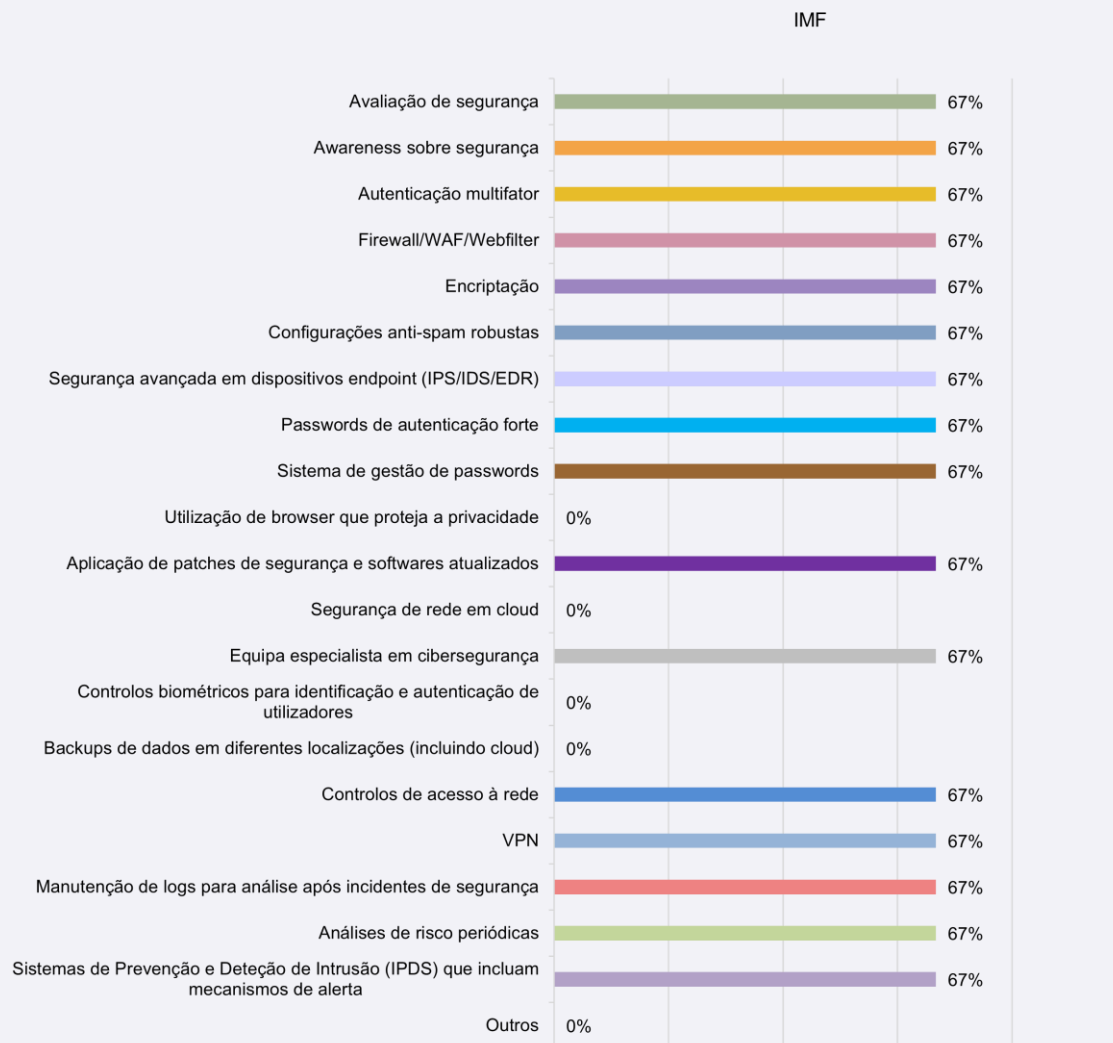


Gráfico 66.5 - Medidas de proteção contra ameaças de cibersegurança

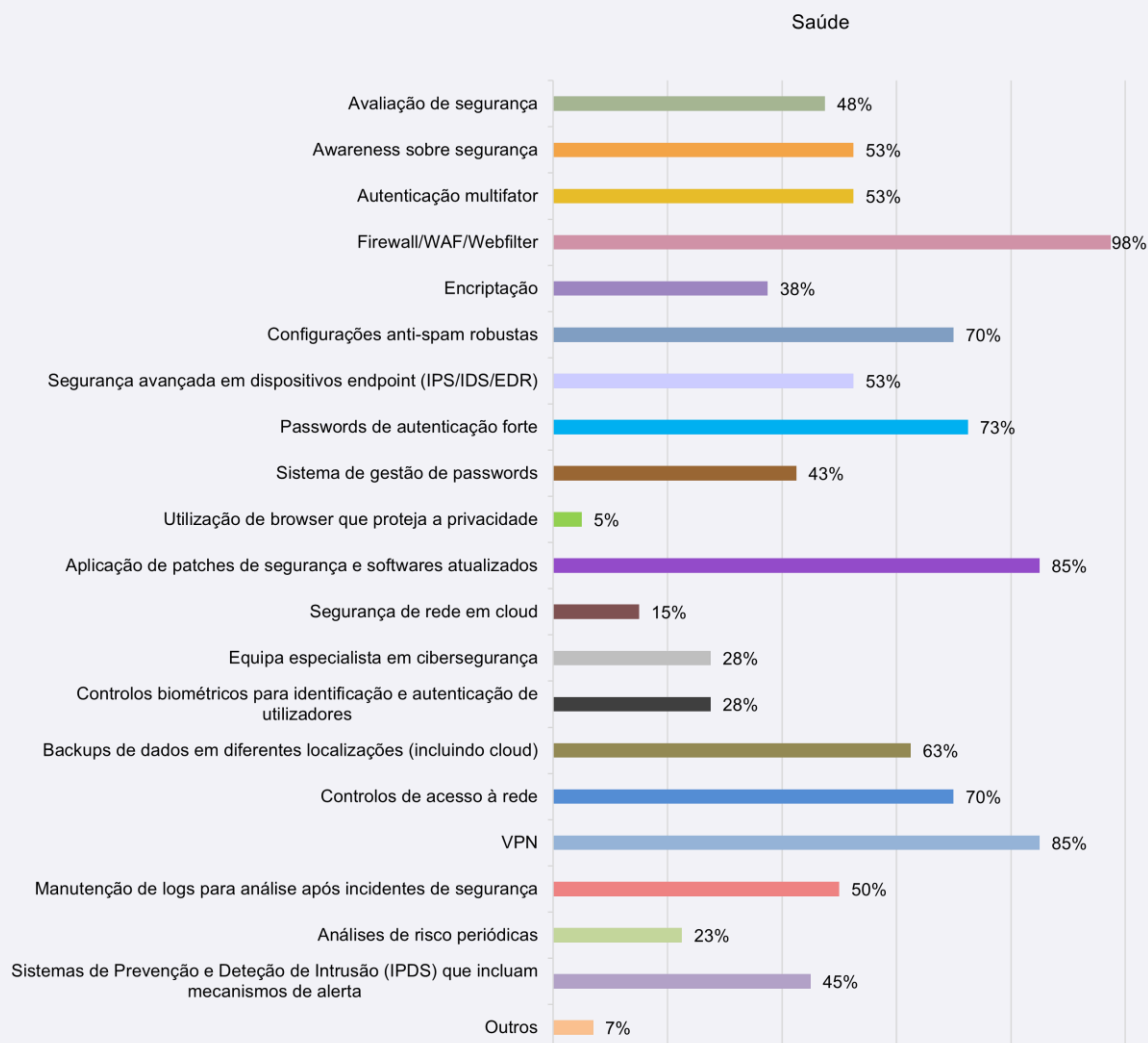


Gráfico 66.6 - Medidas de proteção contra ameaças de cibersegurança

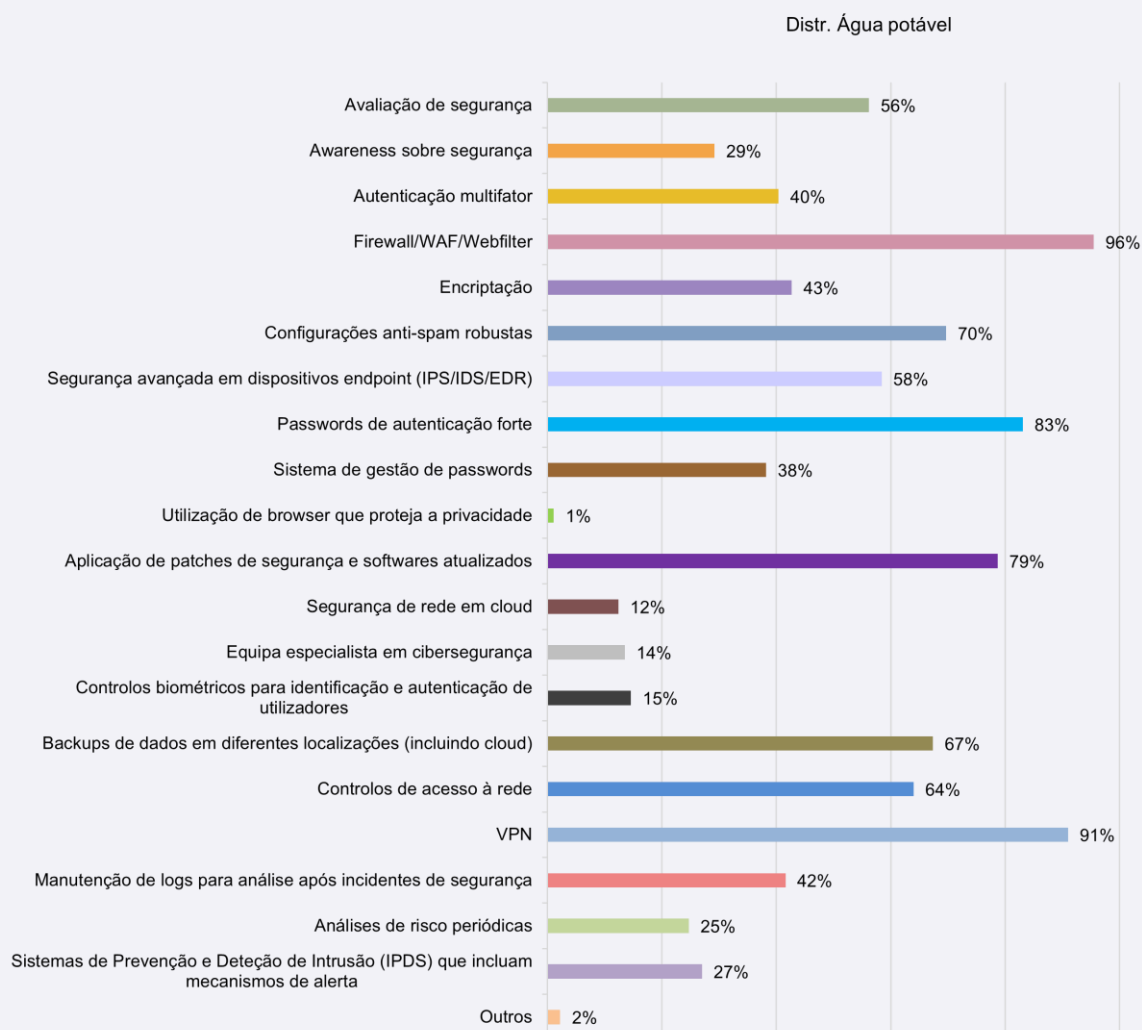


Gráfico 66.7 - Medidas de proteção contra ameaças de cibersegurança



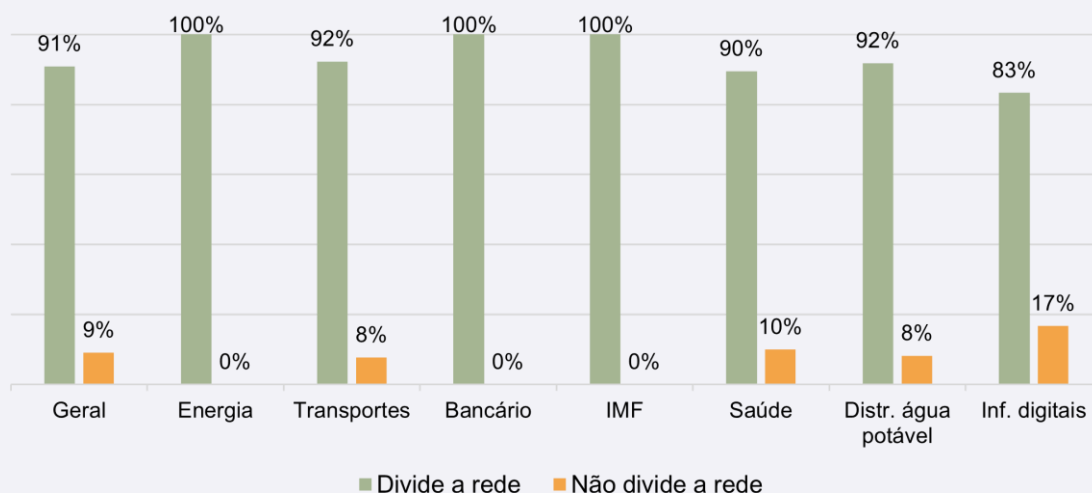
Na análise geral das medidas de segurança utilizadas pelos operadores, é possível verificar que medidas técnicas como a utilização de *Firewall/WAF/Webfilter*, utilização de *VPN*, palavras-passe de autenticação forte, aplicação de *patches* de segurança, a atualização dos softwares e backups de dados em diferentes localizações são das mais utilizadas pelos OSE dos vários setores. Verifica-se, também, que a aplicação de medidas como autenticação multifator, criptografia, ou de manutenção de *logs* para análise pós-incidente é feita por menos de 50% dos operadores inquiridos. Por outro lado, medidas como a realização de sessões de sensibilização para a cibersegurança junto dos colaboradores ou de análises de risco periódicas são também pouco utilizadas, estando aplicadas por menos de 40% e por menos de 30% dos OSE inquiridos, respetivamente. Há que destacar, no entanto, a vasta utilização das medidas de segurança mencionadas no setor bancário, com quase 90% dos operadores a fazer uso da maioria das medidas indicadas. As medidas de proteção segurança de rede em *cloud*, ter uma equipa de especialistas em cibersegurança e controlos biométricos para identificação e autenticação de

utilizadores são medidas menos utilizadas pelos operadores, com menos de 25% destes a implementá-las.

Segundo o IUTICE de 2022, no que respeita às principais medidas de segurança das TIC utilizadas em 2021, 84,0% das empresas procedem à autenticação através de uma palavra-passe segura, 73,7% utiliza o *backup* de informação em local distinto (incluindo *backup* para a *cloud*), 62,5% efetua o controlo de acesso à rede (gestão dos direitos dos utilizadores na rede da empresa) e 53,8% conserva ficheiros de registo (histórico) que permitem a análise após incidentes de segurança das TIC. As restantes medidas de segurança utilizadas registam percentagens inferiores a 50%, sendo a autenticação através de métodos biométricos para aceder aos sistemas TIC da empresa a medida menos utilizada, com 12,3%⁴⁴.

Consta do estudo da Microsoft sobre o estado da cibersegurança em Portugal, que há um esforço já concretizado pelas organizações a nível nacional que importa destacar: 50% investiu mais em cibersegurança nos últimos anos, nomeadamente com a implementação de: antivírus e *malware* (81%), medidas de autenticação fortes para o acesso a sistemas críticos (71%), *firewalls* (61%), autenticação multifator (37%) e criptografia de dados, para proteger os ativos da empresa (36%)⁴⁵.

Gráfico 67 - Divisão entre rede dos colaboradores e rede para *guests*

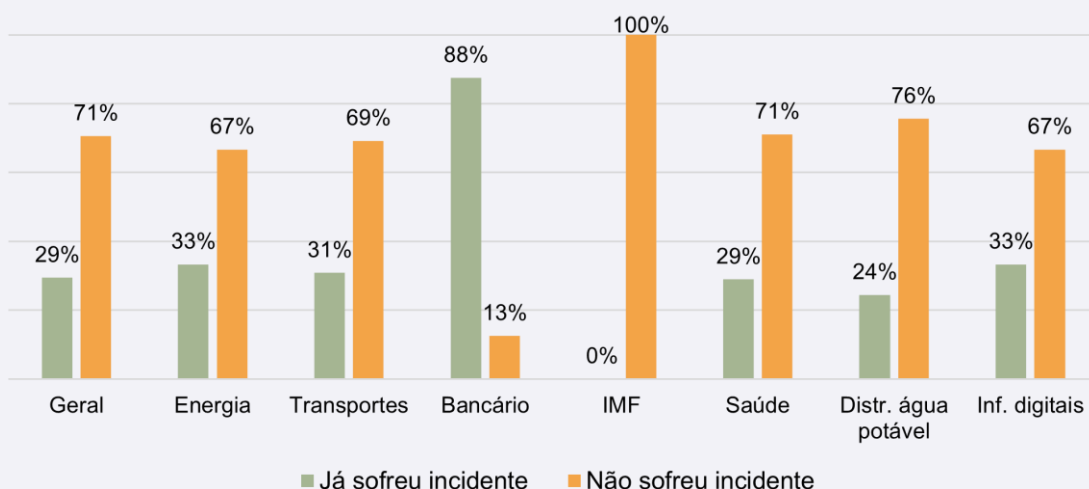


Cerca de 90% dos operadores inquiridos indicaram que distinguem a rede dos colaboradores da rede para estranhos ao serviço (rede *guest*). A quantidade de operadores que não faz essa separação não chega, em qualquer um dos setores, a atingir os 20%. Destacam-se os setores da energia, bancário e infraestruturas do mercado financeiro onde 100% dos operadores referem fazer a divisão da rede.

⁴⁴ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 18.

⁴⁵ Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 7.

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



Em contexto TIC, pelo observado no gráfico, conclui-se que a maioria dos OSE inquiridos (71%) não sofreu incidentes neste contexto. No entanto, no setor bancário, essa tendência inverte-se, tendo sido muitos mais os operadores que referiram já ter sofrido incidentes de segurança do que os que não (88% dos inquiridos do setor já sofreu um incidente). De acordo com os dados obtidos, o setor das infraestruturas do mercado financeiro não sofreu qualquer incidente.

Sendo o IUTICE de 2022, Portugal registou a segunda menor proporção de empresas com incidentes de segurança das TIC na União Europeia (UE). Em 2021, 89,7% das empresas em Portugal, e 91,8% no total da UE, utilizaram pelo menos uma medida para garantir a integridade, a disponibilidade e a confidencialidade dos seus dados e sistemas de Tecnologias de Informação e Comunicação (TIC)⁴⁶.

O Fórum Económico Mundial (FEM) publicou um inquérito em janeiro de 2024, no qual contou com 199 empresas de 49 países. Neste inquérito, cerca de 29% das organizações reportaram que foram afetadas materialmente por um incidente de cibersegurança nos últimos 12 meses. Destas empresas, cerca de 41% afirmaram que o incidente ou incidentes foram causados por terceiros⁴⁷.

⁴⁶ INE, “Inquérito à Utilização das TIC nas Empresas”, 2022, 18.

⁴⁷ World Economic Forum, “Global Cybersecurity Outlook 2024”, janeiro de 2024, 5, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

Gráfico 69 - Tipos de incidentes ocorridos

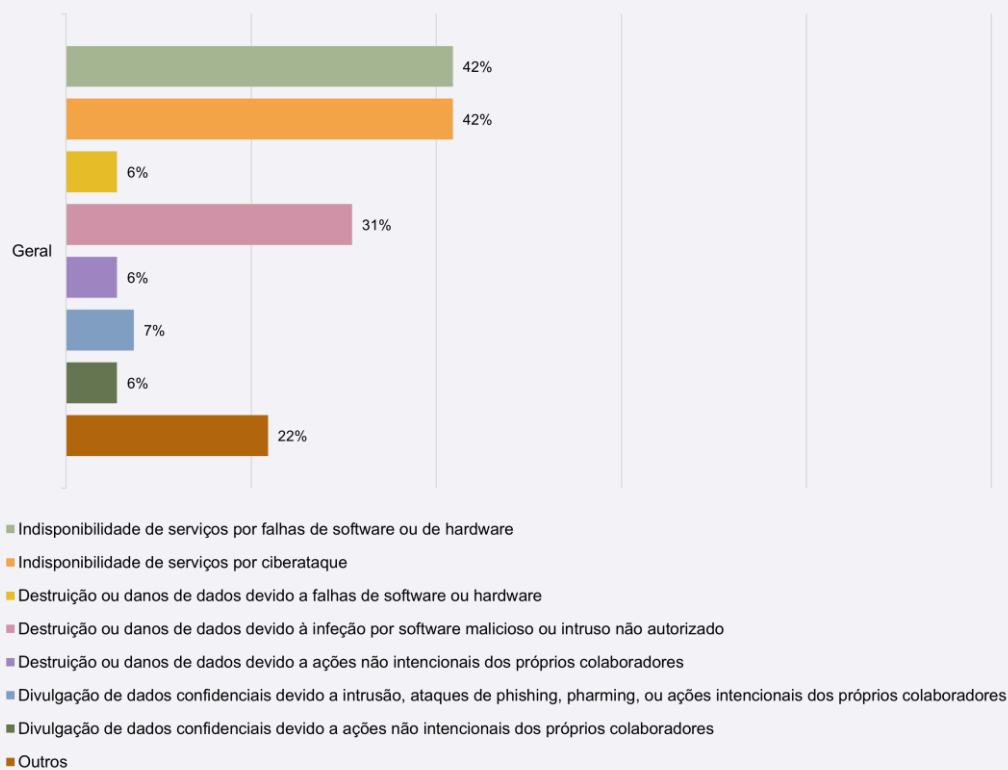


Gráfico 69.1 - Tipos de incidentes ocorridos

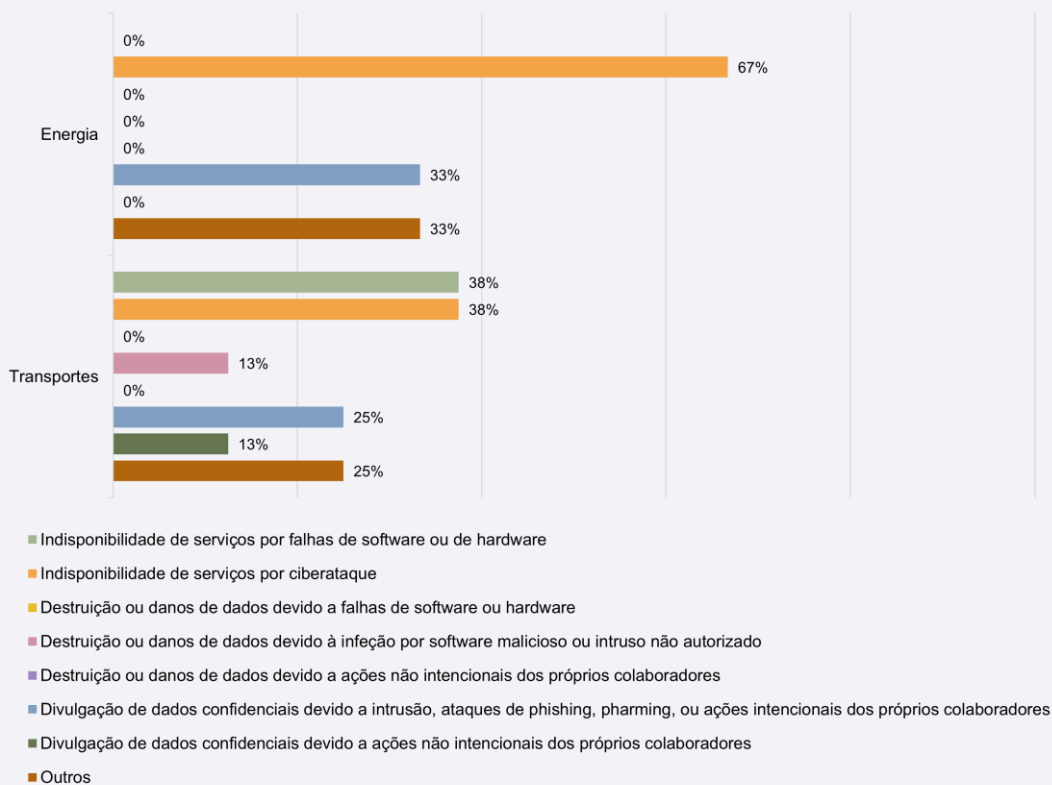


Gráfico 69.2 - Tipos de incidentes ocorridos

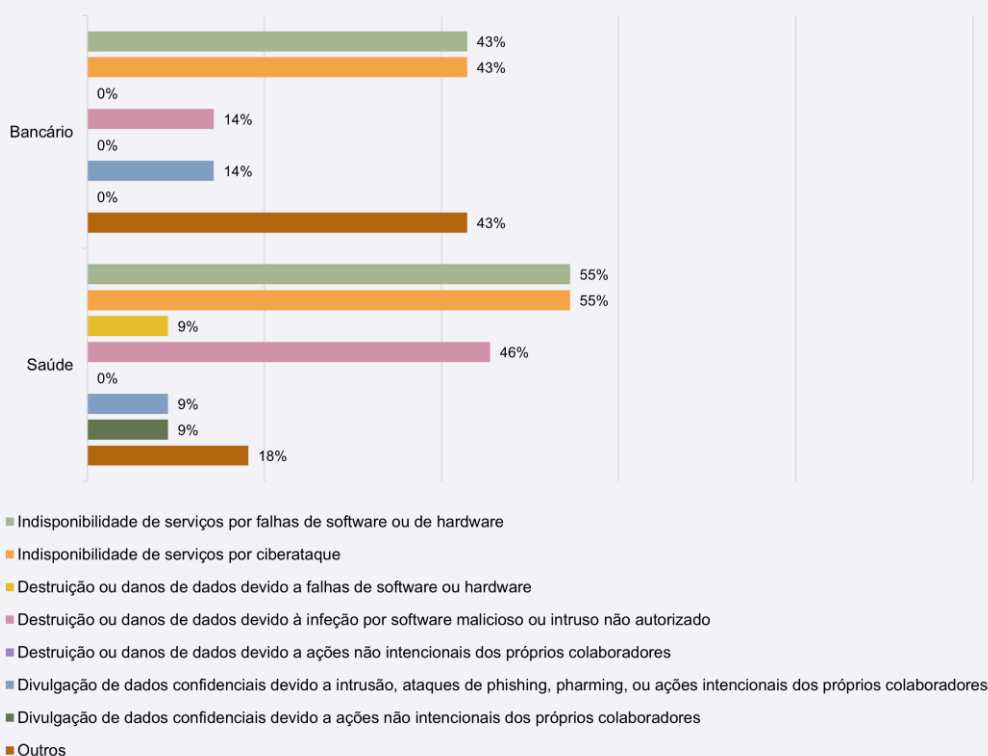
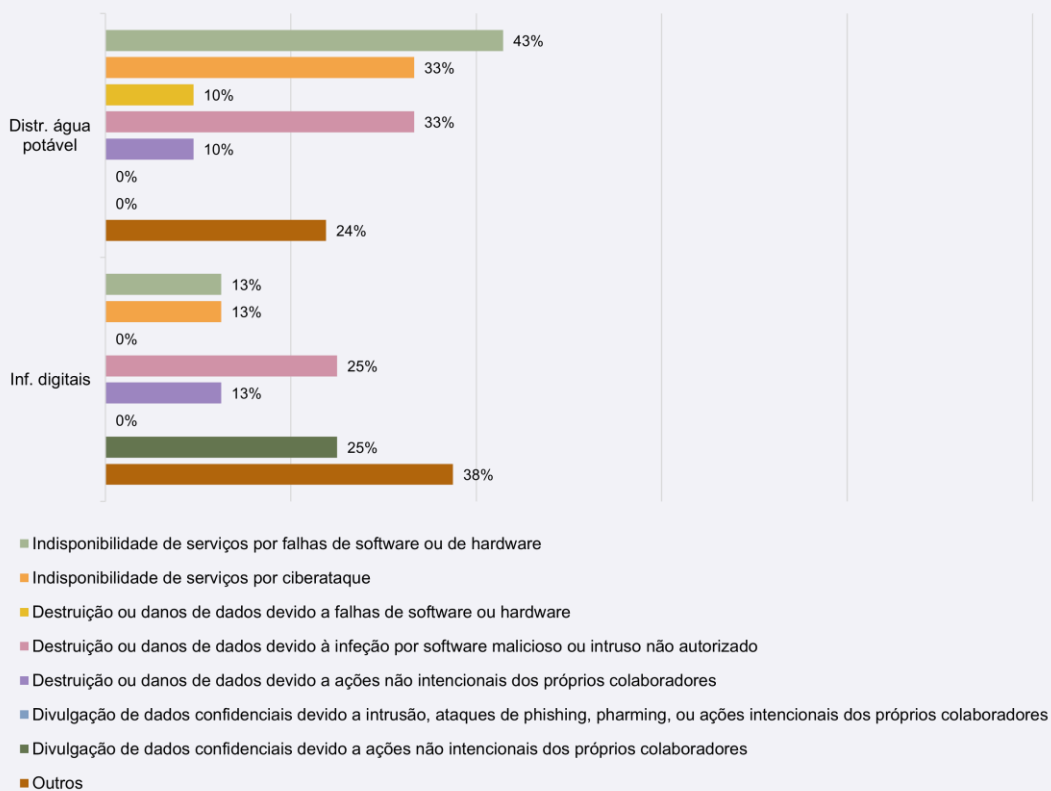


Gráfico 69.3 - Tipos de incidentes ocorridos



A grande maioria dos incidentes ocorridos afetou a disponibilidade dos serviços, quer por falha de *software* ou de *hardware*, quer por ciberataque. Depois destes, seguem-se os incidentes que resultaram na destruição de dados devido à infeção por *malware* ou devido a intrusão. Os operadores que referiram ter sofrido outros tipos de incidentes indicaram o comprometimento das contas de e-mail, a indisponibilidade de serviços por ataque a terceiros/prestadores de serviços e ainda tentativas de extorsão através de engenharia social. Destaca-se o setor da energia pela prevalência de incidentes que resultaram na indisponibilidade de serviços devido a ciberataque (67%). Nos setores dos transportes, bancário, saúde e infraestruturas digitais os efeitos dos incidentes dividem-se entre a indisponibilidade de serviços por falha de *software* ou *hardware* e indisponibilidade de serviços por ciberataque. O setor das infraestruturas do mercado financeiro mencionou nunca ter sofrido nenhum incidente logo a questão não se aplica.

Nos “outros” incidentes ocorridos, referidos por os inquiridos que já sofreram incidentes, foram mencionados um acesso indevido a um computador empresarial na rede *guest*, fraude e compromisso dos prestadores de serviço, *DDoS* ou causados por terceiros bem como indisponibilidade de serviços por ataque a terceiros prestadores de serviços e ainda tentativas de extorsão através de engenharia social.

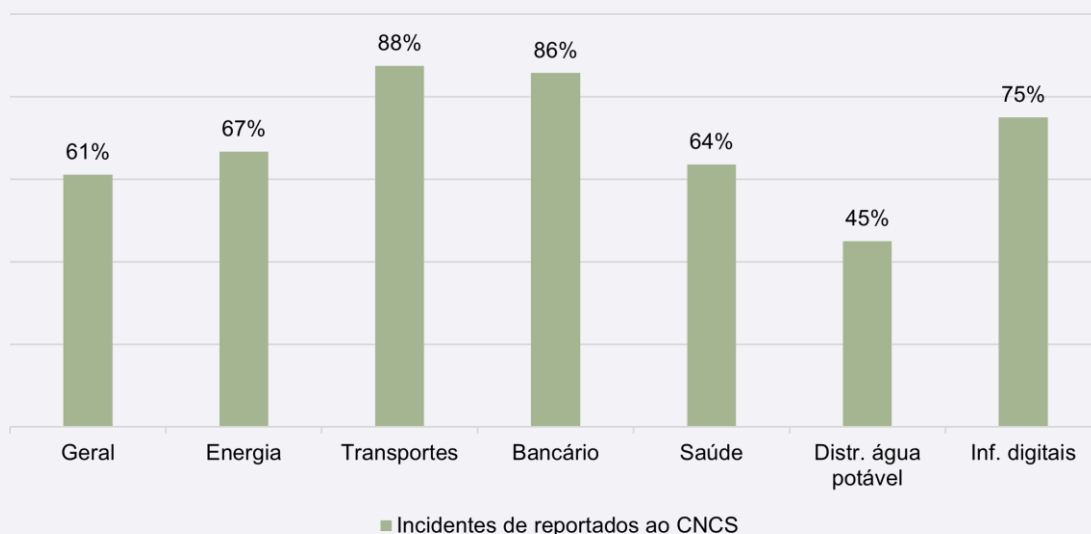
Segundo dados do IUTICE de 2022, em 2021, 11,5% das empresas experienciaram pelo menos um problema, seja de indisponibilidade de serviços TIC, de destruição ou corrupção de dados, ou de divulgação de dados confidenciais, devido a um incidente de segurança relacionado com as TIC. As consequências mais referidas destes incidentes foram a indisponibilidade de serviços TIC devido a falhas de *hardware* ou *software* e a ataques do exterior (8,3% e 2,5%, respetivamente), seguindo-se a destruição ou corrupção de dados devido a infeção de *software* malicioso ou intrusão não autorizada e devido a falhas de *hardware* ou *software* (2,1% e 1,8%, respetivamente)⁴⁸.

Segundo o estudo da Microsoft sobre o estado da cibersegurança em Portugal publicado em 2023, 70% dos inquiridos destaca o *phishing*, 63% dos inquiridos destaca os *softwares* maliciosos com cifragem de dados e pedido de resgate, 29% dos inquiridos destaca os ataques de negação de serviço *DDoS* pela sua capacidade de explorar vulnerabilidades nas redes e dispositivos programáveis da organização e, desta forma, perturbar os serviços e recursos das aplicações⁴⁹.

⁴⁸ INE, “Inquérito à Utilização das TIC nas Empresas”, 2022, 20.

⁴⁹ Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024, 6.

Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS

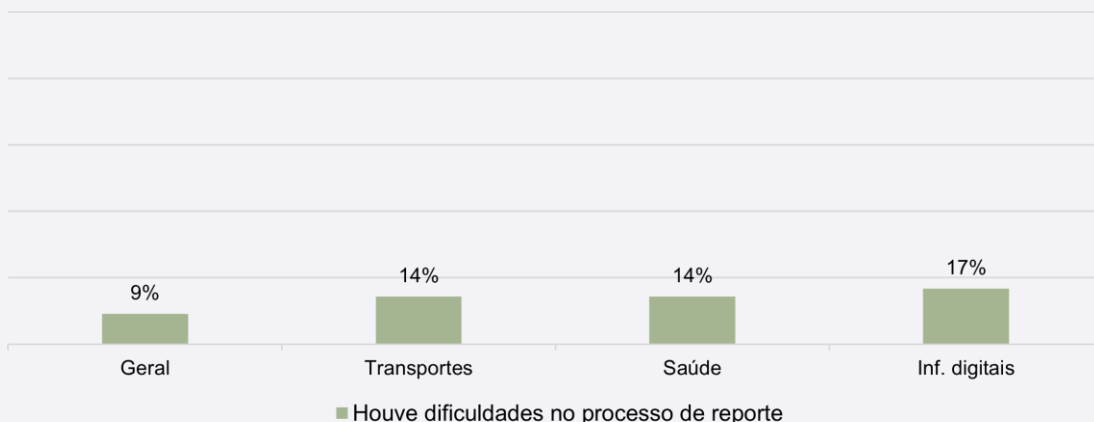


De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n.º 1 do artigo 16.º da lei n.º 46/2018, de 13 de agosto, os OSE estão apenas obrigados à notificação do incidente quando este tem “um impacto relevante na continuidade dos serviços essenciais por si prestados”. A ausência desse impacto relevante na continuidade dos serviços foi um dos motivos para a não notificação do incidente, como se verificará no **Gráfico 75**.

Nos setores bancário, saúde, de fornecimento e distribuição de água potável e infraestruturas digitais, observa-se a mesma tendência que na generalidade, onde a maior parte dos operadores notificaram o CNCS. No entanto, como podemos verificar no **Gráfico 75**, em todos os casos onde o incidente não foi notificado, o impacto não foi relevante para a continuidade dos serviços.

Nos setores de energia e transportes, observa-se mais reportes de incidentes que na generalidade, onde mais de 86% dos operadores notificaram o CNCS. No entanto, como podemos verificar no **Gráfico 75**, em todos os casos onde o incidente não foi notificado, o impacto não foi relevante para a continuidade dos serviços. O setor de infraestruturas do mercado financeiro não reportou sofrer nenhum incidente, por isso não é aplicável.

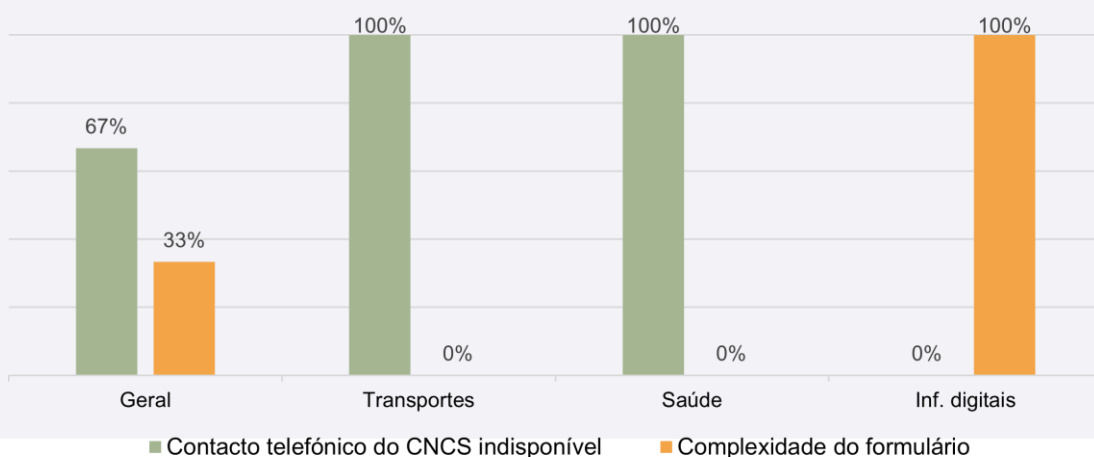
Gráfico 71 - Dificuldades no processo de notificação ao CNCS



De modo geral, os operadores não tiveram dificuldades no processo de notificação de incidentes ao CNCS. No entanto, a nível geral, houve ainda cerca de 9% dos operadores a indicarem dificuldades na notificação.

Nos setores da energia, bancário, fornecimento e distribuição de água potável e infraestruturas do mercado financeiro, não existiram dificuldades no processo de notificação ao CNCS. Nos restantes setores, mais de 10% dos operadores afirmam ter dificuldades no processo de notificação ao CNCS.

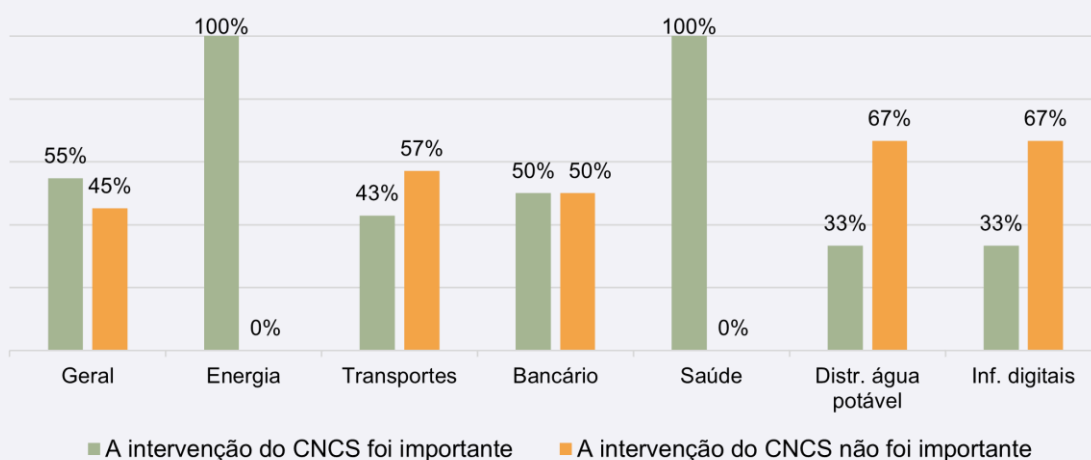
Gráfico 72 - Dificuldades encontradas pelos OSE durante a notificação de incidentes ao CNCS



Entre os setores que identificaram dificuldades na notificação de incidentes ao CNCS, dois (setores de transportes e saúde) referiram que a principal dificuldade durante o processo de notificação foi a indisponibilidade do contacto telefónico e um (infraestruturas digitais) atribuiu a principal dificuldade à complexidade do formulário de notificação.

Os setores de energia, bancário, infraestruturas do mercado financeiro e fornecimento e distribuição de água potável não identificou dificuldades na notificação de incidentes ao CNCS.

Gráfico 73 - Importância da intervenção do CNCS na resolução do incidente



A maioria dos operadores que notificou o CNCS de um incidente considerou que a intervenção deste foi importante na sua resolução (55%). Nos setores de energia e saúde, é unânime (100%) a opinião de que a intervenção do CNCS foi importante na resolução do incidente notificado.

No setor de transportes, fornecimento e distribuição de água potável e infraestruturas digitais, predomina a opinião de que a intervenção do CNCS não foi relevante para a resolução do incidente notificado. No setor bancário, metade dos inquiridos (50%) são da opinião que a intervenção do CNCS não foi relevante para a resolução do incidente notificado, enquanto a outra metade é da opinião que a intervenção foi importante. O setor de infraestruturas do mercado financeiro não reportou sofrer nenhum incidente, por isso a questão não é aplicável.

Gráfico 74 - Avaliação da resposta dada pelo CNCS

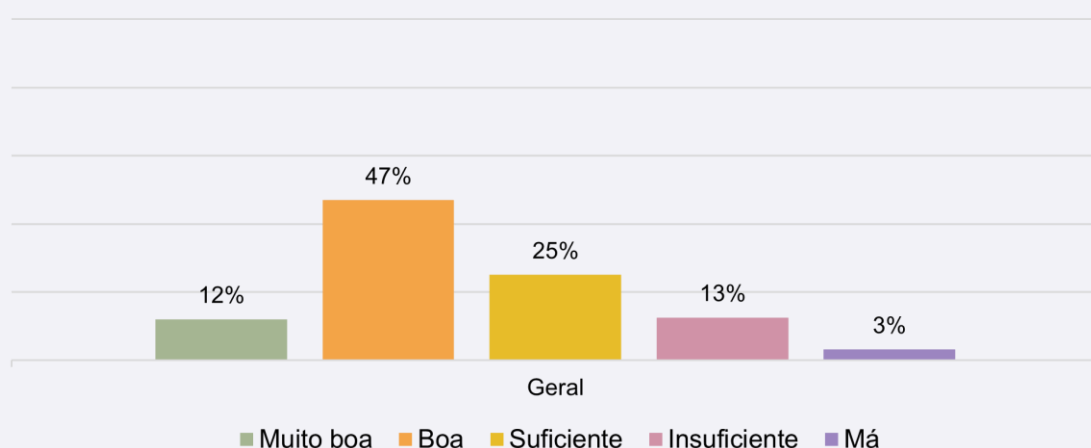


Gráfico 74.1 - Avaliação da resposta dada pelo CNCS

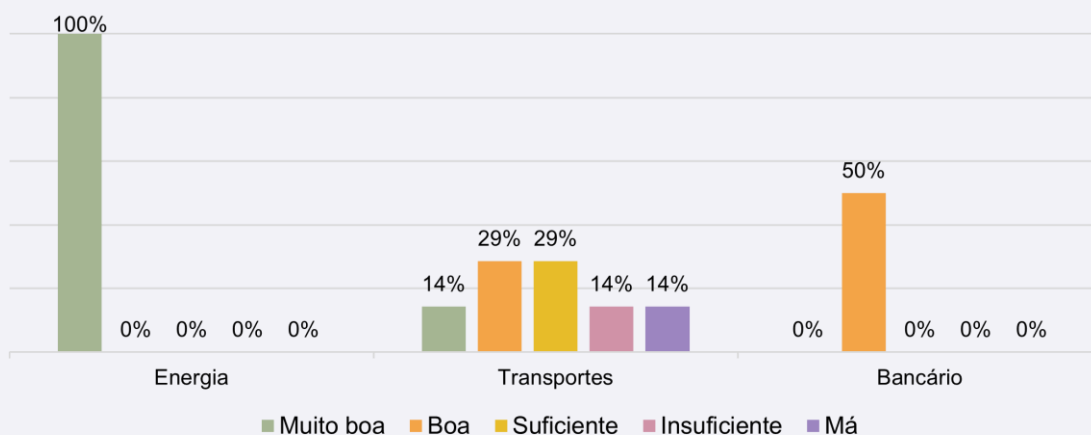
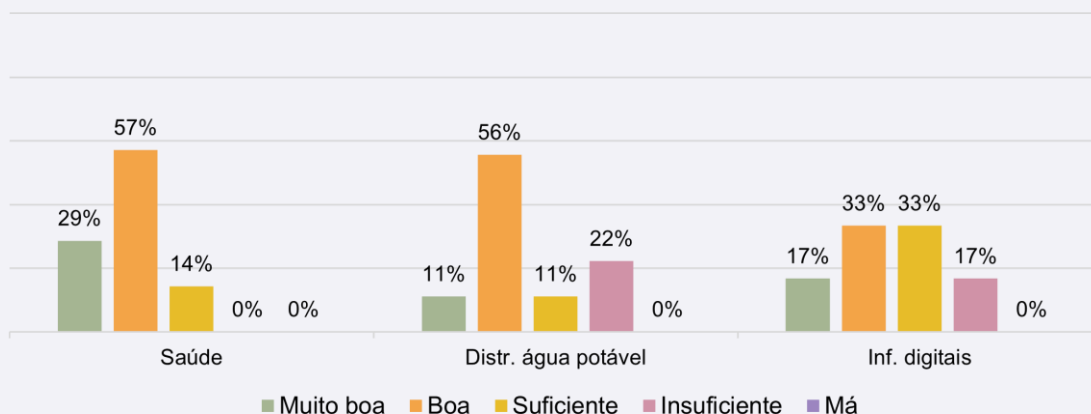


Gráfico 74.2 - Avaliação da resposta dada pelo CNCS



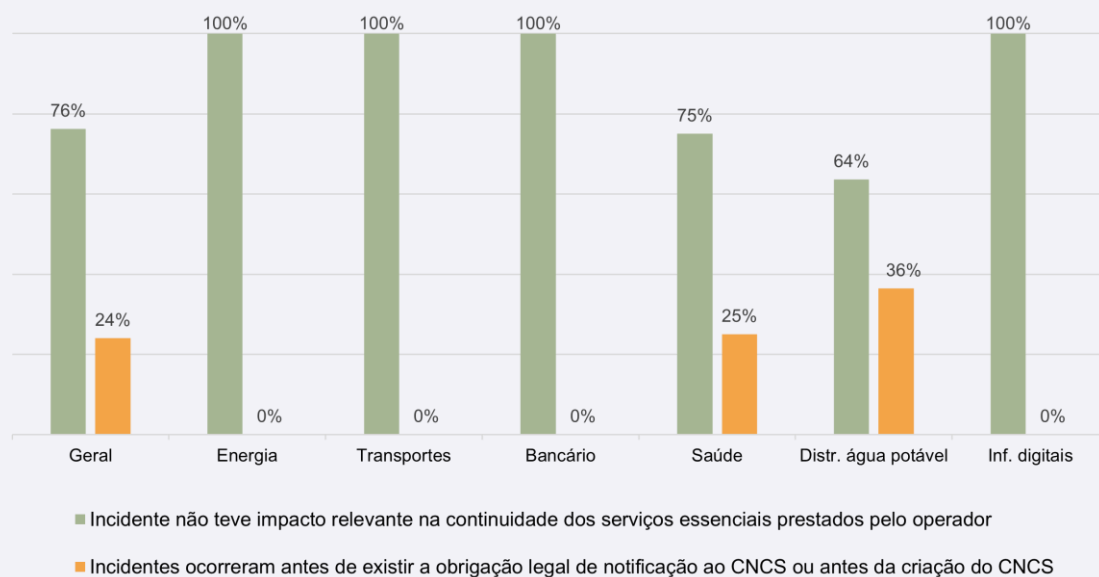
Relativamente à qualidade da resposta dada pelo CNCS ao incidente, existe alguma discrepância nas perspetivas dos diferentes operadores. Mais da metade dos operadores inquiridos (59%) considera que a resposta dada foi boa (47%) ou muito boa (12%). Um quarto dos inquiridos avaliou ainda a resposta dada como suficiente e 16% avaliaram a resposta como insuficiente (13%) ou má (3%).

No setor de energia, 100% dos colaboradores inquiridos consideram que a resposta dada por parte do CNCS foi muito boa.

Nos setores de transportes e infraestruturas digitais existem algumas discrepâncias nas perspetivas dos diferentes operadores. Em geral, a opinião foi positiva, no entanto, mais de 15% classificou a resposta do CNCS como insuficiente ou má. No setor bancário, a perspetiva geral é positiva. Os operadores afirmam a resposta ter sido ou boa (50%) ou suficiente (50%). Nenhum operador do setor classificou a resposta do CNCS como insuficiente ou má.

O setor do mercado financeiro não reportou sofrer nenhum incidente, por isso a questão não é aplicável. Nos setores da saúde e do fornecimento e distribuição de água potável, a perspetiva geral é novamente positiva. Sendo que no caso do setor da saúde nenhum operador do setor classificou a resposta do CNCS como insuficiente ou má. Já no setor de fornecimento e distribuição de água potável quase um quarto dos inquiridos classificaram a resposta do CNCS como insuficiente.

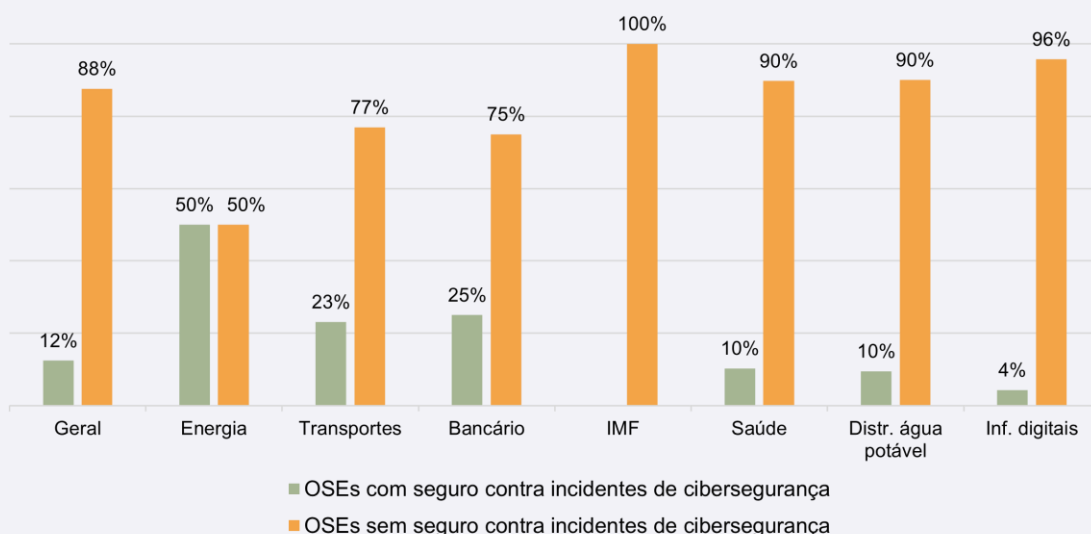
Gráfico 75 - Motivos para a não notificação de incidentes de cibersegurança ao CNCS



Como referido no **Gráfico 70**, a não notificação dos incidentes foi justificada. O principal motivo para a não notificação de incidentes de cibersegurança ao CNCS, segundo os OSE, foi o facto de o incidente não ter tido impacto na continuidade dos serviços essenciais por si prestados (76%). Nos restantes casos (24%) o incidente ocorreu antes de existir a obrigação legal de notificação ou até mesmo antes da criação do CNCS.

O setor das infraestruturas do mercado financeiro não reportou sofrer nenhum incidente, por isso a questão não é aplicável.

Gráfico 76 - Seguro contra incidentes de cibersegurança



Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. Nenhum OSE do setor de infraestruturas do mercado financeiro possui seguro contra incidentes de cibersegurança. O setor da energia é o setor onde mais operadores têm seguro contra incidentes de cibersegurança, chegando aos 50% de operadores com seguro. A lógica geral mantém-se nos setores dos transportes, bancário, saúde, distribuição de água potável e infraestruturas digitais, com a maior parte dos inquiridos a não possuírem este tipo de seguro.

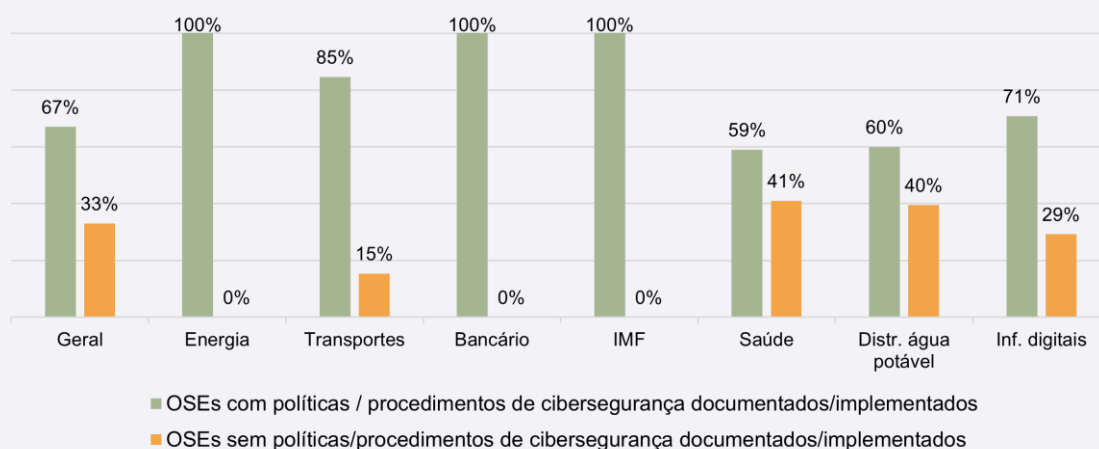
Segundo dados da ENISA (Relatório *NIS Investments* de 2023), cerca de 58% dos inquiridos não tinham qualquer seguro relacionado com cibersegurança. A discrepância entre os valores da ENISA e os obtidos pelo questionário realizado poderá dever-se à composição da amostra, uma vez que a do estudo da ENISA inclui operadores de serviços essenciais e prestadores de serviços digitais. Já o questionário realizado pelo CNCS contemplou apenas operadores de serviços essenciais⁵⁰.

No inquérito elaborado pelo Fórum Económico Mundial, as empresas foram divididas em dois tipos: empresas com receita elevada e empresas com receita baixa, o que permite observar que as empresas do primeiro tipo tendem a adquirir seguros de cibersegurança - 75% das empresas com receita elevada fizeram-no. Já entre as empresas com receitas mais baixas, apenas cerca 25% destas adquiriram seguros de cibersegurança⁵¹.

⁵⁰ ENISA, "NIS Investments", 2023, 16 e 24.

⁵¹ Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", 9.

Gráfico 77 - Documentação/implementação de políticas e procedimentos de cibersegurança



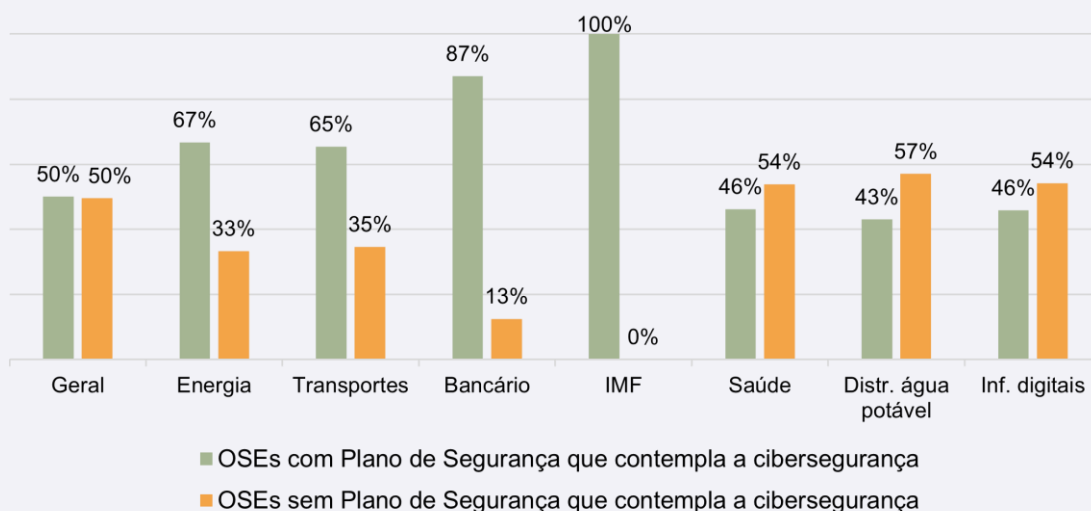
Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados.

Nos setores de energia, bancário e de infraestruturas do mercado financeiro, todos os operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados. Nos setores de transportes e infraestruturas digitais, esta proporção é maior que a geral, onde a maioria refere ter políticas ou procedimentos de cibersegurança documentados ou implementados.

Nos setores da saúde e distribuição de água potável, esta proporção é menor que a geral, mesmo assim, a maioria dos operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados. Segundo dados do IUTICE, em 2022, cerca de 54.4% do total de empresas tinha documentos sobre medidas, práticas ou procedimentos em matéria de segurança⁵².

⁵² INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

Gráfico 78 - Existência de Plano de Segurança que contemple a cibersegurança



O plano de segurança é obrigatório ao abrigo do decreto-lei n.º 65/2021, de 30 de julho. No entanto, metade dos operadores inquiridos, 50%, ainda não tem um plano de segurança que contemple a área da cibersegurança.

Nos setores de energia, transportes e bancário, a maior parte dos operadores já tem um plano de segurança que contemple a área da cibersegurança. O setor de infraestruturas do mercado financeiro é o único onde todos os inquiridos referem que já tem um plano de segurança que contemple a área da cibersegurança. Nos restantes setores, a percentagem de operadores com plano de segurança fica acima dos 40%, mas aquém dos 50%.

Segundo um estudo realizado pela Microsoft, mais de 40% das empresas inquiridas têm projetado um investimento em cibersegurança. Destas empresas, cerca de 69% irá investir em avaliações regulares de risco de cibersegurança e 66% em auditorias de segurança e monitorização de ameaças em tempo real⁵³.

⁵³ Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 5.

Gráfico 79 - Políticas incluídas no Plano de Segurança

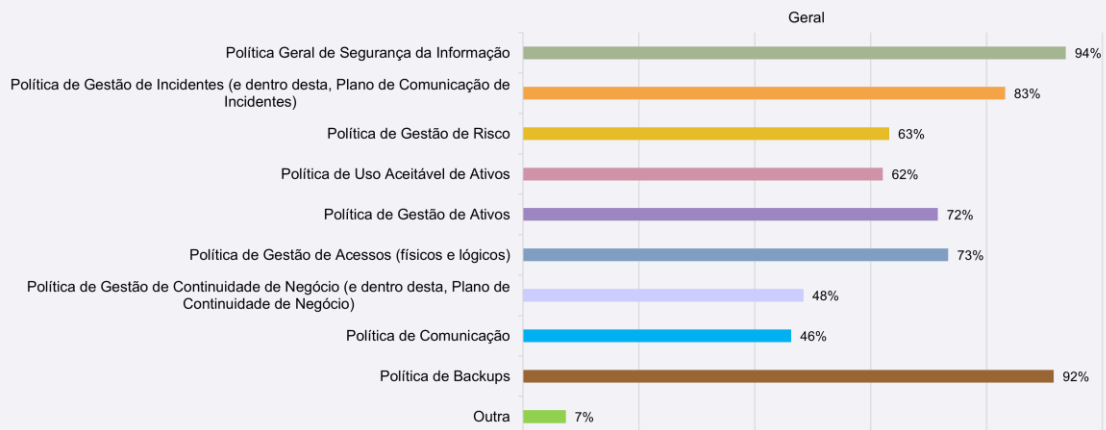


Gráfico 79.1 - Políticas incluídas no Plano de Segurança

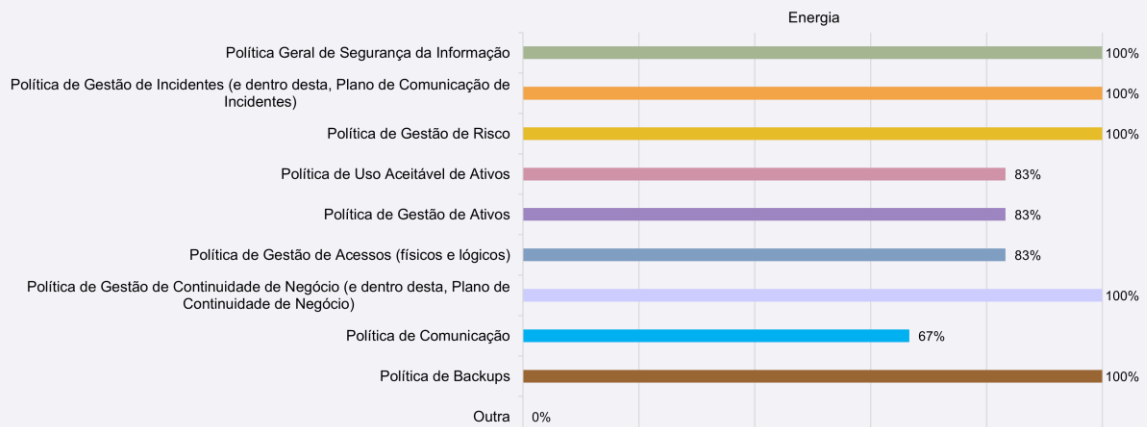


Gráfico 79.2 - Políticas incluídas no Plano de Segurança

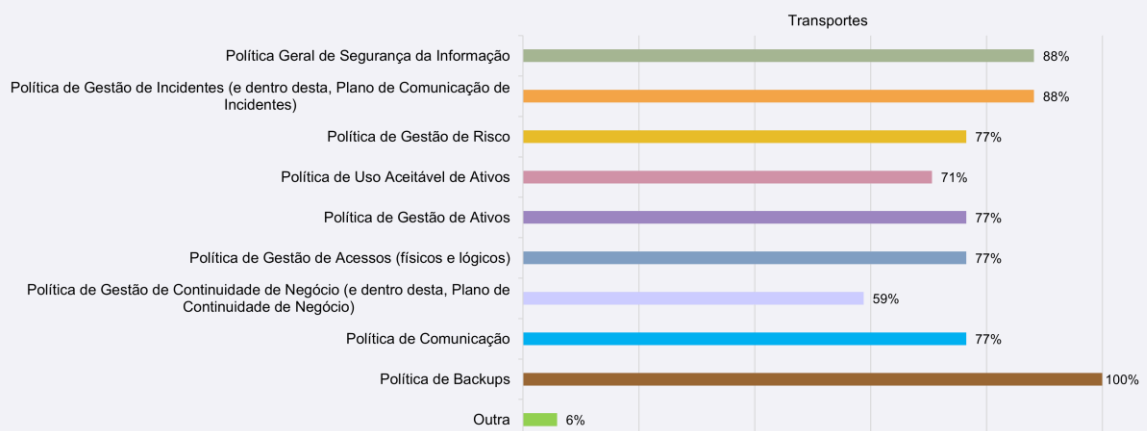


Gráfico 79.3 - Políticas incluídas no Plano de Segurança

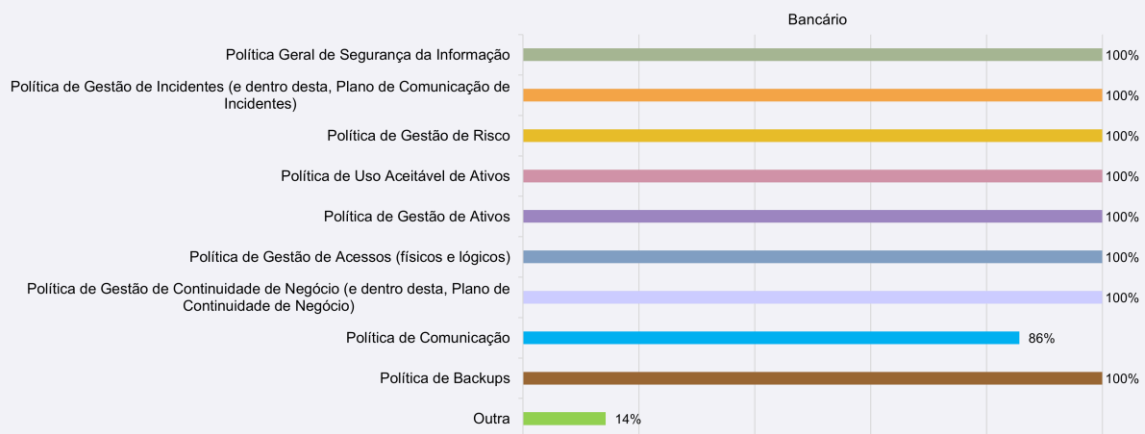


Gráfico 79.4 - Políticas incluídas no Plano de Segurança

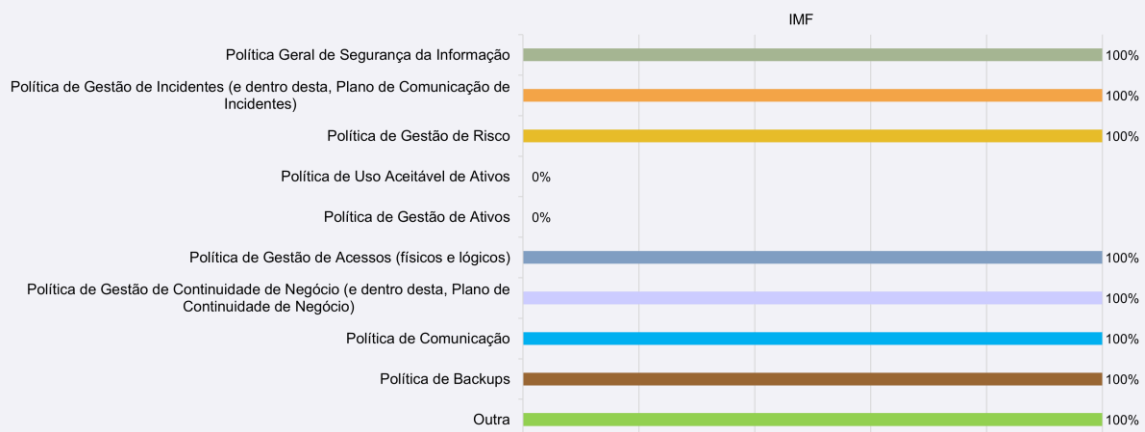


Gráfico 79.5 - Políticas incluídas no Plano de Segurança

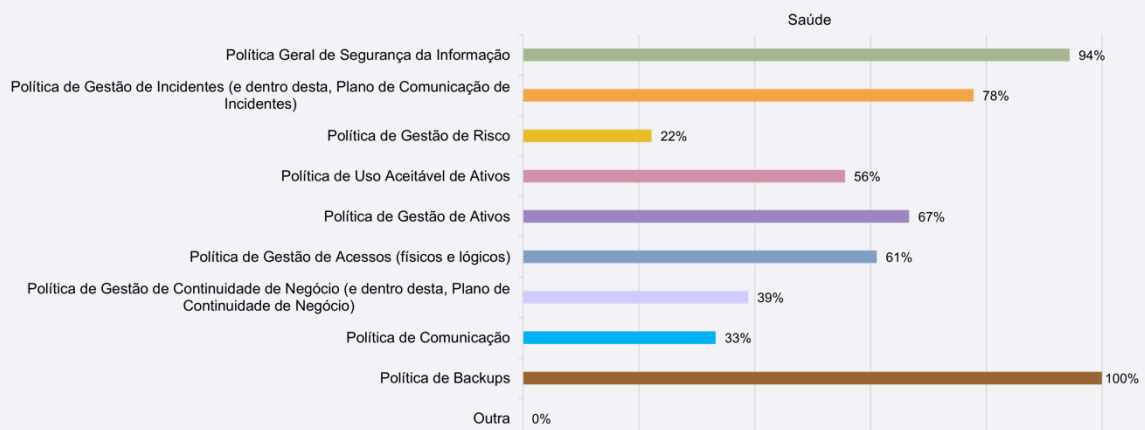


Gráfico 79.6 - Políticas incluídas no Plano de Segurança

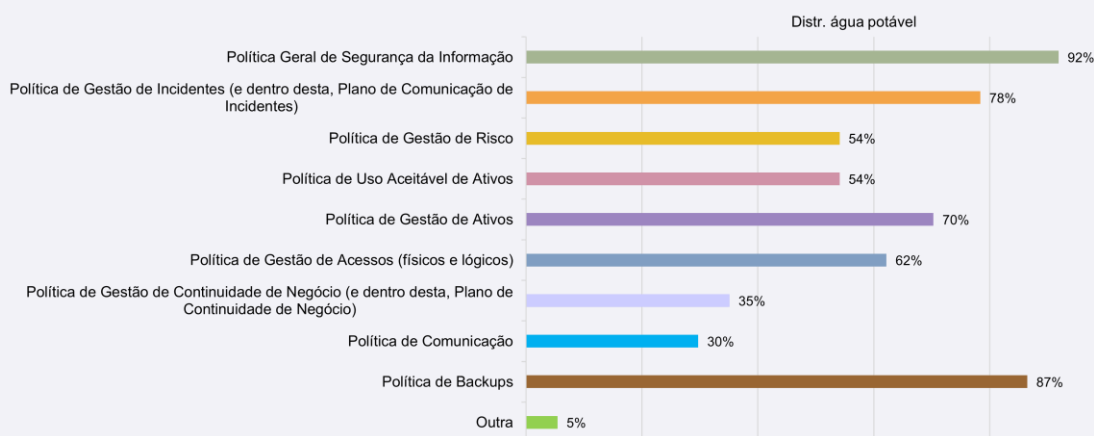
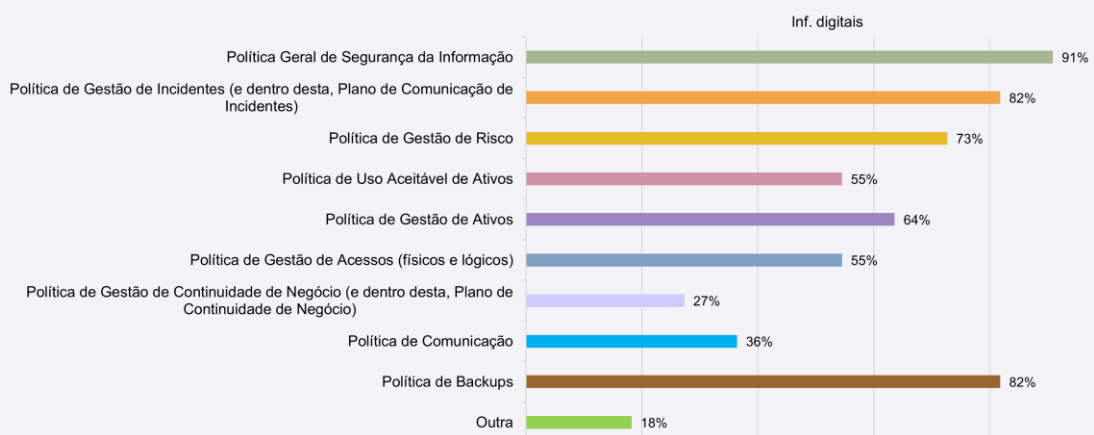


Gráfico 79.7 - Políticas incluídas no Plano de Segurança

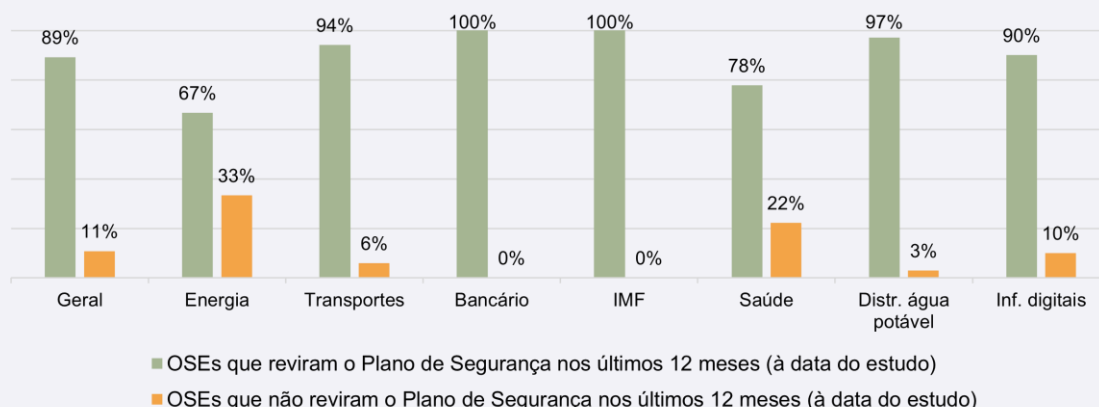


Os gráficos acima representam a percentagem de operadores com plano de segurança que tem as diversas políticas elencadas elaboradas no âmbito desse mesmo plano.

As políticas mais comuns são a Política de Geral de SI (94%), a Política de Backups (92%), a Política de Gestão de Incidentes (83%), a Política de Gestão de Acessos (73%), a Política de Gestão de Ativos (72%), a Política de Gestão de Risco (63%) e a Política de Uso Aceitável de Ativos (62%). As políticas menos adotadas entre os operadores são a Política de Continuidade de Negócio (48%) e a Política de Comunicação (46%).

Entre as “outras” políticas (7%), contam-se a Política de Utilização de Correio Eletrónico, Política de *Passwords*, Política de Teletrabalho, Política de Classificação e Manuseamento de Informação, Política de Segurança Física, Política de Gestão de Alterações, Política de Criptografia, Política de Recursos Humanos para a Cibersegurança e Política de Privacidade e Proteção de Dados.

Gráfico 80 - Revisão do Plano de Segurança



Cerca de 89% dos operadores com plano de segurança fizeram a revisão anual do mesmo nos últimos 12 meses, à data do estudo, seguindo as exigências do artigo 7º do decreto-lei nº 65/2021. Entre estes, destacam-se os operadores dos setores bancário e das infraestruturas do mercado financeiro, nos quais todos os operadores com plano de segurança realizaram a revisão anual deste. Nos setores dos transportes, do fornecimento e distribuição de água potável e o das infraestruturas digitais, a grande maioria dos operadores com plano de segurança realizou a revisão do mesmo. Apenas nos setores da saúde e da energia os resultados estão abaixo dos 80% de operadores que reviram o plano de segurança nos últimos 12 meses, à data do estudo.

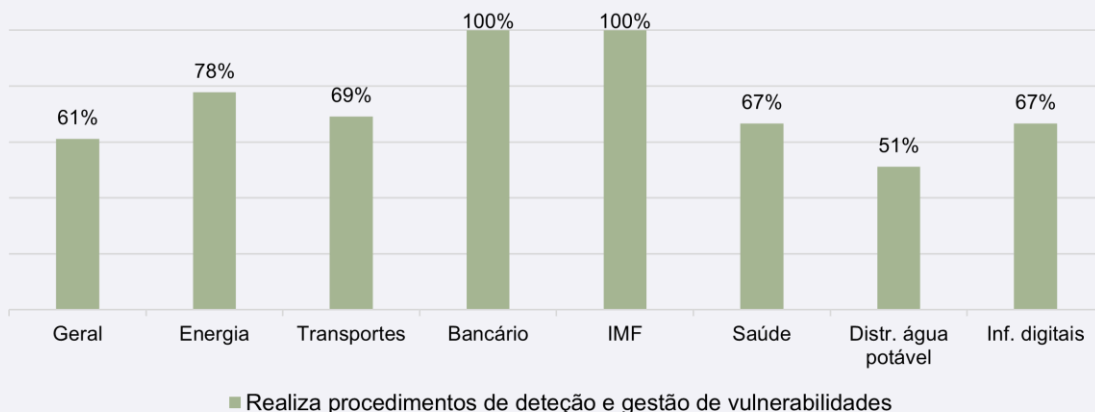
No setor da energia existe uma significativa divergência entre os operadores do setor em matéria da revisão do plano de segurança, com cerca de 67% a referir que reviram o plano nos últimos 12 meses (à data do estudo), seguindo as exigências do artigo 7º do decreto-lei nº 65/2021 e 33% a indicar que não efetuaram a revisão. Nos setores dos transportes e fornecimento e distribuição de água potável, apenas uma minoria dos operadores refere não realizar o plano de segurança nos últimos 12 meses (à data do estudo).

No setor bancário e no setor das infraestruturas de mercado financeiro, todos os operadores reviram o plano nos últimos 12 meses (à data do estudo), seguindo as exigências do artigo 7º do decreto-lei nº 65/2021. Nos setores da saúde e das infraestruturas digitais, apenas 22% e 10%, respetivamente, dos operadores refere não realizar o plano de segurança nos últimos 12 meses (à data do estudo).

Segundo dados do IUTICE 2022, a maioria (61,7%) das empresas definiu ou fez uma revisão aos documentos sobre medidas, práticas ou procedimentos de segurança nos últimos 12 meses⁵⁴.

⁵⁴ INE, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

Gráfico 81 - OSE que realizam procedimentos de deteção e gestão de vulnerabilidades

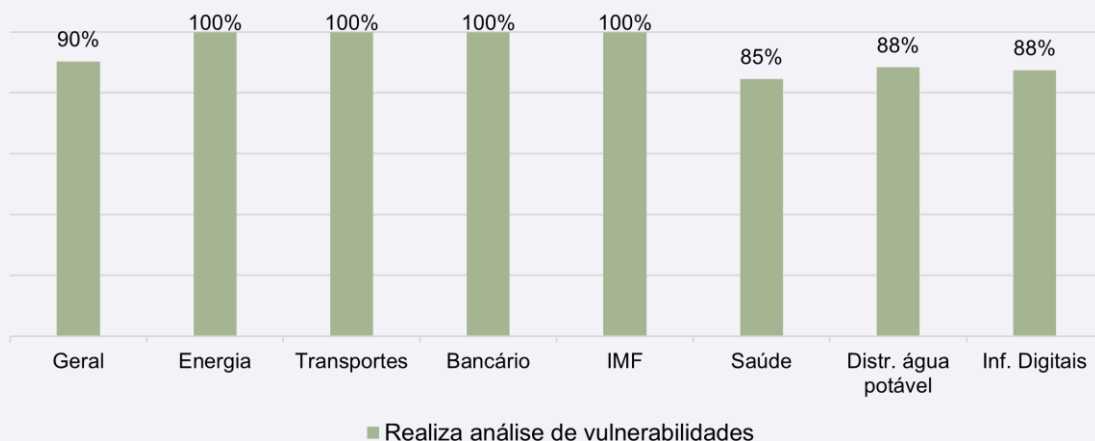


Mais de 60% dos operadores inquiridos dos diferentes setores referem realizar procedimentos de deteção e gestão de vulnerabilidades.

Os setores bancário e das infraestruturas do mercado financeiro surgem uma vez mais em destaque, uma vez que todos os operadores inquiridos realizam também procedimentos de deteção e gestão de vulnerabilidades.

Nos restantes setores, a percentagem de operadores que realiza estes procedimentos ultrapassa os 60%, com exceção do setor do fornecimento e distribuição de água potável, que fica aquém desse valor, fixando-se próximo dos 51%.

Gráfico 82 - OSE que dentro dos procedimentos de deteção e gestão de vulnerabilidades realizam análise de vulnerabilidades



Entre os operadores que realizam procedimentos de deteção e gestão de vulnerabilidades, a vasta maioria (90%) faz também a análise das mesmas.

Nos setores da energia, dos transportes, bancário e das infraestruturas do mercado financeiro, todos os operadores que já realizavam procedimentos de deteção e gestão de vulnerabilidades, fazem também a análise das mesmas.

Nos setores da saúde, do fornecimento e distribuição de água potável e das infraestruturas digitais, embora a análise de vulnerabilidades não seja realizada por todos os operadores de cada setor, esta é realizada por pelo menos 85% dos operadores inquiridos.

Gráfico 83 - Frequência da análise de vulnerabilidades

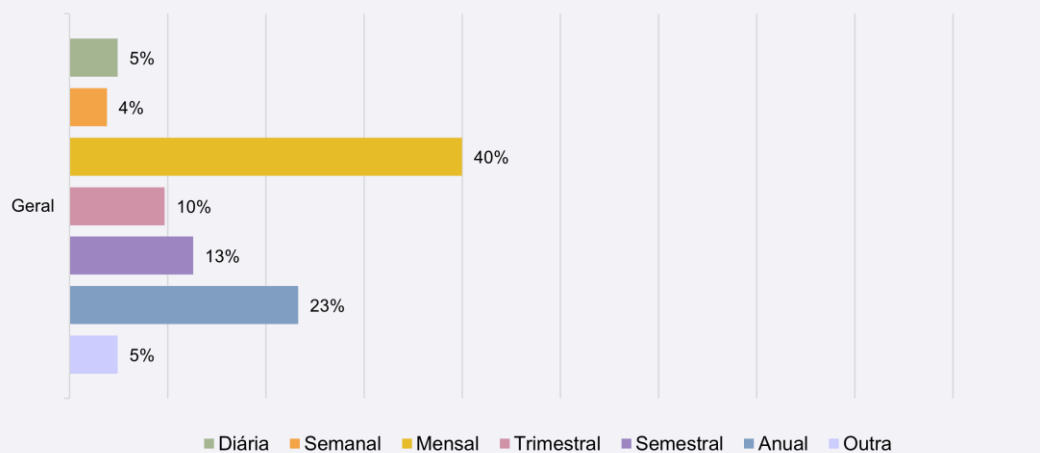


Gráfico 83.1 - Frequência da análise de vulnerabilidades

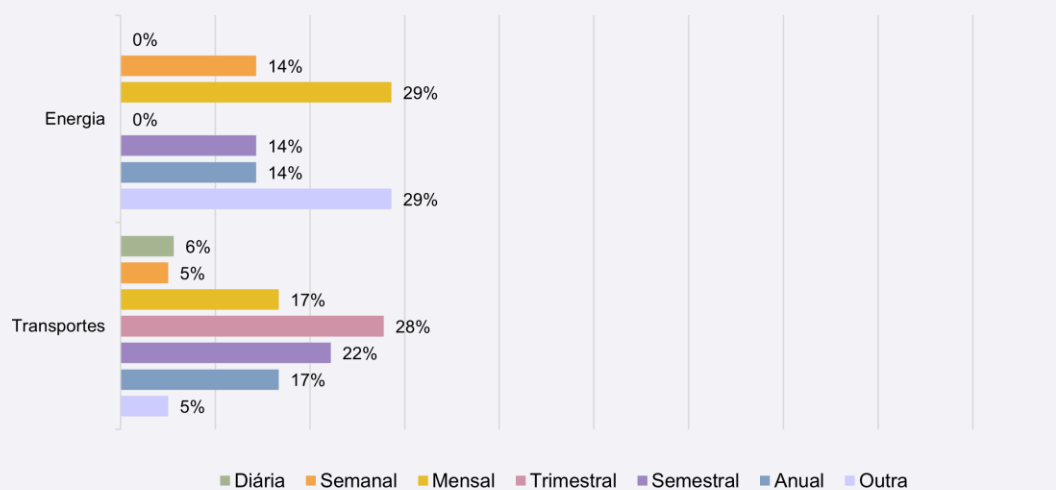


Gráfico 83.2 - Frequência da análise de vulnerabilidades

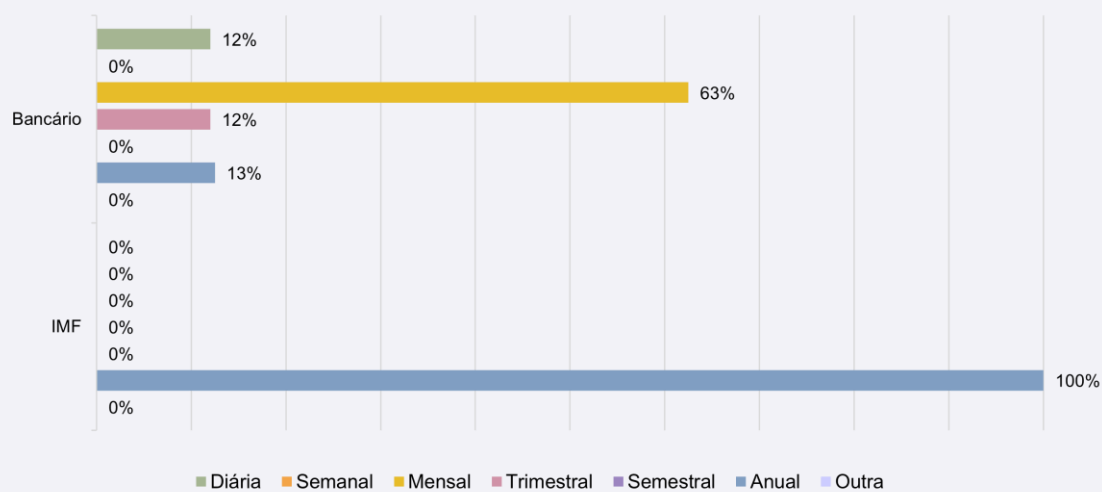


Gráfico 83.3 - Frequência da análise de vulnerabilidades

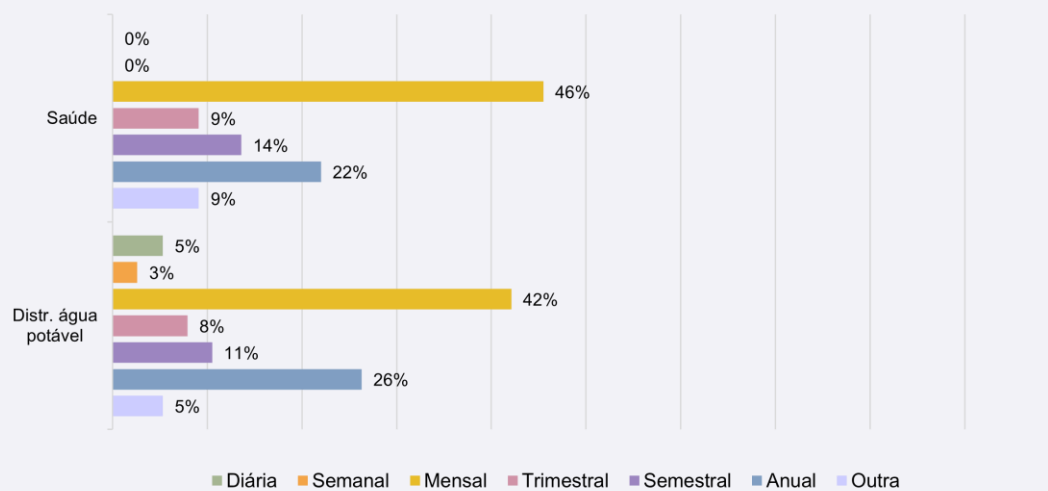
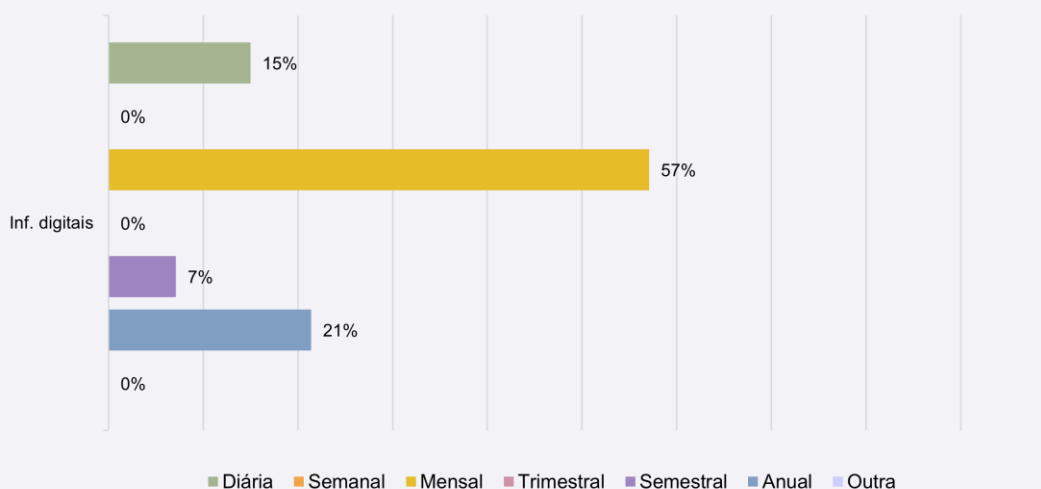


Gráfico 83.4 - Frequência da análise de vulnerabilidades



A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.

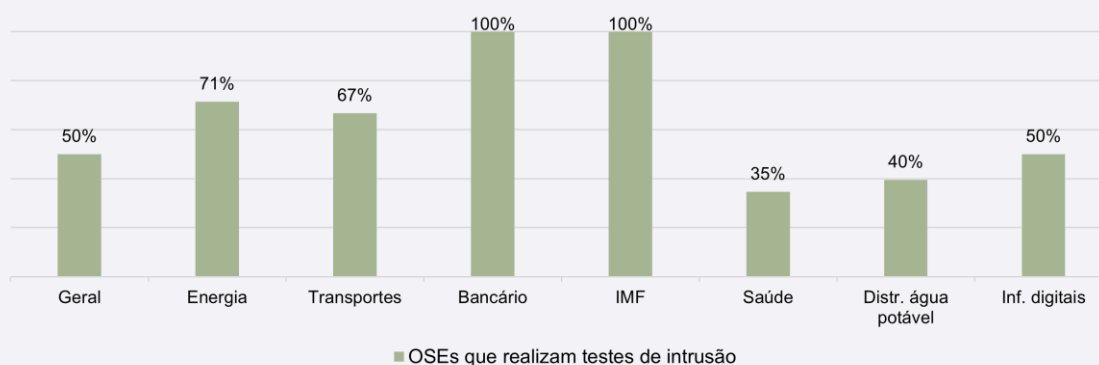
Destaca-se o setor das infraestruturas do mercado financeiro, no qual todos os operadores indicaram realizar análise de vulnerabilidades com frequência anual.

A frequência semanal é a menos observada, não tendo sido indicada por qualquer operador nos setores bancário, das infraestruturas do mercado financeiro, da saúde ou das infraestruturas digitais.

Há ainda operadores, embora poucos, que realizam análise de vulnerabilidades diariamente, nomeadamente nos setores dos transportes, bancário, do fornecimento e distribuição de água potável e das infraestruturas digitais.

No setor da energia, existe alguma discrepância no tipo de frequência de análise de vulnerabilidades entre os operadores. Neste setor, as frequências mensal ou contínua são as que se verificam mais frequentemente. Nenhum operador referiu realizar análises de vulnerabilidades de frequência diária ou trimestral.

Gráfico 84 - Realização de testes de intrusão



Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).

Há que destacar os setores bancário e o das infraestruturas do mercado financeiro, nos quais todos os inquiridos referiram realizar testes de intrusão. São de salientar, também, os setores da energia e dos transportes, nos quais 71% e 67% dos operadores, respetivamente, realizam testes de intrusão.

Contrastando com estes, surgem os setores das infraestruturas digitais, da saúde e do fornecimento e distribuição de água potável. No setor das infraestruturas digitais, há 50% dos inquiridos a realizar testes de intrusão. Nos outros dois setores, saúde e distribuição e fornecimento de água potável, os operadores que realizam estes testes já se encontram em minoria. Em ambos, a percentagem de operadores que realiza testes de intrusão é inferior a 40%.

Gráfico 85 - Frequência de testes de intrusão

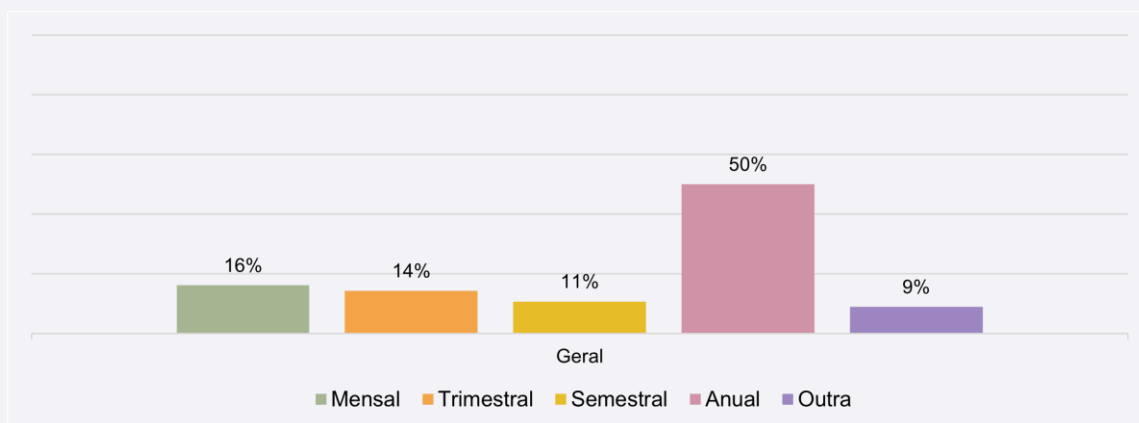


Gráfico 85.1 - Frequência de testes de intrusão

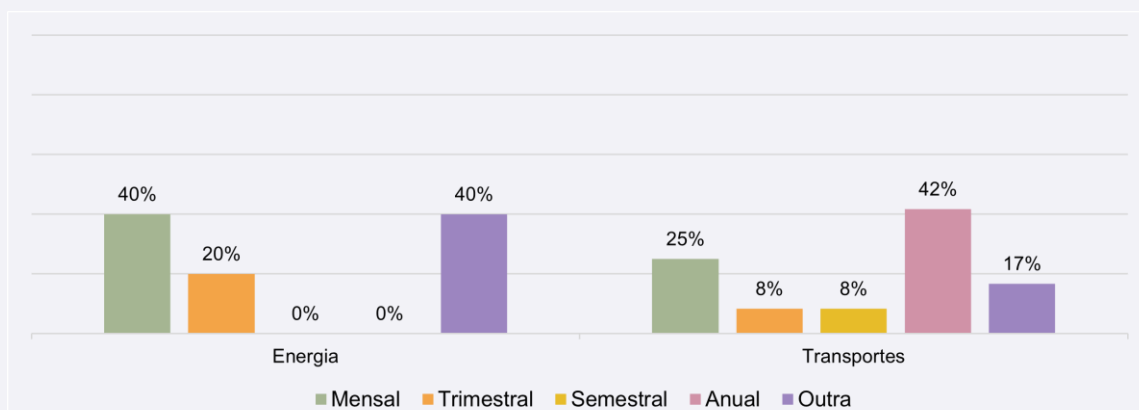


Gráfico 85.2 - Frequência de testes de intrusão

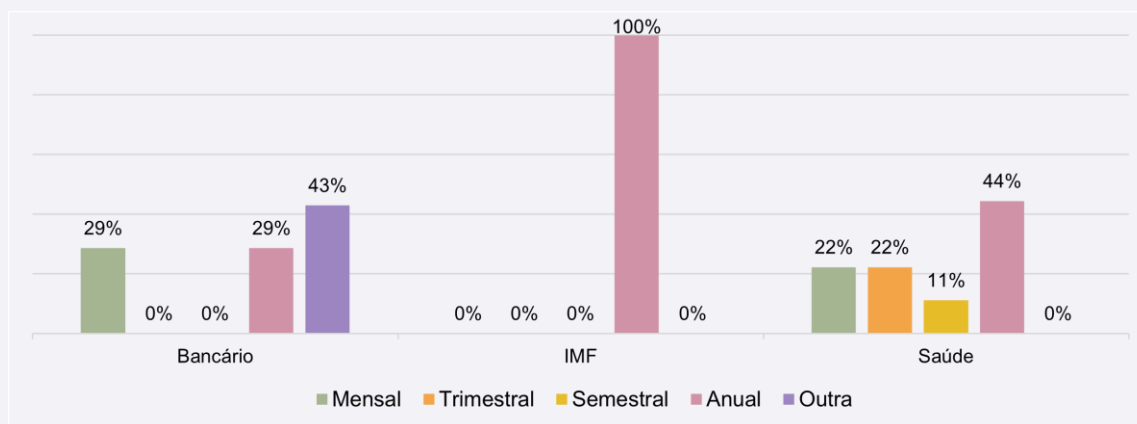
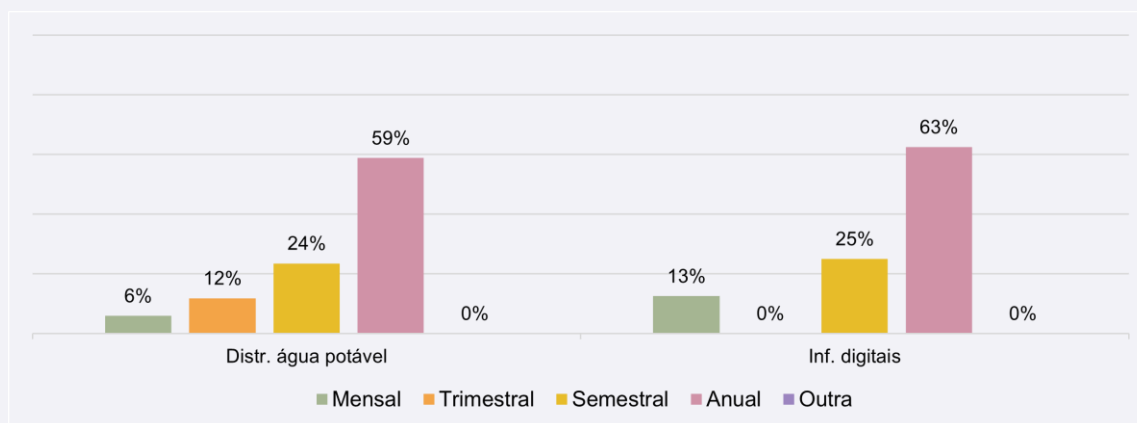


Gráfico 85.3 - Frequência de testes de intrusão



Com exceção dos operadores de serviços essenciais do setor da energia e do setor bancário, os operadores dos setores tendem a realizar testes de intrusão anualmente.

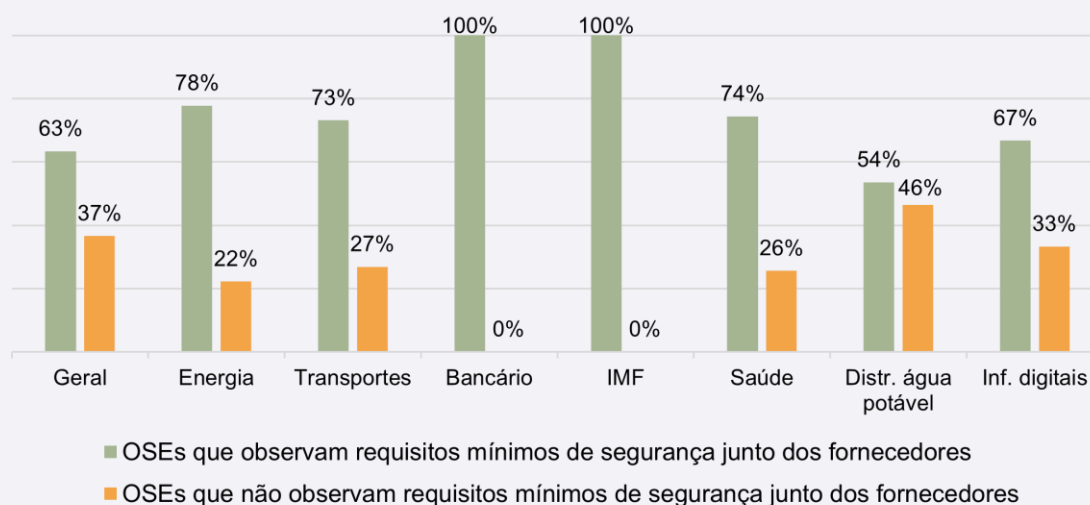
A exceção verificada no setor da energia prende-se com o facto de todos os operadores realizarem esses testes com uma frequência superior à anual e semestral. Entre os inquiridos, uma minoria realiza testes de intrusão pelo menos trimestralmente, sendo que a maioria realiza mensalmente ou de forma ainda mais frequente, para que os testes possam ser realizados por secções ou áreas da organização.

Por sua vez, no setor bancário, 43% indicou realizar testes de intrusão com uma frequência também superior à mensal porque há operadores que os realizam de forma contínua, operadores que conduzem estes testes sempre que as versões das aplicações utilizadas são atualizadas e operadores que realizam estes testes sempre que novos ativos são introduzidos.

Apenas no setor nas infraestruturas do mercado financeiro se registou a mesma frequência entre todos os operadores - os testes de intrusão são realizados anualmente.

Nos restantes setores, embora prevaleça a periodicidade anual para estes testes, é possível verificar operadores a optar por períodos mais curtos entre cada momento de teste.

Gráfico 86 - Observação de requisitos mínimos e segurança por parte dos fornecedores em contexto de cadeia de abastecimento



Na generalidade, e também em cada setor, a maioria dos operadores (mais de 60%) procura que os seus fornecedores estejam alinhados com os requisitos mínimos de segurança por si exigidos. Novamente, destacam-se os setores bancário e das infraestruturas do mercado financeiro, nos quais se verifica, para todos os operadores, a observação de requisitos mínimos de segurança por parte dos seus fornecedores.

Depois destes, seguem-se os setores da energia, saúde e transportes, com a observação dos requisitos de segurança por parte dos fornecedores em quase 80% dos operadores. Por último, surgem os setores das infraestruturas digitais e de fornecimento e distribuição de água potável, com os requisitos a serem cumpridos por menor percentagem de operadores, mas atingindo a maioria.

Gráfico 87 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS

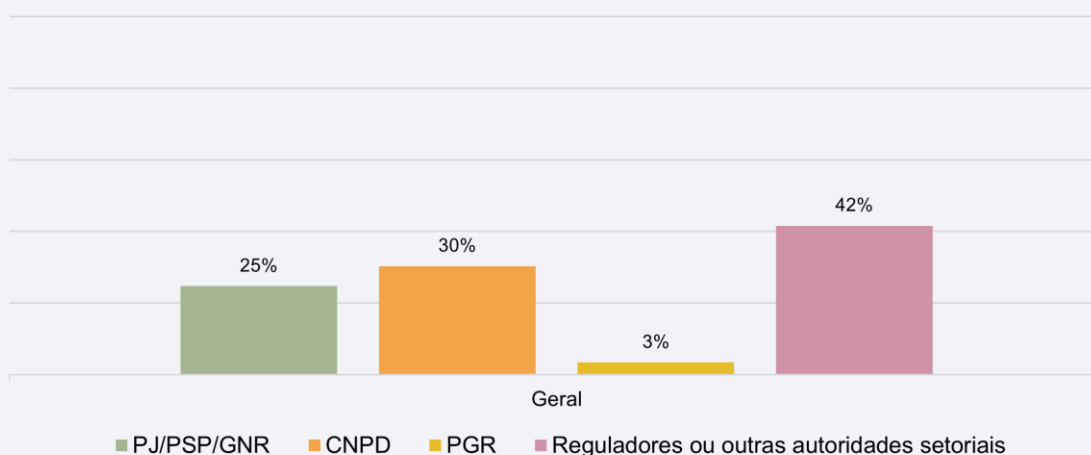
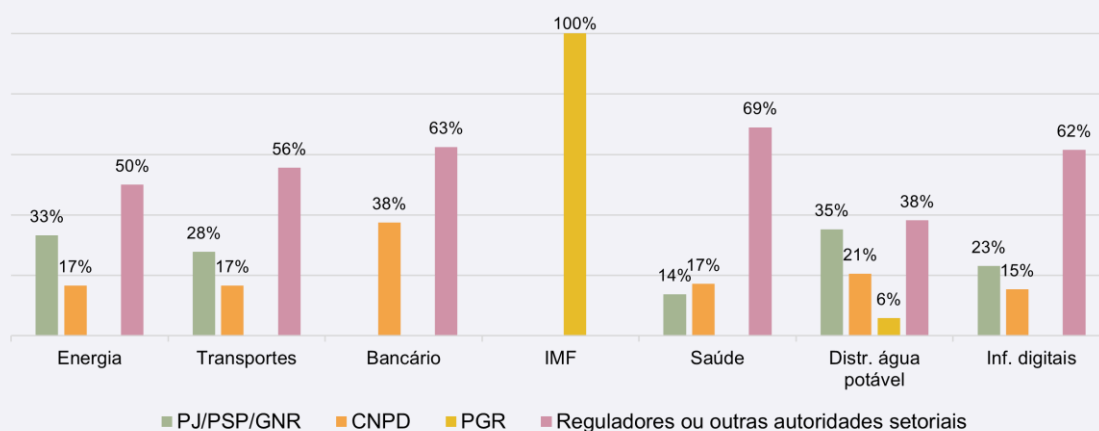


Gráfico 87.1 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS



Embora não seja obrigatório, cerca de 40% dos operadores optam por notificar as entidades reguladoras do seu setor ou outras autoridades setoriais caso sofram um ciberataque ou incidente de cibersegurança.

Apenas uma quantidade muito reduzida dos operadores tem previsto fazer qualquer tipo de notificação à Procuradoria-Geral da República (PGR).

A Comissão Nacional de Proteção de Dados (CNPD) surge em 2º lugar nas intenções de notificação em caso de ciberataque/incidente dos inquiridos, estando em 3º lugar as intenções de notificação à PJ/PSP/GNR.

Em caso de ciberataque os OSE concordam em contactar, para além do CNCS, os reguladores ou outras entidades setoriais. Verifica-se que contactar a PGR foi a opção com menos destaque seguida do CNPD.

Destacam-se os setores das infraestruturas do mercado financeiro e de fornecimento e distribuição de água potável onde, no caso do primeiro, todos os inquiridos referem optar por contactar a PGR e, no caso do último, uma minoria. De referir que nenhum dos outros setores optou, em algum caso, contactar a PGR.

Os restantes setores privilegiam a notificação aos reguladores ou outras entidades setoriais em caso de ciberataque ou incidentes. Depois destas entidades encontra-se a PJ/PSP/GNR.

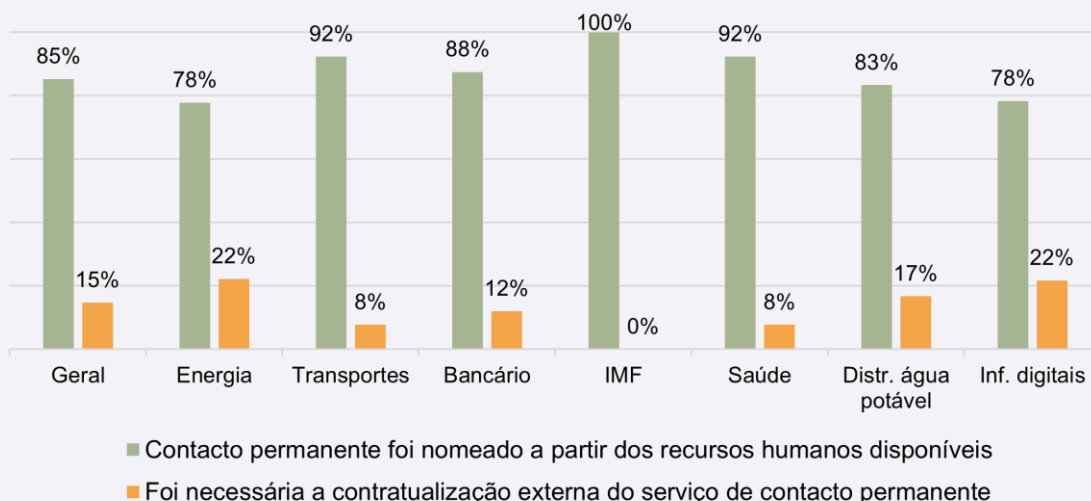
Os setores da energia, transportes, fornecimento e distribuição de água potável e infraestruturas digitais optam, em segundo lugar, pela notificação à PJ/PSP/GNR, sendo que os restantes optam, em segunda instância, pela notificação à CNPJ.

Gráfico 88 - Nomeação do contacto permanente que assegura os fluxos de informação de nível operacional e técnico com o CNCS



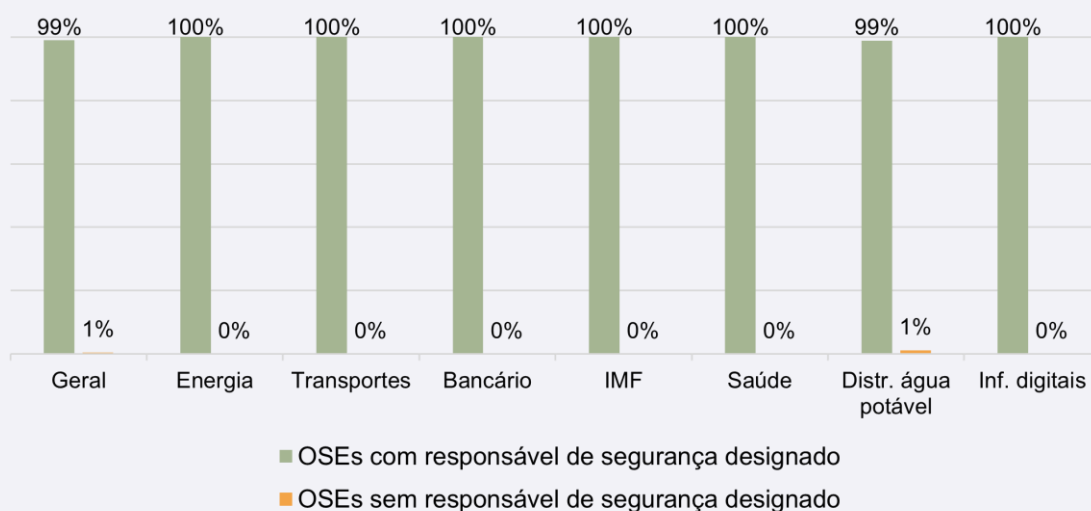
98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado. Verificam-se exceções no setor do fornecimento e distribuição de água potável e no setor das infraestruturas digitais. Em cada um destes setores, houve uma entidade inquirida que ainda não tinha nomeado o contacto permanente.

Gráfico 89 - Designação do contacto permanente



A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No entanto, houve ainda alguns operadores que tiveram de recorrer à contratualização externa do serviço de contacto permanente, com particular destaque para os setores da energia, distribuição e fornecimento de água potável e das infraestruturas digitais, nos quais a percentagem de operadores que necessitou de contratualizar o serviço foi acima de 17%. É de salientar, também, o setor das infraestruturas do mercado financeiro, no qual todos os inquiridos nomearam o contacto permanente a partir dos recursos humanos disponíveis.

Gráfico 90 - Designação do responsável de segurança



Tal como no requisito da nomeação do contacto permanente, também o requisito de ter designado um responsável de segurança é amplamente cumprido pelos OSE. Entre todos os inquiridos, apenas no setor do fornecimento e distribuição de água potável se verificou um operador que ainda não tinha designado o seu responsável de segurança. Todos os outros encontram-se em conformidade com a exigência do decreto-lei n.º 65/2021.

Gráfico 91 - Critérios utilizados para a designação do responsável de segurança

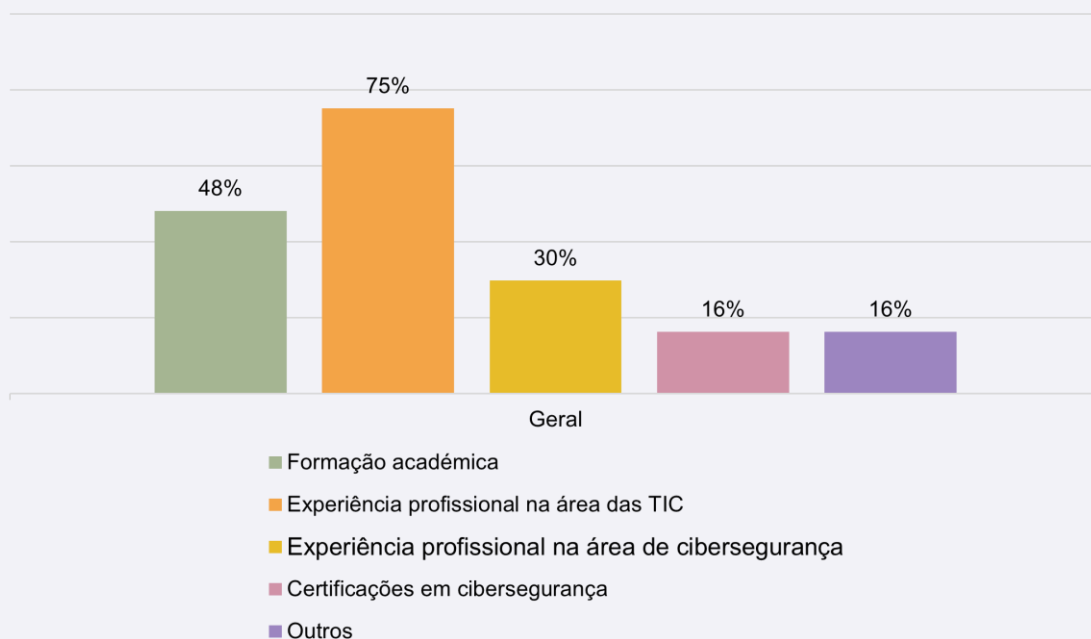


Gráfico 91.1 - Critérios utilizados para a designação do responsável de segurança

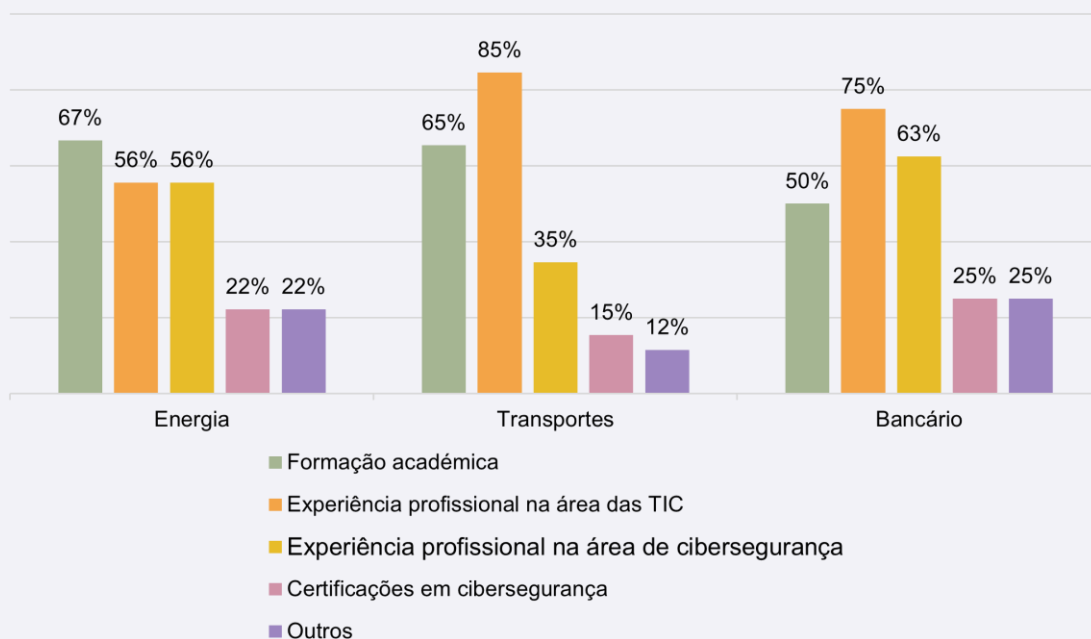


Gráfico 91.2 - Critérios utilizados para a designação do responsável de segurança

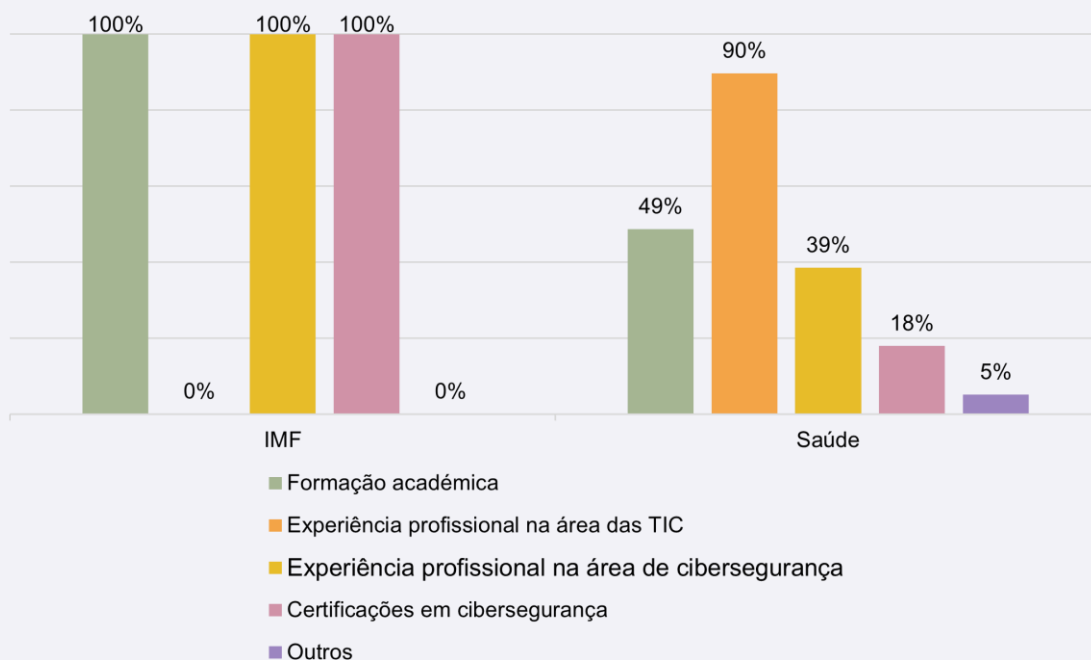
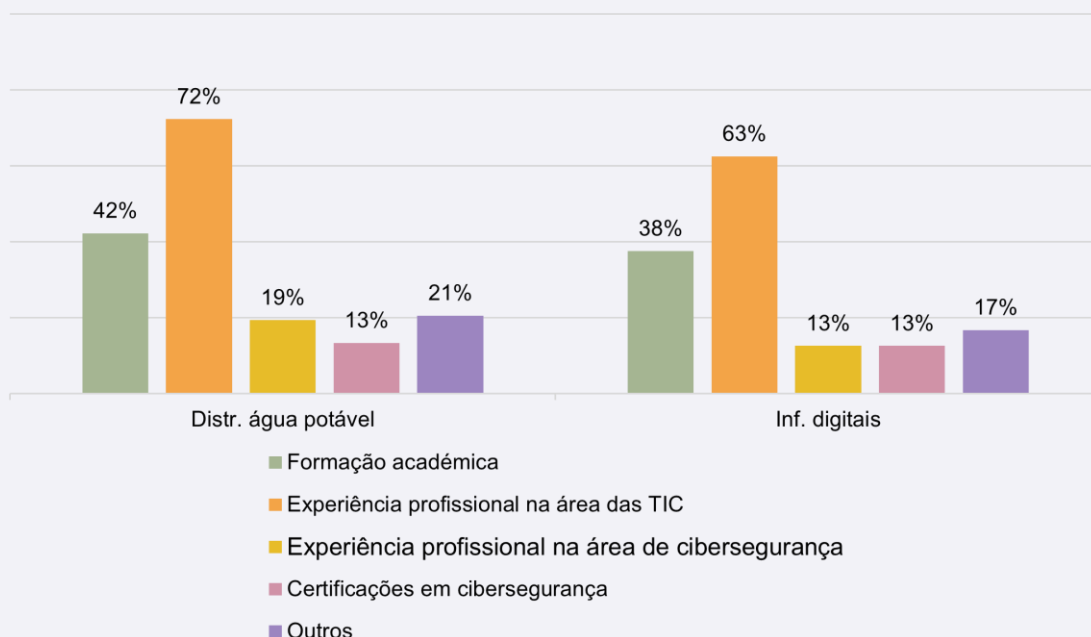


Gráfico 91.3 - Critérios utilizados para a designação do responsável de segurança



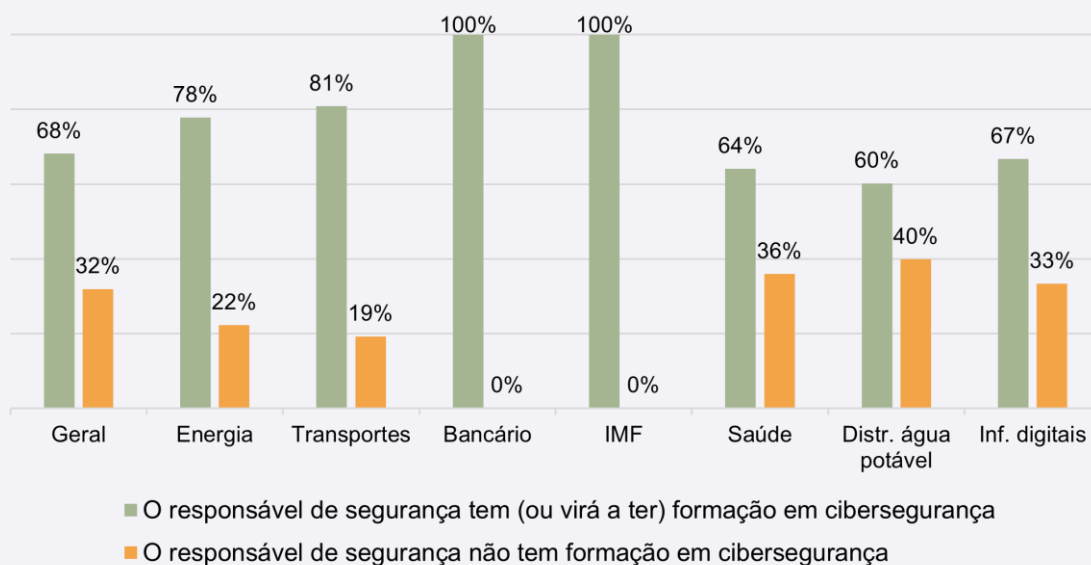
A formação académica e a experiência profissional na área das TIC e na área de cibersegurança foram os critérios mais importantes para a designação do responsável de segurança dos operadores. Na generalidade, a experiência profissional nas TIC foi um critério em 75% dos casos, a formação académica foi um critério em 43% dos casos e a experiência profissional em cibersegurança foi também critério em 30% dos casos. Aliás, no setor das infraestruturas do mercado financeiro, estes três critérios foram os únicos a ser aplicados, e foram aplicados por todos os operadores do setor.

Nos restantes setores, embora tenham sido tidos em conta outros critérios, como as certificações em cibersegurança e outros como a capacidade de liderança ou o conhecimento da organização, estes, também, foram os principais critérios usados.

Verifica-se, contudo, duas exceções, o setor da energia e infraestruturas do mercado financeiro, nestes setores o critério mais aplicado foi a formação académica, ao contrário do que é possível observar nos outros setores.

É também importante referir que se verificaram casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de câmara, com o caso de serviços municipalizados.

Gráfico 92 - Formação específica de cibersegurança do responsável de segurança

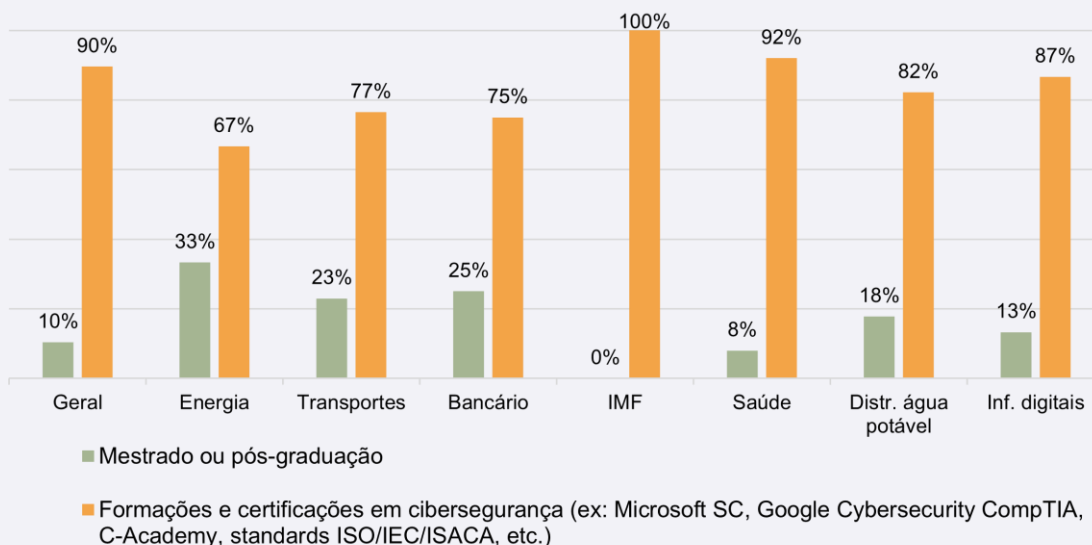


Em cerca de 70% dos casos, o responsável de segurança tem ou virá a ter formação específica em cibersegurança. Nos setores bancário e das infraestruturas do mercado financeiro, todos os responsáveis de segurança designados têm ou virão a ter formação nesta área.

Os setores onde mais se verificam operadores cujo responsável de segurança não tem formação em cibersegurança são os setores da saúde, do fornecimento e distribuição de água potável e das infraestruturas digitais, nos quais mais de 30% dos responsáveis de segurança não têm formação em cibersegurança, nem está planeado que venham a ter proximamente.

Nos setores da energia e dos transportes, a maioria dos operadores refere que o responsável de segurança tem (ou virá a ter) formação em cibersegurança.

Gráfico 93 - Tipo de formação específica em cibersegurança



As formações e certificações em cibersegurança, tais como as formações *Microsoft Security Certifications*, *Google Cybersecurity*, *CompTIA*, da *C-Academy* do CNCS e em normas internacionais como a ISO/IEC 27001 são visivelmente mais comuns entre os responsáveis de segurança do que as formações universitárias como mestrados ou pós-graduações em cibersegurança. Cerca de 90% dos responsáveis de segurança tem uma mais das formações do primeiro tipo.

O setor onde se verifica mais responsáveis de segurança com o grau de mestre ou de pós-graduado é o da energia, com mais de 30% dos responsáveis a terem este nível de qualificação.

Nos restantes setores, essa percentagem não ultrapassa os 30%, embora nos setores dos transportes e da banca os responsáveis de segurança com mestrado ou pós-graduação em cibersegurança se estabeleçam acima dos 20%. De referir que no setor das infraestruturas do mercado financeiro, registam-se responsáveis de segurança somente com formações e certificações, sem mestrados ou pós-graduações.

Gráfico 94 - Motivos pelos quais o responsável de segurança não tem formação específica em cibersegurança



Gráfico 94.1 - Motivos pelos quais o responsável de segurança não tem formação específica em cibersegurança

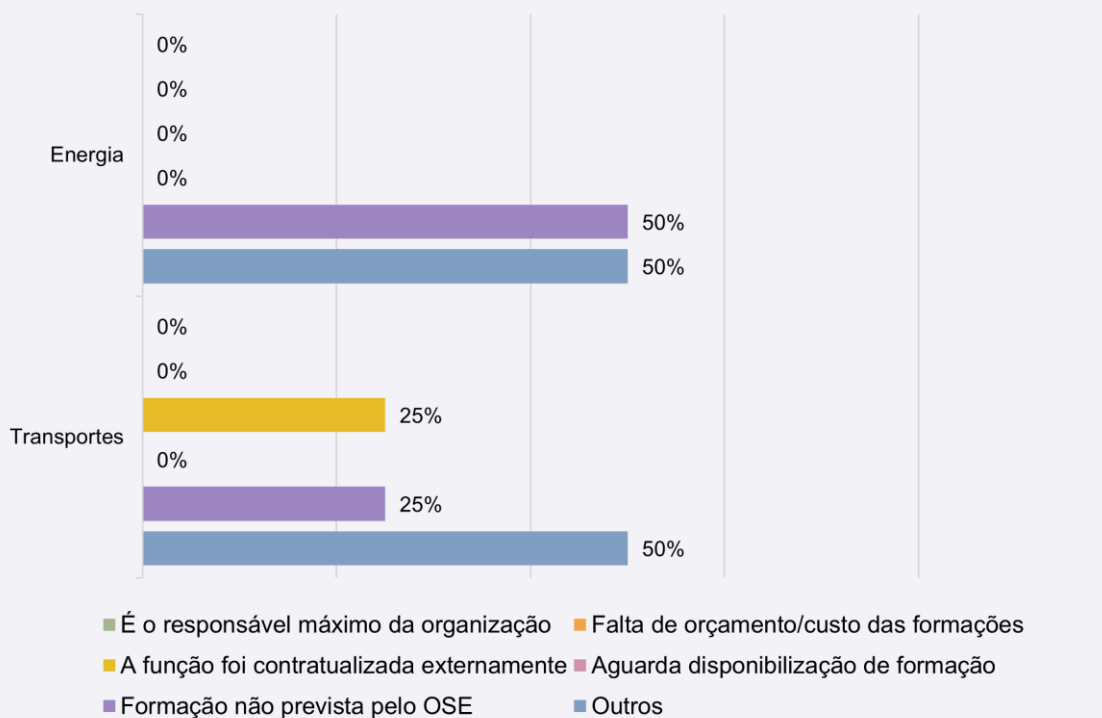
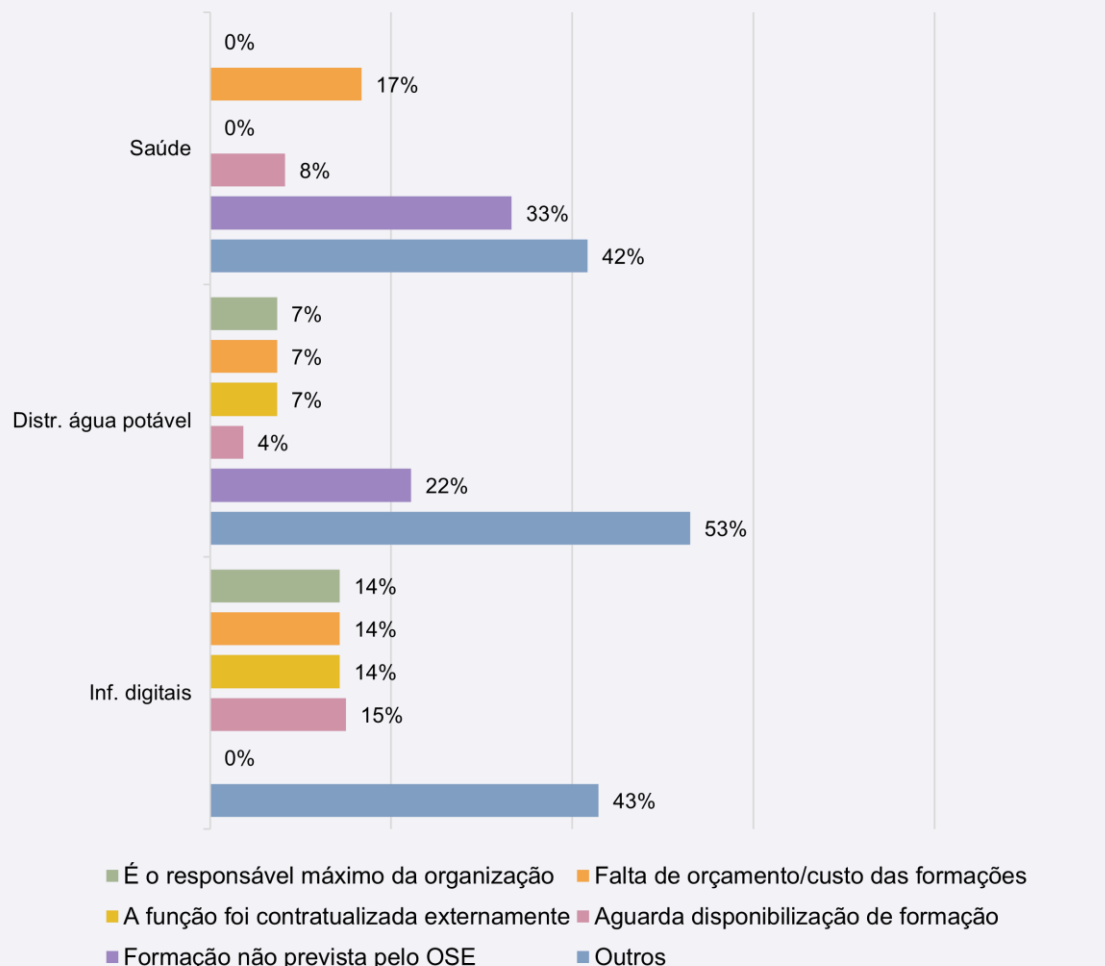


Gráfico 94.2 - Motivos pelos quais o responsável de segurança não tem formação específica em cibersegurança



Os motivos pelos quais um responsável de segurança de um operador não tem formação específica em cibersegurança são diversificados. Na generalidade, o motivo mais vezes observado, em cerca de 40% dos operadores onde o responsável não tem formação na área, é o facto de essa formação não estar prevista pelo OSE.

Em segundo lugar, surge a resposta “outros”, dada por cerca de 30% dos OSE onde o responsável de segurança não tem formação em cibersegurança. Entre esses “outros” motivos, encontram-se explicações tais como a falta de oportunidade ou disponibilidade de realizar a formação; tentativas de incluir formação interna apesar de o serviço ser prestado externamente, mas sem sucesso até ao momento do estudo; o objetivo da nomeação do responsável de segurança ter sido apenas cumprir o decreto-lei; ter-se simplesmente nomeado o responsável pela informática e ainda o facto de pedidos de formação terem sido recusados a nível superior.

Tal como já referido, houve também situações em que a nomeação do responsável de segurança pouco teve que ver com a formação ou conhecimento em cibersegurança da pessoa nomeada, tendo em cerca de 10% dos casos sido nomeado o responsável máximo da organização. A falta de orçamento foi indicada também em cerca de 10% dos casos, tendo maior expressividade (cerca de 25%) apenas no setor dos transportes. A justificação que recai sobre a função ter sido contratualizada externamente surge também em 10% dos casos.

O motivo menos frequente foi a espera pela disponibilização da formação, indicado em menos de 5% dos casos.

No setor da energia, a principal motivação para que o responsável de segurança não tenha formação específica em cibersegurança é maioritariamente o facto de a formação não estar prevista ou ainda estarem a analisar a possibilidade de integrar um CISO.

No setor dos transportes, as principais motivações para que o responsável de segurança não tenha formação específica em cibersegurança são os critérios da equipa de recursos humanos e o facto de a informática estar integrada numa unidade orgânica que abrange diversas temáticas. Para além destas, também o facto de a função estar a ser contratualizada externamente e a formação não estar prevista pelos operadores.

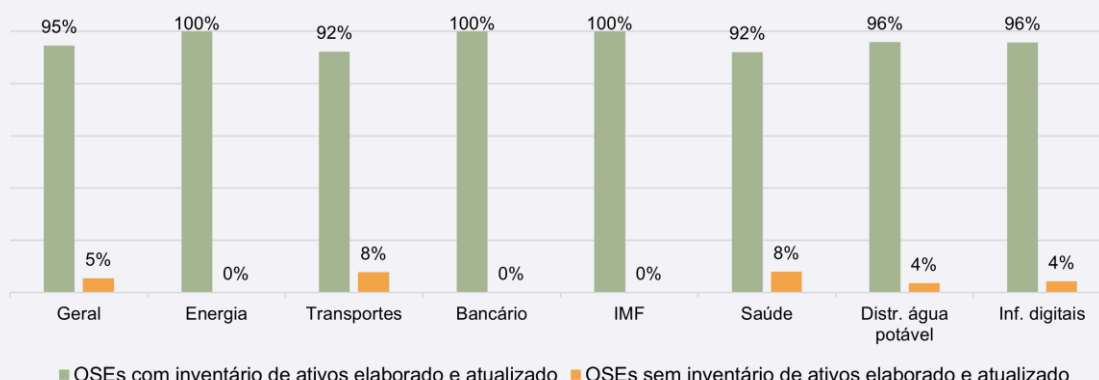
No setor da saúde, as principais motivações para que o responsável de segurança não tenha formação específica em cibersegurança são o facto de já ter completado as formações necessárias, estar em fase de recrutamento, a formação não estar prevista, falta de orçamento /custo das formações e aguardam disponibilização de formação.

No setor da distribuição e fornecimento de água potável, as principais motivações para que o responsável de segurança não tenha formação específica em cibersegurança são: o facto de não existir nenhum plano de formação nesta área em específico, o facto de não estar previsto, estar já agendada, o facto de ser o responsável máximo da organização, falta de orçamento/custo das formações e o facto de a função ter sido contratualizada externamente.

No setor das infraestruturas digitais as motivações para que o responsável de segurança não tenha formação específica em cibersegurança estão bastante divididas. Essas motivações incluem o facto de o responsável de segurança ser o responsável máximo da organização ou a falta de orçamento/custo.

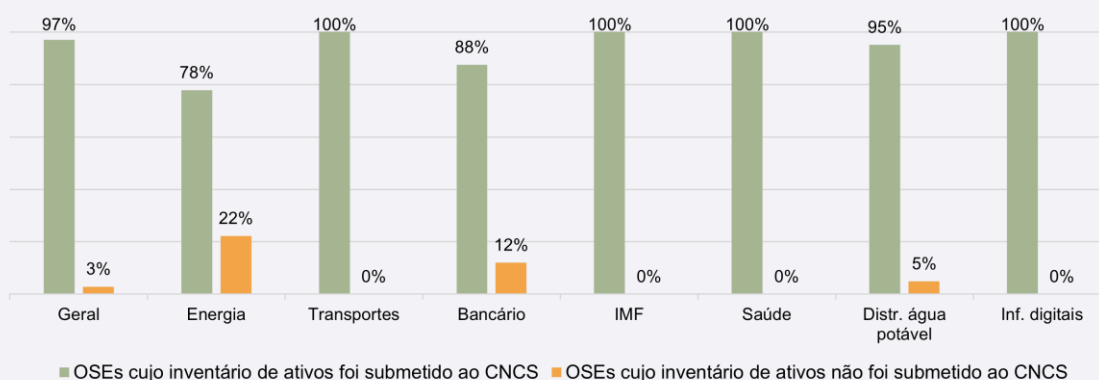
Tal como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado “Compromisso C-Academy” que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança dos setores que não têm formação em cibersegurança obter a mesma. Entre os principais benefícios do programa contam-se: “Reconhecimento público pela promoção da cibersegurança”, “Aumento da resiliência e da capacidade de resposta a ataques”, “Acesso a conteúdos formativos de elevada qualidade” e “Reforço da cibersegurança da organização, setor ou região (para os casos de parceiros setoriais ou regionais)”.

Gráfico 95 - Inventário de ativos essenciais elaborado e atualizado



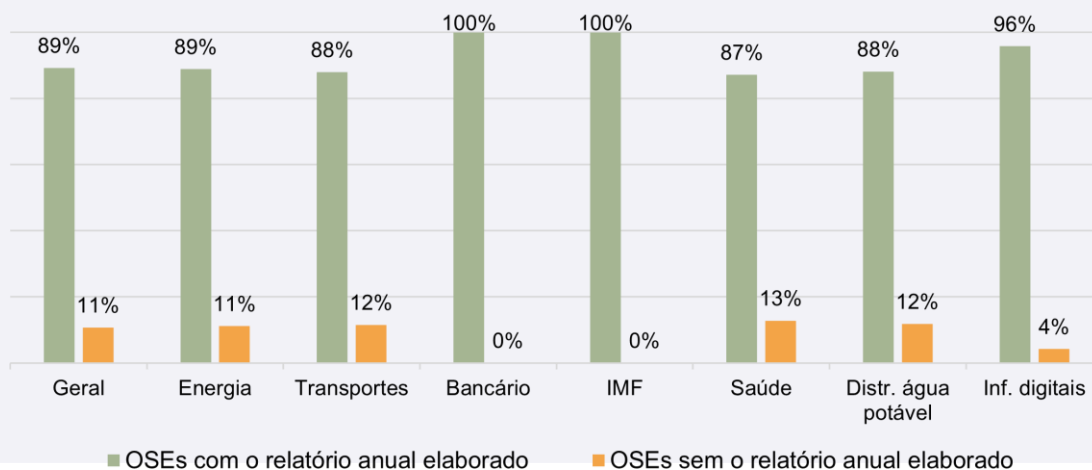
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. Destacam-se os setores da energia, o bancário e o setor das infraestruturas do mercado financeiro, nos quais todos os operadores têm o seu inventário elaborado e atualizado. Verificam-se exceções nos setores dos transportes, da saúde, do fornecimento e distribuição de água potável e no das infraestruturas digitais, mas em qualquer um destes setores a percentagem de operadores cujo inventário de ativos essenciais não está elaborado e atualizado é inferior a 10%.

Gráfico 96 - Submissão do inventário de ativos ao CNCS



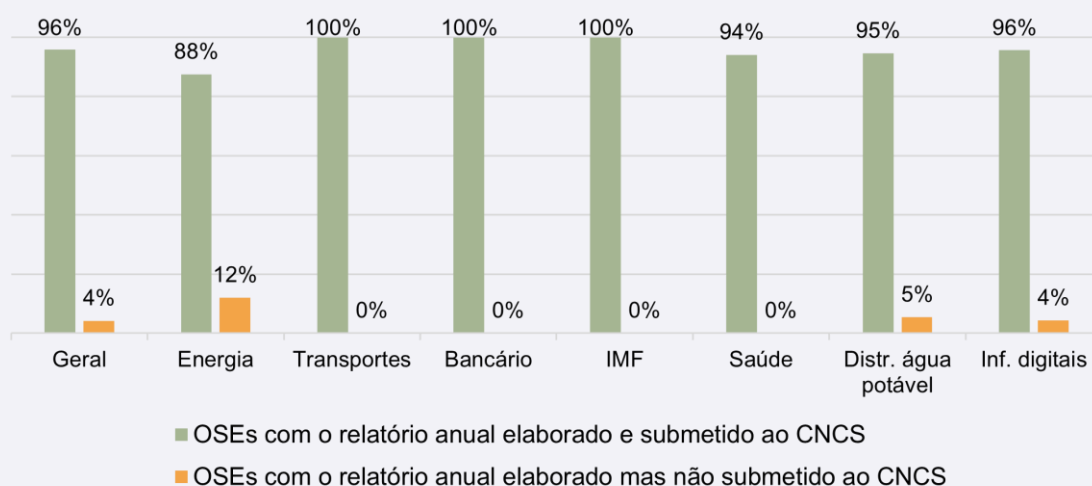
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. Destacam-se os setores dos transportes, das infraestruturas do mercado financeiro, da saúde e das infraestruturas digitais, nos quais todos os operadores com inventário de ativos elaborado efetuaram a submissão do mesmo. As exceções são observadas no setor da energia (o único em que se ultrapassam os 20% de operadores que não submeteram o inventário), o setor bancário (com 12% a não ter submetido o inventário) e o setor do fornecimento e distribuição de água potável (aproximadamente 5% dos operadores não submeteram o inventário).

Gráfico 97 - Elaboração do relatório anual previsto pelo decreto-lei n.º 65/2021, de 30 de julho



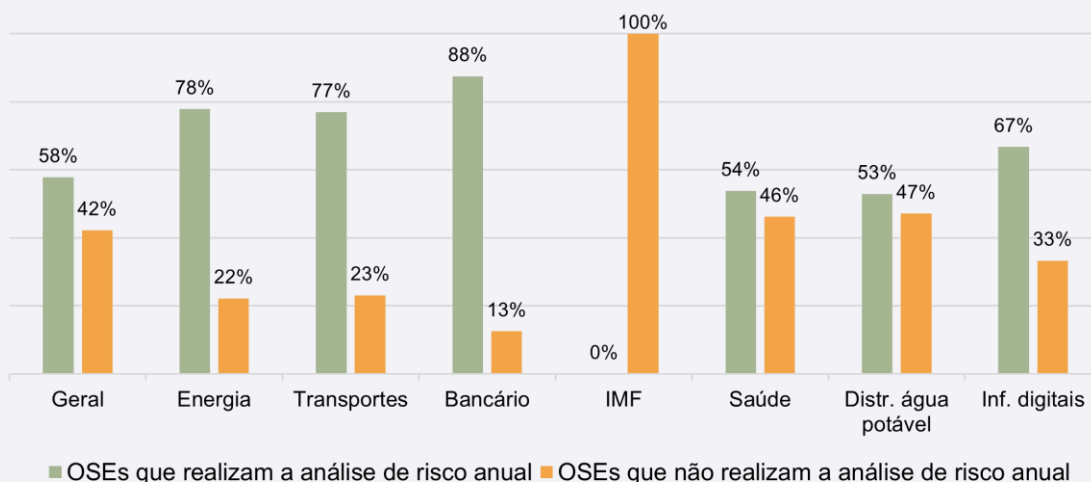
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. Os setores bancário e das infraestruturas do mercado financeiro são os únicos onde a totalidade dos operadores refere ter elaborado o relatório anual. Nos restantes setores, a percentagem de operadores que não elaborou o relatório anual encontra-se entre os 11% e os 13%, com exceção do setor das infraestruturas digitais, onde essa percentagem se fica pelos 4%.

Gráfico 98 - Submissão do relatório anual ao CNCS



Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 97% submeteram-no ao CNCS. Destacam-se os setores dos transportes, bancário e das infraestruturas do mercado financeiro, nos quais todos os operadores com relatório elaborado submeteram o mesmo ao CNCS. Os casos em que tal não se verificou, ou seja, em que o relatório foi elaborado, mas não submetido, ocorreram em operadores do setor energético (12,5%), do setor da saúde (6%), do fornecimento e distribuição de água potável (5%) e das infraestruturas digitais (4%).

Gráfico 99 - Realização de análise de riscos anual no âmbito de cibersegurança



A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter carácter obrigatório, cerca de 42% dos operadores não a realizam. Os setores nos quais maior percentagem dos operadores realiza esta análise são os da energia (78%), o dos transportes (77%), o setor bancário (88%) e o das infraestruturas digitais (67%). No setor da saúde e no setor do fornecimento e distribuição de água potável, a percentagem de operadores que efetua a análise de risco fica aquém dos 60%, fixando-se nos 54% para a saúde e nos 53% para o fornecimento e distribuição de água potável. Já no caso do setor das infraestruturas do mercado financeiro, no qual se tinha vindo a observar ampla conformidade com as obrigações decorrentes do decreto-lei, surpreende que nenhum dos inquiridos tenha referido realizar a análise de risco exigida.

Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança

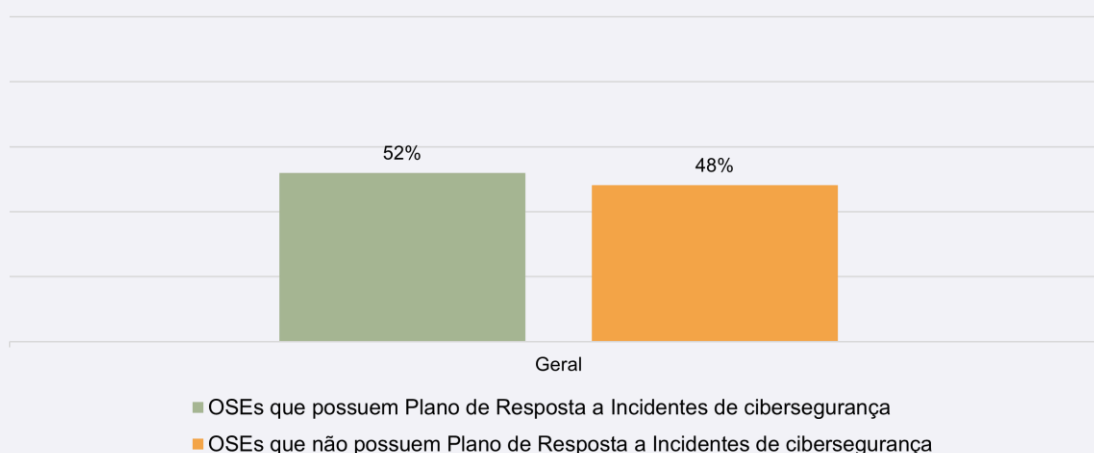
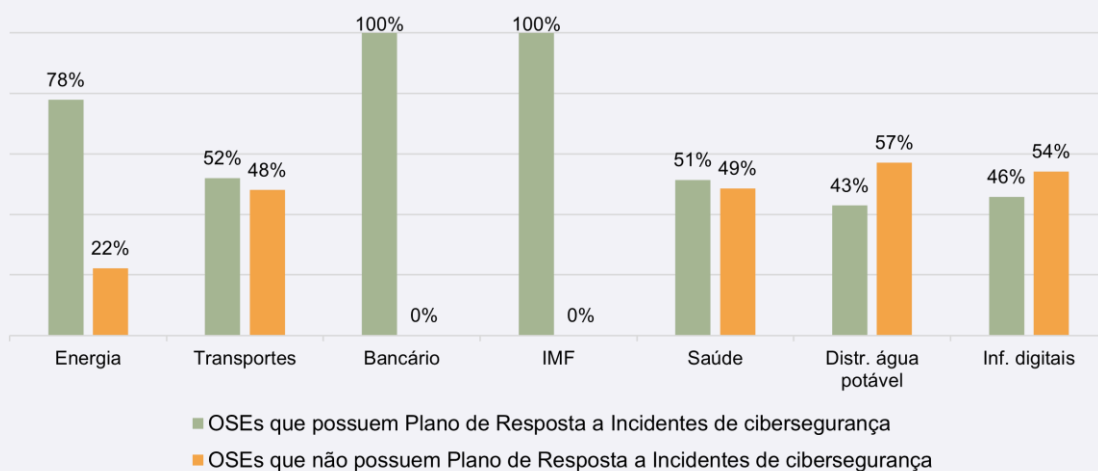
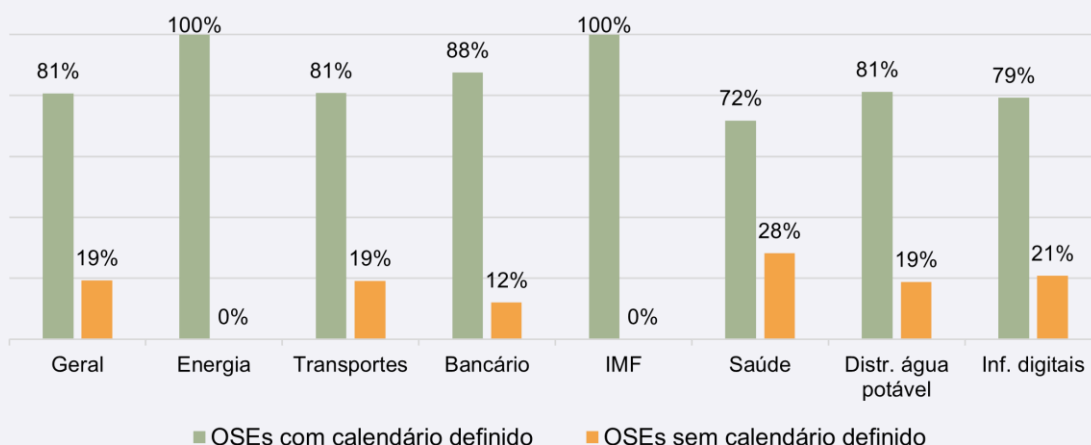


Gráfico 100.1 - Plano de Resposta a Incidentes de Cibersegurança



Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. Novamente, destacam-se os setores bancário e das infraestruturas do mercado financeiro, nos quais todos os inquiridos indicam possuir esse plano. O setor da energia apresenta o segundo resultado mais elevado, atingindo os 78%. Depois destes, só nos setores dos transportes e da saúde se verificam mais de 50% dos operadores com plano de resposta a incidentes. No setor do fornecimento e distribuição de água potável e no setor das infraestruturas digitais, os operadores sem plano de resposta a incidentes superam os operadores com plano, havendo apenas 43% de operadores com plano no setor do fornecimento de água e 46% no setor das infraestruturas digitais.

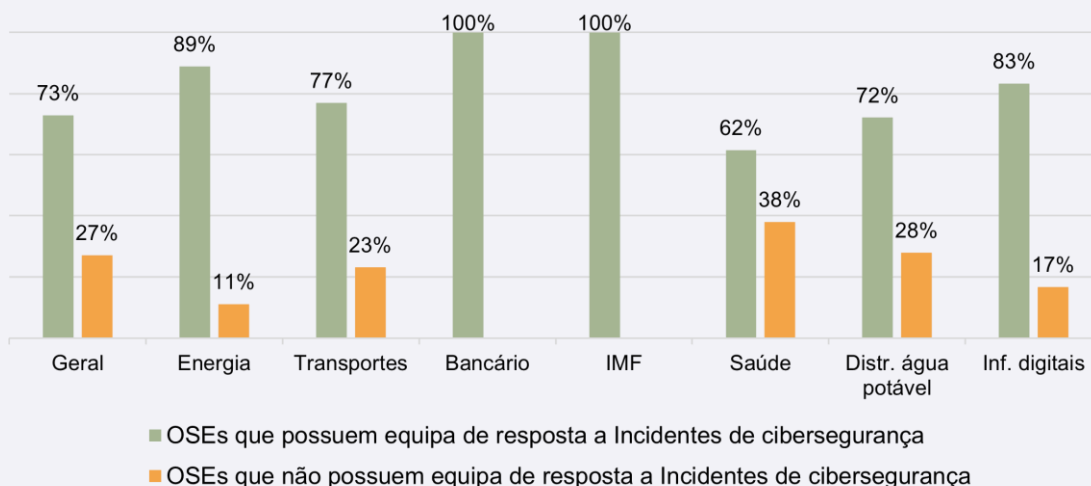
Gráfico 101 - Definição de calendário para cumprimento das obrigações decorrentes do decreto-lei n.º 65/2021, de 30 de julho



A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. No setor da energia e das infraestruturas do mercado financeiro indicam ter tal calendário definido. O setor da saúde é aquele onde maior percentagem de operadores não define esse calendário, atingindo os 28%. Nos restantes setores, essa percentagem não ultrapassa os 20%. Há que salientar ainda que, tal como revelam os gráficos anteriores, mesmo com calendário definido, existem situações em que os

operadores não elaboraram ou submeteram o seu inventário de ativos essenciais ou o seu relatório anual, como, por exemplo, no setor da energia.

Gráfico 102 - Equipa de resposta a incidentes de cibersegurança



A nível geral, 73% dos operadores possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de operadores que possui tal equipa é sempre superior a 60%. Destacam-se os setores bancário e das infraestruturas do mercado financeiro, nos quais todos os operadores inquiridos possuem equipa de resposta a incidentes de cibersegurança. Também os setores da energia e das infraestruturas digitais apresentam elevadas percentagens de operadores com equipas de resposta a incidentes, ambos ultrapassando os 80%. Os operadores dos setores dos transportes e do fornecimento e distribuição de água potável ficam um pouco aquém desse limiar dos 80%, mas ainda acima dos 70%. O setor da saúde é aquele onde menos operadores têm equipa de resposta a incidentes, ficando-se pelos 62%.

Gráfico 103 - Composição da equipa de resposta a incidentes de cibersegurança

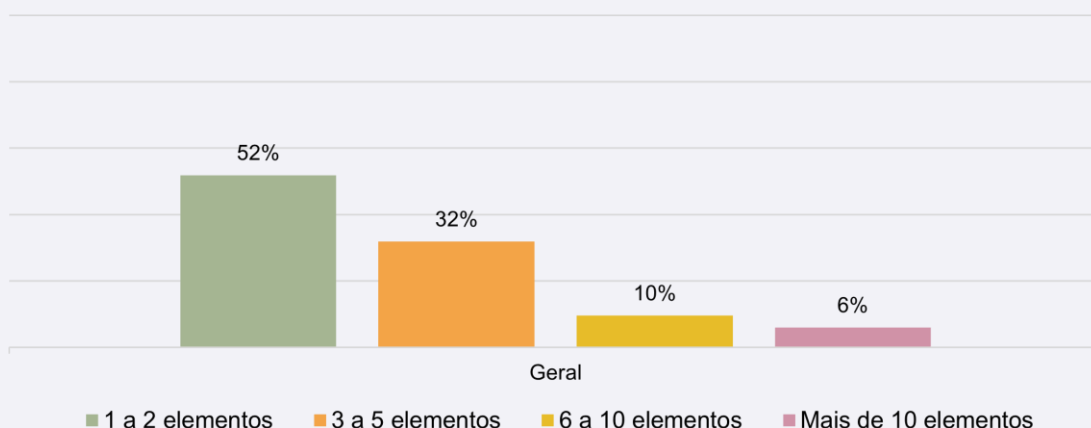


Gráfico 103.1 - Composição da equipa de resposta a incidentes de cibersegurança

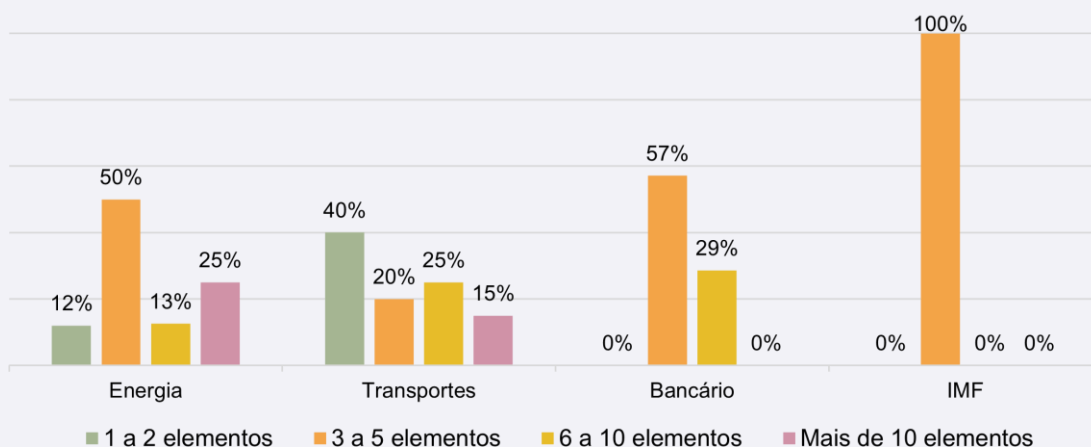
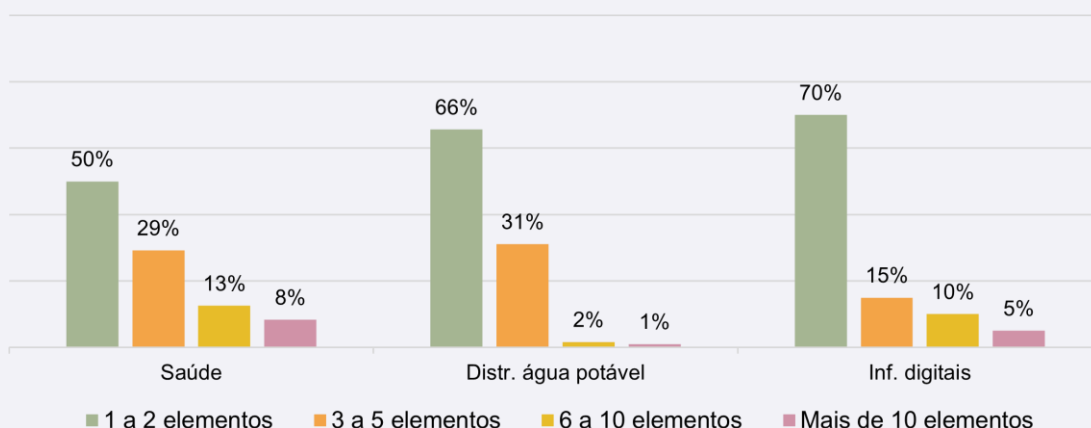


Gráfico 103.2 - Composição da equipa de resposta a incidentes de cibersegurança



Na visão geral, 55% dos operadores com equipa de resposta a incidentes de cibersegurança conta com equipas compostas por 1 a 2 elementos. A nível setorial, a prevalência de equipas de resposta a incidentes com 1 a 2 elementos repete-se nos setores dos transportes (40%), da saúde (50%), do fornecimento e distribuição de água potável (65%) e das infraestruturas digitais (70%). Seguem-se os setores nos quais a maioria das equipas de resposta dos operadores são compostas por 3 a 5 elementos. No setor da energia, essa composição verifica-se em 50% dos operadores com equipa definida, no setor bancário, em 57% e, no setor das infraestruturas do mercado financeiro, em todos os operadores inquiridos. Ressalva-se ainda que embora equipas com 6 ou mais elementos se verifiquem menos vezes, estas chegam a verificar-se em até 40% dos operadores com equipa de resposta a incidentes, sobretudo quando se atenta nos setores da energia, dos transportes e da banca.

Em resumo, a composição das equipas de resposta a incidentes de cibersegurança tende a ser maioritariamente pequena, especialmente nos setores de Distribuição de Água Potável e Infraestruturas Digitais, com uma proporção maior de equipas muito pequenas. No setor da Saúde, observa-se uma maior diversidade no tamanho das equipas.

Gráfico 104 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança

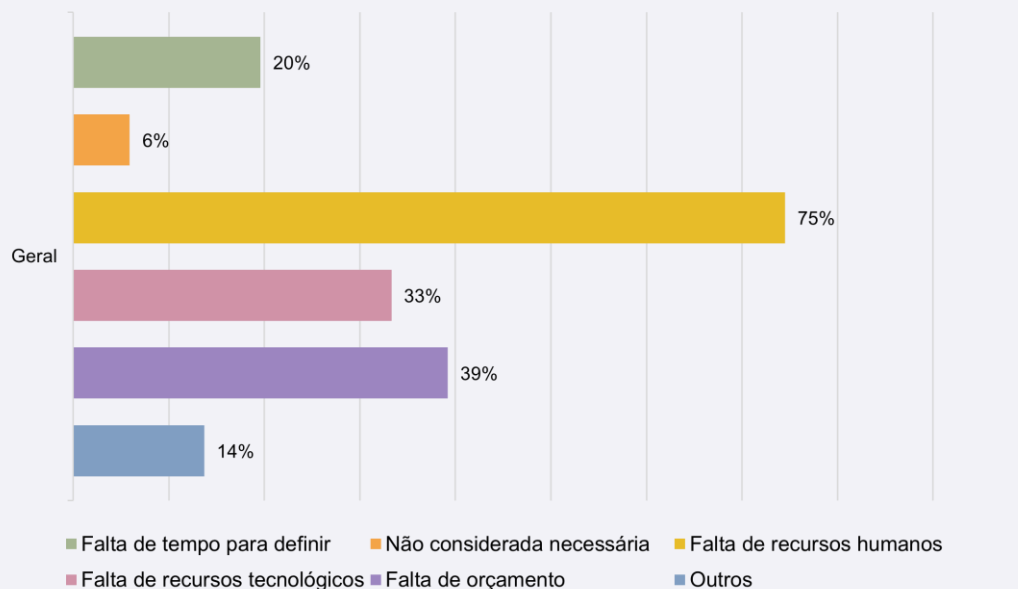


Gráfico 104.1 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança

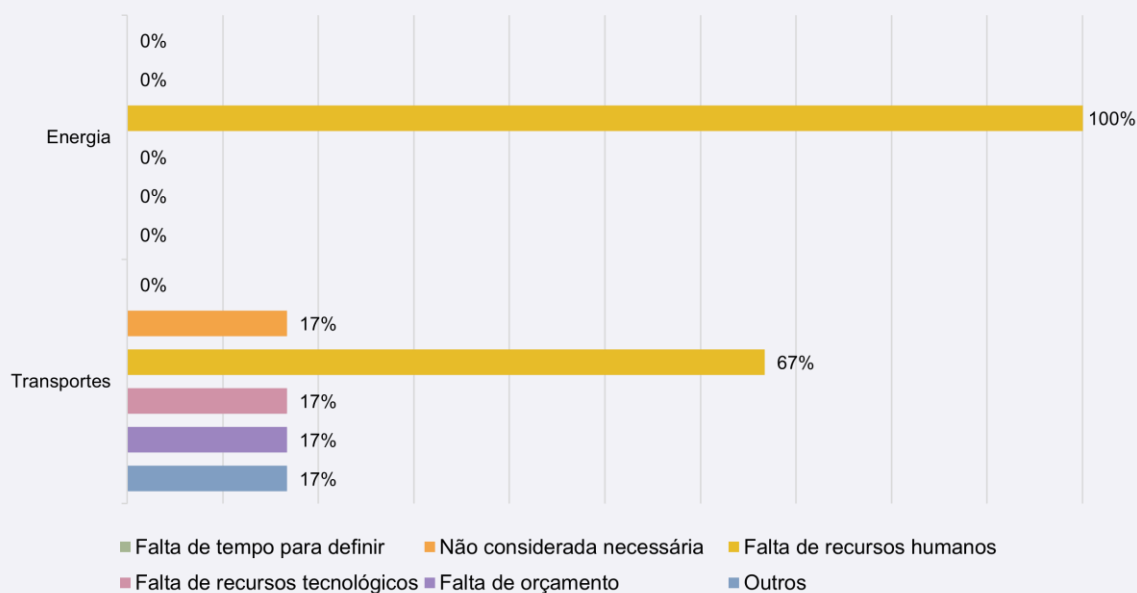
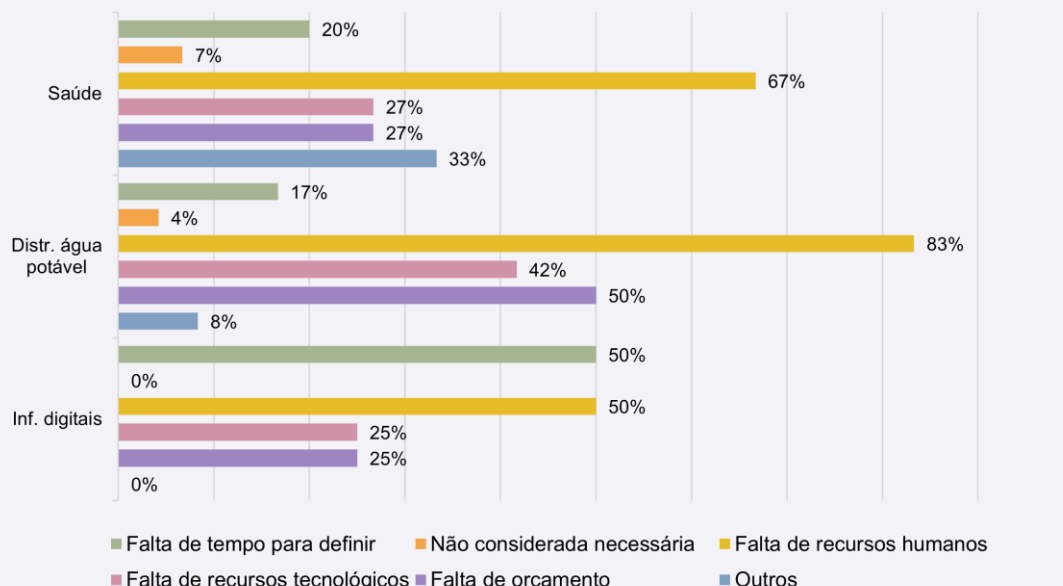
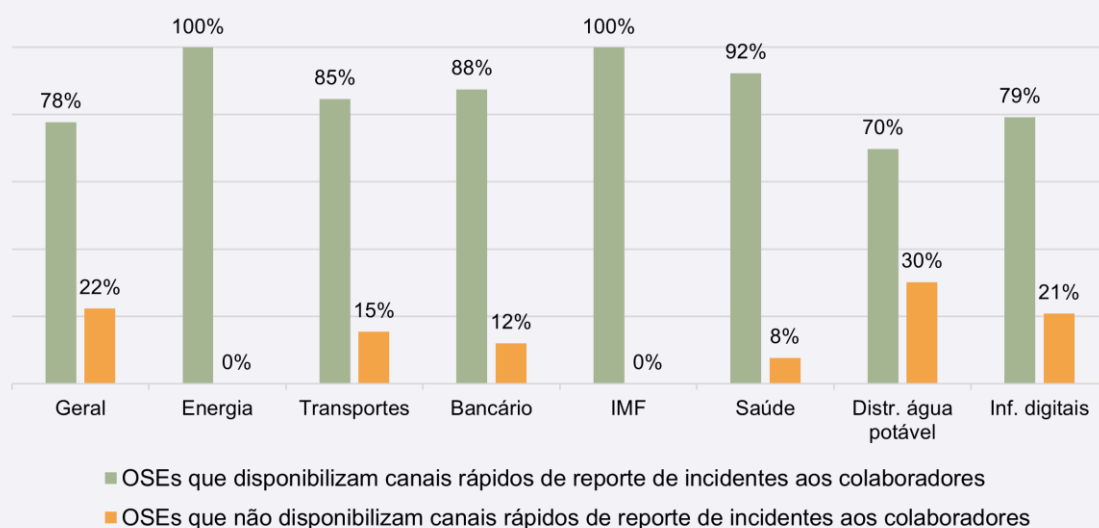


Gráfico 104.2 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança



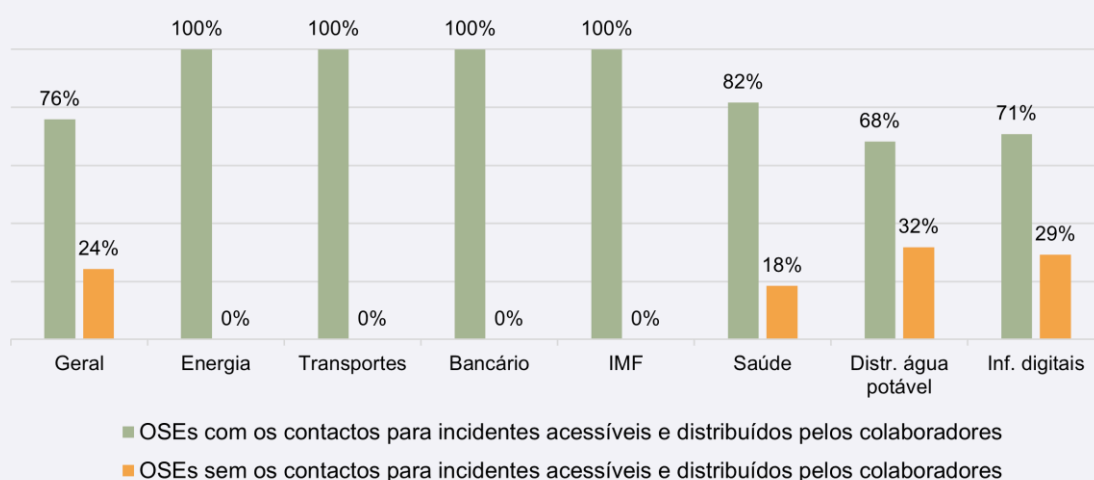
O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. No caso dos operadores do setor da energia, esse é mesmo o único motivo indicado. O único setor onde a escassez de recursos humanos não é o motivo mais apontado entre os restantes é o das infraestruturas digitais, no qual houve tantos operadores a indicar como motivo a escassez de recursos humanos, bem como a indicar a falta de tempo para definir a equipa de resposta a incidentes. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. O setor que mais indica a falta de orçamento como um impedimento para que se possua equipa de resposta a incidentes é o setor do fornecimento e distribuição de água potável, onde este motivo é indicado por 50% dos operadores sem equipa, embora este motivo continue a figurar atrás da falta de recursos humanos. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores sem equipa de resposta a incidentes. Novamente, é no setor do fornecimento e distribuição de água potável que há uma maior percentagem de operadores a indicar este motivo, ultrapassando os 40%. A falta de tempo para definir a equipa surge com menos expressividade, sendo indicada por 20% dos operadores sem equipa, com exceção dos operadores do setor das infraestruturas, como já referido. Os operadores que não consideram necessária uma equipa de resposta a incidentes necessária são, no cômputo geral, menos de 10%, embora no setor dos transportes essa percentagem atinja os 17%. Os operadores que selecionaram a opção “outros” (14%) indicaram motivos tais como estar a ser planeada a criação da equipa, a equipa estar a receber formação, ou mesmo o descuido para com a área de cibersegurança.

Gráfico 105 - Disponibilização aos colaboradores de canais rápidos para reporte de incidentes



No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. Destacam-se os setores da energia e das infraestruturas do mercado financeiro, nos quais todos os operadores inquiridos disponibilizam tais canais aos seus colaboradores. Seguem-se os setores da saúde, com 92%, bancário, com 88%, e dos transportes, com 85%. No setor das infraestruturas digitais, a percentagem de operadores que disponibiliza estes canais rápidos fixa-se nos 79%. O setor onde a menor percentagem de operadores disponibiliza estes canais é o do fornecimento e distribuição de água potável, mas onde, ainda assim, 70% das entidades disponibilizam canais rápidos aos colaboradores.

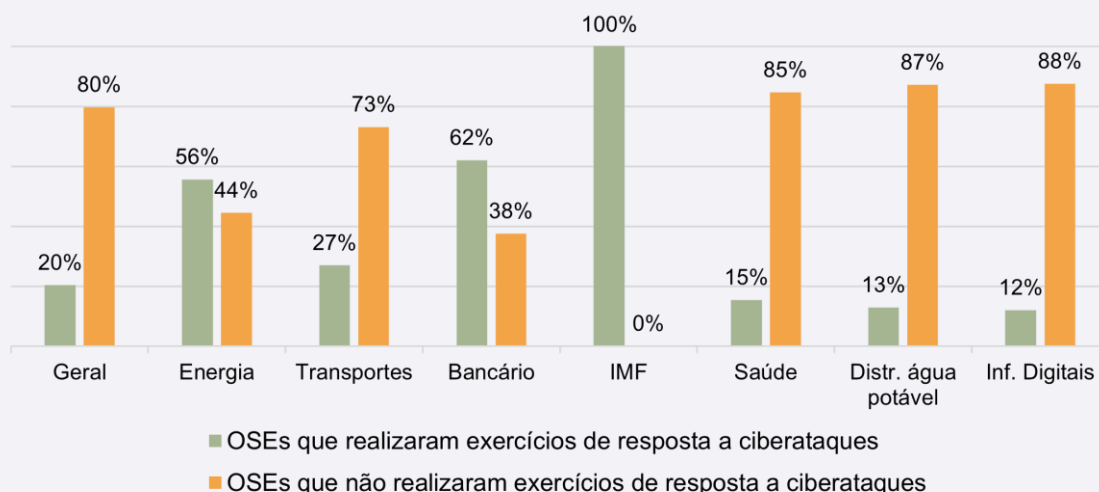
Gráfico 106 - Acessibilidade e distribuição por todos os colaboradores dos contactos a utilizar em caso de incidente de cibersegurança



Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores.

Destacam-se os setores da energia, dos transportes, bancário e das infraestruturas do mercado financeiro, nos quais todos os inquiridos responderam positivamente a esta questão. Seguem-se os setores da saúde, onde 80% dos operadores têm estes contactos distribuídos e acessíveis por todos os colaboradores, o das infraestruturas digitais, com 71%, e, por fim, o do fornecimento e distribuição de água potável, com 68%.

Gráfico 107 - Realização de exercícios de resposta a ciberataques



De acordo com as respostas obtidas, apenas 20% dos operadores inquiridos realizam exercícios de resposta a ciberataques. No entanto, há ainda três setores que se destacam por a maioria dos operadores realizar estes exercícios. Esses setores são o das infraestruturas do mercado financeiro, onde todos os inquiridos indicam realizar exercícios de resposta a ciberataques, o setor bancário, com cerca de 62% dos inquiridos a realizar exercícios, e o setor da energia, com resposta positiva de 56% dos inquiridos. Nos restantes setores, são mais os operadores que não realizam exercícios de resposta do que os que realizam. Entre estes, o setor dos transportes é o único onde ainda mais de 25% realizam tais exercícios. Nos setores da saúde, do fornecimento e distribuição de água potável e das infraestruturas digitais, as percentagens de operadores que realizam estes exercícios variam entre os 12% e os 15%.

Gráfico 108 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança

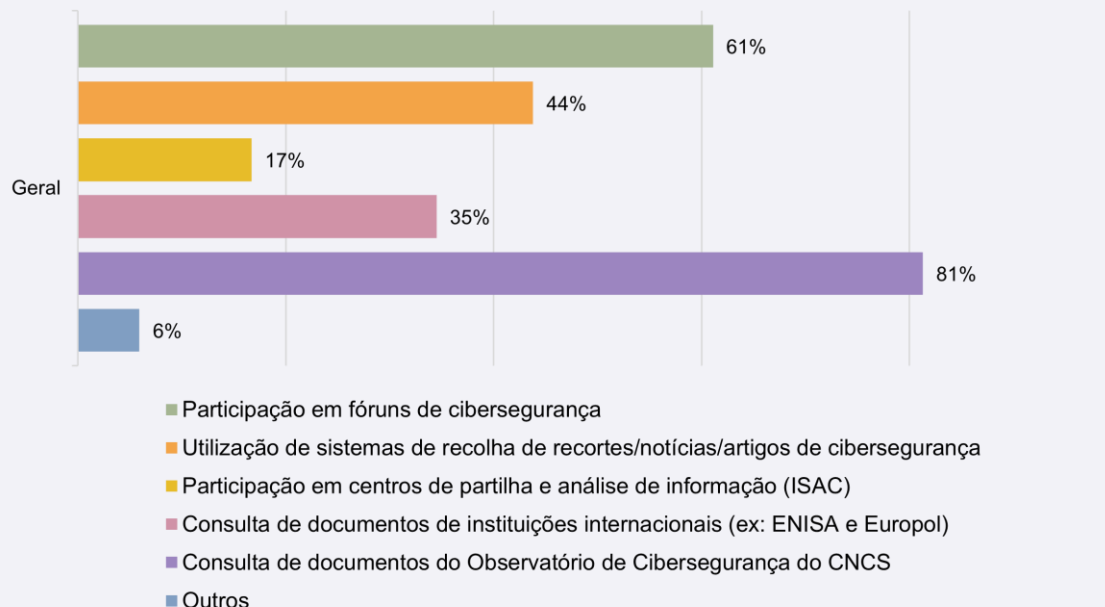


Gráfico 108.1 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança

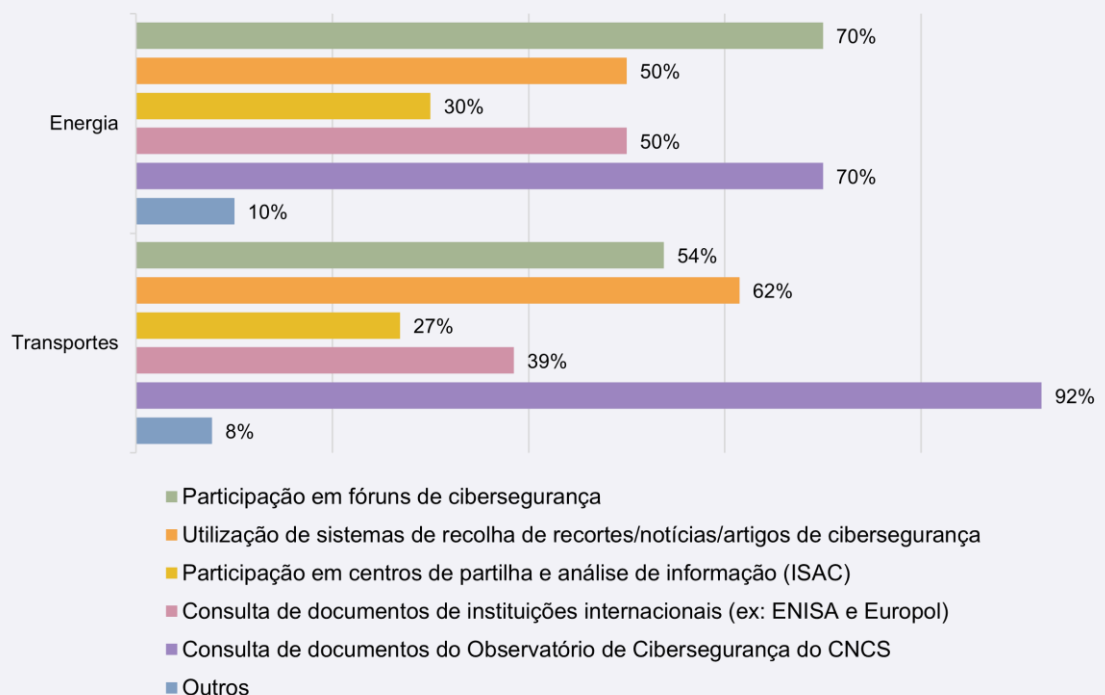


Gráfico 108.2 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança

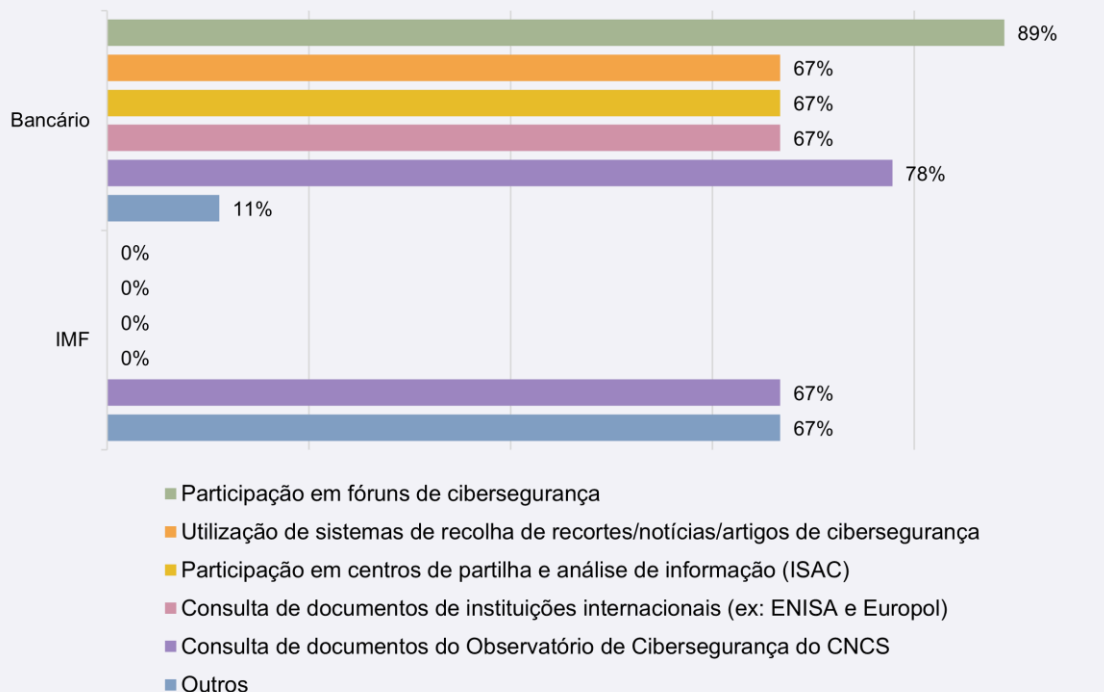


Gráfico 108.3 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança

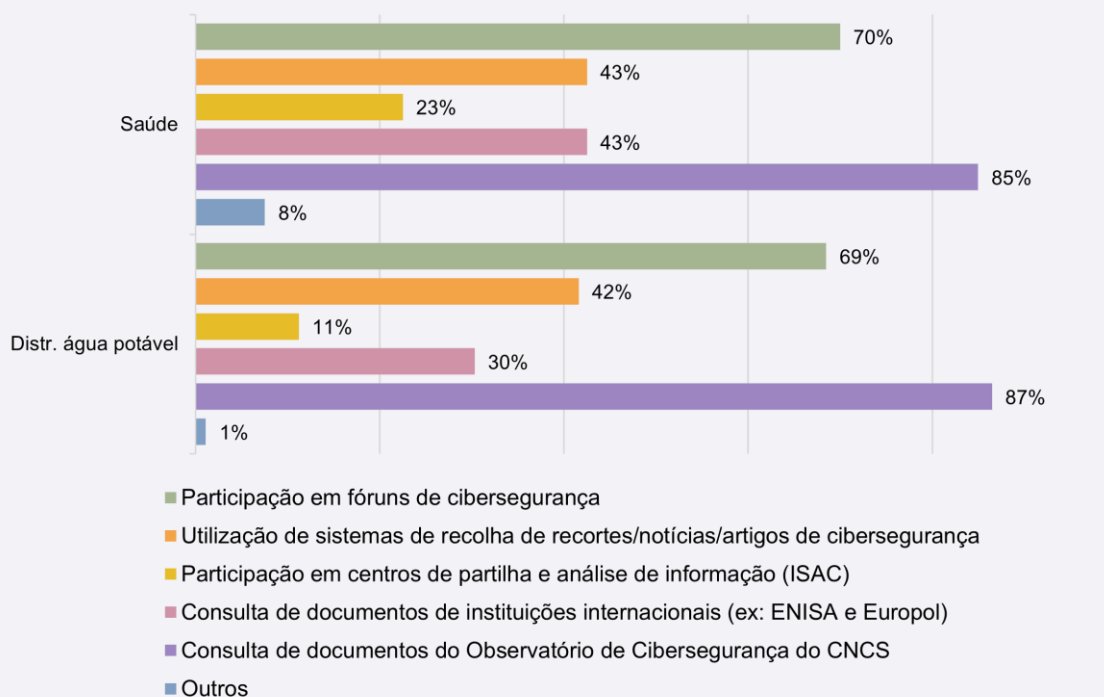
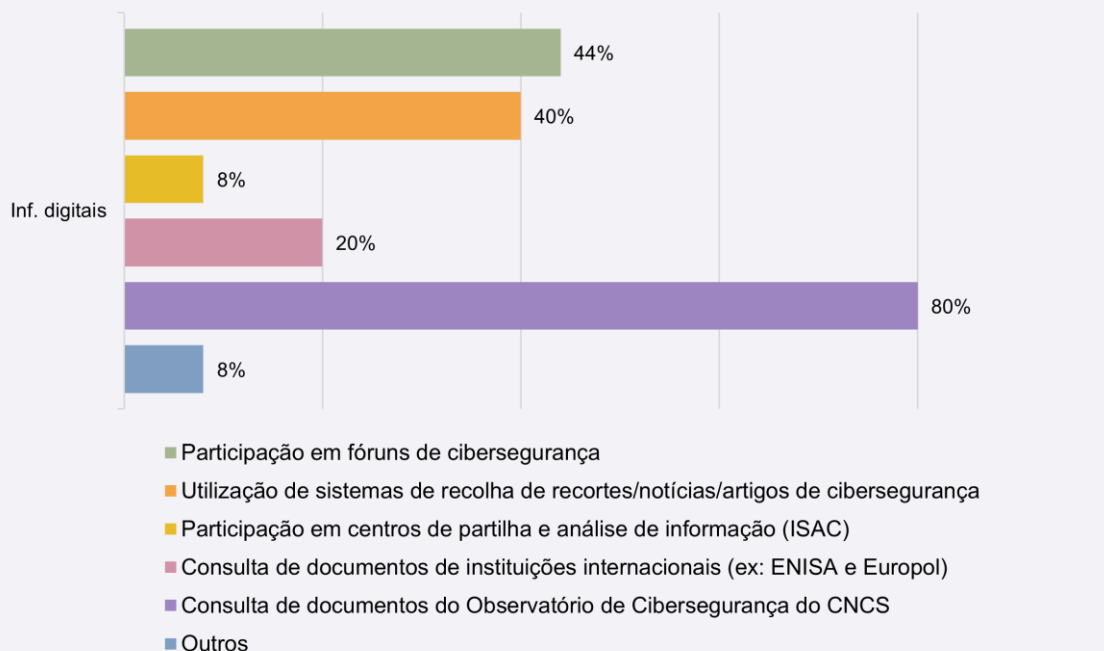


Gráfico 108.4 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança



Independentemente dos métodos utilizados ou das fontes escolhidas para recolher informação sobre boas práticas relativas a riscos e incidentes de cibersegurança, verifica-se que a totalidade dos operadores inquiridos faz essa recolha. Os dois métodos mais comumente utilizados pelos operadores são a consulta de documentos do Observatório de Cibersegurança (cerca de 80%) e a participação em fóruns de cibersegurança (60%). Seguem-se a utilização de sistemas de recolha de notícias e artigos sobre cibersegurança, usada por 44% dos inquiridos, a consulta de documentos de instituições internacionais, como a ENISA e a Europol, praticada por cerca de 35% dos inquiridos. A participação em centros de partilha e análise de informação (ISACs) é a prática menos observada, sendo indicada por apenas 17% dos operadores inquiridos. Estes dados diferem grandemente dos registados pela ENISA, que dão conta de pelo menos 35% dos OSE em Portugal a participarem em ISACs⁵⁵.

Destaca-se o setor bancário por ser aquele que apresenta maior diversificação dos métodos e fontes de recolha de informação utilizados pelos seus operadores. Com este, contrasta o setor das infraestruturas do mercado financeiro, no qual os operadores indicaram utilizar apenas os documentos produzidos pelo Observatório de Cibersegurança e “outros” métodos. Entre esses “outros”, foi mencionado o recurso a uma entidade externa que presta serviços de cibersegurança, nos quais se inclui a recolha deste tipo de informações.

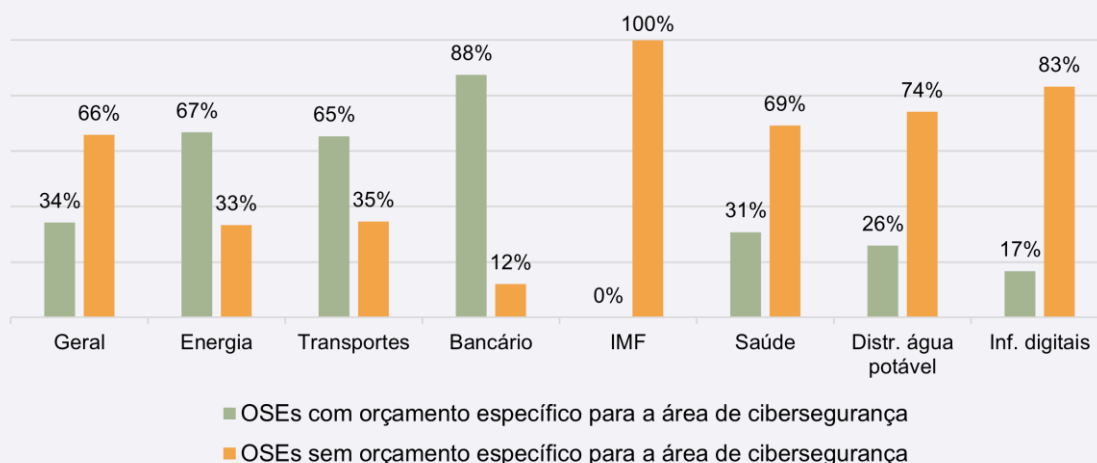
A baixa participação registada nos ISACs merece alguma reflexão. Estes centros de análise e partilha de informação “consistem em parcerias para troca de informação e experiência, assentes no pressuposto de que a partilha consistente de informação e análise de incidentes, ameaças,

⁵⁵ ENISA, “NIS Investments 2023”, 59-61.

tendências e boas práticas favorece a resiliência digital individual e coletiva”⁵⁶. O próprio CNCS dinamiza seis ISACs, nomeadamente nos seguintes setores: energia, águas, portos marítimos; *media*; retalho e distribuição; e saúde. O CNCS dinamiza também um ISAC regional na Região Autónoma dos Açores. Há ainda um outro ISAC do setor financeiro, do qual o CNCS é membro, mas não promotor⁵⁷.

Existem também diversos ISACs de nível europeu - no setor da energia, no setor dos transportes, havendo ISACs específicos para os subsectores do transporte aéreo, ferroviário e marítimo, no setor financeiro, no setor da saúde, no setor do fornecimento e distribuição de água potável, e no setor das infraestruturas digitais⁵⁸. A par destes, existem ainda outros ISACs europeus que não são específicos dos setores em análise, mas que se dedicam à recolha e análise de informações no âmbito dos sistemas de controlo industrial (ICS) e dos sistemas de supervisão e aquisição de dados (SCADA), e até mesmo no âmbito das cidades e órgãos de administração pública nelas presentes. Estes ISACs realizam um extenso trabalho de recolha e análise de informação no domínio da cibersegurança, reunindo os contributos de diversas entidades, produzindo, entre vários documentos, guias úteis a diversos níveis, como o da gestão do risco, do tratamento e resposta a incidentes, da gestão de informações sobre ameaças (*threat intelligence management*)⁵⁹. Estes ISACs acabam também por fazer uma importante articulação entre os vários elementos dos diversos setores e a Comissão Europeia, sobretudo quando esta procura obter a análise e os contributos daqueles a quem nova legislação europeia será aplicável⁶⁰.

Gráfico 109 - Orçamento específico para a área de cibersegurança



Praticamente dois terços dos operadores inquiridos (66%) não possuem orçamento específico para a área de cibersegurança. Contudo, nos setores da energia, dos transportes e no setor bancário são mais os operadores que possuem orçamento específico para essa área do que aqueles que não. No setor bancário, cerca de 88% dos inquiridos possuem esse orçamento.

⁵⁶ CNCS, ISAC, <https://www.cncs.gov.pt/pt/isac/>.

⁵⁷ CNCS, ISAC, <https://www.cncs.gov.pt/pt/isac/>.

⁵⁸ Empowering EU ISACs, “European ISACs”, <https://www.isacs.eu/european-isacs>.

⁵⁹ Exemplos retirados do European Energy Information Sharing & Analysis Centre (EE-ISAC), “Impact”, <https://www.ee-isac.eu/impact/#>.

⁶⁰ Exemplo retirado do EE-ISAC, “Impact”.

Na energia e nos transportes, essas percentagens fixam-se nos 66% e 65%, respetivamente. Nos restantes setores, prevalecem os operadores que não possuem este orçamento. No setor da saúde, têm orçamento cerca de 31% dos operadores. No setor do fornecimento e distribuição de água potável, essa percentagem fixa-se nos 26%. Já no setor das infraestruturas digitais, essa percentagem não ultrapassa os 17%. O setor das infraestruturas do mercado financeiro foi o único onde nenhum dos inquiridos indicou ter orçamento específico para a área de cibersegurança.

O Relatório *NIS Investments* de 2021 foi o último relatório da série da ENISA a analisar a questão de um orçamento específico para a cibersegurança, tendo os últimos dois relatórios, de 2022 e 2023, orientado o seu foco para orçamentos dedicados a riscos terceiros (*third-party risk*) e à formação em cibersegurança, respetivamente. No relatório de 2021, os resultados verificados ao nível da UE são próximos dos obtidos a nível nacional no questionário realizado pelo CNCS: na UE, apenas cerca de 38% dos OSE inquiridos tinham orçamentos dedicados à cibersegurança⁶¹, próximo dos 33% registados pelo CNCS. O mesmo relatório indica que a maioria dos OSE aloca fundos à cibersegurança a partir do orçamento dedicado à parte informática.

Importa também referir que a Diretiva NIS (RJSC) não obriga os OSE a ter orçamentos específicos para cibersegurança. No entanto, um estudo da Comissão Europeia e do Banco Europeu de Investimento (BEI) sobre a criação de uma plataforma de investimento em cibersegurança constatou que as ausências desses orçamentos específicos dificultam grandemente a análise do investimento realizado nesta área. Segundo o mesmo estudo, a própria UE não tinha, no ano de 2022, um orçamento dedicado ao financiamento da sua estratégia de cibersegurança⁶². Este orçamento surgiu apenas em 2023, no âmbito do Programa Europa Digital, com um orçamento global de 1,3 mil milhões de euros, dos quais 375 milhões são dedicados à cibersegurança no biénio 2023-2024⁶³. No âmbito da investigação e inovação, surge também o programa Horizonte Europa, com um orçamento global de 95,5 mil milhões de euros a ser executado entre 2021 e 2027, alocando 1,9 mil milhões de euros neste período à área da cibersegurança⁶⁴.

⁶¹ ENISA, *NIS Investments*, 2021, 7-8.

⁶² Comissão Europeia e Banco Europeu de Investimento, “European Cybersecurity Investment Platform”, 2022, 29.

⁶³ Comissão Europeia, “€1.3 billion from the Digital Europe Programme for Europe’s digital transition and cybersecurity”, <https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity>.

⁶⁴ Conselho Europeu, “Horizonte Europa”, <https://www.consilium.europa.eu/pt/policies/horizon-europa/>.

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

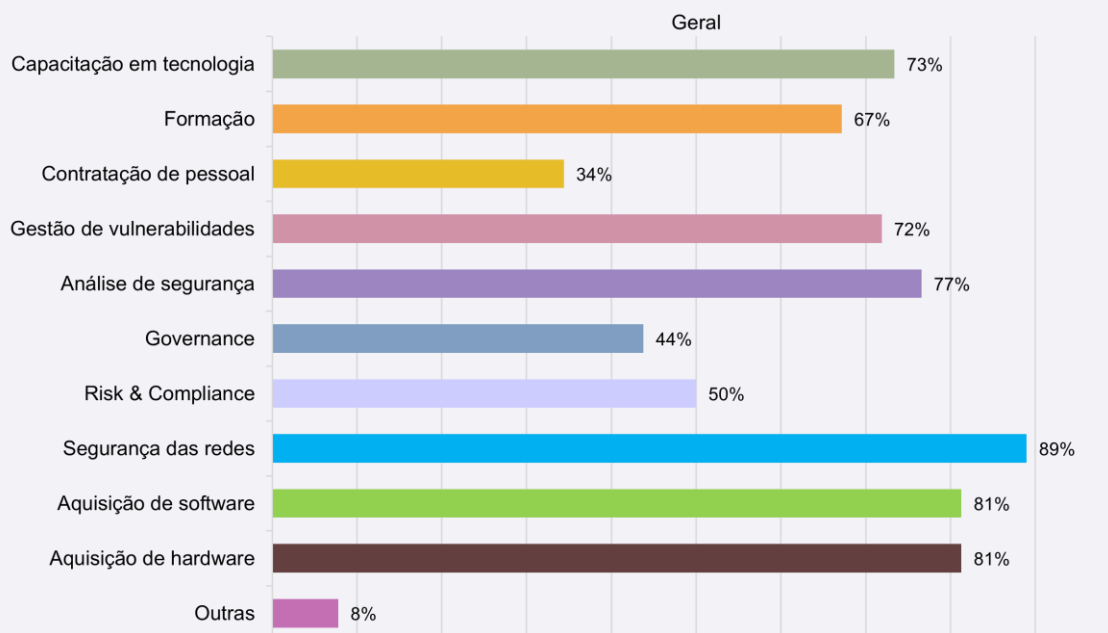


Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança

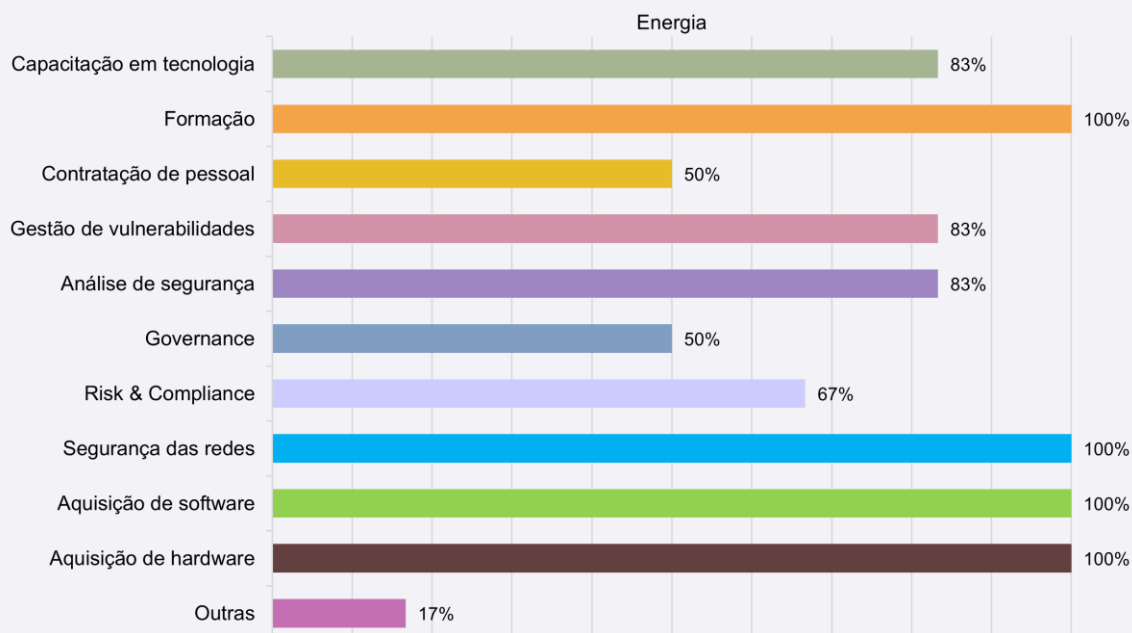


Gráfico 110.2 - Áreas de aplicação dos orçamentos específicos para cibersegurança

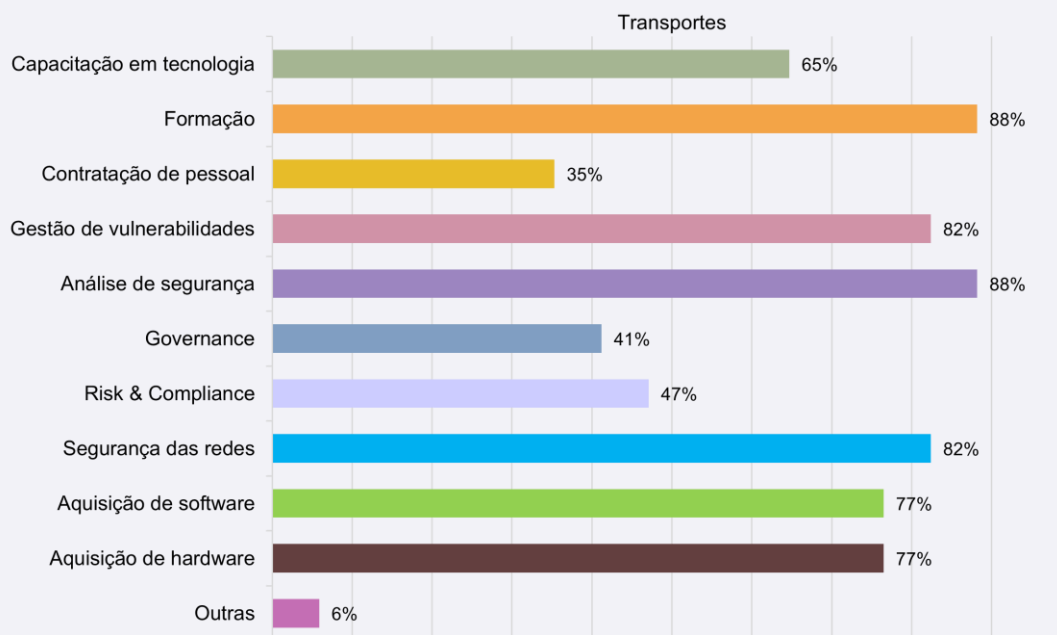


Gráfico 110.3 - Áreas de aplicação dos orçamentos específicos para cibersegurança

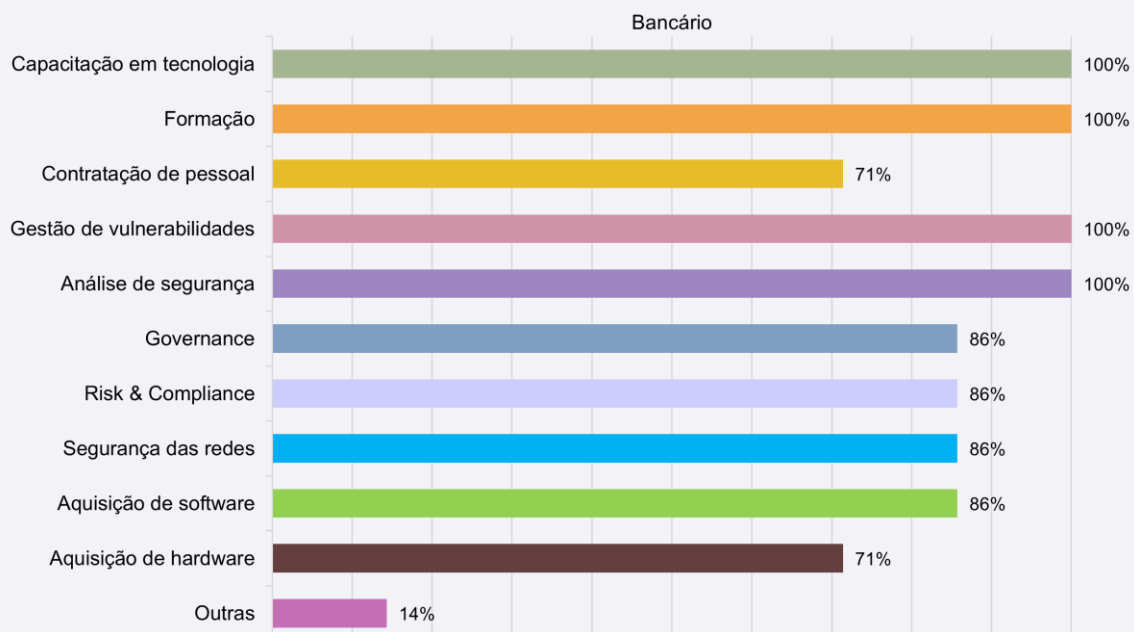


Gráfico 110.4 - Áreas de aplicação dos orçamentos específicos para cibersegurança

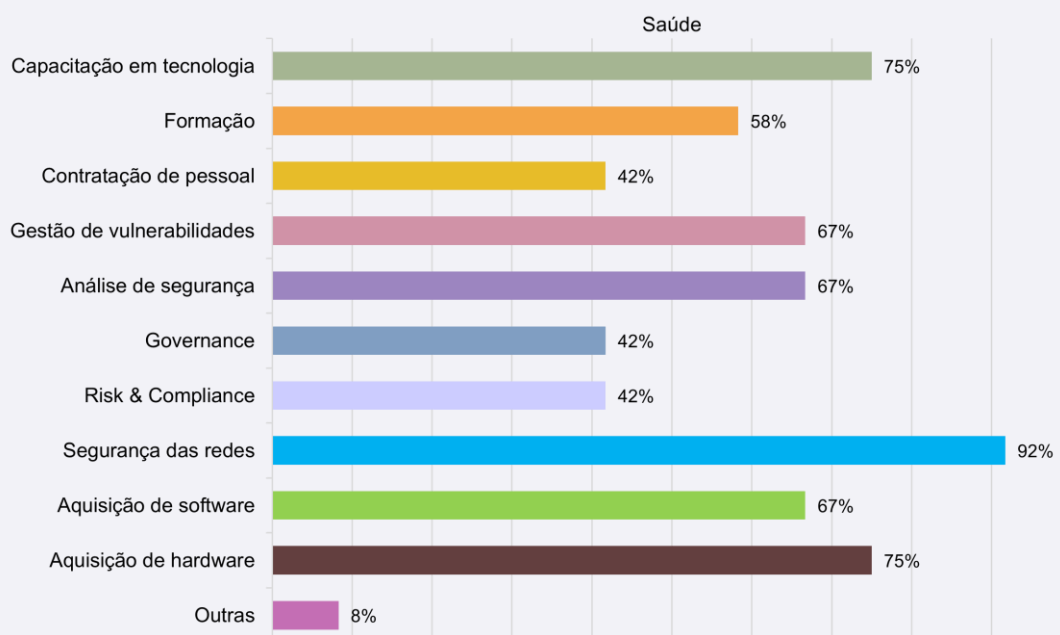


Gráfico 110.5 - Áreas de aplicação dos orçamentos específicos para cibersegurança

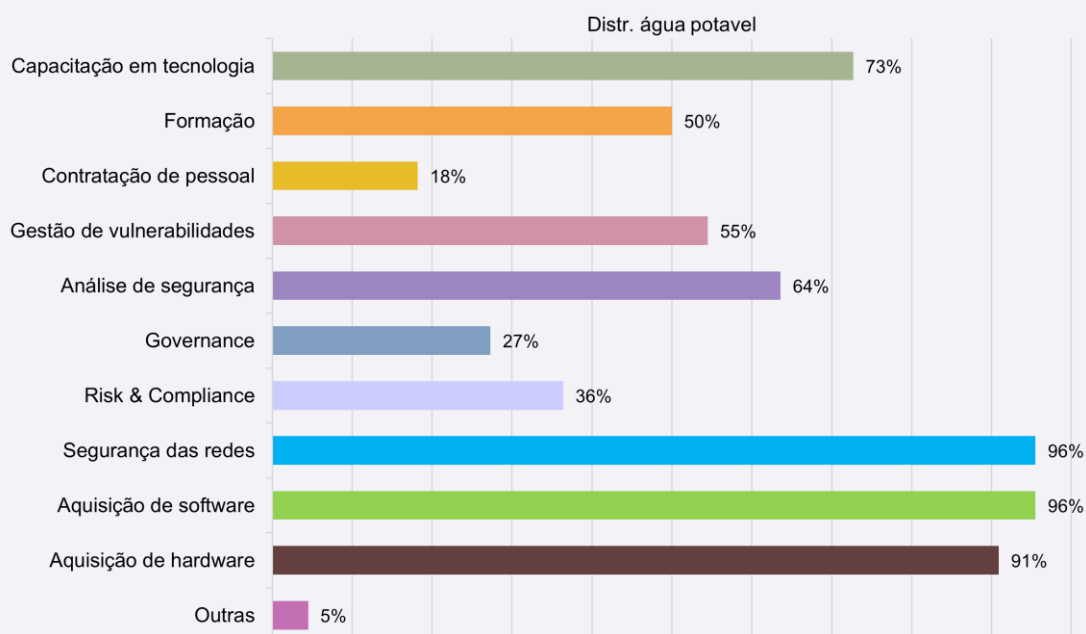
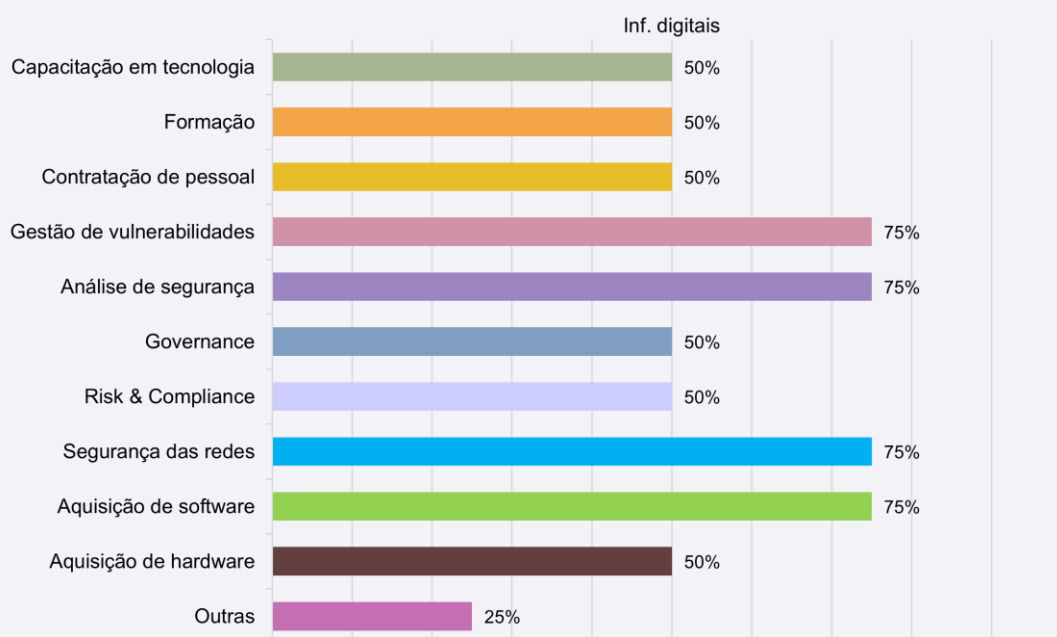


Gráfico 110.6 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Entre os operadores que possuem orçamento específico para a cibersegurança, as áreas onde estes são mais comumente aplicados são a capacitação em tecnologia (73%), a formação dos colaboradores (67%), a gestão de vulnerabilidades (72%), análises de segurança (77%), *Risk & Compliance* (50%), segurança das redes (89%), aquisição de *software* (81%) e aquisição de *hardware* (81%). As áreas às quais estes orçamentos menos são alocados são a contratação de pessoal (34%) e *Governance* (44%). Nas “outras” áreas, surgem sobretudo a contratação de serviços externos para a área de cibersegurança, processos de implementação de normas (*standards*) como a NIST e a aquisição de serviços *cloud*.

Como o setor das infraestruturas do mercado financeiro não apresentam orçamento para a área a questão não se aplica.

A ENISA realizou um inquérito a 251 organizações OSE e prestadores de serviços digitais (oriundas da França, Alemanha, Itália, Espanha e Polónia). Segundo o inquérito, o orçamento médio para a implementação da diretiva NIS é 175 mil euros. A maioria das organizações do inquérito priorizaram os domínios de *Governance*, *Risk & Compliance* e Segurança das Redes.⁶⁵ De acordo com um estudo da NIS de 2023, a média de impacto anual dos incidentes informáticos foi de 365 mil euros e a mediana de 250 mil euros, tendo sido estes dados recolhidos de 38 entidades⁶⁶.

⁶⁵ ENISA, “NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist”, 11 de dezembro de 2020, <https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist>.

⁶⁶ ENISA, “NIS Investments”, 2023

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança

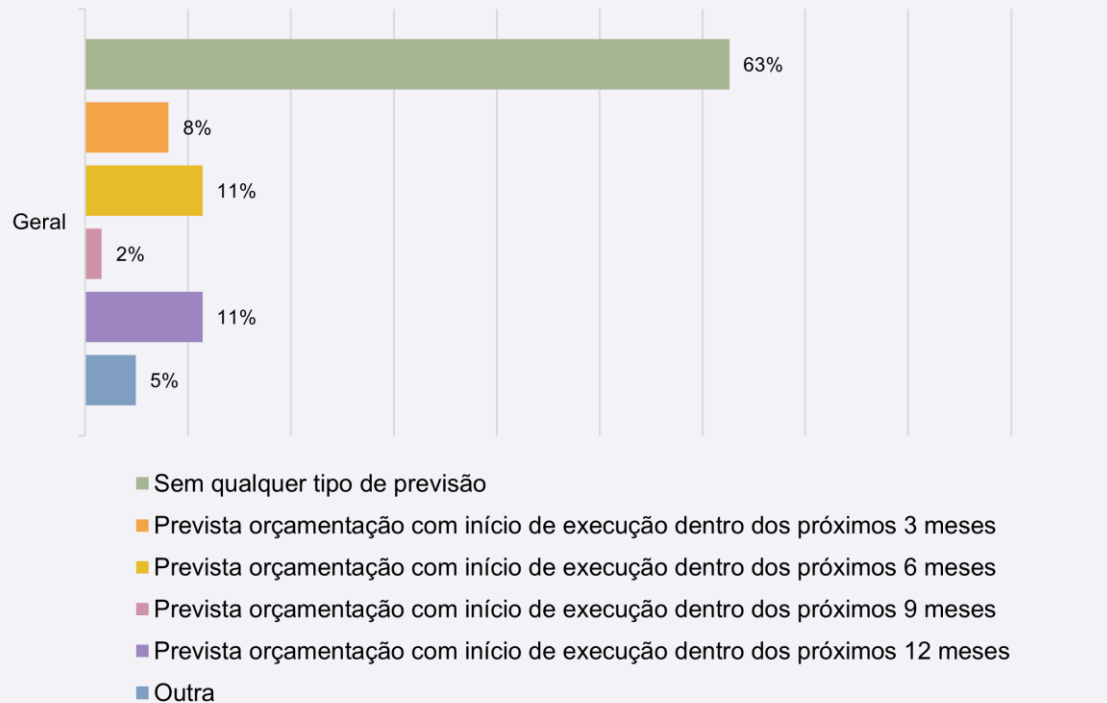


Gráfico 111.1 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança

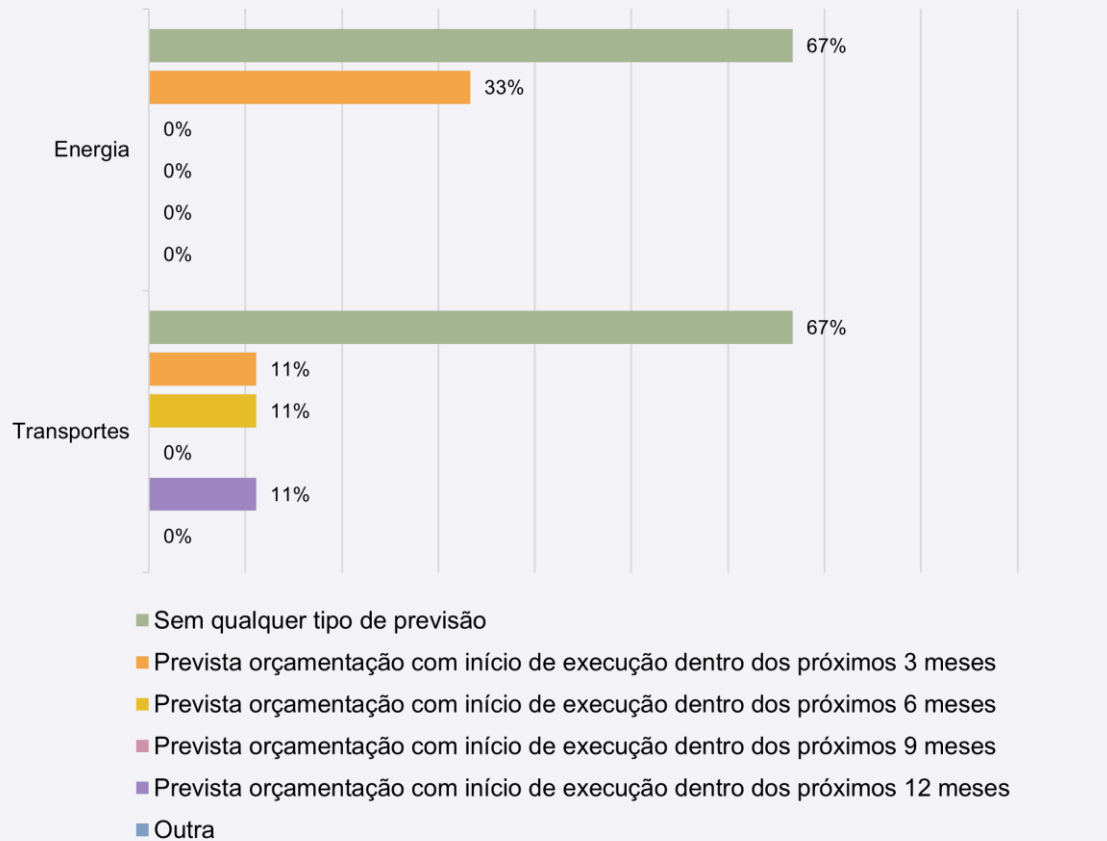


Gráfico 111.2 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança

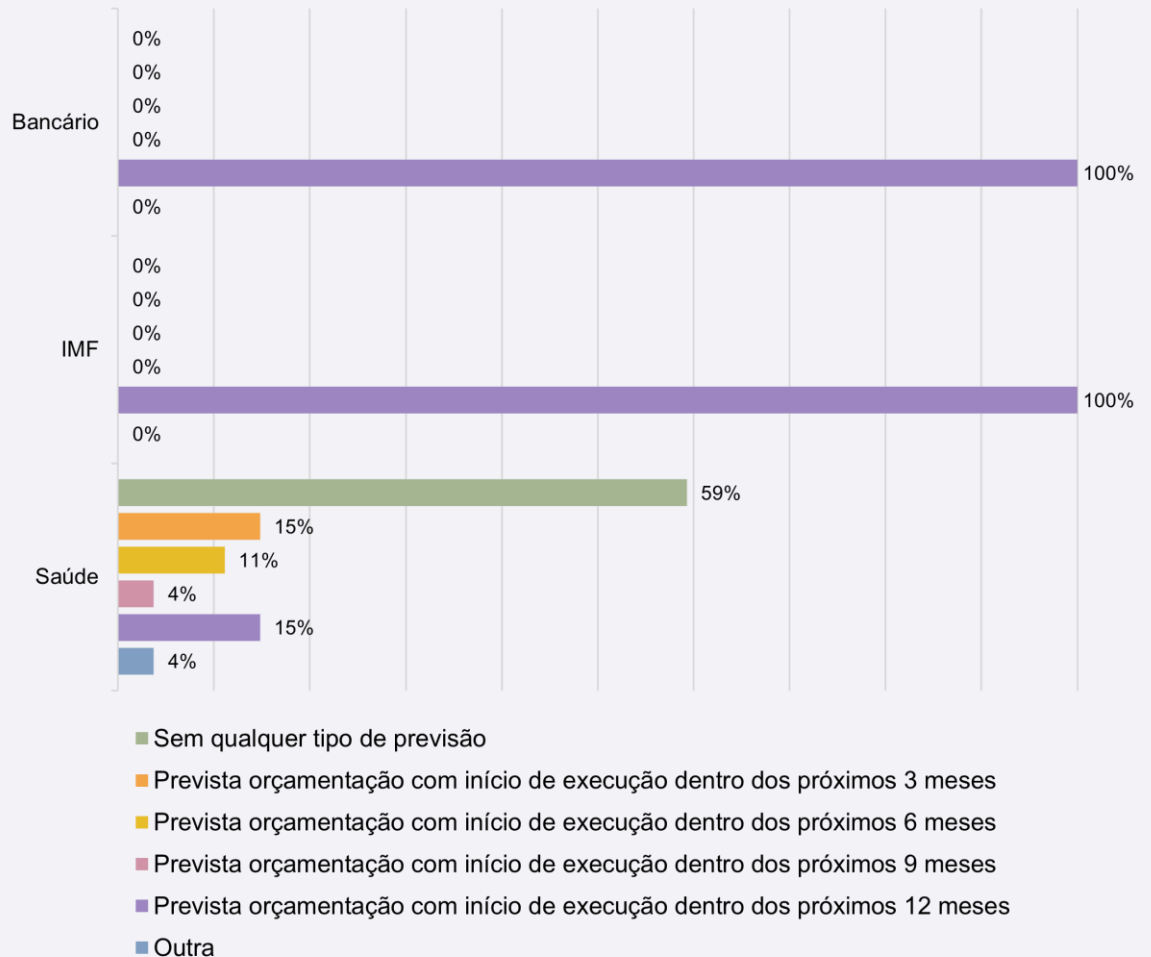
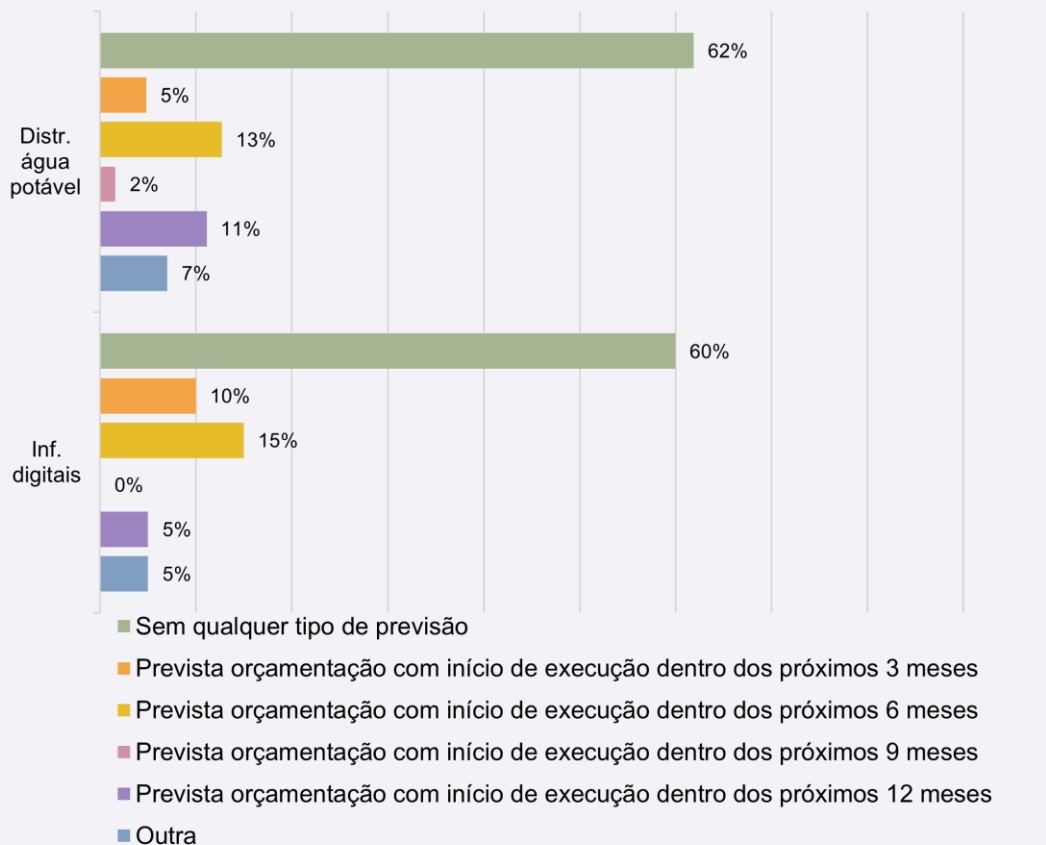
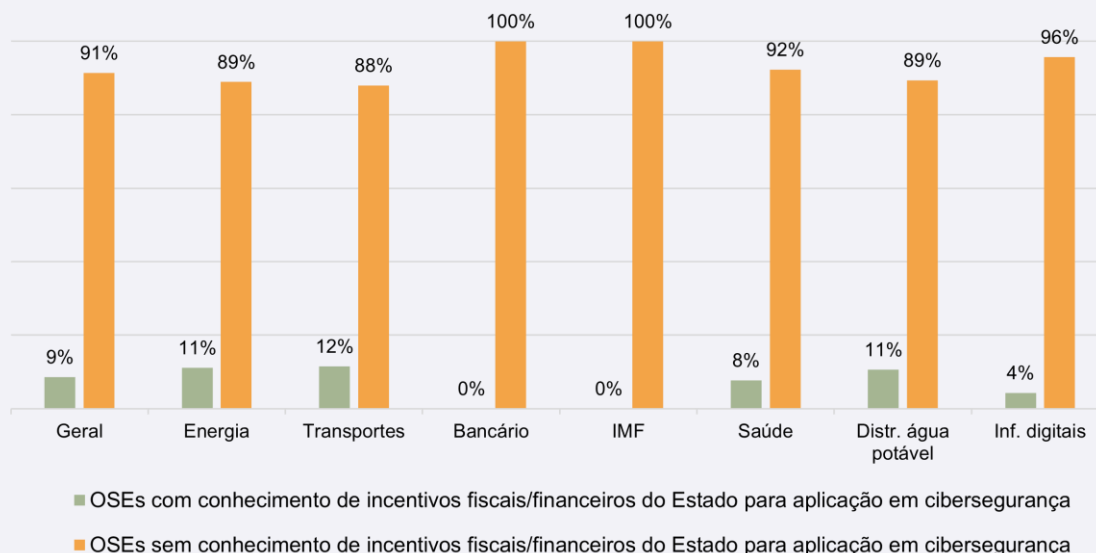


Gráfico 111.3 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024. 63% destes não têm qualquer previsão de vir a ter tal orçamento. Apesar deste panorama, no setor da energia previa-se que um terço dos operadores sem orçamento viria ainda a iniciar a execução de um durante o último trimestre de 2023. Já nos setores bancário e das infraestruturas do mercado financeiro, todos os operadores sem orçamento específico para cibersegurança à data da realização do questionário tinham previsto iniciar a execução de um durante os 12 meses subsequentes, ou seja, até ao último trimestre de 2024. Nos restantes setores, a previsão de vir a iniciar a execução de um orçamento específico para cibersegurança ainda durante o ano de 2024 existe para entre 33% a 40% dos operadores. Quanto às “outras” respostas, estas corresponderam globalmente a situações em que os orçamentos atribuídos à cibersegurança se incluem ou decalcam dos orçamentos dedicados à área de informática.

Gráfico 112 - Conhecimento de incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança

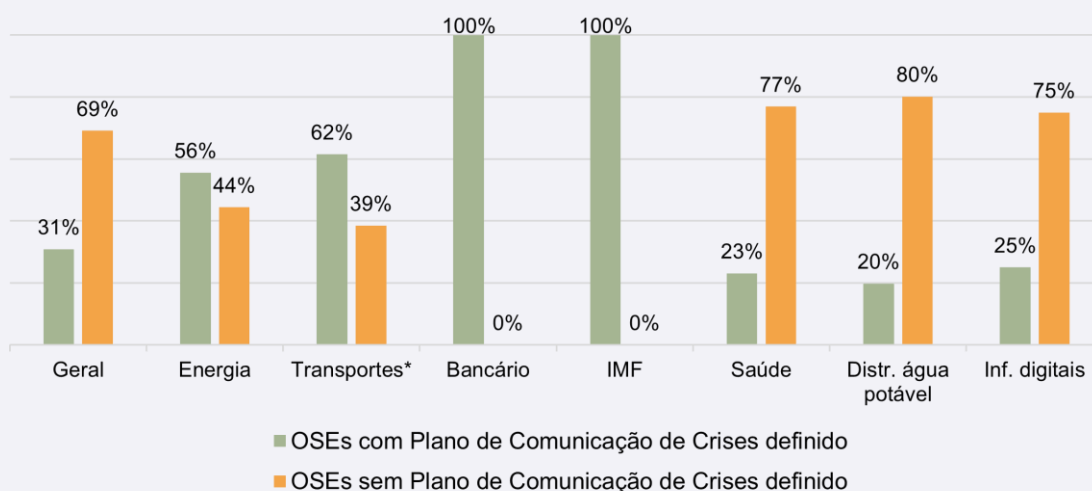


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No entanto, havia ainda alguns operadores nos setores da energia, dos transportes, da saúde, do fornecimento e distribuição de água potável e das infraestruturas digitais com conhecimento sobre tais incentivos. As percentagens de operadores com esse conhecimento nos vários setores são, contudo, reduzidas, variando entre os 4% e os 12%. Nos setores bancário e das infraestruturas do mercado financeiro não foram registados quaisquer operadores com conhecimento desses incentivos.

Cabe assim recordar que o Estado português lançou, em 2022, a medida Cheque-Formação + Digital, integrada no Programa Emprego + Digital 2025, que permite aos trabalhadores portugueses candidatarem-se a um cheque de formação digital de até 750 euros que pode ser aplicado em formações de cibersegurança⁶⁷.

⁶⁷ IEFP, Cheque-Formação + Digital, <https://www.iefp.pt/cheque-formacao-digital>.

Gráfico 113 - Plano de Comunicação de Crises



Muitos dos operadores de serviços essenciais não têm definido um plano de comunicação de crises. Apenas 31% dos inquiridos referiram ter tal plano definido. Nos setores bancário e das infraestruturas do mercado financeiro todos os inquiridos declaram ter plano de comunicação de crises definido. Tal deve-se ao facto de existir legislação setorial em vigor que obriga os operadores destes setores a terem este plano definido. Há que destacar, também, os outros setores onde ainda se verifica uma maioria de operadores com esse plano definido. Esses setores são o da energia (com 56%) e o dos transportes (com 62%). Nos restantes setores - saúde, fornecimento e distribuição de água potável e infraestruturas digitais - a percentagem de operadores com plano de comunicação de crises varia entre 20% e 25%.

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises

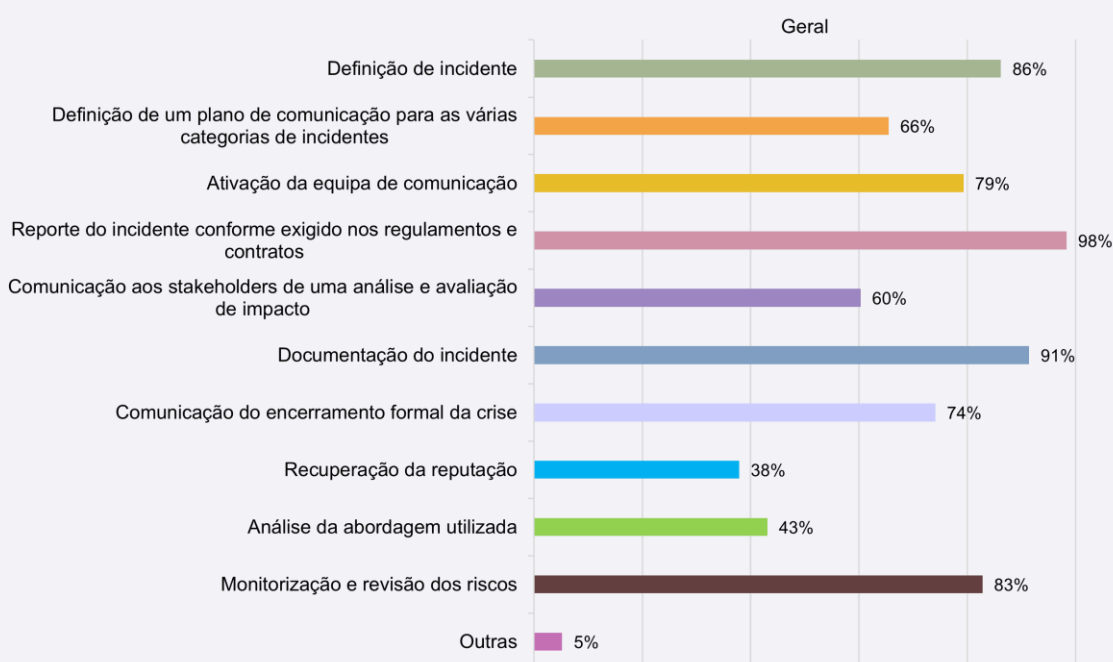


Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises

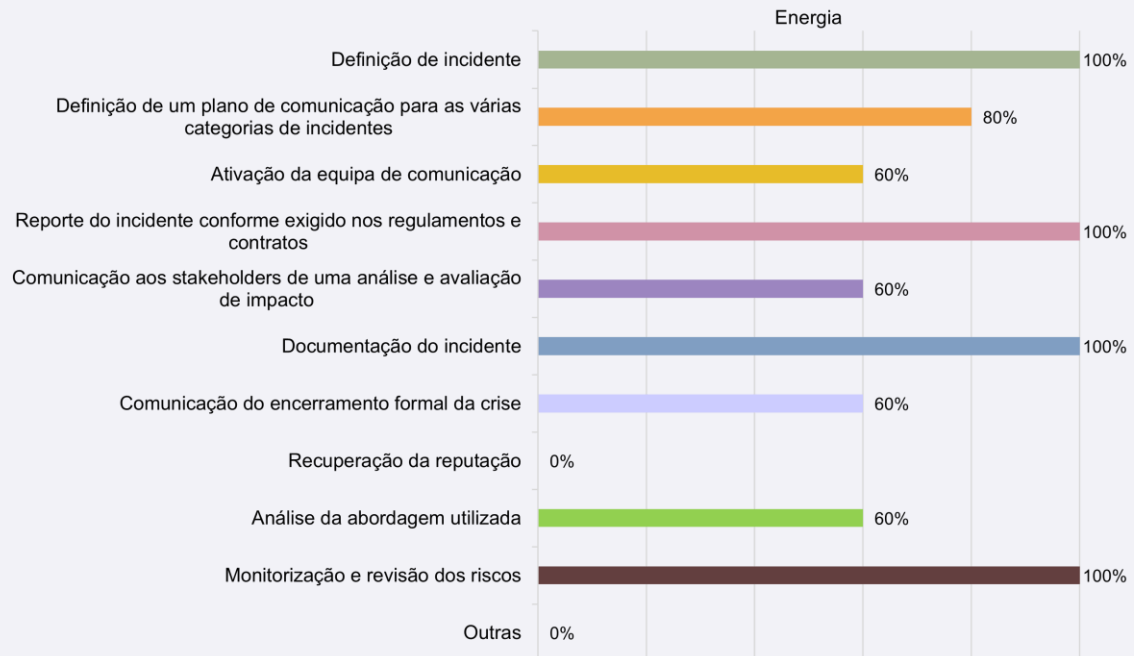


Gráfico 114.2 - Secções definidas no Plano de Comunicação de Crises

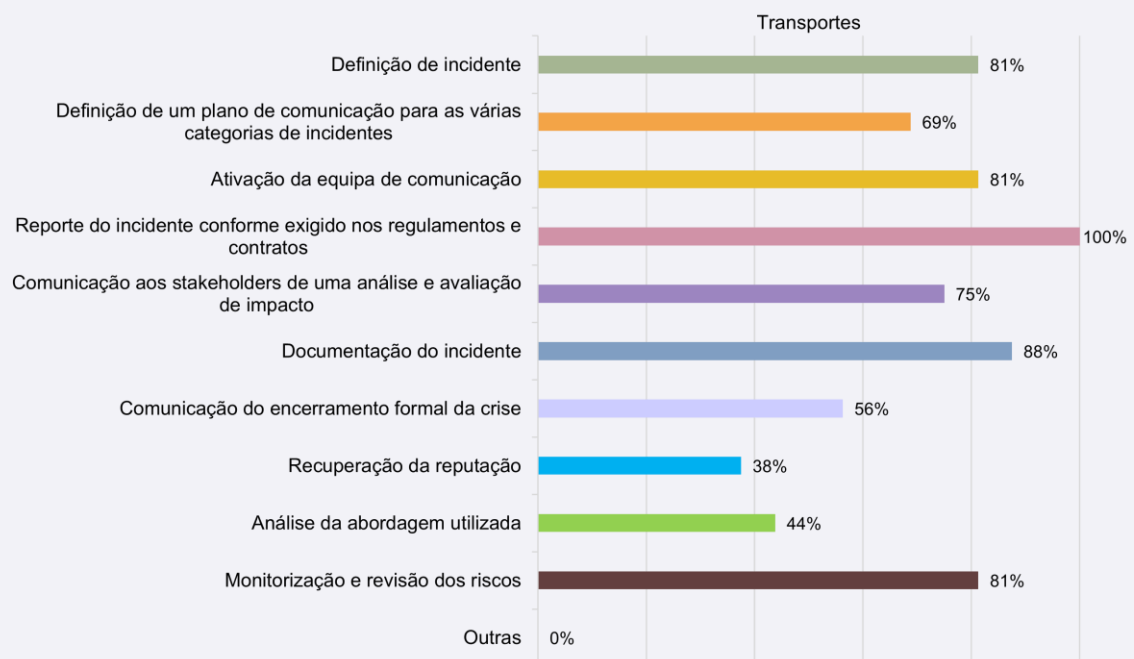


Gráfico 114.3 - Secções definidas no Plano de Comunicação de Crises

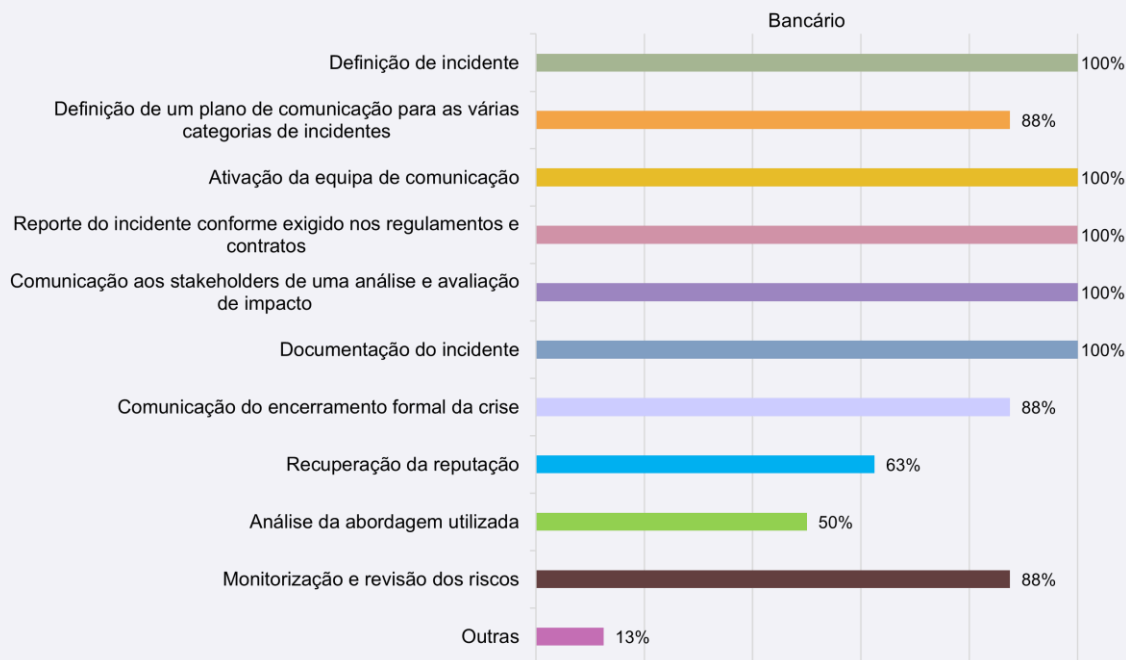


Gráfico 114.4 - Secções definidas no Plano de Comunicação de Crises

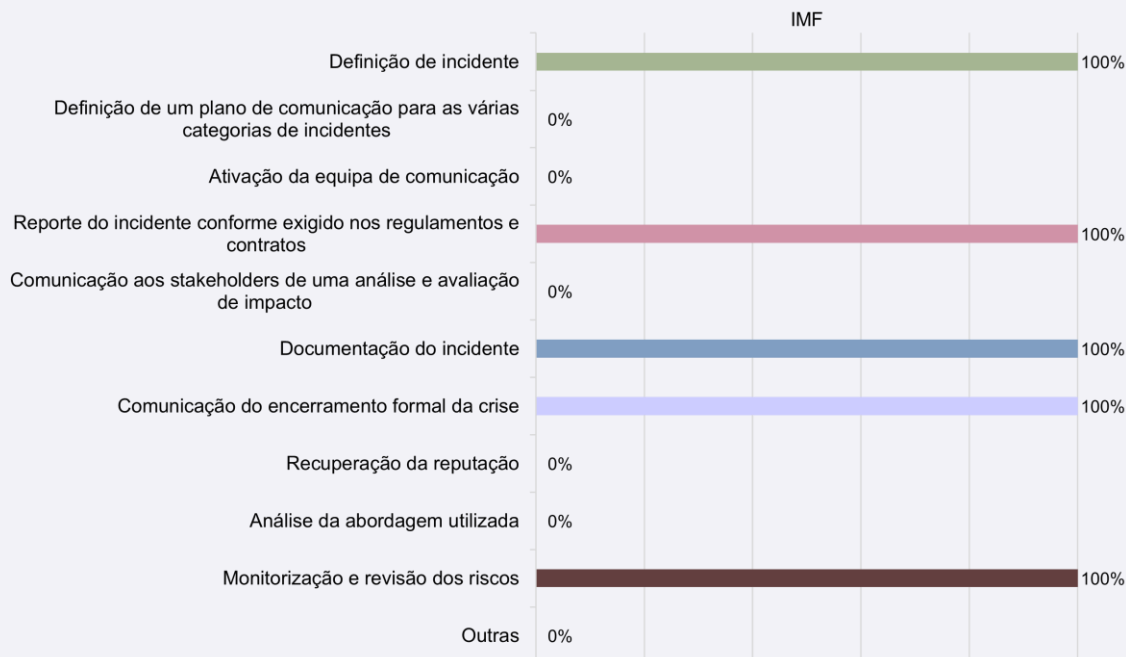


Gráfico 114.5 - Secções definidas no Plano de Comunicação de Crises

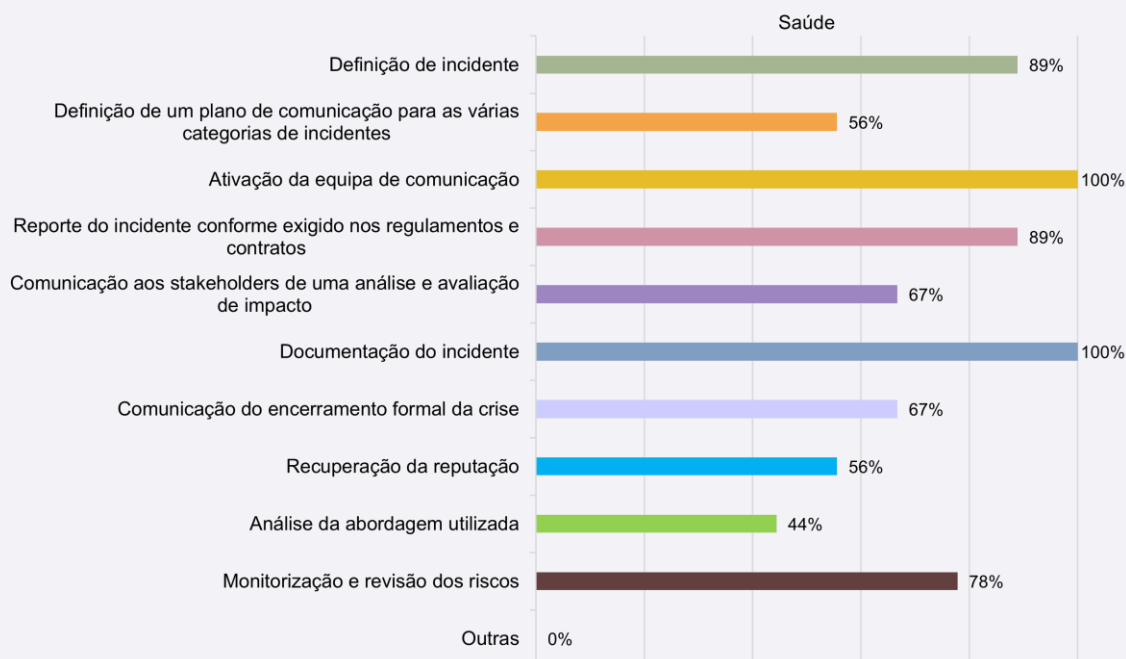


Gráfico 114.6 - Secções definidas no Plano de Comunicação de Crises

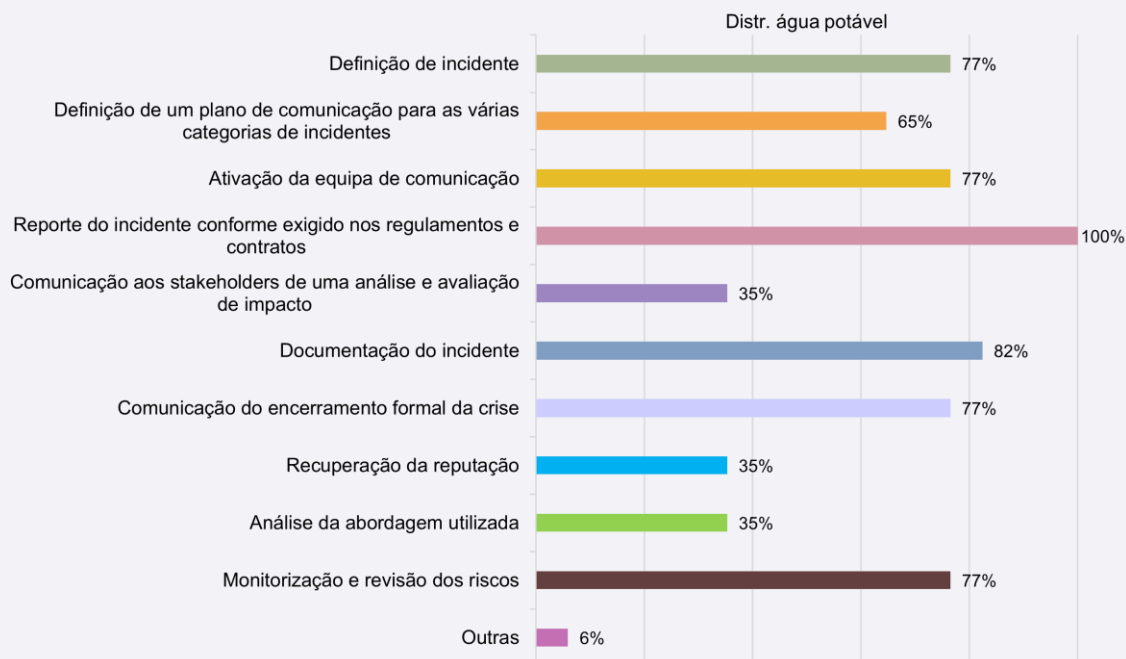
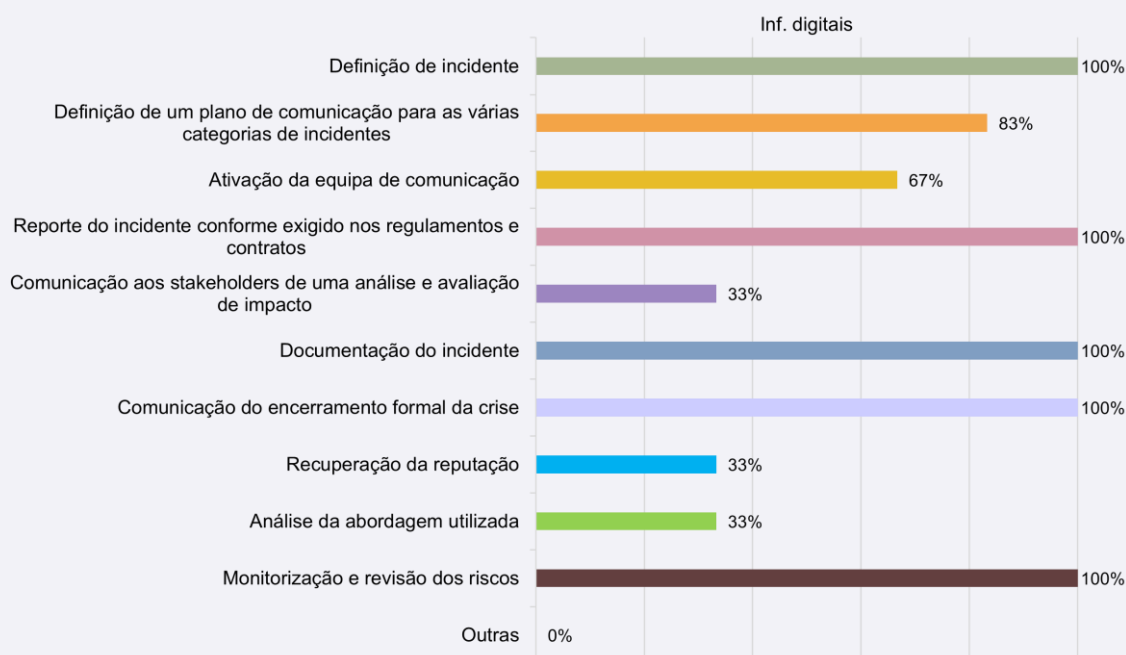


Gráfico 114.7 - Secções definidas no Plano de Comunicação de Crises



Na análise das secções incluídas nos planos de comunicação de crises, foram incluídas dez secções. Verifica-se que sete destas secções estão incluídas em pelo menos 60% dos planos já definidos. As sete secções mais presentes são a definição de incidente, a definição de um plano de comunicação para várias categorias de incidentes, a ativação da equipa de comunicação, a notificação do incidente conforme exigido nos regulamentos e contratos, a comunicação aos grupos de interesse de uma análise e avaliação do impacto do incidente, a documentação do incidente e a análise da abordagem utilizada.

Por sua vez, as três secções que menos vezes estão incluídas nos planos de comunicação são as relacionadas com a comunicação do encerramento formal da crise, com a recuperação da reputação, e com a monitorização e revisão dos riscos.

A nível setorial, destacam-se os setores da energia, bancário e da saúde, por serem os setores onde mais planos incluem as secções elencadas. No setor das infraestruturas do mercado financeiro, apesar de se verificarem cinco secções incluídas em todos os planos, há outras cinco que não constam em qualquer um dos planos definidos pelos operadores do setor.

Gráfico 115 - Motivos para a não definição de Plano de Comunicação de Crises

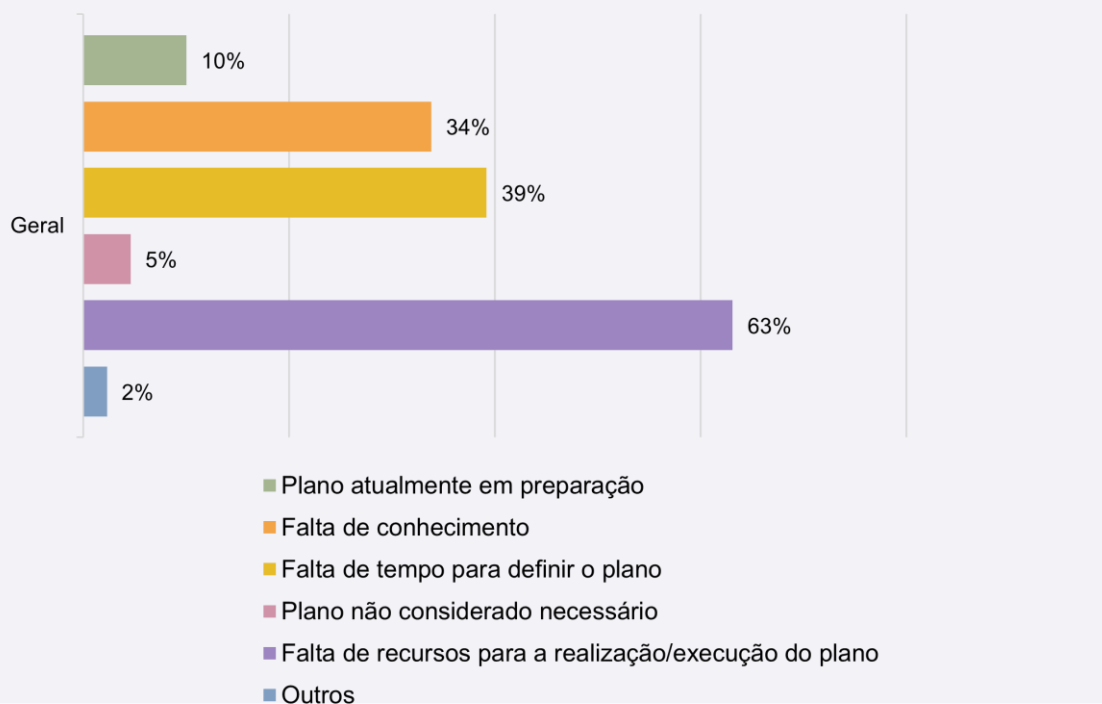


Gráfico 115.1 - Motivos para a não definição de Plano de Comunicação de Crises

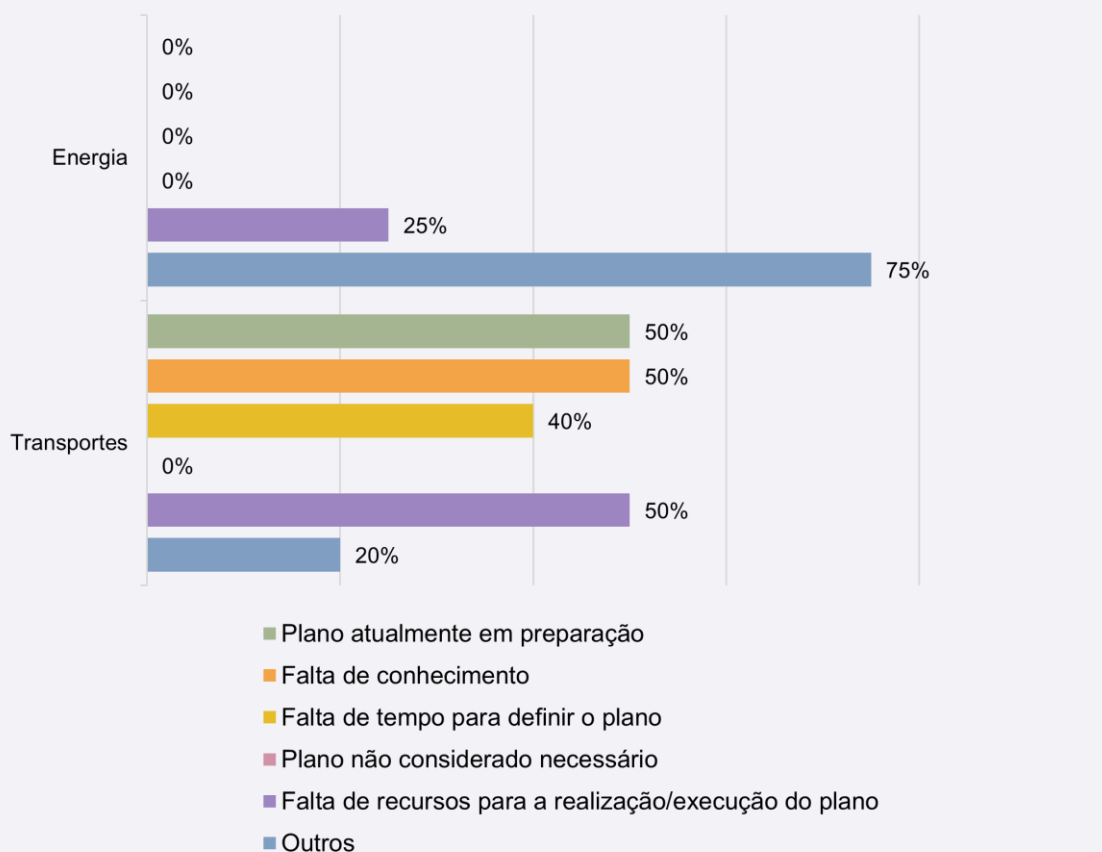
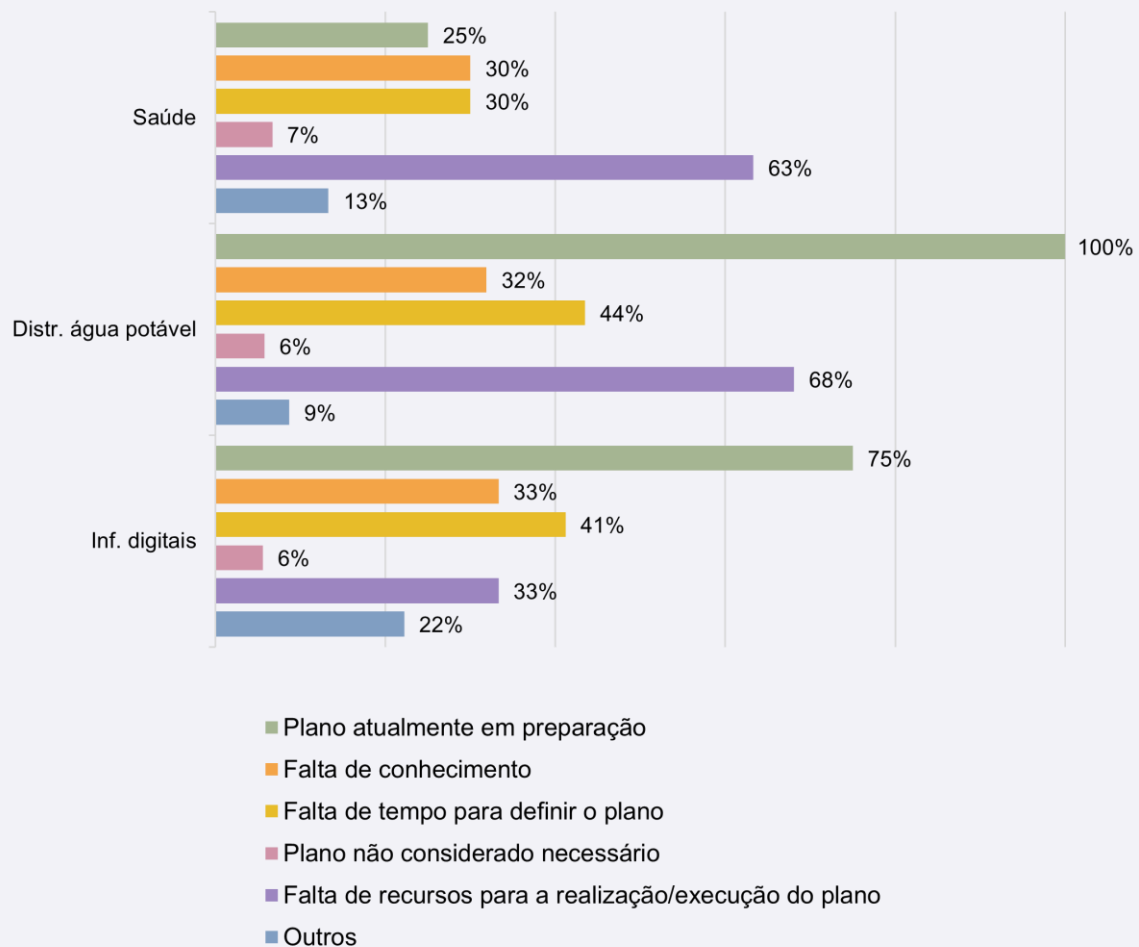


Gráfico 115.2 - Motivos para a não definição de Plano de Comunicação de Crises



O principal motivo identificado para a não definição do plano de comunicação de crises dos setores em análise, é a falta de recursos para a elaboração do mesmo, tendo sido indicado por cerca de 63% dos operadores sem plano. Seguem-se a falta de tempo para definir o plano, indicada por cerca de 39% dos operadores sem plano, e a falta de conhecimento para definir esse plano, indicada por 34% dos operadores.

Outros motivos foram mencionados como estar prevista a implementação do plano para 2024/2025 ou mesmo o plano já se encontrar em elaboração.

O setor bancário e de infraestruturas de mercado financeiro afirmam já ter o plano definido. Desta forma a questão não se aplica.

Análise Setorial

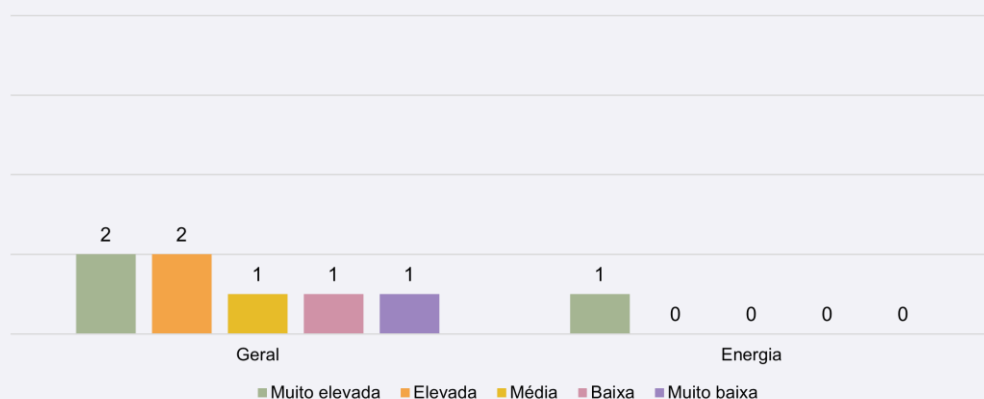
1. Energia

1.1. Contextualização setorial

No âmbito da Diretiva 2016/1148⁶⁸, também conhecida como Diretiva NIS, e Lei n.º 46/2018⁶⁹, que transpõe a Diretiva e estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), o setor da energia abrange três subsectores: o da eletricidade, o do petróleo e o do gás. Embora estas formas de energia sejam conhecidas há mais tempo (por exemplo, há evidências da utilização de petróleo e de gás natural que datam de 4.000 a 6.000 anos a.C.), a sua difusão ocorreria nos finais do século XIX, fruto da Revolução Industrial, substituindo gradualmente o carvão, que era a principal fonte de energia nos vários ramos industriais, bem como no transporte ferroviário.

Veja-se, antes de mais, uma breve caracterização do setor energético na atualidade. De acordo com o questionário realizado, o regulador do setor considera que a maturidade deste em cibersegurança é muito elevada (**Gráfico 9**).

Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores

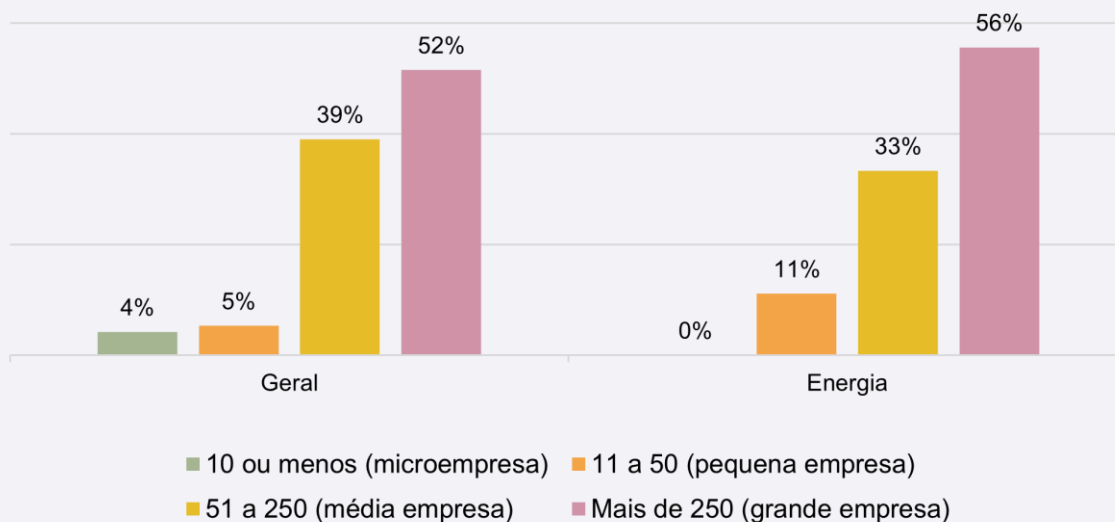


⁶⁸ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, Anexo I, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148>.

⁶⁹ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

O tecido empresarial dos OSE do setor energético é sobretudo composto por grandes empresas, representando estas 56% dos operadores do setor, com as PME's a constituírem os restantes 44% (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



A perceção dos reguladores sobre maturidade em cibersegurança nos setores pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (**Gráfico 38**) e pelas medidas de proteção cibersegurança adotadas (**Gráfico 66.1**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

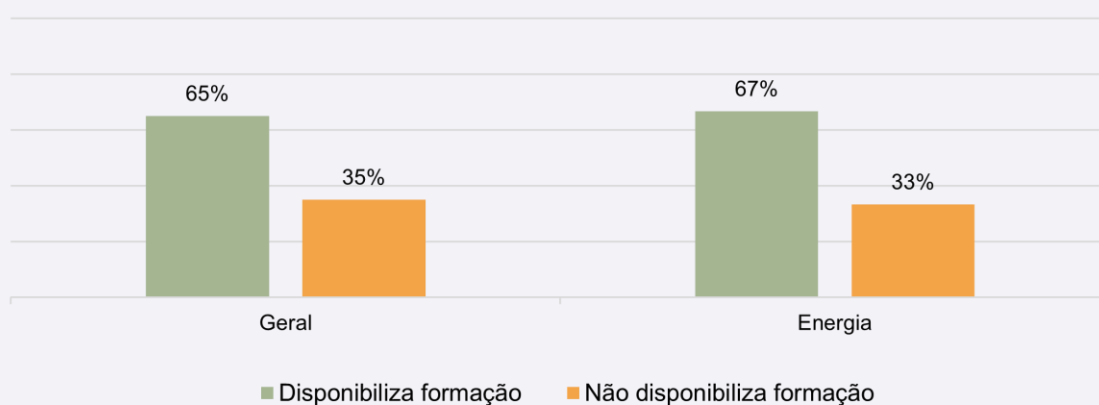
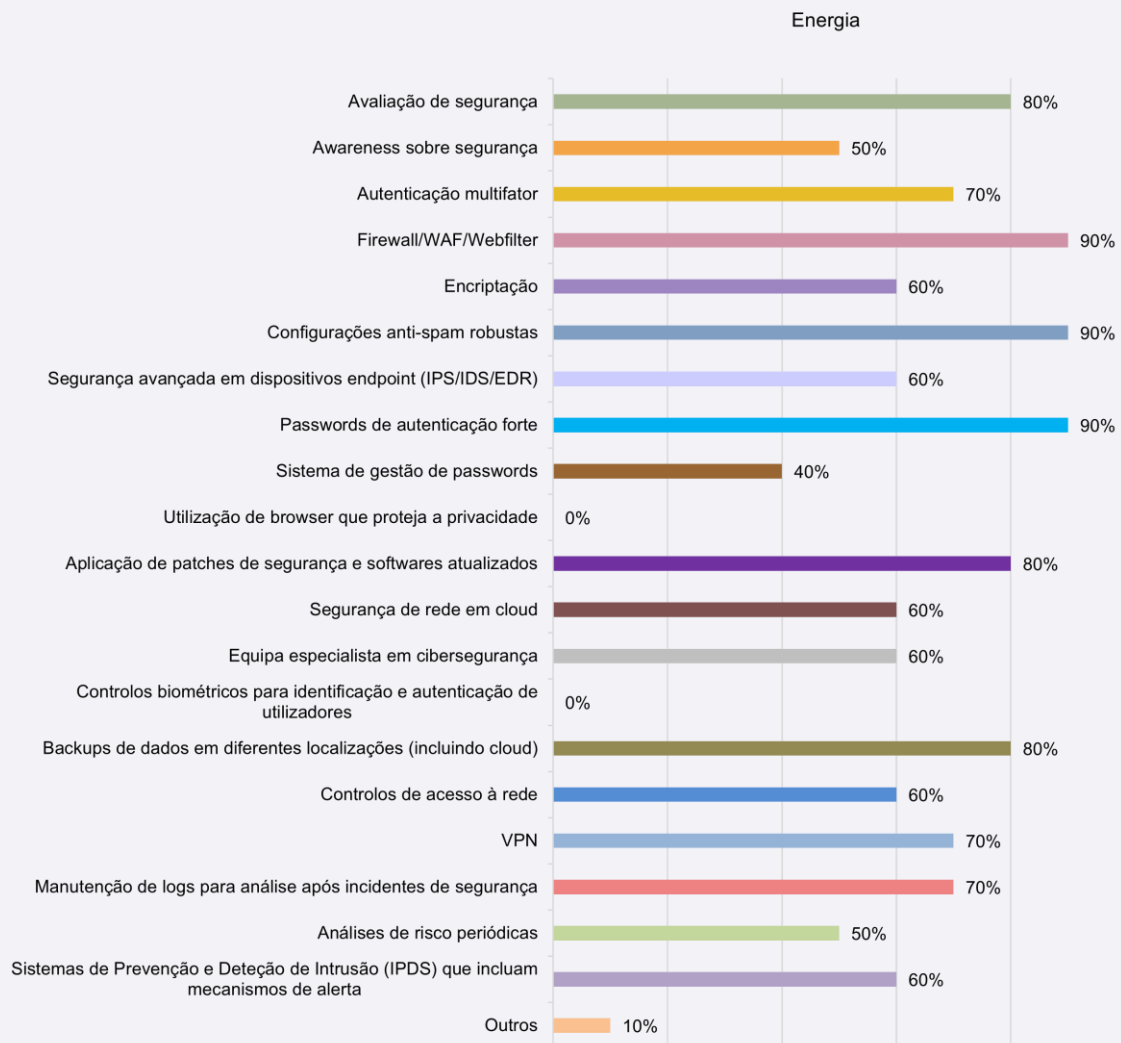
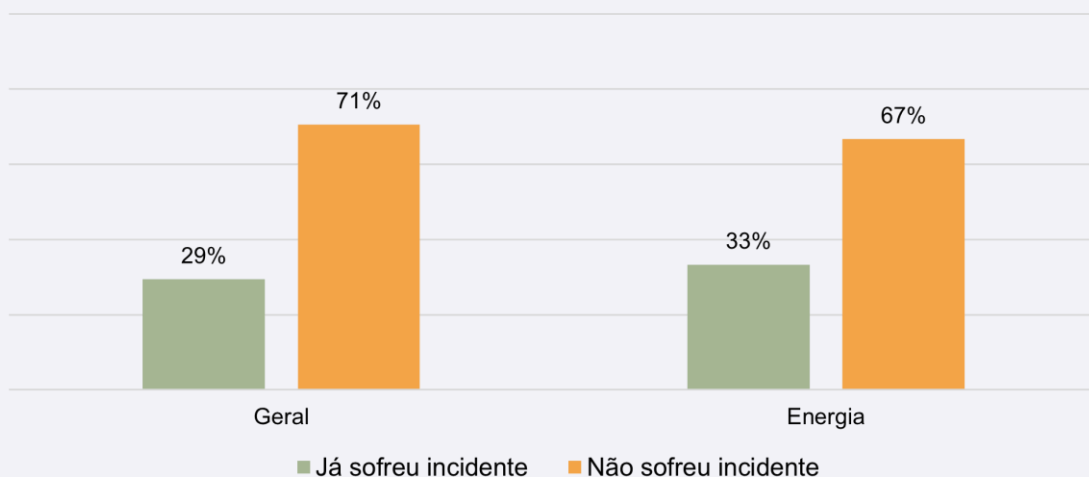


Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança



É também um setor que tem, por enquanto, beneficiado de uma baixa incidência de ciberataques, ainda assim superior à média geral (**Gráfico 68**).

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



As políticas de cibersegurança e relacionadas implementadas (**Gráfico 79.1**) e o facto de já dois terços dos operadores dedicarem orçamentos específicos à área de cibersegurança (**Gráfico 109**) também contribuí para a perceção dos reguladores sobre a maturidade em cibersegurança.

Gráfico 79.1 - Políticas incluídas no Plano de Segurança

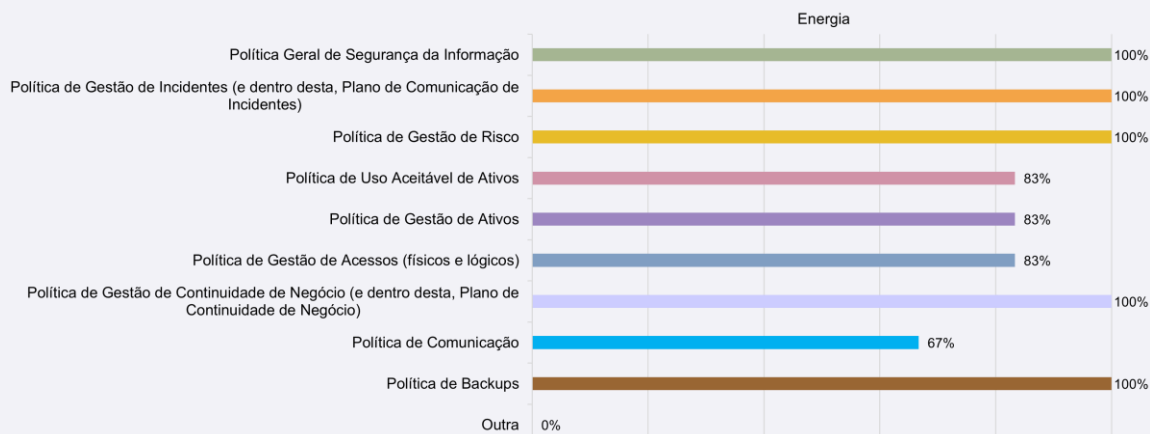
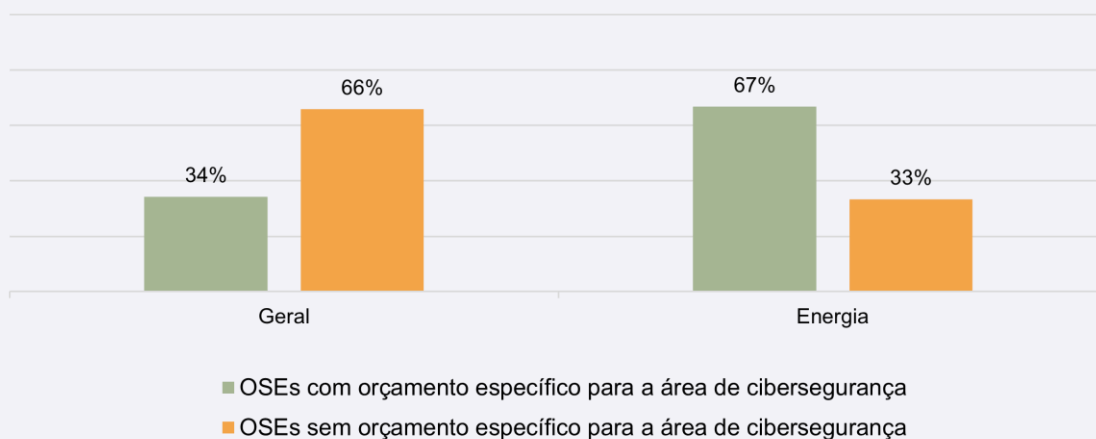


Gráfico 109 - Orçamento específico para a área de cibersegurança



De seguida, ver-se-á como evoluiu a produção e a distribuição em Portugal de cada uma das fontes de energia referidas.

Subsetor da Eletricidade

A história da eletrificação em Portugal iniciou-se em finais do século XIX e ficou marcada por diversos avanços e recuos. O primeiro passo no processo de eletrificação do país iniciou-se com a iluminação pública. A primeira experiência elétrica de que há notícia deu-se a 28 de setembro de 1878, por ocasião do 15.º aniversário do ainda príncipe D. Carlos, no qual se acenderam candeeiros elétricos na esplanada da Cidadela de Cascais⁷⁰. O evento real marcou o início da eletrificação em Portugal. Eram até feitas excursões de famílias a Lisboa para ver os novos candeeiros elétricos, que já não deixavam o cheiro do petróleo pelo ar⁷¹.

No seguimento deste evento, e do fascínio que o mesmo tinha deixado junto da população portuguesa, começaram a surgir as primeiras empresas de produção e distribuição elétrica:

- 1891 - Companhias Reunidas Gás e Eletricidade (CRGE);
- 1903 - Construção da Central da Boavista;
- 1908 - Central do Ouro;
- 1909 - Construção da Central do Desterro;
- 1914 - Central Tejo;
- 1919 - União Elétrica Portuguesa.

Destas, a Central Tejo foi uma das mais marcantes, pois tendo começado por alimentar o centro de Lisboa, foi crescendo sucessivamente até chegar a alimentar os concelhos limítrofes da capital.

Apesar de marcante, o processo de eletrificação foi lento. Foi impulsionado pelo Estado Novo, através da Lei da Eletrificação, publicada em 1944, que estabeleceu como prioridade o desenvolvimento das centrais hidroelétricas. Na década de 50, a construção de barragens era parte integrante do quadro de industrialização do país e, nas regiões onde as barragens eram construídas, eram sinónimo de desenvolvimento económico e social para as populações. Durante a mesma década, o Estado aplicou uma política de apoio económico à eletrificação. Municípios, federações de municípios e concessionários privados podiam recorrer às participações, e através destas foram construídas pequenas centrais térmicas, redes de transporte e distribuição de energia e redes de pequena distribuição rural e urbana⁷².

A década seguinte foi a década da consolidação de infraestruturas, da atualização do inventário dos recursos nacionais de produção hídrica e térmica e de definir o seu aproveitamento. Enquanto o processo de eletrificação do país parecia estar próximo da sua conclusão nas zonas urbanas, havia ainda muitas freguesias rurais onde não chegava eletricidade. Assim o Estado teve de alargar os apoios à eletrificação rural de forma a conseguir chegar a estas⁷³.

⁷⁰ EDP, “Uma história de dois séculos: Portugal acende a primeira lâmpada”, *Histórias EDP*, 14 de agosto de 2019, <https://www.edp.com/pt-pt/historias-edp/uma-historia-de-dois-seculos-portugal-acende-a-primeira-lampada>.

⁷¹ EDP, “Uma história de dois séculos”, *Histórias EDP*, 14 de agosto de 2019.

⁷² EDP, “Uma história de dois séculos”, *Histórias EDP*, 14 de agosto de 2019.

⁷³ EDP, “Uma história de dois séculos”, *Histórias EDP*, 14 de agosto de 2019.

No final da década, o Estado determinou a fusão de 14 empresas concessionárias de aproveitamentos hidroelétricos, de empreendimentos termoeletricos e de transporte de energia. Esta concessão unificada foi atribuída à Companhia Portuguesa de Eletricidade, que ficou responsável por 95% da energia elétrica produzida no país e que foi a antecessora da atual Energias de Portugal (EDP), constituída em 1976⁷⁴.

Por sua vez, a década de 70 foi uma década conturbada. No mesmo ano da aprovação da Constituição, a EDP herdava um cenário complexo de desequilíbrio na eletrificação do território que vigorava desde a década anterior, em que a distribuição de energia elétrica estava concentrada nos grandes centros urbanos. Parte do país estava ainda “às escuras”. Simultaneamente, a eletricidade tornava-se indispensável para cada vez mais utilizações, pelo que era também necessário aumentar a capacidade de produção de energia elétrica. A estes desafios, somavam-se a precariedade industrial do país, a falta de organização do setor elétrico e as inesperadas crises do petróleo (1979-1980)⁷⁵.

Ainda assim, a EDP tinha três grandes objetivos: a eletrificação total do território, a melhoria da qualidade dos serviços prestados e a uniformização tarifária⁷⁶. A uniformização tarifária foi o primeiro a ser cumprido, em 1980. A eletrificação total do território foi concluída na década de 90. A melhoria da qualidade dos serviços foi sendo feita à medida que o território era eletrificado e que a capacidade de produção de energia era aumentada. Mais energia produzida significa menos interrupções de serviços e mais circuitos instalados significam mais circuitos alternativos em caso de interrupção no fornecimento de energia⁷⁷.

O subsetor da eletricidade tem também sido caracterizado por uma forte aposta na produção de energia elétrica a partir de fontes renováveis. Segundo dados da REN, a produção renovável abasteceu 61% do consumo de energia elétrica em Portugal em 2023, num total de 31,2 TWh, o valor mais elevado de sempre no sistema nacional. A energia eólica abasteceu 25% do consumo em Portugal, a hidroelétrica 23%, a fotovoltaica 7% e a biomassa 6%⁷⁸. Estes valores colocam Portugal entre os países da UE que mais energia elétrica produzem a partir de fontes renováveis, junto da Áustria, Dinamarca, Finlândia e Suécia⁷⁹.

Subsetor do Petróleo

O petróleo tem uma história muito mais longa do que a eletricidade. A utilização do petróleo pelo Homem remonta a 4.000 a.C., época em que povos do Médio Oriente já utilizavam betume na pavimentação de estradas, na calafetação de grandes construções e no aquecimento e na iluminação de casas. No entanto, o petróleo apenas passou a ser considerado valioso em meados do século XIX, com o desenvolvimento de técnicas de destilação na separação de querosene do crude e com a crescente necessidade destes produtos devido à Revolução Industrial. Foram estes produtos refinados que vieram substituir o óleo e o carvão e que ainda hoje abastecem viaturas, aviões, unidades de produção de energia e aquecimento doméstico⁸⁰.

⁷⁴ EDP, “Uma história de dois séculos”, *Histórias EDP*, 14 de agosto de 2019.

⁷⁵ EDP, “Uma história de dois séculos”, *Histórias EDP*, 14 de agosto de 2019.

⁷⁶ EDP, “Uma história de dois séculos”, *Histórias EDP*, 14 de agosto de 2019.

⁷⁷ Francisco de la Fuente Sánchez, entrevistado por Jorge Branco em “Eletrificação total do território”, ISCTE, 2013, 838.

⁷⁸ “Produção de energia renovável bate recorde em 2023”, REN, 2 de janeiro de 2024, <https://www.ren.pt/pt-pt/media/noticias/producao-de-energia-renovavel-bate-recorde-em-2023>.

⁷⁹ “Renewable energy statistics”, Eurostat, dados relativos a 2022, extraídos em dezembro de 2023, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.

⁸⁰ Colégio Nacional de Energia e Minas, “O petróleo nas nossas vidas. Com exceção da água, o petróleo é o líquido mais presente nas nossas vidas”, *Ingenium*, II Série, n.º 158 (março/abril de 2017): 61.

Em Portugal, a história da exploração petrolífera remonta ao século XIX, com o início das atividades de pesquisa e exploração datando do ano de 1844, através da concessão relativa à mina de asfalto do “Canto do Azeche”, localizada em Nossa Senhora da Vitória, no concelho de Alcobaça⁸¹.

No entanto, a real evolução do setor só aconteceria já no Estado Novo. Em 1936 foi realizado um concurso público para a concessão de uma área destinada à pesquisa de hidrocarbonetos em regime de exclusividade. O alvará de concessão n.º 2138 foi concedido a dois cidadãos ingleses, conforme aprovado pelo Decreto 28575, de 7 de abril de 1938. Estes cidadãos ingleses viriam a transmitir os direitos e obrigações à empresa *Anglo Portuguese Oil Company Ltd.*, que desenvolveu a atividade até 1941, sendo interrompida pela segunda guerra mundial⁸².

Esta primeira fase incidiu na região de Torres Vedras, havendo duas sondagens com indícios de petróleo. No entanto, na época, a falta de recursos adequados impediu a realização de testes de produção. Uma segunda fase de pesquisa ocorreu entre 1946 e 1969, durante a qual foram encontrados sinais promissores de petróleo e gás. Contudo, os testes de produção realizados demonstraram que as quantidades não eram viáveis para a comercialização⁸³.

Com o intuito de criar e consolidar uma nova ordem económica, o regime reforçou a proteção da economia com diversas medidas, como a Lei da Reconstituição Económica e a Lei do Recondicionamento Industrial, entre outras. A Lei do Recondicionamento Industrial, enquanto medida de proteção económica, previa a concessão de licenças de instalação a “novas indústrias de importância económica e custos de instalação excecionais, ou indispensáveis à defesa nacional”. A primeira sociedade a beneficiar dessa proteção foi precisamente uma do setor petrolífero - a Sociedade Anónima Concessionária da Refinação de Petróleos em Portugal (Sacor). Esta competia com outras companhias portuguesas no mercado de distribuição, como a Sociedade Nacional de Petróleos (Sonap) e ainda com outras estrangeiras, como a Shell e a British Petroleum (BP)⁸⁴.

Apesar da presença de companhias estrangeiras no mercado português, este era de pequena dimensão na escala europeia. Em 1938, o consumo total nacional rondava as 200 mil toneladas por ano, enquanto em Itália este rondava os 2 milhões de toneladas e em França os 6 milhões. Tal correspondia a um consumo por habitante em Portugal a cerca de 60% do consumo médio de um habitante italiano e a 20% do consumo médio de um habitante francês⁸⁵.

Ainda assim, o mercado do petróleo foi crescendo gradualmente em Portugal, e, à medida que iam surgindo novas necessidades de consumo, surgiam também novas necessidades de produção. As medidas protecionistas do Estado Novo foram também limitando a entrada de outros intervenientes no mercado, pelo que o mercado petrolífero se encontrava essencialmente nas mãos de quatro grandes operadores em meados da década de 70. Eram estes a Sacor, a Sonap, a Cidla e a Petrosul. Com a Revolução de Abril, estas viriam depois a ser nacionalizadas (1975) e a constituir a Petrogal em 1976⁸⁶, que adotaria no mesmo ano o nome comercial Galp⁸⁷.

⁸¹ “História da Exploração Petrolífera em Portugal: Avanços e Desafios na Indústria”, *TORRES VEDRAS WEB*, 14 de fevereiro de 2024, <https://torresvedrasweb.pt/historia-da-exploracao-petrolifera-em-portugal-avancos-e-desafios-na-industria/>.

⁸² Direção-Geral de Energia e Geologia, “História da Prospeção e Pesquisa”, <https://www.dgeg.gov.pt/pt/areas-setoriais/geologia/petroleo-armazenamento-de-co2/geologia-do-petroleo/historia-da-prospecao-e-pesquisa/>.

⁸³ Direção-Geral de Energia e Geologia, “História da Prospeção e Pesquisa”.

⁸⁴ David Castaño et al., *Os Petróleos em Portugal: Do Estado à Privatização 1937-2012* (Lisboa: Imprensa de Ciências Sociais, 2017), 19-22.

⁸⁵ Castaño et al., *Os Petróleos em Portugal*, 22.

⁸⁶ Castaño et al., *Os Petróleos em Portugal*, 30-31.

⁸⁷ “As nossas raízes: cronologia ilustrada”, Galp, <https://www.galp.com/corp/pt/sobre-nos/a-galp/as-nossas-raizes>.

Atualmente, a Galp continua a ser uma das maiores empresas petrolíferas do país, controlando cerca de 50% do comércio de combustíveis e a totalidade da capacidade refinadora de Portugal⁸⁸.

Subsetor do Gás

O gás natural foi descoberto na Pérsia entre 6000 a.C. e 2000 a.C., na China, é conhecido desde 900 a.C., mas o conhecimento da primeira utilização do gás natural data de 347 a.C., com um manuscrito desse período a descrever um “ar de fogo” que podia ser usado para iluminação⁸⁹.

Na Europa, o gás natural foi descoberto no século XVII, embora não tenha despertado grande interesse. O gás de iluminação pública na Europa era produzido a partir do carvão. Em 1778, Alessandro Volta descobriu o potencial energético do gás natural quando verificou que o gás capturado nas bolhas emergentes da água, no lago Maggiore, ardia com uma chama azulada. Volta ficaria conhecido por ter sido quem isolou pela primeira vez o gás metano⁹⁰. Os gases butano e propano (aqueles que se veem comercializados em botijas) viriam a ser obtidos com o desenvolvimento das técnicas de destilação e refinação do petróleo desenvolvidas a partir de meados do século XIX, bem como através da captura de gases durante o processo de extração do gás natural⁹¹.

Em 1807 são acesos, pela primeira vez no mundo, candeeiros a gás na Rua Pall Mall em Londres. Por sua vez, em 1846, é atribuída uma concessão de iluminação pública de Lisboa à CLIG e, esta, arranca com o sistema de gás iluminante⁹². Em 1857 surgia o primeiro fogão a gás e, em 1885, com a invenção do bico de Bunsen, que permitia a queima segura de gás natural sem que esta se propagasse pelo tubo, foram compreendidas as vantagens deste gás como fonte de energia para o aquecimento ambiente, aquecimento de água e utilização na cozinha⁹³. No ano de 1899 a rede de gás canalizado estende-se até Cascais, Oeiras e Sintra. É inaugurada, em 1944, a fábrica de gás da Matinha, em Lisboa, com uma capacidade de produção diárias de 75 000 m³ e dez anos depois é iniciada a produção de Gases de Petróleo Liquefeito (GPL)⁹⁴.

A decisão de introduzir o gás natural na UE e em Portugal, e de criar a infraestrutura de canalização necessária para o seu abastecimento seria apenas tomada no final da década de 80, no seguimento das crises do petróleo e de modo a combater a dependência energética face aos produtos petrolíferos. Em 1990, estimava-se que a dependência de Portugal dos produtos petrolíferos fosse na ordem dos 70%⁹⁵.

Em 2000 são iniciados os trabalhos de preparação do terreno para as obras de implantação do terminal de Gás Natural Líquido (GNL) em Sines e dois anos depois é iniciada a construção do gasoduto entre Setúbal e Sines. No ano de 2012 ocorrem as obras de ampliação do Terminal de GNL de Sines⁹⁶.

⁸⁸ “Cotação Galp Energia”, Rankia, <https://www.rankia.pt/cotacao/galp-energia/>.

⁸⁹ ERSE, “Caracterização do Sector do Gás Natural em Portugal”, janeiro de 2007, 3.

⁹⁰ ERSE, “Caracterização do Sector do Gás”, janeiro de 2007, 3.

⁹¹ ERSE, “Caracterização do Sector do Gás”, janeiro de 2007, 3.

⁹² Fundação Galp Energia, “Gás A História Natural”, 4, <https://www.fundacaogalp.com/Portals/1/Documentos/livro-gas-a-historia-natural.pdf>.

⁹³ “Gás natural e gás propano e butano - conheça as diferenças”, Repsol, <https://www.repsol.pt/particulares/assessoramento/gas-natural-e-gas-propano-e-butano/>.

⁹⁴ Fundação Galp Energia, “Gás A História Natural”, 4.

⁹⁵ “Introdução do gás natural em Portugal”, RTP, 25 de setembro de 1990, <https://arquivos.rtp.pt/conteudos/introducao-do-gas-natural-em-portugal/>.

⁹⁶ Fundação Galp Energia, “Gás A História Natural”, 5-6.

A introdução do gás natural em Portugal visava dar ao país o acesso a uma nova fonte de energia competitiva, cómoda e limpa. Simultaneamente, criou-se um projeto estruturante na economia portuguesa e diversificador de abastecimento de hidrocarbonetos. Em resumo, o país passou a poder aumentar a competitividade da sua indústria, principalmente a de maior intensidade energética, a facilitar o desenvolvimento social e o bem-estar das populações e a melhorar a segurança do abastecimento energético. Todos estes aspetos de política económica e energética foram reconhecidos pela UE, que apoiou o projeto com subsídios ao investimento a fundo perdido e com empréstimos bonificados do Banco Europeu de Investimento (BEI)⁹⁷.

Embora as principais linhas de distribuição de gás natural se estendam atualmente por praticamente todo o país, o gás natural não chega a todos. Um estudo da Marktest, quantificava, em 2018, que o número de indivíduos em Portugal com gás canalizado em casa era aproximadamente 3,9 milhões, o que corresponderia a cerca 45,3% dos residentes com 15 ou mais anos no continente⁹⁸.

1.1.1. Impacto socioeconómico

O setor energético exerce um papel fundamental na economia e na sociedade. É este setor que permite, nas casas e empresas, que as luzes, os eletrodomésticos, as máquinas, grandes e pequenas, e os transportes, privados ou públicos, funcionem. É um dos setores essenciais que mais dependências provoca nos restantes - sem energia, todos os outros ficam comprometidos. A maior dependência energética verifica-se nos setores dos transportes, da indústria, da agricultura e da pecuária que, segundo o Banco de Portugal (BdP), são os que mais intensamente consomem energia no país⁹⁹.

É também um setor que move muitos milhões de euros. Para que se tenha uma ideia, o volume de negócios (VVN) da maior empresa do subsector da eletricidade em 2022 foi de, pelo menos, 12,7 mil milhões de euros. Somando os volumes de negócio das principais empresas dos setores do petróleo (14,9 mil milhões) e do gás (4,5 mil milhões), ultrapassam-se os 32 mil milhões de euros, o que corresponde a quase 13% do PIB português em 2022¹⁰⁰.

Concomitantemente, é um setor gerador de empregos. Segundo dados da PORDATA, os setores da eletricidade, gás e água empregavam, em 2023, 56,9 mil colaboradores¹⁰¹. No subsector do petróleo, estima-se que haja também cerca de 53 mil colaboradores¹⁰². Retirando os quase 10 mil colaboradores que trabalham no setor da água, o setor energético será responsável por cerca de 100 mil empregos em Portugal. Além dos 100 mil empregos já criados, a aposta nas energias renováveis poderá vir a triplicar este número, uma vez que se estima que as energias renováveis irão gerar mais 95 mil postos de trabalho diretos e outros 95 mil indiretos¹⁰³. Se tal se confirmar, o setor será responsável por cerca de 293 mil postos de trabalho em Portugal.

⁹⁷ ERSE, "Caracterização do Sector do Gás", 5.

⁹⁸ "Gás canalizado: penetração aumenta mas não chega à maioria da população", Marktest, 11 de dezembro de 2018, <https://www.marktest.com/wap/a/n/id-2470.aspx>.

⁹⁹ Banco de Portugal, "Economia numa imagem", março de 2022, <https://www.bportugal.pt/page/economia-numa-imagem-148-0>.

¹⁰⁰ "Quais são as empresas com maior volume de negócios em Lisboa?", *Executive Digest*, 25 de agosto de 2023, https://executivedigest.sapo.pt/noticias/quais-sao-as-empresas-com-maior-volume-de-negocios-em-lisboa/?doing_wp_cron=1709902761.2706060409545898437500.

¹⁰¹ PORDATA, "População empregada: total e por setor de atividade económica. Quantas pessoas trabalham na agricultura, indústria, comércio ou outros serviços?", Indicador: Eletricidade, gás e água (2023), <https://www.pordata.pt/portugal/populacao+empregada+total+e+por+setor+de+atividade+economica-3384-304037>.

¹⁰² Apetro, "A Contribuição Económica do Setor Petrolífero Português", setembro de 2020, 9.

¹⁰³ Ana Oliveira, "Emprego nas renováveis cresce a pique com solar a brilhar. E os "fósseis"?" *CNN Portugal*, 22 de julho de 2023, <https://cnnportugal.iol.pt/energia/energias-renovaveis/emprego-nas-renovaveis-cresce-a-pique-com-solar-a-brilhar-e-os-fosseis/20230722/64b902ccd34e72171a0b5971>.

Como já se referiu em 1.1. Contextualização setorial, o setor energético desempenha um papel fundamental na sociedade, ao abastecer não só os equipamentos necessários para trabalhar, mas também para aqueles de que se usufruem fora do contexto de trabalho, como o aquecimento da água, a confeção de alimentos, a iluminação pública e a regulação da temperatura dentro das habitações, entre muitos outros. O acesso à energia tem-se assim tornado um critério essencial para as boas condições de vida. No entanto, Portugal enfrenta um problema de pobreza energética.

A pobreza energética é definida como “a falta de acesso de um agregado familiar a serviços energéticos essenciais, quando tais serviços proporcionam níveis básicos e dignos de vida e de saúde, nomeadamente aquecimento, água quente, arrefecimento e iluminação adequados e a energia necessária para os eletrodomésticos, tendo em conta o contexto nacional, a política social e outras políticas nacionais pertinentes, causada por uma combinação de fatores, incluindo, pelo menos, a falta de acessibilidade dos preços, um rendimento disponível insuficiente, elevadas despesas energéticas e a fraca eficiência energética das habitações”¹⁰⁴.

A pobreza energética não é um problema exclusivamente português, mas Portugal figura entre os países da UE com índice de pobreza energética mais elevado, estando apenas melhor do que a Eslováquia, a Hungria e a Bulgária¹⁰⁵. Estima-se que entre 1,8 e 3 milhões de pessoas em Portugal se encontrem nesta situação, das quais 660 mil se encontrem em pobreza energética severa¹⁰⁶.

Uma consequência direta da pobreza energética é a falta de conforto térmico, que pode ser compreendida como a capacidade de manter a temperatura de uma habitação nos intervalos entre os 18.º C e os 21.º C, no inverno, e os 19.º C e os 23.º C¹⁰⁷, no verão, é sobretudo atribuída a dois motivos. O primeiro é algo que persiste na maioria das habitações em Portugal, onde se estima que cerca de 75% não possuem condições de isolamento térmico.

O segundo motivo é o preço da energia. Embora os preços da energia em Portugal se mantenham mais ou menos em linha com os praticados na União¹⁰⁸, importa sublinhar que o salário médio em Portugal está abaixo do da média europeia. O salário médio português ocupa a 17.ª posição dos salários médios da Europa a 27¹⁰⁹.

Embora Portugal importe apenas 10% de seu gás natural da Rússia, o rompimento das relações diplomáticas e comerciais entre a União Europeia e a Rússia, que era o principal fornecedor de gás natural do bloco, levou a procura a mudar repentinamente para outros fornecedores, como a Argélia, de onde Portugal importava a maioria do seu gás natural, fazendo o preço escalar. Tendo presente que a guerra se iniciou a 24 de fevereiro de 2022, importa salientar que a 2 de março do mesmo ano o preço do gás natural já tinha aumentado 55%¹¹⁰ e a 6 de março o preço da eletricidade já tinha disparado 115%¹¹¹.

¹⁰⁴ Diretiva (UE) 2023/1791 do Parlamento Europeu e do Conselho, de 13 de setembro de 2023, relativa à eficiência energética e que altera o Regulamento (UE) 2023/955, art. 2.º, alínea 52).

¹⁰⁵ “Pobreza Energética em Portugal” *Histórias EDP*, EDP, 16 de março de 2021, <https://www.edp.com/pt-pt/historias-edp/pobreza-energetica-em-portugal>.

¹⁰⁶ “Estratégia de Longo Prazo de Combate à Pobreza Energética aprovada em Conselho de Ministros”, PORTUGAL.GOV.PT, 23 de novembro de 2023, <https://www.portugal.gov.pt/pt/gc23/comunicacao/comunicado?i=estrategia-de-longo-prazo-de-combate-a-pobreza-energetica-aprovada-em-conselho-de-ministros>.

¹⁰⁷ “Pobreza Energética em Portugal”, EDP, 23 de novembro de 2023.

¹⁰⁸ “Electricity price statistics”, Eurostat, dados extraídos em outubro de 2023, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_price_statistics#Electricity_prices_for_household_consumers.

¹⁰⁹ “New indicator on annual average salaries in the EU”, Eurostat, 19 de dezembro de 2022, <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/DDN-20221219-3>.

¹¹⁰ Rita Neto, “Gás natural dispara 55% e bate recorde com guerra na Ucrânia”, *Eco*, 2 de março de 2022, <https://eco.sapo.pt/2022/03/02/gas-natural-dispara-55-para-recorde-de-194-euros-por-mwh/>.

¹¹¹ Gonçalo Almeida, “Preço da eletricidade dispara para novo máximo. Já subiu 115% com a guerra”, *CNN Portugal*, 6 de março de 2022, <https://cnnportugal.iol.pt/geral/eletricidade-em-portugal-atinge-novo-maximo-historico-segunda-feira-preco-subiu-115-com-a-guerra/20220306/6224b6bc0cf2cc58e7e70a67>.

Todos estes fatores se conjugam para criar uma situação em que mesmo quem não é pobre economicamente possa ser pobre energeticamente. Para enfrentar esta situação, o Estado português criou a Estratégia de Longo Prazo de Combate à Pobreza Energética 2023-2050 (ELPPE)¹¹².

As medidas previstas na ELPPE estão organizadas em quatro eixos estratégicos:

- Promover a sustentabilidade energética e ambiental da habitação;
- Promover o acesso universal a serviços energéticos essenciais;
- Promover a ação territorial integrada;
- Promover o conhecimento e a atuação informada¹¹³.

As medidas previstas passam pelo Vale Eficiência, a Tarifa Social de Energia, a redução dos custos do acesso à rede, o acesso ao mercado regulado, a aplicação de benefícios fiscais, como a aplicação da taxa reduzida do IVA à componente fixa das tarifas de acesso às redes nos fornecimentos de eletricidade e nos fornecimentos de gás natural, mediante o consumo, e a aplicação da taxa reduzida de IVA à entrega e instalação de painéis solares térmicos e fotovoltaicos, bem como por programas de apoio à melhoria das condições do conforto térmico das habitações, quer estas passem por intervenções nas mesmas ou pela aquisição de equipamentos e soluções energeticamente eficientes¹¹⁴.

As principais metas da ELPPE são:

- Reduzir a população a viver em agregados sem capacidade para manter a casa adequadamente aquecida de 17,5%, em 2020, para menos de 1%, em 2050, com objetivos intermédios de 10%, em 2030, e 5%, em 2040;
- Reduzir a população a viver em habitações não confortavelmente frescas durante o verão de 35,7%, em 2012, para menos de 5%, em 2050, com objetivos intermédios de 20%, em 2030, e 10%, em 2040;
- Reduzir a população a viver em habitações com problemas de infiltrações, humidade ou elementos apodrecidos de 25,2%, em 2020, para menos de 5%, em 2050, com objetivos intermédios de 20%, em 2030, e 10%, em 2040;
- Eliminar as situações em que a despesa com energia representa mais de 10% do total de rendimentos dos agregados familiares (em 2016, encontravam-se nesta situação 1 202 567 agregados)¹¹⁵.

Um outro impacto pelo qual o setor é e continuará a ser responsável durante os próximos anos é o da transição energética, que é tanto um desafio como um objetivo.

De forma resumida, a temperatura global do planeta tem vindo a aumentar e está a prejudicar todas as formas de vida terrestre, sejam animais ou plantas. As temperaturas elevadas são responsáveis por fenómenos climáticos acentuados e são várias as zonas do globo que sofrem com secas extremas ou com inundações e tempestades. Regiões que, até meados do século XIX, nunca tinham passado por estas situações¹¹⁶.

¹¹² Direção-Geral de Energia e Geologia (DGE), “Estratégia Nacional de Longo Prazo para o Combate à Pobreza Energética 2023-2050”, <https://www.dgeg.gov.pt/pt/areas-transversais/relacoes-internacionais/politica-energetica/estrategia-nacional-de-longo-prazo-para-o-combate-a-pobreza-energetica/>.

¹¹³ DGE, “Estratégia de Longo Prazo de Combate à Pobreza Energética”.

¹¹⁴ Resolução do Conselho de Ministros n.º 11/2024, de 8 de janeiro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/11-2024-836222486>.

¹¹⁵ “Estratégia de Longo Prazo de Combate à Pobreza Energética”, PORTUGAL.GOV.PT, 23 de novembro de 2023.

¹¹⁶ “O que é a transição energética e qual o impacto na forma como vivemos?”, EDP, <https://www.edp.com/pt-pt/o-que-e-a-transicao-energetica-e-qual-o-impacto-na-forma-como-vivemos>.

Quando se começou a estudar a razão destas alterações, a opinião científica foi unânime: todos apontaram como causa a emissão de gases de efeito de estufa, sendo o principal responsável o dióxido de carbono (CO₂). E estes, por sua vez, são emitidos através da queima de combustíveis fósseis: o petróleo, o carvão e o gás¹¹⁷.

O grande objetivo estabelecido com o Acordo de Paris em 2015, de momento, é fazer com que a temperatura média do planeta não ultrapasse em mais de 1,5°C a temperatura média dos anos pré-revolução industrial até 2030 e atingir a neutralidade carbónica até 2050¹¹⁸. Para tal, é necessário reduzir as emissões de gases com efeito de estufa, como o CO₂. Essa redução passa, em grande parte, pela transição energética, ou seja, pela transição da utilização e queima de combustíveis fósseis, para energia produzida a partir de fontes renováveis e limpas, como a hídrica, a eólica, a solar e o hidrogénio.

Portugal e a UE pretendem, até 2030, reduzir as emissões de gases com efeito estufa em entre 45% e 55%, atingir uma produção energética onde 47% dessa energia provenha de fontes renováveis e ter pelo menos 20% dos transportes alimentados também por fontes renováveis¹¹⁹.

O desafio é grande, uma vez que cerca de 70% da energia consumida na Europa e em Portugal ainda depende dos combustíveis fósseis¹²⁰. Essa dependência não se deve tanto à produção de energia elétrica, que em Portugal já provém de fontes renováveis em mais de 60%, mas deve-se muito ao consumo de combustíveis fósseis nos transportes rodoviários, na indústria e nos transportes aéreos¹²¹.

Contudo, esperam-se impactos positivos e muito significativos com a prossecução dos objetivos para a transição energética. Para além de se limitarem os fenómenos naturais graves que decorrem das alterações climáticas, como as secas, tempestades e outros, melhorar-se-á também a qualidade do ar, impactando positivamente a saúde das pessoas, e estima-se que a transição energética se possa também tornar um motor do crescimento económico, criando cerca de 3,5 milhões na UE até 2030¹²², podendo ascender aos 8 milhões de empregos criados na UE até 2050 se se cumprirem todos os objetivos estabelecidos no Acordo de Paris até esse ano¹²³.

Subsetor da Eletricidade

Em 2023, do total de energia consumida, 880 toneladas equivalente de petróleo (tep) foram geradas a partir de eletricidade¹²⁴. No ano anterior, o consumo total atingiu 49 385 044 097 kWh, distribuídos da seguinte forma: 13 857 147 276 kWh no uso doméstico, 12 002 356 981 kWh de uso não doméstico, 19 675 607 910 kWh na indústria, 998 563 917 kWh na agricultura, 1 030 333 394 kWh na iluminação das vias públicas, 1 376 131 397 kWh nos edifícios do estado e 444 903 221 kWh noutras aplicações¹²⁵.

¹¹⁷ IPCC, "Framing and Context", <https://www.ipcc.ch/sr15/chapter/chapter-1/>.

¹¹⁸ "Plano Nacional Energia e Clima 2021-2030", Portugal Energia, <https://www.portugalenergia.pt/setor-energetico/bloco-3/>.

¹¹⁹ "Plano Nacional Energia e Clima 2021-2030", Portugal Energia.

¹²⁰ Ana Oliveira, "Dependência europeia de combustíveis fósseis subiu em 2022. Portugal fica ligeiramente abaixo dos 70%", *ECO*, 30 de janeiro de 2024, <https://eco.sapo.pt/2024/01/30/dependencia-europeia-de-combustiveis-fosseis-subiu-em-2022-portugal-fica-ligeiramente-abaixo-dos-70/>.

¹²¹ Michael McGovern, Sophie Heald e Jamie Pirie, "Oil Dependency in the EU", *Cambridge Econometrics*, maio de 2020, 8.

¹²² Oliveira, "Emprego nas renováveis cresce a pique", *ECO*, 30 de janeiro de 2024.

¹²³ Rafael Correia, "Acordo de Paris pode criar oito milhões de empregos na energia até 2050", *Revista Sustentável*, 30 julho de 2021, <https://www.revistasustentavel.pt/destaques/acordo-de-paris-pode-criar-oito-milhoes-de-empregos-na-energia-ate-2050/>.

¹²⁴ PORDATA, "Consumo de energia primária: total e por tipo de fonte de energia", maio de 2024, https://www.pordata.pt/sites/default/files/2024-09/PORTUGAL_314.xlsx.

¹²⁵ PORDATA, "Consumo de energia elétrica: total e por tipo de consumo", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Consumo_de_energia_eletrica_total_e_por_tipo_de_consumo.xlsx.

Foram gerados aproximadamente 49 043 GWh a partir de fontes renováveis em 2023¹²⁶, representando 75,8% da produção total de energia elétrica¹²⁷. No mesmo ano, a produção bruta de energia elétrica alcançou 49 043 GWh, sendo composta por 13 145 GWh foi energia eólica, 208 GWh de energia geotérmica, 14 868 GWh de energia hídrica, 15 662 GWh de energia térmica e 5 160 GWh de energia fotovoltaica¹²⁸.

Subsetor do Petróleo

Em 2021, as famílias portuguesas consumiram aproximadamente 50 345 Terajoule (TJ) de gasóleo e 33 001 TJ de gasolina¹²⁹. Em 2023, do total da energia consumida, 8 542 tep foram derivadas do petróleo¹³⁰. De acordo com dados do INE, em 2022 foram vendidas cerca de 994 577 toneladas (t) de gasolina sem chumbo 95, 78 612 t de gasolina sem chumbo 98, 4 455 058 t de gasóleo rodoviário, 316 590 t de Gasóleo colorido, 71 548 t de Gasóleo para aquecimento, 344 995 t de *fuel*, 218 373 t de coque de petróleo e de 342 t de outros produtos de petróleo¹³¹. O preço médio do litro de gasolina sem chumbo 95 foi de 1,73 €/L, a gasolina sem chumbo 98 teve o preço médio de 1,92 €/L, o gasóleo rodoviário custou 1,60 €/L e o *fuel* 1,06 €/L¹³².

Em relação à importação de petróleo e derivados, a maior parte foi proveniente do Brasil, com aproximadamente 4 053 300 Nm3. Em seguida, foi importado de Espanha 2 162 915 Nm3. A Argélia e a Nigéria aparecem a seguir com 1 351 847 Nm3 e 1 207 800, respetivamente. Por fim, encontram-se o Azerbaijão com 769 597 Nm3, a Angola com 387 725 Nm3 e o Reino Unido com 58 223 Nm3, totalizando 13 260 549 Nm3¹³³.

Subsetor do Gás

De acordo com os dados divulgados pelo INE, em 2021, as famílias portuguesas consumiram cerca de 12 005 TJ de energia em gás natural e 15 354 TJ de GPL¹³⁴. Em 2023, aproximadamente 3 815 de tep consumidas em Portugal vinham do gás natural¹³⁵. No ano anterior, segundo dados do INE, foram vendidas cerca de 222 406 toneladas (t) de gás butano, 546 678 t de gás propano e de 35 664 t de GPL¹³⁶, tendo a garrafa de gás butano chegado aos 2,40 €/kg, o propano em garrafa teve o preço médio de 2,79 €/kg e o propano canalizado foi de 2,84 €/kg¹³⁷.

¹²⁶ PORDATA, “Produção de energia elétrica: total e a partir de fontes renováveis”, outubro de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Consumo_de_energia_eletrica_total_e_por_tipo_de_consumo.xlsx.

¹²⁷ PORDATA, “Produção de energia elétrica a partir de fontes renováveis (%)”, outubro de 2024, https://www.pordata.pt/sites/default/files/2024-10/Portugal_Producao-de-energia-eletrica-a-partir-de-fontes-renovaveis-percentagem.xlsx.

¹²⁸ PORDATA, “Produção bruta de energia elétrica: total e por tipo de produção de energia elétrica”, outubro de 2024, https://www.pordata.pt/sites/default/files/2024-10/Portugal_Producao-eletrica-por-fonte-de-energia.xlsx.

¹²⁹ PORDATA, “Consumo energético das famílias: total e por alguns produtos energéticos”, maio de 2024, https://www.pordata.pt/sites/default/files/202406/Portugal_Consumo_energetico_das_familias_total_e_por_alguns_produtos_energeticos.xlsx.

¹³⁰ PORDATA, “Consumo de energia primária: total e por tipo de fonte de energia”, maio de 2024.

¹³¹ PORDATA, “Venda de combustíveis para consumo”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Venda_de_combustiveis_para_consumo.xlsx.

¹³² PORDATA, “Preços médios de venda ao público dos combustíveis líquidos e gasosos - Continente”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Precos_medios_de_venda_ao_publico_dos_combustiveis_liquidos_e_gasosos_-_Continente.xlsx.

¹³³ PORDATA, “Importações de energia: total e por principais países de origem”, outubro de 2024, https://www.pordata.pt/sites/default/files/2024-10/Portugal_Importacoes-de-energia-por-principais-paises-de-origem.xlsx.

¹³⁴ PORDATA, “Consumo energético das famílias: total e por alguns produtos energéticos”, maio de 2024.

¹³⁵ PORDATA, “Consumo de energia primária: total e por tipo de fonte de energia”, maio de 2024.

¹³⁶ PORDATA, “Venda de combustíveis para consumo”, maio de 2024.

¹³⁷ PORDATA, “Preços médios de venda ao público dos combustíveis líquidos e gasosos - Continente”, maio de 2024.

Relativamente à importação de gás natural, a maior parte do gás foi importado à Nigéria, com cerca de 1 784 873 Nm³, logo de seguida encontra-se os EUA onde foi importado 1 695 801 Nm³ e por último encontra-se a Rússia com 373 739 Nm³, totalizando 4 075 560 Nm³¹³⁸.

Atualmente, o gás natural possui diversas aplicações, incluindo os setores da mobilidade, terciário, indústria e uso doméstico¹³⁹. Cada uma destas utilizações oferece vantagens em comparação com outros tipos de combustíveis, tais como:

- **Setor da mobilidade:** O Gás Natural Veicular (GNV) e o Gás Natural Comprimido (GNC) oferecem uma redução de aproximadamente 20% nas emissões de CO₂ em comparação com a gasolina e até 25% em relação ao gasóleo. Além disso, são mais baratos, exigem menos manutenção, são menos inflamáveis e emitem menos odor em comparação com os veículos com motores movidos a combustíveis tradicionais¹⁴⁰;
- **Setor terciário:** O preço é mais competitivo em comparação aos outros combustíveis, tem uma elevada eficiência, existe um fornecimento contínuo sem necessidade de armazenamento e tem uma elevada compatibilidade com equipamentos de *catering* e climatização¹⁴¹;
- **Indústria:** O gás não produz cinzas nem outros resíduos sólidos, não necessita de estar armazenado nem de ser abastecido, tem um fornecimento contínuo e tem uma vasta cobertura nacional¹⁴²;
- **Utilização doméstica:** É mais sustentável em comparação com os restantes combustíveis fósseis, tem uma queima mais limpa reduzindo assim os custos de manutenção nos equipamentos e não tem necessidade de armazenamento¹⁴³.

1.1.2. Especificidades tecnológicas

As tecnologias usadas no setor energético, desde turbinas instaladas nas barragens a turbinas eólicas (ou aerogeradores), a painéis fotovoltaicos, ou a sensores existentes nos oleodutos e gasodutos, inserem-se nas classificações de Tecnologia Operacional (TO), Sistemas de Controlo Industrial (SCI) e Sistemas de Supervisão e Aquisição de Dados (SCADA).

A TO refere-se ao uso de *hardware* e *software* para monitorizar e controlar infraestruturas, processos e dispositivos físicos. A TO é principalmente composta por sistemas que desempenham múltiplas tarefas, desde funções de monitorização às de controlo de máquinas industriais. Por sua vez, estes sistemas são normalmente designados como Sistemas de Controlo Industrial, e incluem diversos dispositivos (ex: sensores de deteção de perda de água), sistemas e controlos e redes dos quais dependem múltiplos aspetos da gestão industrial. Os sistemas mais comuns são os SCADA, sistemas que recolhem dados de diversos locais e os enviam para o seu destino de tratamento¹⁴⁴.

¹³⁸ PORDATA, "Importações de energia: total e por principais países de origem", outubro de 2024.

¹³⁹ Associação Portuguesa de Empresas de Gás, "Utilizações e Vantagens", <https://www.apeg.pt/gas-natural/utilizacoes-vantagens/>.

¹⁴⁰ Associação Portuguesa de Empresas de Gás, "Utilização no setor da mobilidade", <https://www.apeg.pt/gas-natural/utilizacao-no-setor-da-mobilidade/>.

¹⁴¹ Associação Portuguesa de Empresas de Gás, "Utilização no Terciário", <https://www.apeg.pt/gas-natural/setor-terciario/>.

¹⁴² Associação Portuguesa de Empresas de Gás, "Utilização na Indústria", <https://www.apeg.pt/gas-natural/industria/>.

¹⁴³ Associação Portuguesa de Empresas de Gás, "Utilização Doméstica", <https://www.apeg.pt/gas-natural/utilizacao-domestica/>.

¹⁴⁴ Fortinet, "What is OT Security?" <https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security>.

O sistema de controlo SCADA é fundamental nas redes de transmissão e distribuição no setor da energia, sendo utilizado para monitorizar instalações em tempo real e controlar remotamente as operações das centrais. Estes sistemas permitem a recolha contínua de dados críticos, como a voltagem, corrente e frequência, possibilitando uma resposta rápida e eficiente a falhas ou interrupções, o que garante uma maior confiabilidade e segurança¹⁴⁵.

Os *PLCs* (*Programmable Logic Controller*) são fundamentais na gestão dos dispositivos nas subestações, como disjuntores, transformadores e sistemas de proteção. Graças à sua robusteza e uma rápida capacidade de resposta, os *PLCs* desempenham um papel crucial nas operações de controlo, assegurando a eficiência e confiabilidade nos processos essenciais para o funcionamento seguro e contínuo de todos os sistemas¹⁴⁶.

Um *Distributed Control System* (*DCS*), possibilita o controlo dos processos em múltiplas áreas, garantindo uma operação integrada e segura. No subsetor do petróleo, por exemplo, este sistema assegura que as condições críticas, como a pressão e a temperatura, permanecem dentro dos parâmetros de segurança, contribuindo para a eficiência e confiabilidade das operações¹⁴⁷.

Subsetor da Eletricidade

No setor da eletricidade em Portugal, algumas destas tecnologias incluem, por exemplo, na parte de produção, dispositivos de telemetria para medir os caudais, o fluxo de água nas barragens e detetar fugas¹⁴⁸, e para medir os ventos e fazer análises preditivas relativas aos parques eólicos. Já na parte da distribuição, crescem os sistemas de gestão das reservas estratégicas de energia, sistemas de monitorização de incêndios perto de redes elétricas, que despoletam o envio de uma equipa ao terreno para avaliar/prevenir danos nos ativos e na população, sistemas de deteção de interrupção do fornecimento de energia elétrica, alimentados por algoritmos que auxiliam na deteção de falhas na infraestrutura de distribuição e sistemas dedicados que preveem as condições meteorológicas de determinadas zonas geográficas e assim sugerir as configurações corretas para os equipamentos instalados nessas zonas¹⁴⁹.

O *Energy Management System* (*EMS*) é uma extensão avançada do SCADA, projetada para otimizar o equilíbrio entre a oferta e a demanda de energia no subsetor da eletricidade. Este sistema auxilia na redução de perdas e no planeamento das operações, permitindo a integração eficiente das fontes renováveis e a gestão da resposta à demanda em tempo real¹⁵⁰.

Verifica-se também a utilização de *machine learning* e de Inteligência Artificial (IA) nalguns campos. Por exemplo, como foi referido em cima, já são aplicadas soluções para derivar a velocidade do vento observável num parque eólico e testar qual será o *output* energético num outro parque eólico com base nesses dados¹⁵¹.

¹⁴⁵ SCADA INFO, "SCADA and Energy Management System", <https://www.scadainfo.com/scada-and-energy-management-system/>.

¹⁴⁶ Ephrem Ryan Alphonsus e Mohammad Omar Abdullah, "A review on the applications of programmable logic controllers (PLCs)", julho de 2016, 2, <https://www.sciencedirect.com/science/article/abs/pii/S1364032116000551>.

¹⁴⁷ Arkadiusz Hulewicz, Zbigniew Krawiecki e Krzysztof Dziarski, "Distributed control system DCS using a PLC controller", 15 de julho de 2019, 1, https://www.itm-conferences.org/articles/itmconf/pdf/2019/05/itmconf_zkwe2019_01041.pdf.

¹⁴⁸ Lusa, "Portugal desperdiça todos os anos várias barragens do Alqueva em fugas de água", *Público*, 6 de maio de 2023, <https://www.publico.pt/2023/05/06/azul/noticia/portugal-desperdiça-anos-varias-barragens-alqueva-fugas-agua-2048583>.

¹⁴⁹ EDP, "A nossa transformação digital", *Inovação na EDP*, <https://www.edp.com/pt-pt/inovacao/transformacao-digital>.

¹⁵⁰ SCADA INFO, "SCADA and Energy Management System".

¹⁵¹ EDP, "A nossa transformação digital", *Inovação na EDP*.

Está a ocorrer um investimento em sete áreas chave. O investimento nestas áreas reflete um alinhamento com as necessidades específicas do subsetor e as tendências globais da transição energética. Cada uma destas áreas aborda desafios técnicos, económicos e ambientais essenciais para a modernização e descarbonização do subsetor elétrico. Apesar disto, a relevância destes projetos também é estratégica, já que torna o subsetor mais eficiente, sustentável e adaptado aos desafios futuros. Alguns projetos já estão em andamento¹⁵²:

- **Energias renováveis:** *BladeBug*, entre outros;
- **Redes:** *IONATE*, *eNeuron*, *RESCCUE*, entre outros;
- **Sistemas distribuídos de energia:** *ProLight*, *AI4PV*, *SocialWatt*, entre outros;
- **Hidrogénio verde:** *Behyond* e *FLEXnCONFU*;
- **Armazenamento de energia e flexibilidade:** *FIRMe*, *MAGPIE*, *SunLab*, entre outros;
- **Mobilidade sustentável:** *PRR Be Neutral*, *POCITYF*, entre outros;
- **Descarbonização de usos de energia:** *Aria 2*, *Bairro Solar*, *Dominoes*, entre outros;

A *BladeBug* está a desenvolver um projeto com o objetivo de resolver os desafios operacionais na manutenção e inspeção de turbinas eólicas. Tradicionalmente, estas inspeções, são manuais, complexas e dispendiosas, apresentando riscos para os técnicos envolvidos. Utilizando sistemas robóticos de inspeção nas turbinas eólicas, é esperado que se possa reduzir custos, minimizar os riscos para os trabalhadores e aumentar a eficácia da manutenção. Em junho de 2024, foi realizado um projeto-piloto em Albacete, utilizando robôs para a inspeção de pás de turbinas inacessíveis por corda. No decorrer desta ação foram realizadas inspeções de ensaios não destrutivos assim como funcionais¹⁵³.

Na área das redes de distribuição de energia e com o objetivo de tornar a distribuição mais inteligente, eficiente e resiliente, a EDP está a testar o Transformador Híbrido Inteligente (HIT) inovador da *IONATE*, que aumenta a visibilidade dos dados e o controlo do fluxo da energia das redes elétricas em tempo real. Esta inovação consegue estabilizar os fluxos de energia e aumenta a tolerância da rede às energias renováveis, maximizando assim a quantidade de energia transportada. Este projeto é importante para ajudar na transformação gradual da rede num sistema flexível e inteligente¹⁵⁴.

Atualmente, as centrais fotovoltaicas enfrentam desafios na identificação de falhas, que muitas vezes são difíceis de detetar. O projeto *AI4PV* visa aprimorar o desempenho operacional destas instalações fotovoltaicas por meio da aplicação de IA e análise de dados. Espera-se que, com a implementação deste projeto, a confiabilidade e a eficiência operacional melhorem significativamente, permitindo uma deteção precoce de falhas e diagnósticos mais precisos. Como resultado, o desempenho económico também deverá aumentar, reduzindo o tempo de inatividade das centrais¹⁵⁵.

Na área do hidrogénio verde, está a ser desenvolvido o programa *BEHYOND* que visa criar protótipos e implementar um projeto piloto para validar uma nova tecnologia de produção de hidrogénio em *offshore*. Os principais objetivos deste programa incluem o desenvolvimento de um módulo de produção de hidrogénio através de eletrólise, a criação de um sistema inovador para lidar com os desafios de intermitência das energias renováveis e a ampliação da participação do hidrogénio na demanda energética, promovendo assim a sustentabilidade¹⁵⁶.

¹⁵² EDP, "Inovação na EDP", <https://www.edp.com/pt-pt/inovacao>.

¹⁵³ EDP, "BladeBug: Inspeção e Manutenção de Turbinas Eólicas", <https://www.edp.com/pt-pt/edp-group/bladebug-inspecao-e-manutencao-de-turbinas-eolicas>.

¹⁵⁴ EDP, "IONATE", <https://www.edp.com/pt-pt/inovacao/ionate>.

¹⁵⁵ EDP, "AI4PV", <https://www.edp.com/pt-pt/inovacao/new/ai4pv>.

¹⁵⁶ EDP, "BEHYOND: sinergias entre o hidrogénio e a eólica offshore", <https://www.edp.com/pt-pt/inovacao/behond-sinergias-entre-o-hidrogenio-e-a-eolica-offshore>.

O projeto FIRMe, lançado em 2023 pela E-REDES, é o primeiro mercado local de serviços de flexibilidade. O objetivo deste projeto é adaptar-se às exigências deste subsetor e testar o mercado, incentivando os prestadores de serviços a participar. Os consumidores e produtores são desafiados a ajustar o seu consumo ou a injetar energia na rede, recebendo em troca um valor acordado pela disponibilidade que oferecem. A plataforma disponibiliza informações sobre as necessidades e oportunidades, permitindo que todos os agentes do mercado participem¹⁵⁷.

A Agenda *Be.Neutral* tem como objetivo colocar Portugal na vanguarda da exportação de produtos ciber-físicos de mobilidade com emissões zero para várias cidades. O projeto visa desenvolver, industrializar e operar novos produtos e serviços de mobilidade¹⁵⁸. O projeto ARIA2 tem como objetivo desenvolver e avaliar os serviços de informação com base em dados de observação do planeta para o setor de energia eólica, focando-se em infraestruturas *offshore* na Região Atlântica. Irá ser criado um painel integrado que irá centralizar os acessos a serviços, permitindo a visualização avançada de dados. Através da avaliação da erosão causada por chuva nas turbinas, será possível prever as necessidades de reparação dos sistemas de proteção. Este projeto tem como destinatários os proprietários e operadores de parques eólicos¹⁵⁹.

Subsetores do Petróleo e do Gás

Nos subsectores do petróleo e do gás, os dispositivos de telemetria desempenham também funções importantes. Permitem sobretudo a rápida deteção de bloqueios e de fugas na rede de abastecimento. Igualmente importantes são os sistemas que permitem agendar e automatizar operações, controlar fluxos, recolher dados e monitorizar os níveis de compressão, tanto nos oleodutos e gasodutos, como nos tanques de armazenamento¹⁶⁰. Também nestes subsectores se começa a verificar a utilização de soluções de IA, orientadas para a criação e análise de modelos geológicos de potenciais locais para novas prospeções de petróleo e gás natural¹⁶¹.

Os *Safety Instrumented Systems (SIS)* são sistemas críticos de segurança que interrompem automaticamente as operações potencialmente perigosas ao detetar condições anormais. São essenciais em ambientes de alto risco, como refinarias e plataformas, desempenhando um papel crucial na prevenção de acidentes graves¹⁶².

Em gasodutos, são utilizados sistemas específicos para a deteção de fugas, conhecidos como *Leak Detection Systems (LDS)*. Estes são implementados ao longo das redes de gasodutos e previnem acidentes graves ao monitorizar e identificar fugas por meio de sensores de pressão integrados no SCADA, permitindo uma resposta rápida e precisas em emergências¹⁶³.

¹⁵⁷ EDP, "FIRMe: Flexibilidade Integrada em Regime de Mercado", <https://www.edp.com/pt-pt/edp-group/firme-flexibilidade-integrada-em-regime-de-mercado>.

¹⁵⁸ EDP, "PRR Be Neutral – Ubiquitous Charging", <https://www.edp.com/pt-pt/innovation/prr-be-neutral-ubiquitous-charging>.

¹⁵⁹ EDP, "ARIA 2", <https://www.edp.com/pt-pt/inovacao/aria-2>.

¹⁶⁰ ARC Advisory Group, "Oil & Gas Operations Technology and Supplier Selection", <https://www.arcweb.com/technology-evaluation-and-selection/oil-gas-operations-technology-supplier-selection>.

¹⁶¹ Ana Guerra, "IBM e Galp juntas em projeto de Inteligência Artificial", *Ntech.news*, 12 de julho de 2018, <https://www.ntech.news/ibm-e-galp-juntas-em-projeto-de-inteligencia-artificial/>.

¹⁶² Yury Redutskiy, "Optimization of Safety Instrumented System Design and Maintenance Frequency for Oil and Gas Industry Processes", março de 2017, 46, https://www.researchgate.net/publication/315971691_Optimization_of_Safety_Instrumented_System_Design_and_Maintenance_Frequency_for_Oil_and_Gas_Industry_Processes.

¹⁶³ Lawrence Boaz, Shubi Kaijage e Ramadhani Sinde, "An overview of pipeline leak detection and location systems", julho de 2014, 133, <https://ieeexplore.ieee.org/abstract/document/7055147>.

Com o avanço da tecnologia, a eficiência na produção do subsetor do petróleo e gás tem sido significativamente aprimorada por meio da *Enhanced Oil Recovery (EOR)*, um processo de extração que ajuda a extrair mais matéria-prima dos poços após a utilização dos processos convencionais. Existem quatro métodos principais de *EOR*: térmico, gás, químico e outros, como os acústicos e microbiológicos. A escolha do método mais adequado deve ter em consideração as características do fluido e do reservatório.

O método químico envolve a injeção de reagentes químicos para limpar a zona de perfuração, o que pode aumentar a eficácia do deslocamento de fluidos e possibilitar um aumento de até 35% na recuperação do poço. Já o método térmico é recomendado para situações em que a extração enfrenta dificuldades físicas e geológicas, permitindo uma recuperação entre 30 e 58%. Por sua vez, o método do gás é o mais utilizado e consiste na injeção do gás no reservatório, o que reduz a tensão superficial e pode resultar num aumento da recuperação entre 5 e 19%¹⁶⁴.

A PETRONAS, uma das principais companhias de petróleo e de gás da Malásia, implementou o programa *AVEVA Predictive Analytics* com o objetivo de otimizar as suas operações e aumentar a eficiência na gestão de ativos. Este programa utiliza técnicas avançadas de análise preditiva para monitorizar o desempenho dos equipamentos e prever possíveis falhas. Mais de 200 modelos foram aplicados no primeiro ano resultando em 51 alertas de possíveis falhas nos equipamentos, e numa poupança de 17,4 milhões de dólares, o que corresponde a 14 vezes o montante do investimento¹⁶⁵.

O projeto *Hyfuelup* tem como objetivo desenvolver uma tecnologia inovadora para produzir gás natural renovável a partir de resíduos florestais, com um investimento de 10,3 milhões de euros. Em parceria com 11 entidades, incluindo o Laboratório Nacional de Energia e Geologia e o Instituto Politécnico de Portalegre, o projeto utiliza um processo de gaseificação a temperaturas entre 800 e 1.000 graus *celsius* para converter a biomassa num gás combustível, rico em metano e hidrogénio. Esta inovação reside na produção de metano através deste processo. O foco deste projeto são os setores do transporte e mobilidade, permitindo a distribuição do metano para áreas sem acesso à rede de gás natural¹⁶⁶.

O *Green Pipeline Project*, liderado pela Galp Gás Natural Distribuição e financiado pelo Fundo de Apoio à Inovação, pretende injetar hidrogénio verde na rede de gás natural do Seixal. O projeto abrangerá 80 clientes residenciais, terciários e industriais e, inicialmente, será injetado 2% de hidrogénio, com aumento gradual até um máximo de 20%¹⁶⁷.

¹⁶⁴ Douglas Silva, Caio Catarina e Eric Battle, "Advanced oil recovery associated with carbon capture and storage", janeiro de 2022, 4-5, <http://dx.doi.org/10.33448/rsd-v11i1.24599>.

¹⁶⁵ AVEVA, "AVEVA Predictive Analytics", 2023, https://www.aveva.com/content/dam/aveva/documents/brochures/Brochure_AVEVA_PredictiveAnalytics_23-02.pdf

¹⁶⁶ HYFUELUP, "Shaping a better tomorrow with renewable natural gas", <https://hyfuelup.eu/>.

¹⁶⁷ catimProjetos, "Green Pipeline Project", <https://www.projetoscatim.com/projects-green-pipeline>.

1.2. Ameaças

A referida importância do setor da energia, bem como a dependência dos demais setores face a este, tornam-no um alvo atrativo para os agentes de ameaça que procuram o simples ganho financeiro, ou mesmo para aqueles que procuram perturbar o normal funcionamento de um país e afetando as suas dimensões política, militar ou económica.

Os ataques que comprometam a cibersegurança podem ter um impacto brutal, interrompendo o funcionamento de centrais elétricas, estações de transformação e afetar gravemente a distribuição de energia, provocando apagões, impossibilitando o aquecimento dos edifícios (habitações ou locais de trabalho) ou impedindo o abastecimento dos transportes.

Este setor acaba por estar exposto a outras ameaças devido às tecnologias utilizadas. Grande parte da TO envolve, muitas vezes, máquinas industriais grandes, pesadas e caras, cuja substituição ou atualização é também ela dispendiosa. Por estes motivos, o ciclo de vida dos equipamentos utilizados costuma também ser longo (podendo chegar a 20, 30 ou mais anos), resultando na utilização de sistemas *legacy*.

Os sistemas *legacy* consistem em *hardware* ou *software* antigo que ainda cumpre as funções para as quais foi adquirido¹⁶⁸, mas que são difíceis de tornar seguros por já não receberem atualizações. Como são sistemas antigos, não podem ser integrados com outras tecnologias ou sistemas mais recentes, criando silos de dados^{169 170}. Devido à sua obsolescência, as capacidades criptográficas destes sistemas são limitadas, o que os torna vulneráveis a ameaças como o *ransomware* e ataques *DDoS*¹⁷¹.

Segundo o *Threat Landscape Report de 2023* da ENISA, este setor, apesar de não deixar de ser um alvo, ficou na última posição em relação aos outros setores essenciais tendo sofrido, entre julho de 2022 e junho de 2023, cerca de 190 incidentes de cibersegurança (4% do total de incidentes registados)¹⁷². Os principais ataques passaram pelo comprometimento da disponibilidade dos serviços e da informação (ataques de negação de serviço: “*Denial of Service*”, *DoS*), ataques de *ransomware*, contando-se ainda ameaças relativas a dados (*data breaches* e furto de dados)¹⁷³. O ataque predominante foi o *ransomware*, onde 25% dos casos foram operações de um só grupo (*Lockbit*) e 87% dos casos vieram de apenas 20 grupos¹⁷⁴.

¹⁶⁸ “Securing Legacy OT Systems: Challenges and Strategies”, *Security Boulevard*, 24 de abril de 2023, <https://securityboulevard.com/2023/04/securing-legacy-ot-systems-challenges-and-strategies/>.

¹⁶⁹ Zahir Irani et al., “The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis”, 2023, 2, <https://www.sciencedirect.com/science/article/pii/S0740624X22001204>.

¹⁷⁰ Um “silo de dados” é um repositório de dados isolado dos restantes sistemas da organização. Geralmente, um silo de dados é criado quando um sistema é incompatível com os restantes, dificultando o acesso e a utilização dos dados recolhidos.

¹⁷¹ “Securing Legacy OT Systems”, *Security Boulevard*, 24 de abril de 2023.

¹⁷² ENISA, “ENISA Threat Landscape 2023”, 19 de outubro de 2023, 13.

¹⁷³ ENISA, “ENISA Threat Landscape 2023”, 19 de outubro de 2023, 14.

¹⁷⁴ ENISA, “ENISA Threat Landscape 2023”, 19 de outubro de 2023, 16 e 17.

Outra ameaça prende-se com o protocolo IEEE 1588 (*Precision Time Protocol - PTP*)¹⁷⁵. Este protocolo, essencial para garantir a sincronização temporal de forma precisa, desempenha um papel crucial nas funções de proteção e controlo (P&C). Este protocolo apresenta vulnerabilidades significativas relativamente a incidentes de sincronização do tempo no setor de energia. Ataques como a introdução de atrasos e modificações de pacotes podem comprometer a fiabilidade do protocolo. Este comprometimento pode levar a atrasos na resposta a falhas e pode, também, comprometer a análise e o controlo dos sistemas nas subestações. Como a sincronização dos relógios nos sistemas SCADA e EMS é essencial para a coordenação dos sistemas, caso ocorra uma falha nesta sincronização, a tomada de decisões em tempo real pode ficar afetada¹⁷⁶.

Ainda sobre as ameaças relativas foram realizados testes experimentais com diferentes tipos de ataques ao protocolo *PTP*, incluindo atrasos, modificações de pacotes, ataques *DDoS* e *PTP Spoofing*. O *PTP* estabelece uma hierarquia de temporização *master-slave*¹⁷⁷ utilizando o algoritmo *Best Master Clock Algorithm (BMCA)*¹⁷⁸. Este algoritmo escolhe o relógio mais preciso e estável para servir o relógio *master* da rede. Esta escolha é feita com base nas mensagens trocadas entre os relógios, que incluem informações como a qualidade e a prioridade do relógio. O *BMCA* garante que todos os dispositivos mantêm a sincronização com o melhor relógio disponível¹⁷⁹.

Existem dois modos de medição de atrasos no *PTP*, o *End-to-End (E2E)* e o *Peer-to-Peer (P2P)*. O princípio *E2E* envolve a emissão de *timestamps* nos pontos de entrada e saída do relógio *master* e do relógio transparente (*Transparent Clock*)¹⁸⁰. Um relógio transparente atualiza as mensagens *PTP* com a informação sobre o tempo necessário para levar as mensagens através da rede desde um ponto de entrada até ao ponto de saída. O relógio transparente é assim responsável por calcular o desvio temporal entre o *master* e o *slave*. Este desvio deve ser ajustado para manter a sincronização precisa entre os relógios *master* e *slave*. Já na comunicação *P2P*, os relógios *master* e *slave* comunicam diretamente entre si para calcular o tempo de ida e volta das mensagens, determinando o atraso da rede entre eles. Cada relógio *slave* calcula e ajusta o tempo em função dos atrasos registados, sem a necessidade de comunicarem com o relógio *master*. Existem, neste teste, dois *slaves* denominados X e Y e um *master*¹⁸¹.

¹⁷⁵ IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", 24 de julho de 2008, <https://standards.ieee.org/ieee/1588/4355/>.

¹⁷⁶ Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588 under Time Synchronization Attacks", 4 de Agosto de 2019, 1, <https://ieeexplore.ieee.org/abstract/document/8973494>.

¹⁷⁷ Num sistema de comunicação, o *master* controla a comunicação e o *slave* apenas responde aos comandos do *master*. (Fonte: Ingrams Time Systems, "Master & Slave Systems", <https://www.ingrams.com.au/master-and-slave-systems>.)

¹⁷⁸ Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588", 4 de agosto de 2019, 1 e 2.

¹⁷⁹ Nokia, "Best Master Clock Algorithm", <https://infocenter.nokia.com/public/7705SAR234R1A/index.jsp?topic=%2Fcom.nokia.basic-system-guide%2Fbest-master-clock-algorithm.html>.

¹⁸⁰ Um relógio transparente ou *transparent clock* atualiza as mensagens *PTP* com a informação sobre o tempo necessário para levar as mensagens através da rede desde um ponto de entrada até ao ponto de saída.

¹⁸¹ Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588", 4 de agosto de 2019, 2.

De seguida, relativamente ao ataque de modificação de pacotes, foram introduzidos erros de 500 e 1000 microssegundos no campo *correctionField* das mensagens *Sync* (no modo de um e dois passos) e *Follow_Up* (no modo de dois passos), com o mecanismo de *P2P* ativo. Os resultados mostraram que esta modificação comprometeu a precisão da sincronização. Já no ataque de *DDoS*, os resultados experimentais mostraram que a sincronização dos relógios *slave* foi afetada pelo tráfego excessivo. Devido a esta injeção de tráfego, os pacotes *PTP* não conseguiram chegar aos relógios escravos, resultando na perda de sincronização entre os *slaves* X e Y e o relógio *master*. Por fim, no ataque de *spoofing*, quando o relógio de *spoofing* foi conectado ao sistema, conseguiu vencer a eleição no algoritmo *BMCA* (devido à alteração do campo da prioridade pelo emulador), ficando assim com maior prioridade em relação ao relógio *master* verdadeiro. Ambos os relógios *slave* detetaram a mudança e sincronizaram com o relógio de *spoofing*. Quando desconectado, os relógios *slave* voltaram a sincronizar com o *master* verdadeiro¹⁸². Os resultados evidenciam a necessidade de reforçar a segurança deste protocolo para prevenir ataques que podem comprometer os sistemas de controlo neste setor¹⁸³.

O artigo "*Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed*" apresenta uma plataforma de testes em tempo real para a análise vulnerabilidades de cibersegurança no protocolo Modbus RTU/Modbus TCP. Este protocolo é amplamente utilizado nos sistemas SCADA, em redes elétricas inteligentes (*smart grids*) e nos subsectores de petróleo e gás¹⁸⁴.

O protocolo *Modbus RTU/Modbus TCP* foi utilizado como referência para demonstrar a eficácia da plataforma de testes na execução de ciberataques a protocolos dos sistemas do subsector da energia. A escolha deste protocolo deve-se a diversos fatores: o protocolo ainda é amplamente utilizado nos sistemas do setor. É considerado um protocolo simples e fácil de implementar, e as bibliotecas do protocolo estão disponíveis de forma gratuita para as empresas o implementarem. Apesar de ser amplamente utilizado, o protocolo apresenta vulnerabilidades significativas, como a ausência de criptografia e mecanismos de autenticação robustos¹⁸⁵. Este protocolo funciona num modelo de comunicação *master-slave*, onde o *slave* inicia as consultas e o *master* responde. A comunicação pode ocorrer via rede, *TCP* ou *UDP*. Como o *Modbus* não inclui autenticação, autorização ou criptografia, permite que qualquer pedido bem formatado seja processado como válido. Este protocolo é composto por seis campos¹⁸⁶:

- **Identificador da transação:** Correlaciona pedidos e respostas;
- **Identificador do protocolo:** É sempre 0 no protocolo *Modbus*;
- **Comprimento:** Indica o número de bytes restantes;
- **Identificador da unidade:** Identifica o *slave* através de um endereço de IP;
- **Código da função:** Especifica a ação solicitada pelo *master*;
- **Dados:** Campo de comprimento variável.

O *master* envia um pedido e o *slave* responde com o identificador da transação, identificador da unidade e a função, indicando sucesso. Em caso de erro, o código da função tem 128 adicionado ao seu valor. A simplicidade deste protocolo facilita a criação de pacotes falsos¹⁸⁷.

¹⁸² Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588", 4 de agosto de 2019, 4.

¹⁸³ Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588", 4 de Agosto de 2019, 5.

¹⁸⁴ Bo Chen et al., "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed", 25 de junho de 2015, 1, <https://ieeexplore.ieee.org/abstract/document/7129084>.

¹⁸⁵ Bo Chen et al., "Implementing attacks for modbus", 25 de junho de 2015, 2.

¹⁸⁶ Christopher Parian et al., "Fooling the Master: Exploiting Weaknesses in the Modbus Protocol", 2454, <https://www.sciencedirect.com/science/article/pii/S1877050920312576>.

¹⁸⁷ Christopher Parian et al., "Fooling the Master: Exploiting Weaknesses in the Modbus Protocol", 2454.

Um ataque *MITM* ocorre quando um computador não confiável consegue acesso à comunicação entre duas partes, sem que estejam cientes de tal intrusão. Para que este tipo de ataque seja bem-sucedido, o atacante deve estar na mesma sub-rede do computador-alvo e ser capaz de alterar as caches do *Address Resolution Protocol (ARP)*. Desta forma, o atacante pode receber o tráfego de ambas as vítimas e agir como um *router*, encaminhando o tráfego recebido. No ambiente de testes deste estudo, o atacante alterou as *caches* do *ARP* cliente *Modbus*, após isso, conseguiu visualizar os pacotes de consulta e resposta trocados entre o *master* e o *slave* e foi utilizada a ferramenta *Wireshark* para analisar os mesmos. Com o conhecimento dos endereços de IP do *master* e do *slave*, foi possível ao atacante emular o *master* e enviar um comando *Modbus* para desligar o dispositivo eletrónico¹⁸⁸.

Para avaliar a sensibilidade deste protocolo a atrasos, o mesmo foi submetido a um ataque *TCP SYN Flood* para sobrecarregar o *master*. Este tipo de ataque aproveita-se do processo de *handshake* do *TCP* para iniciar várias conexões com endereços de IP falsos, saturando-o com pedidos falsos. Foram enviados cerca de 120 pedidos falsos por segundo. Antes deste ataque, a resposta a um comando era de 300 milissegundos, durante este ataque, a resposta passou a ser de 3 segundos. Este atraso impede que o centro de controlo tenha uma visão atualizada da rede, comprometendo as operações de funções críticas. A análise conclui que a falta de autenticação e proteção no protocolo torna-o vulnerável a ataques que podem afetar a estabilidade. Como recomendações, propõe-se a adição de autenticação, criptografia a nível de *IP* e outros mecanismos de defesa para mitigar estes riscos¹⁸⁹.

Ainda sobre ameaças do setor energético, segundo dados do CERT.PT, registaram-se em Portugal, entre 2019 e 2023, 144 ataques ao setor¹⁹⁰.

Figura 1 - Número de incidentes no setor da Energia anualmente



(Fonte: CNCS, “Incidentes e Setores: 2019-2023”, Conhecimento Situacional: Estatísticas, obtido a 24 de outubro de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

¹⁸⁸ Bo Chen et al., “Implementing attacks for modbus”, 25 de junho de 2015, 1-4.

¹⁸⁹ Bo Chen et al., “Implementing attacks for modbus”, 25 de junho de 2015, 5-6.

¹⁹⁰ CNCS, “Incidentes e Setores”, Conhecimento Situacional: Estatísticas, obtido a 24 de outubro de 2024, <https://www.cncs.gov.pt/pt/estatistica/#cert.pt>.

Subsetor da Eletricidade

Este subsetor enfrenta ameaças constantes, tornando essencial a análise dos impactos de ataques passados para compreender possíveis incidentes futuros.

Em 2001, o operador de eletricidade da Califórnia, foi vítima de um incidente de cibersegurança, onde os atacantes conseguiram acesso à rede interna do operador. Este ataque foi conduzido através de um método de infiltração, utilizando vários servidores e prestadores de serviços de Internet para ocultar a origem dos atacantes¹⁹¹. Apesar disto, os atacantes foram descobertos antes de conseguirem ter acesso ao controlador PLC¹⁹².

Mais tarde, em 2012, foi criado o *malware* conhecido por *Flame*, tendo este sido espalhado pelo Médio Oriente e Norte de África, onde operou por pelo menos dois anos. Este *malware* era extremamente sofisticado e conseguia recolher dados como gravações de áudio, capturas de ecrã e comunicações *Bluetooth*, além de conseguir monitorizar as teclas digitadas. Utilizava certificados digitais falsos da *Microsoft* para se espalhar sem ser detetado¹⁹³. Foi concebido para espionagem e análise de dados, e foi descoberto depois de o Ministério do Petróleo do Irão e a empresa nacional iraniana de petróleo denunciarem o furto e a eliminação de dados críticos nos seus sistemas¹⁹⁴.

Um outro exemplo marcante de um ciberataque com grande impacto foi o ataque à rede elétrica da Ucrânia em dezembro de 2015. Este ataque foi particularmente importante porque foi o primeiro em que efetivamente uma entidade externa ganhou o controlo dos sistemas de uma central elétrica e cortou o abastecimento de energia. Nalgumas zonas, o corte durou apenas uma hora, enquanto noutras só foi resolvido ao fim de seis horas. Ao todo, cerca de 230 mil pessoas foram afetadas pelo corte de energia. Crê-se que o acesso terá sido obtido pelos agentes de ameaça através de uma campanha de *spear-phishing* dirigida aos colaboradores de TI e administradores de sistemas de diversas companhias de distribuição de energia elétrica da Ucrânia¹⁹⁵.

Um outro caso ocorreu em Portugal - o ciberataque à EDP - a 13 de abril de 2020. Tratou-se de um ataque de *ransomware*, que utilizou o vírus *Ragnar Locker*. Parte da rede e dos sistemas da empresa ficaram bloqueados e, segundo a própria EDP, o normal funcionamento de alguns serviços e operações, como o atendimento ao cliente, ficou condicionado, apesar de não se ter registado qualquer impacto na continuidade do fornecimento de energia¹⁹⁶.

¹⁹¹ The New York Times, "Hackers Attacked California Power", 10 de junho de 2001, <https://www.nytimes.com/2001/06/10/us/hackers-attacked-california-power.html>.

¹⁹² ECS, "Energy Networks and Smart Grids", novembro de 2018, 5, <https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf>.

¹⁹³ Kim Zetter, "Meet 'Flame', The Massive Spy Malware Infiltrating Iranian Computers", Wired, 28 de maio de 2012, <https://www.wired.com/2012/05/flame/>.

¹⁹⁴ ECS, "Energy Networks and Smart Grids", novembro de 2018, 6.

¹⁹⁵ CISA, "Cyber-Attack Against Ukrainian Critical Infrastructure", 20 de julho de 2021, <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.

¹⁹⁶ Miguel Prado, "EDP: imune à crise, mas não aos hackers", *Expresso*, 18 de abril de 2020, <https://expresso.pt/economia/2020-04-18-EDP-imune-a-crise-mas-nao-aos-hackers>.

De seguida, apresenta-se uma tabela que faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos¹⁹⁷, de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal¹⁹⁸.
- **Agentes estatais:** caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa¹⁹⁹.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação, por uma forte elaboração ficcionada do ciberataque e das suas consequências bem como pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável²⁰⁰.
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade, podendo ser maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento). Comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer, e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso²⁰¹. No caso, consideraram-se os colaboradores internos maliciosos.

¹⁹⁷ CNCS, “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.

¹⁹⁸ CNCS, “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”, maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf>.

¹⁹⁹ CNCS, “Relatório Riscos & Conflitos 2021”, maio de 2021, 75.

²⁰⁰ CNCS, “Relatório Riscos & Conflitos 2021”, maio de 2021, 75-76.

²⁰¹ CNCS, “Relatório Riscos & Conflitos 2021”, maio de 2021, 76-77.

Tabela 5 - Agentes de ameaça mais prováveis (Eletricidade)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>				
<i>Malware</i>				
Vulnerabilidades				
<i>Phishing</i>				
Acesso indevido a dados pessoais				
<i>DDoS</i>				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:

 - Agente de ameaça provável

Subsetor do Petróleo

O incidente de cibersegurança na Colonial Pipeline, empresa norte-americana detentora do maior oleoduto dos Estados Unidos, ocorreu a 7 de maio de 2021 e foi um ataque de *ransomware* que afetou as operações da mesma durante cerca de cinco dias. O oleoduto, que cobre cerca de 8850 km e é capaz de transportar o equivalente a três milhões de barris de combustível por dia, ao longo do território entre o Texas e Nova Iorque, foi desligado, de modo a impedir que a infeção se alastrasse à TO do mesmo. Apesar de o próprio oleoduto não ter sido comprometido pelo ataque, as notícias do ciberataque e da paragem do funcionamento do oleoduto levaram a população a uma corrida aos postos de abastecimento, resultando em longas filas e a reservas esgotadas na costa leste dos EUA²⁰².

²⁰² CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years", 7 de maio de 2023, <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>.

O acesso inicial à rede e aos sistemas da empresa terá sido obtido através da descoberta de uma palavra-passe de um ex-colaborador da empresa cujo perfil de utilizador ainda não tinha sido desativado. A palavra-passe foi introduzida numa VPN que não possuía autenticação multifator, dando acesso imediato à rede e a diversos sistemas²⁰³. A Colonial Pipeline acabaria por pagar o resgate exigido de 75 *bitcoins*, na altura valorizadas em cerca de 4,4 milhões de dólares, de modo a recuperar o controlo dos seus sistemas. Entre maio e junho, o Departamento de Justiça dos EUA conseguiu recuperar cerca de 85% das *bitcoins* transferidas, mas devido à desvalorização que estas tinham sofrido, as *bitcoins* recuperadas valiam, à data, cerca de 2,3 milhões de dólares, cerca de 52% do valor do resgate pago²⁰⁴.

No final de janeiro de 2022, um ataque de *ransomware* afetou gravemente pelo menos 17 portos e terminais de petróleo na Europa Ocidental, impactando também o armazenamento e transporte de petróleo. O ataque causou o desvio de navios petroleiros, prejudicando as cadeias de abastecimento e dificultando o carregamento e descarregamento de produtos refinados. O grupo de cibercriminosos responsável pelo ataque foi identificado como sendo o grupo BlackCat e os relatórios de investigação sobre este incidente sugerem que o impacto foi maior nos sistemas de TI do que nos sistemas de TO²⁰⁵.

Tal como para o subsetor da eletricidade, volta-se a apresentar uma tabela que compila as principais ameaças do setor e dos agentes de ameaça mais prováveis de as concretizar.

Tabela 6 - Agentes de ameaça mais prováveis (Petróleo)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>				
<i>Malware</i>				
Vulnerabilidades				
<i>Phishing</i>				
<i>DDoS</i>				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:

 - Agente de ameaça provável

²⁰³ Stephanie Kelly e Jessica Resnick-ault, "One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators", *Reuters*, 9 de junho de 2021, <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/>.

²⁰⁴ CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years", 7 de maio de 2023.

²⁰⁵ Pacific Maritime Magazine, "European Oil Port Terminals Crippled by Cyberattack and Ransomware", <https://pacmar.com/article/european-oil-port-terminals-crippled-by-cyberattack-and-ransomware/>.

Subsetor do Gás

Este subsetor, tal como os anteriores, enfrenta ameaças constantes, tornando essencial a análise dos impactos de ataques passados para compreender possíveis incidentes futuros.

Em 1982, num dos primeiros incidentes de cibersegurança conhecidos, ocorreu uma explosão num gasoduto na Sibéria. Este incidente teve origem externa e foi realizado através da introdução de *malware* nos sistemas SCADA de gestão do gasoduto²⁰⁶. Este *malware* duplicou a pressão durante um teste e, alegadamente, como resultado, ocorreu uma explosão equivalente a três toneladas de TNT²⁰⁷.

Em 1999, a Gazprom, sofreu um incidente de segurança, onde um atacante interno conseguiu tomar conta de um quadro de distribuição que controlava o gás nos gasodutos²⁰⁸, este atacante conseguiu invadir os sistemas SCADA da Gazprom com a ajuda interna e utilizando um *Trojan* para ultrapassar a segurança. Através do quadro de distribuição, foi possível controlar temporariamente o fluxo de gás nos gasodutos²⁰⁹.

No mesmo ano, nos Estados Unidos da América (EUA), ocorreu um erro relacionado com um novo desenvolvimento de uma base de dados para o sistema operativo dos sistemas SCADA dos gasodutos da Olympic. Como consequência, ocorreu uma fuga de gás que provocou oito feridos e três mortos²¹⁰. A investigação identificou vários problemas de segurança, incluindo: as escavações realizadas nas proximidades do gasoduto; as avaliações das inspeções internas; a gestão dos dados disponíveis para garantir a integridade do sistema; e o desempenho e segurança do sistema SCADA da Olympic²¹¹.

Em 2012, a Saudi Aramco foi vítima do *malware Shamoon* e cerca de 35 mil computadores tiveram os seus dados parcial ou totalmente apagados pelo vírus. O propósito deste *malware* é apagar todos os dados por completo em vez de exigir resgate. Em resposta ao ataque, a Saudi Aramco desligou fisicamente todos os escritórios da Internet, o que levou a um regresso temporário a sistemas de papel. Apesar dos sistemas de produção de petróleo e gás não terem sido afetados, os sistemas de pagamento ficaram fora de serviço, causando filas de camiões de combustível que não podiam ser carregados por falta do processamento de pagamentos. A empresa demorou cinco meses a recuperar totalmente deste incidente²¹².

Tal como para o subsetor da eletricidade e do petróleo, volta-se a apresentar uma tabela que compila as principais ameaças do setor e dos agentes de ameaça mais prováveis de as concretizar.

²⁰⁶ ECS, "Energy Networks and Smart Grids", novembro de 2018, 4.

²⁰⁷ RISI, "CIA Trojan Causes Siberian Gas Pipeline Explosion", <https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion>.

²⁰⁸ ECS, "Energy Networks and Smart Grids", novembro de 2018, 5.

²⁰⁹ RISI, "Hacker Takes Over Russian Gas System", <https://www.risidata.com/Database/Detail/hacker-takes-over-russian-gas-system>.

²¹⁰ ECS, "Energy Networks and Smart Grids", novembro de 2018, 5.

²¹¹ NTSB, "Pipeline Rupture and Subsequent Fire in Bellingham, Washington", 4, <https://www.nts.gov/investigations/AccidentReports/Reports/PA0202.pdf>.

²¹² Zakariya Dehlawi e Norah Abokhodair, "Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident", *paper* apresentado na 2013 IEEE International Conference on Intelligence and Security Informatics, junho de 2013. https://www.researchgate.net/publication/261456882_Saudi_Arabia's_response_to_cyber_conflict_A_case_study_of_the_Shmoon_malware_incident.

Tabela 7 - Agentes de ameaça mais prováveis (Gás)

Tipo de ameaça	Cibercriminosos	Agentes estatais	<i>Hacktivistas</i>	Colaboradores internos
<i>Ransomware</i>				
<i>Malware</i>				
Vulnerabilidades				
<i>Phishing</i>				
<i>DDoS</i>				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:

 - Agente de ameaça provável

1.3. Capacitação

Os operadores do setor energético entendem ter-se tornado largamente dependentes da sua infraestrutura digital para a realização de operações e na prestação de serviços eficientes. Entendem, também, que o aumento dessa dependência conduz a uma maior exposição a riscos de cibersegurança. Por este motivo, têm envidado esforços no sentido de se capacitarem e de se tornarem mais resilientes ao nível da cibersegurança²¹³.

Essa capacitação tem passado pela melhoria contínua da segurança dos sistemas internos, pela aquisição, implementação ou melhoria dos serviços de SOC, dedicados à monitorização contínua da segurança das infraestruturas de TI e de TO, pela realização de testes de resiliência operacional, pela aposta na formação na área dada aos colaboradores tanto ao nível de aquisição de competências técnicas, como de sensibilização, pela integração em grupos internacionais de partilha de informações sobre ameaças, técnicas e boas práticas de cibersegurança, bem como pela aquisição de seguros de cibersegurança^{214 215}.

A par destas medidas, verifica-se que tem havido no setor uma aposta nas ferramentas de IA. Por enquanto, estas são essencialmente procuradas para a automatização de processos e para o processamento de grandes quantidades de dados sensíveis, e não tanto para funções diretamente relacionadas com cibersegurança. Os operadores referem, no entanto, que a cibersegurança continua a ser uma preocupação sempre que se procura adquirir ou implementar uma nova ferramenta que recorra a IA, investindo nas competências dos colaboradores para utilizarem estas ferramentas e limitando os seus ambientes de utilização, garantindo a segurança das entidades durante a utilização das ferramentas, bem como dos dados sensíveis por estas tratados²¹⁶.

Subsetor da Eletricidade

No subsetor elétrico, há também uma aposta crescente nas redes inteligentes ou *smart grids*. Estas redes são redes elétricas que utilizam tecnologias digitais, sensores e *software* para uma melhor resposta à oferta de energia em tempo real, de modo a minimizar custos e a manter a estabilidade e confiabilidade da rede. Estas redes inteligentes estão intimamente ligadas à cibersegurança, devido à dependência das tecnologias como os sensores e *software* para gerir e monitorizar a distribuição da energia em tempo real. Estas redes conectam uma vasta gama de dispositivos, o que aumenta a vulnerabilidade a incidentes de cibersegurança. Em Portugal, registou-se um crescimento de 15% nas *smart grids* em 2022, face a 2021, e em 2023 registou-se um crescimento de 22% face aos números de 2022²¹⁷.

A iniciativa "Cyber Range" da EDP, focada em cibersegurança e formação dos colaboradores, foi lançada em 2016 e procura consciencializar e capacitar a equipa de cibersegurança para identificar e responder a ciberataques, oferecendo um laboratório de segurança, uma área para exercícios práticos e uma academia de formação²¹⁸.

²¹³ EDP, "Relatório Anual Integrado 2023", 51.

²¹⁴ EDP, "Relatório Anual Integrado 2023", 51-52.

²¹⁵ Galp, "Relatório Integrado Anual 2022", 138-139.

²¹⁶ EDP, "Relatório Anual Integrado 2023", 51.

²¹⁷ EDP, "Relatório Anual Integrado 2023", 68-69.

²¹⁸ EDP, "Cyber Range: Promover a sensibilização da cibersegurança", julho de 2020, 1-2, https://www.edp.com/sites/default/files/2021-03/10_cyber_range_novo_PT.pdf.

A Endesa, em parceria com a CGI, iniciou uma transformação digital de forma a modernizar o seu modelo de negócio e aprimorar a experiência do cliente. Este projeto envolve a migração para um modelo de serviços flexível, permitindo ajustar os seus serviços com base na demanda, reduzir custos e acelerar o lançamento de novos produtos. Neste projeto de transformação digital, a cibersegurança é essencial para proteger as novas infraestruturas digital. Foram implementadas medidas para proteger os dados sensíveis dos clientes e garantir a segurança das operações digitais, abrangendo o CRM, análise de dados e plataformas de atendimento. Assim, é possível reduzir os riscos e manter a integridade dos sistemas num ambiente cada vez mais interconectado²¹⁹.

A E-Redes tem investido numa estratégia de capacitação em cibersegurança para proteger a infraestrutura digital crítica que sustenta as suas operações. Este investimento é essencial, visto que a empresa administra uma rede essencial para o fornecimento contínuo de energia elétrica, o que exige resiliência contra incidentes de cibersegurança. Entre as medidas, está a formação dos profissionais e colaboração com entidades especializadas para identificar e mitigar vulnerabilidades. Além disso, a E-Redes, adota uma política abrangente de segurança da informação, que inclui prevenção, integridade e disponibilidade dos dados²²⁰.

Subsetor do Petróleo e Gás

Os subsectores do petróleo e gás são das indústrias mais relevantes e influentes a nível global, desempenhando um papel fundamental na economia e na sociedade moderna. A extração e a refinação, tanto de petróleo como de gás, fornecem combustível para os setores do transporte e aquecimento, mas também são essenciais para a produção de uma ampla gama de produtos químicos e materiais, incluindo plásticos, fertilizantes e medicamentos. A formação especializada também é crucial para assegurar a segurança nas operações, uma vez que o gás natural e os gases alternativos requerem conhecimentos técnicos e normas específicas para prevenir os riscos. Desta forma, a capacitação no setor do gás não atende apenas aos requisitos de conformidade legal, mas também promove a modernização da infraestrutura energética²²¹.

A Repsol, em parceria com o Instituto do Emprego e Formação Profissional (IEFP), integrou 26 novos colaboradores no seu Complexo Industrial de Sines, onde foram formados como Técnicos de Operação de Unidades Industriais. Este projeto fez parte de uma iniciativa para expandir e modernizar o complexo, com um investimento de 657 milhões de euros. O programa oferece uma formação extensa, abrangendo aulas práticas, teóricas e operacionais com foco na segurança e sustentabilidade, contribuindo para o desenvolvimento de uma indústria química mais sustentável e inovadora em Portugal²²². Em parceria com a Escola Tecnológica do Litoral Alentejano (ETLA), a Repsol oferece cursos técnicos em áreas como a Mecatrónica e Química Tecnológica, além de estágios práticos e formação para jovens locais. Este compromisso tem como objetivo melhorar a segurança, bem-estar e desenvolvimento socioeconómico da comunidade²²³.

²¹⁹ CGI, "Endesa aposta na transformação digital e reinventa o seu modelo de negócio", <https://www.cgi.com/portugal/pt-pt/case-study/business-consulting/endesa-aposta-na-transformacao-digital-e-reinventa-o-seu-modelo-de->

²²⁰ E-Redes, "Cybersecurity: New challenges, the same priority", <https://www.e-redes.pt/en/networks-of-future/cybersecurity/cybersecurity>.

²²¹ Compete 2030, "Europa lidera combate à emergência climática", 8 de julho de 2024, <https://www.compete2030.gov.pt/comunicacao/europa-lidera-combate-a-emergencia-climatica/>.

²²² Epcol, "Repsol contrata novo grupo de colaboradores e lança curso com o IEFP para os formar", 17 de março de 2022, <https://www.epcol.pt/noticias-das-associadas/repsol-contrata-novo-grupo-de-colaboradores-e-lanca-curso-com-o-iefp-para-os-formar/1236>.

²²³ REPSOL, "Formação", <https://sines.repsol.pt/pt/comunidade/seguranca/formacao/index.cshtml>.

As principais empresas de petróleo e gás em Portugal, como a Galp, estão fortemente focadas em fortalecer a cibersegurança. No caso da Galp, a empresa participa da Rede Nacional de CSIRT, uma rede nacional que promove a resposta rápida a incidentes de cibersegurança e a partilha de informações com outras empresas públicas e privadas²²⁴. A Galp também integra a iniciativa global "Cyber Resilience Pledge" do Fórum Económico Mundial, que promove a colaboração internacional para fortalecer a resiliência digital, implementando práticas de cibersegurança específicas para estes subsetores²²⁵.

Internamente, a Galp adotou um modelo de cibersegurança em colaboração com a Microsoft, utilizando uma plataforma integrada de monitorização e resposta a ameaças, como o Microsoft 365 E5. Esta plataforma consolida informações de segurança num único painel, permitindo à equipa de cibersegurança visualizar e controlar as vulnerabilidades de maneira centralizada, uma medida especialmente importante para a proteção das suas operações. Com uma equipa especializada de cibersegurança, a Galp também realiza auditorias frequentes e investe na formação para garantir que todos os colaboradores estejam preparados para adotar práticas seguras no uso dos sistemas digitais, adaptando as políticas de segurança às necessidades das diferentes funções e localizações do trabalho²²⁶.

²²⁴ Security Magazine, "GALP dá mais um passo na sua segurança e integra rede nacional CSIRT", 20 de julho de 2021, <https://www.securitymagazine.pt/2021/07/20/galp-da-mais-um-passo-na-sua-seguranca-e-integra-rede-nacional-csirt/>.

²²⁵ Galp, "Galp e empresas de energia unidas contra ciber-ataques no Fórum Económico Mundial", 25 de maio de 2022, <https://www.galp.com/media/comunicados-de-imprensa/comunicado/id/1351/galp-e-empresas-de-energia-unidas-contra-ciber-ataques-no-forum-economico-mundial>.

²²⁶ Security Magazine, "Galp Energia mantém segurança dos serviços críticos com plataforma xDR com M365 E5", 6 de setembro de 2024, <https://www.securitymagazine.pt/2024/09/06/galp-energia-mantem-seguranca-dos-servicos-criticos-com-plataforma-xdr-com-m365-e5/>.

1.4. Investimento em cibersegurança

O relatório *NIS Investments 2022*, da ENISA, que investigou em maior detalhe os setores da saúde e da energia, oferece dados sobre os investimentos realizados em cibersegurança. Segundo o relatório, a cibersegurança tem-se tornado uma prioridade dentro do investimento tecnológico, com cerca de 74% dos operadores europeus a terem aumentado o volume de investimento em cibersegurança face ao ano anterior (2020). Os operadores na UE têm investido, sobretudo, nas capacidades de análise de dados, IA e *machine learning*. O aumento das redes de sensores utilizados para a recolha de dados e telemetria tem também sido um objetivo da maioria dos operadores²²⁷.

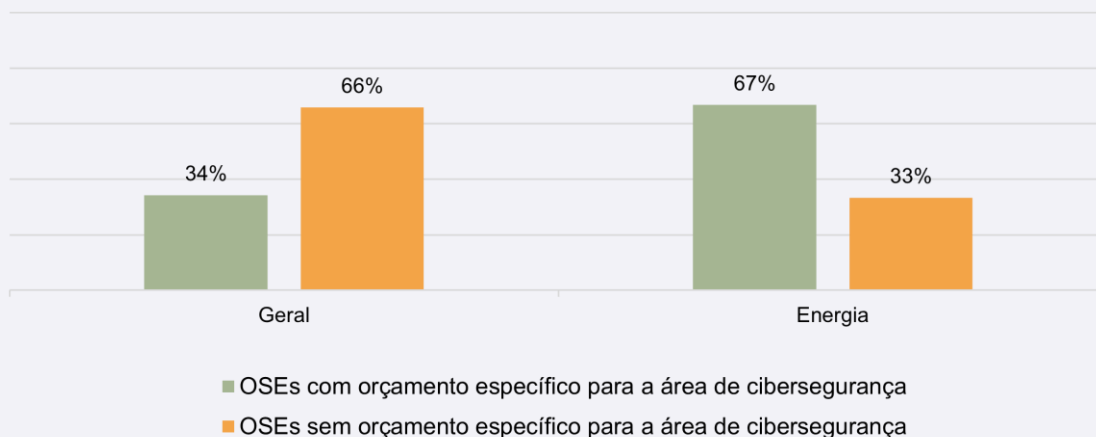
A aquisição de serviços em nuvem (*cloud services*) tem também crescido, com cerca 45% dos operadores a terem aumentado os investimentos nesta área. Concomitantemente, 39% dos operadores procuram reduzir os custos com sistemas *legacy* e *data centres* internos, transferindo-os para a nuvem²²⁸.

Durante o ano de 2021, a mediana do investimento nas TIC foi de cerca de 20 milhões de euros entre os operadores do setor energético a nível europeu. Já o investimento em TI teve um valor mediano de um milhão de euros. Terá ainda havido, em Portugal, um investimento médio de cerca de 150 mil euros em TO durante o ano de 2021²²⁹.

A CLC, juntamente com Galp, REN, EDP e E-REDES, participa ativamente no ISAC-EnergyPT, em colaboração com o Centro Nacional de Cibersegurança, para enfrentar o aumento das ameaças de cibersegurança²³⁰.

Deste setor, cerca de 67% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Relativamente às áreas de aplicação do orçamento de cibersegurança, 100% aplica na segurança das redes, na aquisição de *software* e *hardware*, e formação, 83% na análise de segurança, na capacitação em tecnologia e em gestão de vulnerabilidades, e 50% na contratação de pessoal e governança (**Gráfico 110 e 110.1**).

²²⁷ ENISA, "NIS Investments", novembro de 2022, 11.

²²⁸ ENISA, "NIS Investments", novembro de 2022, 11.

²²⁹ ENISA, "NIS Investments", novembro de 2022, 64.

²³⁰ CLC, "Relatório de Gestão & Contas 2023", 35, https://www.clc.pt/DocsCLC/2024/CLC_RC_2023.pdf.

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

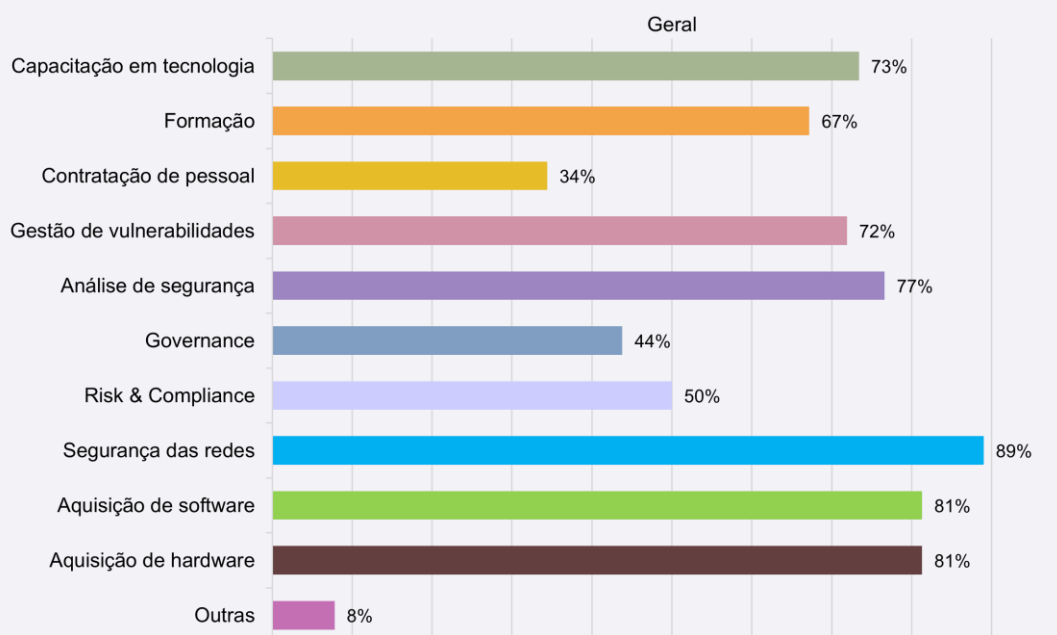
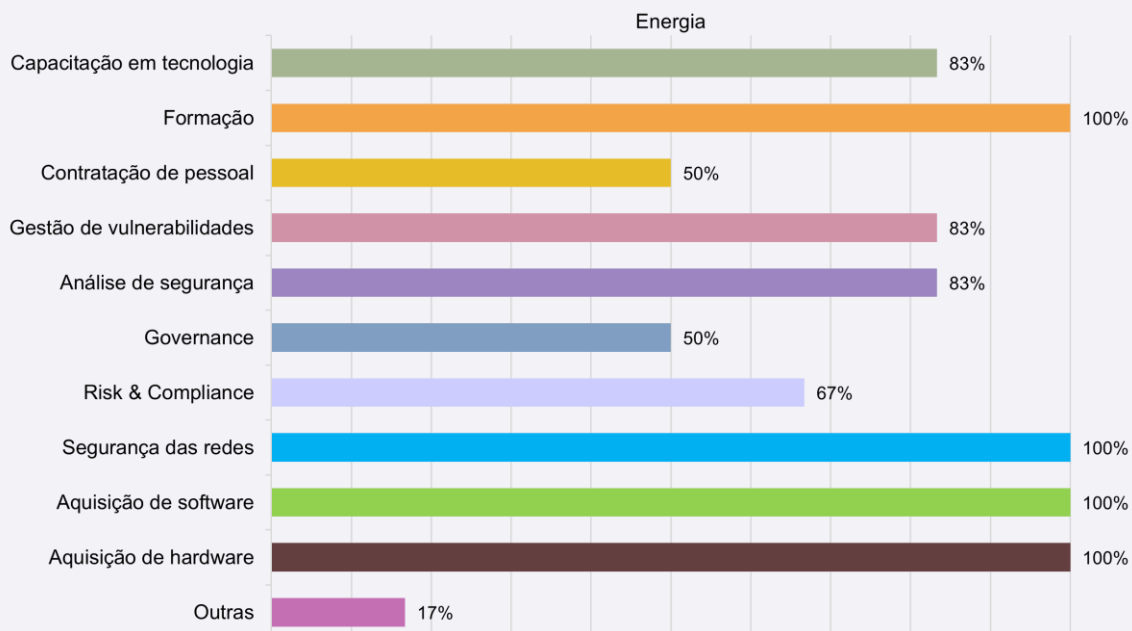
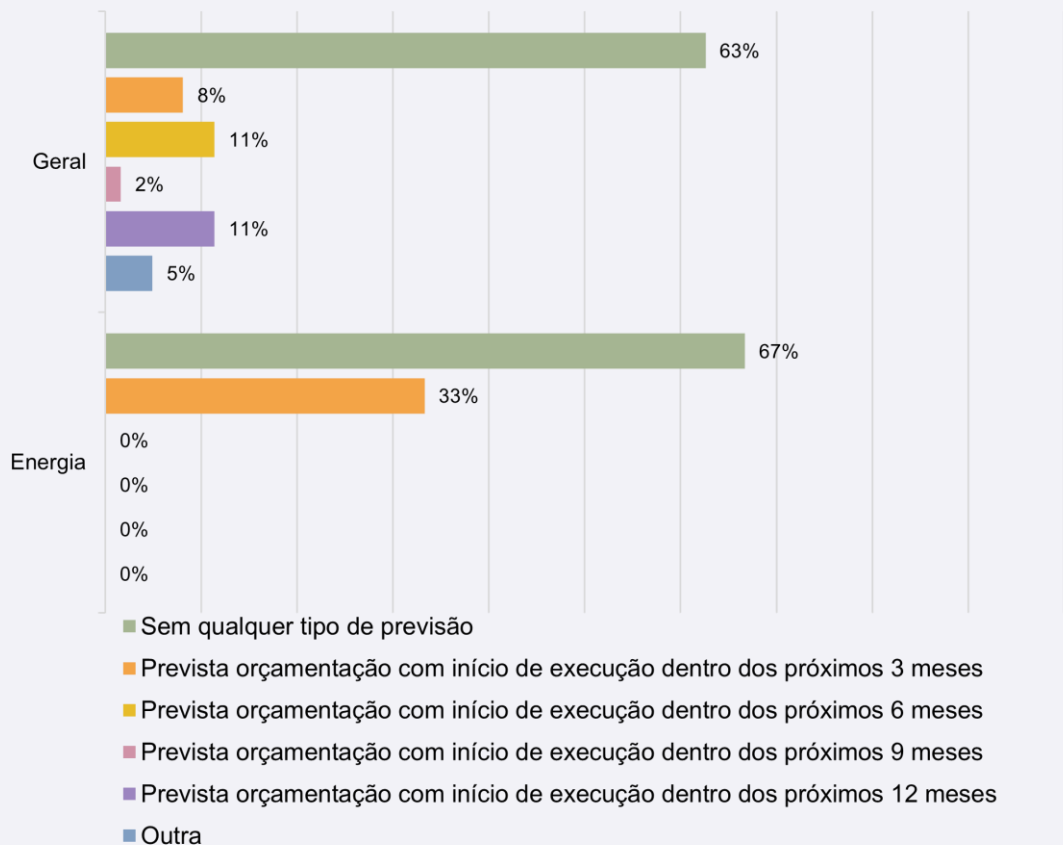


Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 67% não tem qualquer previsão para a orçamentação e 33% tem previsto a orçamentação para os próximos 3 meses (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Subsetor da Eletricidade

O setor energético, mais concretamente o subsetor da eletricidade, tem vindo a investir paulatinamente na área de cibersegurança. Um exemplo disso são as declarações prestadas pela EDP no seguimento do ciberataque de 2020, nas quais se refere que a empresa tinha, recentemente, realizado um investimento na ordem dos 50 milhões de euros em segurança informática²³¹. O relatório de contas de 2023 da mesma empresa indica ainda um investimento global de dois mil milhões de euros, entre 2023 e 2026, na transformação digital, no qual se inclui a cibersegurança e a ciberresiliência, embora não seja indicada a quantia alocada a estas temáticas²³².

²³¹ Prado, "EDP: imune à crise, mas não aos hackers".

²³² EDP, "Relatório Anual Integrado 2023", 52.

De acordo com o relatório de gestão de 2023, a EDP implementou uma transformação digital significativa, investindo cerca de 2 mil milhões de euros em TOTEX digital²³³ entre 2023 e 2026, com foco na ciberresiliência. Apesar dos esforços realizados, o risco de ciberataques cresceu em frequência e em gravidade. Para mitigar estes riscos, a EDP promoveu ações de formação e sensibilização sobre segurança da informação, organizando "digital talks" para aumentar o conhecimento em cibersegurança, e contratou um seguro de risco de cibersegurança.²³⁴

Novamente, a EDP, investiu também na criação da *Digital Global Community*, uma plataforma virtual que promove a colaboração e a partilha de conhecimento em tecnologias digitais, incluindo cibersegurança. Atualmente, esta comunidade conta com quase dois mil membros, refletindo o compromisso da empresa em fomentar a inovação e a troca de experiências no âmbito digital. A EDP ainda implementou outro programa denominado All Cyber, destinado a fortalecer a cibersegurança da organização como um todo. Este programa estabelece um processo global robusto de monitorização e resposta a ameaças e abrange três áreas principais, nomeadamente, a definição de um modelo organizacional de cibersegurança, a criação de um sistema para proteger a documentação e a informação, e o estabelecimento de métricas e KPIs de cibersegurança a nível global²³⁵.

Em 2019, o INESC TEC e o grupo EDP firmaram um contrato-programa de cinco anos para impulsionar a inovação no setor energético, com um investimento superior a um milhão de euros em consultoria avançada, pesquisa, desenvolvimento e formação. O objetivo é maximizar a energia renovável, desenvolver redes inteligentes, integrar veículos elétricos e explorar novas tecnologias. A colaboração, que já conta com mais de 20 anos, abrange também áreas cruciais como cibersegurança, garantindo a proteção das infraestruturas digitais, monitorização em tempo real e a segurança das *smart grids* no contexto da evolução do setor energético²³⁶.

A E-Redes, no seu Plano de Desenvolvimento e Investimento da Rede de Distribuição, para o período de 2021 a 2025, incluiu um foco estratégico na área da cibersegurança. Este investimento, estimado em 6,4 milhões de euro, vista principalmente a atualização dos sistemas de *hardware* e *software* da empresa, fortalecendo a sua infraestrutura digital e protegendo-a contra ameaças emergentes²³⁷.

Subsetor do Petróleo

Em 2023, as métricas de segurança e descarbonização representaram 25% dos indicadores de desempenho anual de todos os colaboradores e membros da Comissão Executiva da Galp. A metodologia OKR (Objectives and Key Results), uma abordagem de gestão que define objetivos claros e mensuráveis e os resultados chave para alcançá-los, também foi implementada, incluindo objetivos focados na sustentabilidade para 2024, abordando temas como cibersegurança, descarbonização e energias renováveis²³⁸.

²³³ O termo TOTEX digital refere-se ao investimento total em ativos digitais, englobando tanto os custos operacionais como os de capital necessários para implementar e manter a infraestrutura digital da empresa. (Fonte: Nicholas Woodroof, "TOTEX: commercial creativity and the supply chain of the future", OilField Technology, 12 de agosto de 2019, <https://www.oilfieldtechnology.com/special-reports/12082019/totex-commercial-creativity-and-the-supply-chain-of-the-future/>).

²³⁴ EDP, "Parte I – Relatório de Gestão 2023", setembro de 2024, 50, <https://www.edp.com/sites/default/files/2024-09/Parte%20I%20-%20Relat%C3%B3rio%20de%20Gest%C3%A3o%202023.pdf>.

²³⁵ EDP, "Parte I – Relatório de Gestão 2023", setembro de 2024, 167-168.

²³⁶ BIP, "INESC TEC e EDP assinam contrato-programa na área de energia", junho de 2019, <https://bip.inesctec.pt/noticias/inesc-tec-e-edp-assinam-contrato-programa-na-area-de-energia/>.

²³⁷ E-Redes, "Plano de Desenvolvimento e Investimento da Rede de Distribuição: Período 2021-2025", 122-123, <https://www.erse.pt/media/0wji5213/anexo-i-j-proposta-ren-porto%C3%A1s-distribui%C3%A7%C3%A3o.pdf>.

²³⁸ GALP, "Parte 1: Relatório Integrado de Gestão 2023", 30, <https://www.galp.com/corp/Portals/0/Recursos/Investidores/IMR2023/PT/RelatorioIntegradoAnual2023HQ.pdf>.

A Galp deu prioridade à cibersegurança para evitar falhas significativas, investindo em infraestruturas de dados e cultivando uma forte cultura em cibersegurança. A empresa conta com uma equipa de resposta a incidentes que opera 24/7. Em 2023, lançou um novo *roadmap* de cibersegurança e iniciou campanhas de sensibilização para colaboradores e clientes. Reconhecida como uma das melhores do setor de energia em cibersegurança, a Galp também promove a cooperação na Aliança Portuguesa de Cibersegurança para fortalecer a proteção da economia digital²³⁹.

É adotada uma abordagem abrangente para mitigar riscos de cibersegurança. A empresa garante a identificação, proteção, deteção e resposta a ciberameaças em todas as operações. Para isso, implementa medidas técnicas e processuais que asseguram a visibilidade de fragilidades nos seus sistemas e nos prestadores de serviços, realizando avaliações regulares e simulando ataques externos. Também é seguido um *roadmap* de melhorias contínuas até 2024, com base em avaliações de maturidade realizadas em 2022²⁴⁰.

Foi iniciado um projeto de revitalização dos PLCs de segurança no Parque de Aveiras, visando substituir processadores e módulos de entrada/saída nos sistemas de controlo (DCS), sistemas de proteção (SGS) e sistemas de incêndio e gás (FGS). O principal objetivo é melhorar o controlo e a segurança da infraestrutura, evitando interrupções nos processos de receção, armazenamento, movimentação e expedição da CLC. Também foram adjudicados dois projetos essenciais para aumentar a disponibilidade e a cibersegurança, sendo o *revamping* do sistema SCADA do oleoduto e a expansão das infraestruturas SCADA do Parque²⁴¹.

A CLC criou uma área dedicada à cibersegurança e desenvolveu um *roadmap* plurianual para melhorar a proteção e maturidade organizacional. Implementou ainda melhorias conforme a *framework* NIST CSF, incluindo processos de *backups*, gestão de vulnerabilidades e uma solução de gestão de acessos privilegiados, *CyberArk*, para controlar os acessos críticos na infraestrutura²⁴². A empresa assegura a identificação, proteção, deteção e resposta a ciberameaças que afetam a sua tecnologia, pessoas e processos, em todas as suas operações. Para garantir a segurança, foi implementado um conjunto de medidas e mecanismos de proteção e deteção, adaptando-se continuamente às ameaças de cibersegurança enfrentadas²⁴³.

De acordo com o relatório de contas de 2023 da Repsol, a empresa investiu aproximadamente 15 milhões de euros em formação, que totalizou mais de 840 mil horas. Este investimento concentrou-se particularmente na capacitação em cibersegurança, fornecendo aos colaboradores as habilidades necessárias para utilizar diversas ferramentas e aplicações digitais²⁴⁴.

Subsetor do Gás

O investimento em cibersegurança no subsetor do gás está a ser impulsionado pela crescente digitalização das infraestruturas críticas e pelo aumento significativo de incidentes de cibersegurança. Segundo um relatório da Accenture, entre 2017 e 2019, os investimentos em cibersegurança aumentaram 49%, enquanto os recursos destinados à *IoT* registaram uma redução de 4%²⁴⁵.

²³⁹ GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 125.

²⁴⁰ GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 171.

²⁴¹ CLC, “Relatório de Gestão & Contas 2023”, 25.

²⁴² CLC, “Relatório de Gestão & Contas 2023”, 26.

²⁴³ CLC, “Relatório de Gestão & Contas 2023”, 35.

²⁴⁴ Repsol, “Integrated Management Report 2023”, 97, https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/informes-anales/2023/integrated-management-report-2023.pdf.

²⁴⁵ Accenture, “Fast forward: accelerating the journey to reinvention”, 8, <https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-157/accenture-fast-forward-accelerating-the-journey-to-reinvention.pdf>.

Em 2023, as métricas de segurança e descarbonização representaram 25% dos indicadores de desempenho anual de todos os colaboradores e membros da Comissão Executiva da Galp²⁴⁶.

A Galp deu prioridade à cibersegurança para evitar falhas significativas, investindo em infraestruturas de dados e cultivando uma forte cultura em cibersegurança. A empresa conta com uma equipa de resposta a incidentes que opera 24/7. Em 2023, lançou um novo *roadmap* de cibersegurança e iniciou campanhas de sensibilização para colaboradores e clientes. Reconhecida como uma das melhores do setor de energia em cibersegurança, a Galp também promove a cooperação na Aliança Portuguesa de Cibersegurança para fortalecer a proteção da economia digital²⁴⁷.

É adotada uma abordagem abrangente para mitigar riscos de cibersegurança. A empresa garante a identificação, proteção, deteção e resposta a ciberameaças em todas as operações. Para isso, implementa medidas técnicas e processuais que asseguram a visibilidade de fragilidades nos seus sistemas e nos prestadores de serviços, realizando avaliações regulares e simulando ataques externos. Também é seguido um *roadmap* de melhorias contínuas até 2024, com base em avaliações de maturidade realizadas em 2022²⁴⁸.

²⁴⁶ GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 30.

²⁴⁷ GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 125.

²⁴⁸ GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 171.

1.5. RJSC e legislação setorial

O setor da energia e respetivos subsectores são alvos de legislação europeia e nacional há largos anos, embora a legislação em matéria de cibersegurança tenha surgido mais tardiamente, sobretudo a partir da segunda metade da década de 2010, altura em que começam a surgir diversos diplomas legais que fazem menção específica à cibersegurança. Não obstante, diplomas anteriores apresentavam já provisões sobre a segurança física e a necessidade de realizar análises de risco entre os produtores e distribuidores de energia. Ver-se-ão, de seguida, alguns desses diplomas, quer de âmbito setorial ou subsectorial, quer de âmbito geral.

Subsetor da Eletricidade

Uma das primeiras Diretivas mais relevantes em matéria de segurança no subsector da Eletricidade foi a Diretiva 2005/89/CE, relativa a medidas destinadas a garantir a segurança do fornecimento de eletricidade e o investimento em infraestruturas, de 18 de janeiro de 2006²⁴⁹. Embora este fosse um diploma sem referências específicas à cibersegurança, o mesmo incluía a necessidade de os operadores manterem um nível adequado de segurança do funcionamento das redes, bem como a disponibilidade de capacidade de produção²⁵⁰. Para tal, os Estados-membros deviam, entre outros pontos, “promover medidas de incentivo à adoção de tecnologias de gestão da procura em tempo real, tais como sistemas de medição tecnologicamente avançados”²⁵¹ junto dos operadores. Esta Diretiva foi depois transposta para a ordem jurídica nacional pelo Decreto-Lei n.º 23/2009, de 20 de janeiro²⁵².

Essa mesma Diretiva só seria atualizada pelas instituições europeias 14 anos depois, já em 2019, através do Regulamento (UE) 2019/941, relativo à preparação para riscos no setor da eletricidade²⁵³. Este Regulamento impõe aos operadores do subsector da eletricidade a necessidade de realizarem avaliações de risco para a segurança de abastecimento de eletricidade, e define também a metodologia a ser adotada para identificar cenários de crise de eletricidade a nível regional e nacional. Esta metodologia inclui a consideração de riscos como “as consequências de ataques maliciosos”²⁵⁴ e de riscos relacionados com os “princípios que regem o tratamento de informações sensíveis”²⁵⁵.

²⁴⁹ Diretiva 2005/89/CE do Parlamento Europeu e do Conselho de 18 de janeiro de 2006 relativa a medidas destinadas a garantir a segurança do fornecimento de eletricidade e o investimento em infraestruturas, *Jornal Oficial da União Europeia*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32005L0089>.

²⁵⁰ Diretiva 2005/89/CE, artigo 1.º.

²⁵¹ Diretiva 2005/89/CE, artigo 5.º, alínea d).

²⁵² Decreto-Lei n.º 23/2009, de 20 de janeiro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/23-2009-602570>.

²⁵³ Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho de 5 de junho de 2019 relativo à preparação para riscos no setor da eletricidade e que revoga a Diretiva 2005/89/CE, *Jornal Oficial da União Europeia*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0941>.

²⁵⁴ Regulamento (UE) 2019/941, artigo 5.º, n.º 2 alínea c).

²⁵⁵ Regulamento (UE) 2019/941, artigo 5.º, n.º 3, alínea e).

Subsetor do Petróleo

O subsetor do petróleo não é amplamente legislado em matéria de cibersegurança a nível setorial, estando principalmente sujeito aos diplomas de âmbito geral ou transversal sobre este tema. Existe, no entanto, a Diretiva 2012/18/UE, mais conhecida como Diretiva SEVESO III²⁵⁶, relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas. Não incidindo especificamente sobre cibersegurança, esta Diretiva exige aos operadores que implementem uma Política de Prevenção de Acidentes Graves²⁵⁷, um Sistema de Gestão de Segurança²⁵⁸ e Planos de Emergência²⁵⁹ em caso de acidente. Embora no ano de publicação da Diretiva o texto não incluísse menções à cibersegurança, os planos, políticas e sistemas exigidos devem ter em consideração os riscos de cibersegurança a que as organizações estejam ou possam vir a estar expostas. Esta Diretiva foi depois transposta para o ordenamento jurídico interno através do Decreto-Lei n.º 150/2015, de 5 de agosto²⁶⁰.

Subsetor do Gás

O subsetor do gás, tal como o do petróleo, também não se encontra amplamente regulado em matéria de cibersegurança. Contudo, neste subsetor, é de referir que foi publicado, em outubro de 2010, o Regulamento (UE) n.º 994/2010, relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás. Este Regulamento impunha aos operadores de gás a obrigação de realizarem avaliações de risco²⁶¹, nas quais poderiam ser também incluídos os riscos de cibersegurança. O Regulamento de 2010 foi depois atualizado em 2017, através do Regulamento (UE) 2017/1938, que, mantendo a imposição da realização de avaliações de risco, inclui entre os riscos específicos a considerar, as avarias de TIC, os ciberataques e a falta de manutenção adequada dos componentes tecnológicos²⁶².

Âmbito geral

No que diz respeito à legislação de âmbito geral para o setor da energia, um dos primeiros diplomas de relevo foi a Diretiva 2008/114/CE, de 8 de dezembro, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção²⁶³. Esta Diretiva estabeleceu as bases para a identificação dos operadores do setor da energia como operadores de infraestrutura crítica, e impôs-lhes obrigações como a elaboração de Planos de Segurança, nos quais deveriam já constar medidas relativas à segurança dos sistemas de

²⁵⁶ A Diretiva acolhe o nome “SEVESO” porque Seveso se refere a uma cidade do norte de Itália onde ocorreu um grave acidente industrial em 1976, no qual uma fábrica de produtos químicos libertou uma grande quantidade de dioxina, um composto altamente tóxico, contaminando a área circundante e afetando gravemente a saúde pública e o meio ambiente.

²⁵⁷ Diretiva 2012/18/UE do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas, que altera e subsequentemente revoga a Diretiva 96/82/CE do Conselho, *Jornal Oficial da União Europeia*, artigo 8.º, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012L0018>.

²⁵⁸ Diretiva 2012/18/EU, artigo 8.º e Anexo III.

²⁵⁹ Diretiva 2012/18/EU, artigo 12.º.

²⁶⁰ Decreto-Lei n.º 150/2015, de 5 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/150-2015-69951097>.

²⁶¹ Regulamento (UE) n.º 994/2010 do Parlamento Europeu e do Conselho de 20 de Outubro de 2010 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga a Diretiva 2004/67/CE do Conselho, *Jornal Oficial da União Europeia*, artigo 9.º, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0001:0022:PT:PDF>.

²⁶² Regulamento (UE) 2017/1938 do Parlamento Europeu e do Conselho de 25 de outubro de 2017 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga o Regulamento (UE) n.º 994/2010, *Jornal Oficial da União Europeia*, Anexo IV, n.º 3, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017R1938>.

²⁶³ Diretiva 2008/114/CE do Conselho de 8 de dezembro de 2008 relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, *Jornal Oficial da União Europeia*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114>.

informação²⁶⁴. Esta Diretiva foi transposta para a ordem jurídica interna portuguesa através do Decreto-Lei n.º 62/2011, de 9 de maio, entretanto atualizado pelo Decreto-Lei n.º 20/2022, de 28 de janeiro. O Decreto-Lei mais recente estabelece já que “as contramedidas e procedimentos de segurança permanentes” devem incluir “soluções em matéria de cibersegurança, nos termos previstos nos artigos 9.º e 10.º do Decreto-Lei n.º 65/2021, de 30 de julho”²⁶⁵.

Para referir o Decreto-Lei n.º 65/2021, de 30 de julho, é importante referir a legislação que conduziu até ao mesmo. Em 2016, foi publicada a Diretiva (UE) 2016/1148, conhecida como Diretiva NIS. A sua transposição para o ordenamento jurídico interno, através da Lei n.º 46/2018, estabeleceu o Regime Jurídico da Segurança do Ciberespaço (RJSC) e que impôs diversas obrigações de cibersegurança à Administração Pública, Operadores de Infraestrutura Crítica e aos Operadores de Serviços Essenciais em análise neste relatório, entre outras entidades. De modo a melhor explicitar as obrigações de cibersegurança decorrentes do RJSC, foi publicado o Decreto-Lei n.º 65/2021, que o regulamenta. É então deste Decreto-Lei que decorrem as obrigações de nomear um ponto de contacto permanente junto do CNCS²⁶⁶, de nomear um responsável de segurança²⁶⁷, de realizar anualmente uma análise de risco de cibersegurança, de elaborar inventário de ativos²⁶⁸ e um relatório anual²⁶⁹ e de os submeter ao CNCS, e de implementar Planos de Segurança que contemplem a cibersegurança²⁷⁰, bem como as obrigações de notificação dos incidentes de cibersegurança relevantes que impactem as operações destas entidades²⁷¹. A Diretiva NIS e a legislação nacional desta decorrente estabelecem-se como os primeiros grandes atos legislativos em matéria de cibersegurança, tendo lançado as bases para mais e melhor legislação, tanto de âmbito setorial como de âmbito geral sobre essa matéria.

Volvidos seis anos após a publicação da Diretiva NIS, as instituições europeias publicaram a Diretiva (UE) 2022/2555²⁷², mais vulgarmente conhecida como NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: “setores de importância crítica”²⁷³ e “outros setores críticos”²⁷⁴. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

Começando pela inclusão de novos setores, a Diretiva NIS 2 passa a visar também, no setor da energia, operadores de sistemas de aquecimento urbano ou sistemas de arrefecimento urbano, bem como operadores de produção, armazenamento e transporte de hidrogénio²⁷⁵. Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos²⁷⁶. Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas

²⁶⁴ Diretiva 2008/114/CE, Anexo II, n.º 3.

²⁶⁵ Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

²⁶⁶ Decreto-Lei n.º 65/2021, artigo 4.º.

²⁶⁷ Decreto-Lei n.º 65/2021, artigo 5.º.

²⁶⁸ Decreto-Lei n.º 65/2021, artigo 6.º.

²⁶⁹ Decreto-Lei n.º 65/2021, artigo 8.º.

²⁷⁰ Decreto-Lei n.º 65/2021, artigo 7.º.

²⁷¹ Decreto-Lei n.º 65/2021, artigos 11.º a 15.º.

²⁷² Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

²⁷³ Diretiva (UE) 2022/2555, Anexo I.

²⁷⁴ Diretiva (UE) 2022/2555, Anexo II.

²⁷⁵ Diretiva (UE) 2022/2555, Anexo I.

²⁷⁶ Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto²⁷⁷.

A nova Diretiva encoraja ainda a que as entidades abrangidas estabeleçam, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como as relacionadas com “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”²⁷⁸.

²⁷⁷ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

²⁷⁸ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

1.6. Standards e boas práticas aplicáveis

Sendo o setor da energia vital ao nível económico e social, é fundamental que a sua disponibilidade não fique comprometida. Para tal, e tal como a Diretiva NIS prevê, foram desenvolvidas várias políticas e *standards* que criam e asseguram uma rede energética europeia transversal e sustentável. No caso da Diretiva NIS, dentro do setor da Energia, são distinguidos três subsectores: Eletricidade, Gás e Petróleo.

Standards e boas práticas do subsector da Eletricidade

No subsector da eletricidade, as empresas de geração, distribuição e transmissão de energia adotam uma abordagem baseada em padrões internacionais de segurança, como a ISO 27001 e a *NIST Cybersecurity Framework*.

A tabela seguinte sumariza os *standards* e boas práticas aplicados ao subsector da Eletricidade²⁷⁹:

Tabela 8 - Standards e Boas Práticas (Subsector Eletricidade)

Standards	Boas práticas
• ISO 27019; • NERC CIP Series; • IEE Standard 1402-2000; • IEC 61850.	• Cybersecurity model electricity subsector cybersecurity capability maturity model (esc2m2) – U.S. Department of Energy; • NISTR 7628 – Guidelines for Smart Grid Cyber Security: Vol. 1; • ENISA Appropriate security measures for Smart Grids – ENISA.

Na tabela anterior estão os *standards* e boas práticas referentes ao subsector da eletricidade. De seguida, apresenta-se um breve sumário de cada um:

- **ISO 27019:** Fornece diretrizes para a segurança da informação nos sistemas de controlo industrial da energia²⁸⁰;
- **NERC CIP Series:** Estabelece uma série de normas e requisitos para a segurança das infraestruturas críticas do setor de energia²⁸¹;
- **IEE Standard 1402-2000:** É uma norma para a avaliação e seleção de sistemas de proteção contra incêndios nas estações elétricas²⁸²;
- **IEC 61850:** É uma norma internacional que define um padrão para a comunicação de estações elétricas e sistemas de automatização de redes elétricas²⁸³;

²⁷⁹ ENISA, "Mapping of OES Security Requirements to Specific Sectors", 18 de Janeiro de 2018, 9, <https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors>.

²⁸⁰ ISO, "ISO/IEC 27019:2017", <https://www.iso.org/standard/68091.html>.

²⁸¹ NERC, "Standards", <https://www.nerc.com/pa/Stand/Pages/Default.aspx>.

²⁸² IEEE, "IEEE Guide for Physical Security of Electric Power Substations", <https://standards.ieee.org/ieee/1402/6050/>.

²⁸³ IEC, "Find out more about IEC 61850", <https://iec61850.dvl.iec.ch/>.

- **Cybersecurity model electricity subsector cybersecurity capability maturity model (esc2m2) – U.S. Department of Energy:** É uma ferramenta que ajuda as organizações a avaliar e melhorar as suas capacidades de cibersegurança²⁸⁴;
- **NISTR 7628 – Guidelines for Smart Grid Cyber Security: Vol. 1:** Fornece orientações de cibersegurança nos sistemas de energia inteligentes²⁸⁵;
- **ENISA Appropriate security measures for Smart Grids – ENISA:** Fornece orientações de cibersegurança nos sistemas de energia inteligentes²⁸⁶.

Standards e boas práticas do subsetor do Petróleo

No subsetor do petróleo, as empresas de exploração, refinação e distribuição de petróleo seguem uma abordagem fundamentada em padrões internacionais de segurança, como a ISO 27001 e a *NIST Cybersecurity Framework*, para salvaguardar as suas operações contra incidentes de cibersegurança e assegurar a integridade dos seus sistemas de controlo e automatização.

A tabela seguinte sumariza os *standards* e boas práticas aplicados ao subsetor do Petróleo²⁸⁷:

Tabela 9 - Standards e Boas Práticas (Subsetor Petróleo)

Standards	Boas práticas
• Chemical Facility Anti-Terrorism Standards (CFATS).	• API STD 1164 - Pipeline SCADA Security; • Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2).

Na tabela anterior estão os *standards* e boas práticas referentes ao subsetor do Petróleo. De seguida, apresenta-se um breve sumário de cada um:

- **Chemical Facility Anti-Terrorism Standards (CFATS):** São regulamentos dos EUA destinados a proteger instalações que lidam com substâncias químicas perigosas²⁸⁸;
- **API STD 1164 - Pipeline SCADA Security:** Estabelece diretrizes para a segurança de sistemas de controlo e de automatização (SCADA) nos oleodutos²⁸⁹;
- **Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2):** É uma ferramenta desenvolvida para ajudar organizações do setor do petróleo e do gás a avaliar e melhorar a sua postura de cibersegurança²⁹⁰.

²⁸⁴ Department of Homeland Security, "ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)", fevereiro de 2014, 1, <https://www.energy.gov/oe/articles/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014>.

²⁸⁵ NIST, "Guidelines for Smart Grid Cybersecurity", <https://csrc.nist.gov/pubs/ir/7628/r1/final>.

²⁸⁶ ENISA, "Appropriate security measures for smart grids", dezembro de 2012, <https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids>.

²⁸⁷ ENISA, "Mapping of OES Security Requirements to Specific Sectors", 14.

²⁸⁸ Kansas Adjutant General's Department, "Chemical Facility Antiterrorism Standards (CFATS)", <https://www.kansastag.gov/310/Chemical-Facility-Antiterrorism-Standard>.

²⁸⁹ API, "API Standard 1164, 3rd Edition", <https://www.api.org/products-and-services/standards/important-standards-announcements/1164>.

²⁹⁰ U.S. Department of Homeland Security, "OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)", fevereiro de 2014, <https://www.energy.gov/oe/articles/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014>.

Standards e boas práticas do subsetor do Gás

No subsetor do gás, as empresas de exploração, transporte e distribuição adotam uma abordagem fundamentada em padrões internacionais de segurança, como a ISO 27001 e a *NIST Cybersecurity Framework*, para salvaguardar as suas operações contra incidentes de cibersegurança e assegurar a integridade dos seus sistemas de controlo e automatização. A tabela seguinte sumariza os *standards* e boas práticas aplicados ao subsetor do Gás²⁹¹:

Tabela 10 - Standards e Boas Práticas (Subsetor Gás)

Standards	Boas práticas
Chemical Facility Anti-Terrorism Standards (CFATS).	- API STD 1164 - Pipeline SCADA Security; - Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2); - GIE - Gas Infrastructure Europe Security Risk Assessment Methodology; - Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry - Interstate Natural Gas Association of America (INGAA).

Na tabela anterior estão os *standards* e boas práticas referentes ao subsetor do Gás. De seguida, apresenta-se um breve sumário de cada um:

- **Chemical Facility Anti-Terrorism Standards (CFATS):** São regulamentos dos EUA destinados a proteger instalações que lidam com substâncias químicas perigosas²⁹²;
- **API STD 1164 - Pipeline SCADA Security:** Estabelece diretrizes para a segurança de sistemas de controlo e de automatização (SCADA) nos oleodutos²⁹³;
- **Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2):** É uma ferramenta desenvolvida para ajudar organizações do setor do petróleo e do gás a avaliar e melhorar a sua postura de cibersegurança²⁹⁴;
- **GIE - Gas Infrastructure Europe Security Risk Assessment Methodology:** É uma *framework* projetada para ajudar os operadores das infraestruturas de gás a avaliar e gerir os riscos de segurança²⁹⁵;
- **Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry - Interstate Natural Gas Association of America (INGAA):** É um conjunto de melhores práticas para proteger sistemas de controlo em *pipelines* de gás natural²⁹⁶.

²⁹¹ ENISA, "Mapping of OES Security Requirements to Specific Sectors", 14.

²⁹² Kansas Adjutant General's Department, "Chemical Facility Antiterrorism Standards (CFATS)", <https://www.kansastag.gov/310/Chemical-Facility-Antiterrorism-Standard>.

²⁹³ API, "API Standard 1164, 3rd Edition", <https://www.api.org/products-and-services/standards/important-standards-announcements/1164>.

²⁹⁴ U.S. Department of Homeland Security, "OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)", fevereiro de 2014, <https://www.energy.gov/oe/articles/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014>.

²⁹⁵ GIE, "Security Risk Assessment Methodology", https://www.gie.eu/wp-content/uploads/filr/2751/GIE_Security_Risk_Assessment_Methodology_May2015.pdf.

²⁹⁶ AGA, "NATURAL GAS CYBERSECURITY GUIDELINES & STANDARDS PORTFOLIO", março de 2017, 1, https://www.aga.org/wp-content/uploads/2022/11/ong_cybersecurity_guidelines_and_standards_002.pdf.

1.7. Desafios

Embora alguns países incluídos no estudo “*Sectorial Implementation of the NIS Directive in the Energy Sector*”, antes do aparecimento da Diretiva NIS, tivessem já as suas abordagens desenvolvidas, outros desenvolveram novas metodologias nela baseadas. As abordagens foram ajustadas e trabalhadas com o objetivo de estarem crescentemente harmonizadas com a Diretiva²⁹⁷.

Para determinar os critérios de identificação dos OSE, os Estados-Membros tiveram em consideração várias fontes, entre as quais:

- 1) Discussões/reuniões com especialistas (37%);
- 2) Dados públicos sobre o setor (19%);
- 3) Estatísticas nacionais (17%);
- 4) Dados de cada setor através de parcerias público-privadas (17%);
- 5) Outros (10%).

Existem duas abordagens seguidas para identificação dos OSE²⁹⁸:

Tabela 11 - Abordagem para identificação de OSE

Abordagem Estatal (73%)	Abordagem orientada pelo operador (27%)
O papel de liderança é assumido por uma ou mais agências governamentais/ministérios que têm a responsabilidade de identificar os Serviços Essenciais e OSE - na maioria dos casos, os próprios ministérios responsáveis.	Os operadores autoavaliam-se quanto ao cumprimento de critérios específicos e, em seguida, registam-se na lista de OSE. Esta abordagem não exige que as autoridades nacionais identifiquem os operadores individuais das infraestruturas críticas – é dever dos operadores notificar as autoridades quando se enquadram nos critérios predefinidos.

Para a identificação de OSE no setor da energia, existem diferentes metodologias seguidas pelos Estados-Membros. Um mesmo Estado-Membro pode decidir seguir uma ou mais metodologias para este processo de identificação no setor energético. A preferida e utilizada pela maioria (13 Estados-Membros) diz respeito à identificação dos OSE (de um modo global) e a segunda metodologia mais escolhida baseia-se na identificação de infraestruturas críticas da Diretiva ECI (*European Critical Infrastructures*) (8). Entre outras metodologias seguidas, encontram-se as análises de risco nacionais (4) e os exercícios/formações (1)²⁹⁹.

²⁹⁷ NIS Cooperation Group, “Sectorial implementation of the NIS Directive in the Energy sector”, outubro de 2019, 4, <https://smart-lighting.es/wp-content/uploads/2019/11/SectorialimplementationoftheNISDirectiveintheEnergysectorpdf.pdf>.

²⁹⁸ NIS Cooperation Group, “Sectorial implementation of the NIS Directive in the Energy sector”, outubro de 2019, 29.

²⁹⁹ NIS Cooperation Group, “Sectorial implementation of the NIS Directive in the Energy sector”, outubro de 2019, 28.

Observa-se um aumento de incidentes de cibersegurança no setor de energia, que podem causar impactos significativos para a sociedade e economia – devido às características dos serviços prestados –, gerar multas regulatórias e prejudicar significativamente a reputação das empresas, em virtude de possíveis paralisações parciais ou totais dos serviços^{300 301}.

Subsetor da Eletricidade

Segundo o Relatório “*Sectorial Implementation of the NIS Directive in the Energy Sector*”, e para a maioria dos inquiridos, o critério mais importante para identificar um OSE no subsetor da eletricidade corresponde ao número de pessoas que dependem dos serviços, de acordo com 11 Estados-Membros. Como segundo e terceiro critérios, com igual valor (apontado por 9 Estados-Membros), encontra-se a prestação de um serviço dependendo da rede e sistemas de informação e a quantidade de serviços ou bens produzidos, tal como os critérios de avaliação de importância para a economia como sociedade³⁰².

O relatório “Cyber-Physical Security Considerations for the Electricity Sub-Sector” indica que, à medida que este subsetor adota tecnologias avançadas, como dispositivos de monitorização, controlo e *IoT*, aumentam as vulnerabilidades. Primeiramente, o subsetor enfrenta riscos significativos no que diz respeito à proteção de cibersegurança dos sistemas SCADA. Estes sistemas, são essenciais para a monitorização e operação das redes, tornam-se vulneráveis a ataques que exploram falhas de segurança nestas tecnologias. Ataques, como os de *ransomware*, podem explorar VPNs e sistemas SCADA para aceder a pontos críticos da infraestrutura.

A segurança física das infraestruturas é também um desafio, principalmente para as subestações distribuídas geograficamente e expostas a invasões físicas e sabotagem. A utilização de dispositivos de pequeno porte, como *drones*, possibilita ataques físicos que evitam os sistemas de segurança convencionais. Além disso, a gestão da cadeia de abastecimento é crucial, pois a aquisição de componentes para os ICS e SCADA depende da segurança dos fornecedores. Se um componente for comprometido, este pode impactar a segurança do sistema, principalmente se estiver amplamente distribuído no setor.

Outro desafio importante é a proteção dos dispositivos de *IoT*, que são amplamente integrados nos sistemas de monitorização e controlo. Estes dispositivos possuem vulnerabilidades específicas relacionadas com *design* e configuração, sendo críticos em casos onde o *software* não recebe atualizações de segurança. Tais falhas tornam o sistema suscetível a invasões que comprometam a integridade dos dados e a segurança da rede, ressaltando a importância de práticas de cibersegurança robustas, como o isolamento das redes e um controlo rigoroso de acessos remotos.

Para mitigar estes desafios, o relatório recomenda práticas como o fortalecimento dos padrões de segurança, monitorização contínuo das redes e a colaboração entre as equipas de segurança física e de cibersegurança³⁰³.

³⁰⁰ PwC, “A leadership agenda to take on tomorrow”, março de 2024, 7, <https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf>.

³⁰¹ CNCS, “Riscos & Conflitos 2024”, 33, <https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercnscs.pdf>.

³⁰² NIS Cooperation Group, “Sectorial implementation of the NIS Directive in the Energy sector”, outubro de 2019, 31.

³⁰³ CISA, “SECTOR SPOTLIGHT: Cyber-Physical Security Considerations for the Electricity Sub-Sector”, novembro de 2022, 1-2, <https://www.cisa.gov/sites/default/files/2022-11/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf>.

Subsetores do Petróleo e do Gás

Também de acordo com o Relatório “*Sectorial Implementation of the NIS Directive in the Energy Sector*”, para a maioria dos inquiridos, os dois critérios mais importantes para a identificação dos OSE no subsetor do petróleo é a prestação de um serviço dependente da rede e dos sistemas de informação, bem como a quantidade de serviço ou bem produzido (indicado por 9 Estados-Membros). Já no subsetor do Gás, para a maioria dos inquiridos, os dois critérios mais importantes para a identificação dos OSE é o número de pessoas que dependem dos serviços (indicado por 11 Estados-Membros) e, de seguida, a importância para a economia e atividades sociais, tamanho da entidade e quantidade de bens produzidos ou transportados (referido por 9 Estados-Membros).

Ainda de acordo com o mesmo relatório, para a maioria dos inquiridos, o critério mais importante de identificação de um OSE no subsetor do gás é a prestação de um serviço dependente de redes e sistemas de informação (12) e depois segue-se a sua importância para a economia (9). Como terceiro critério, surge a quantidade de bens ou serviços produzidos.

A Repsol reconhece os riscos de cibersegurança associados ao aumento da digitalização e à evolução das ameaças, incluindo fatores geopolíticos e avanços na IA. Para enfrentar estes desafios, a empresa implementou um Modelo Operacional de Cibersegurança focado na resiliência dos sistemas e atualiza regularmente os planos estratégicos. Em 2023, não ocorreram incidentes significativos de cibersegurança, graças a processos avançados de deteção e a mais de 50 iniciativas, como avaliações da postura de cibersegurança e otimizações dos processos de resposta a incidentes³⁰⁴.

O setor do petróleo e gás enfrentam desafios críticos de cibersegurança, sobretudo devido à sua complexa infraestrutura digital. A operação integrada das redes industriais, sistemas de controlo e equipamentos digitais expõem estes subsectores a ameaças crescentes. Um incidente de cibersegurança pode impactar tanto a segurança dos trabalhadores como o meio ambiente, além de provocar perdas financeiras significativas e uma interrupção da produção. O foco em ciberresiliência passa por criar defesas robustas e adotar estratégias de recuperação rápidas e eficientes. Isto inclui proteger as redes e os dados sensíveis, assim monitorizar continuamente as ameaças emergentes, bem como promover a formação contínua dos profissionais para que reconheçam os riscos potenciais e ajam proactivamente. Estes esforços são fundamentais para reduzir vulnerabilidades e garantir a segurança das operações numa escala global³⁰⁵.

Os ativos estão frequentemente distribuídos em vastas áreas geográficas, incluindo locais *offshore* remotos e profundos, onde muitos dos equipamentos são antigos e carecem de recursos de segurança modernos, tornando-os alvos vulneráveis. A integração dos sistemas de fornecedores e as dificuldades em estabelecer redes seguras nas plataformas também contribuem para que exista uma superfície de ataque. Os desafios operacionais incluem a necessidade de manter os sistemas num funcionamento contínuo, onde as interrupções podem causar perdas financeiras elevadas. O foco na eficiência operacional frequentemente precede as atualizações de segurança. Por outro lado, os desafios financeiros surgem devido à alta regulamentação e elevados custos da indústria, enquanto os desafios legislativos refletem a falta de normas rigorosas comparadas aos outros OSE, dificultando a proteção efetiva contra incidentes de segurança³⁰⁶.

³⁰⁴ Repsol, “Integrated Management Report 2023”, 108.

³⁰⁵ World Economic Forum, “Strengthening cybersecurity in the oil and gas industry”, janeiro de 2023, www.weforum.org/impact/cyber-resilience-oil-and-gas/.

³⁰⁶ Abubakar Sadiq Mohammed et al., “Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective”, setembro de 2022, 16-18, <https://dl.acm.org/doi/10.1145/3548691>.

De acordo com o Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA, os sistemas de GNL são particularmente vulneráveis a ciberataques devido a riscos intrínsecos, como a dependência de sistemas de terceiros geridos remotamente e tecnologias a bordo vulneráveis, como *PLCs*, *GPS* e *A/S*. Os incidentes de cibersegurança podem resultar em riscos de segurança graves, incluindo fugas de tanques de combustível e libertação de GNL. As ameaças internas são outra preocupação significativa. Aumentar a consciencialização em cibersegurança dos colaboradores é crucial, uma vez que os ataques começam, frequentemente, com a confiança comprometida de funcionários³⁰⁷.

A integração dos sistemas de fornecedores e as dificuldades em estabelecer redes seguras nas plataformas também contribuem para que exista uma superfície de ataque. Os desafios operacionais incluem a necessidade de manter os sistemas num funcionamento contínuo, onde as interrupções podem causar perdas financeiras elevadas. O foco na eficiência operacional frequentemente precede as atualizações de segurança. Por outro lado, os desafios financeiros surgem devido à alta regulamentação e elevados custos da indústria, enquanto os desafios legislativos refletem a falta de normas rigorosas comparadas aos outros OSE, dificultando a proteção efetiva contra incidentes de segurança³⁰⁸.

³⁰⁷ Gas-cybersecurity, "Cybersecurity in the Energy Sector, Gas Subsector", <https://www.gas-cybersecurity.com/>.

³⁰⁸ Abubakar Sadiq Mohammed et al., "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective", setembro de 2022, 16-18.

1.8. Recomendações

Segundo o relatório da ENISA que descreve as ameaças contra os serviços dos fornecedores de energia que dependem da disponibilidade de redes precisas em tempo e comunicação³⁰⁹, as recomendações e boas práticas de segurança a seguir pelo setor dividem-se em recomendações gerais a aplicar e recomendações técnicas baseadas em diferentes cenários tecnológicos.

Técnicas baseadas em cenários tecnológicos:

1. **Unidades de Medida de Fase** (*phasor measurement units* (PMU), no original), são dispositivos críticos na monitorização da rede elétrica em tempo real. Permitem medir a voltagem e a corrente de um sistema de energia e são essenciais para o controlo eficiente e seguro da rede. Contudo, estas unidades podem ser alvos de incidentes de cibersegurança, como intrusões que comprometam a integridade dos dados recolhidos ou até mesmo a operação das PMUs.
 - a) **Estabelecer perímetros de segurança eletrónica:** A recomendação de estabelecer perímetros de segurança para PMUs ajuda a isolar estas unidades de redes mais amplas e protegê-las contra acessos não autorizados. Com um perímetro bem definido, é possível controlar rigorosamente quem pode, e o que pode interagir com as PMUs, reduzindo o risco de incidentes de cibersegurança que poderiam manipular os dados ou sabotar o funcionamento do sistema;
 - b) **Minimizar a quantidade de pontos de acesso eletrónicos:** Reduzir os pontos de acesso minimiza as possibilidades de exploração por atacantes. Quanto menor o número de pontos de entrada, mais fácil é monitorizar e proteger cada um deles;
 - c) **Utilizar segregação de rede:** Implementar segregação da rede, com a criação de zonas de segurança distintas para PMUs, ajuda a limitar os danos caso um agente de ameaça consiga comprometer um dispositivo ou componente da rede garantindo que um possível incidente não se espalhe para outras partes da infraestrutura crítica;
 - d) **Utilizar firewalls com “whitelist” (negar, by default):** A utilização de *firewalls* com regras de “whitelist” faz com que apenas dispositivos ou endereços IP específicos consigam estabelecer conexões com as PMUs, restringindo severamente as tentativas de acesso, pois, por defeito, todas as conexões não autorizadas são bloqueadas.
 - e) **Implementar IPSec nos dispositivos de gateway:** Implementar IPSec nas interfaces de rede dos dispositivos de *gateway* permite a encriptação e autenticação de dados de forma robusta, protegendo contra ataques do tipo *man-in-the-middle*, onde um agente de ameaça interceta ou altera a comunicação entre a PMU e outras partes do sistema.

³⁰⁹ ENISA, “Power Sector Dependencies on Time Service”, 2020.

2. **Camada de transporte (TCP/UDP):** responsável pela comunicação entre dispositivos na rede, podem ser exploradas por agentes de ameaça para comprometer a integridade e confidencialidade dos dados que transitam entre os dispositivos.
- a) **Fecho de portas não utilizadas:** É uma prática fundamental para reduzir a superfície de ataque, onde cada porta aberta num dispositivo ou servidor representa uma possível vulnerabilidade. Ao fechar portas desnecessárias, a organização minimiza as oportunidades para os atacantes explorarem o sistema.
 - b) **Firewalls com regras de “whitelist”:** Semelhante à recomendação anterior, a aplicação de *firewalls* com listas de permissões ajudam a garantir que somente comunicações legítimas possam circular pela rede,
 - c) **Ligações VPN encriptadas:** O uso de VPNs com encriptação assegura que os dados trocados entre sistemas e utilizadores remotos sejam protegidos de intercetção ou alteração por terceiros, principalmente em cenários de comunicação remota ou externa à infraestrutura.
 - d) **Evitar ligações bidirecionais remotas e implementar SSH quando necessário:** Manter ligações remotas unidimensionais, onde a comunicação apenas pode ocorrer de dentro para fora, limita a possibilidade de intrusões ou comandos maliciosos enviados para dentro da rede. Caso a comunicação bidirecional seja necessária, deve ser implementado o uso de protocolos seguros, como o *SSH (Secure Shell)*, para garantir a segurança na transmissão dos dados.
3. **Servidor e protocolo NTP/PTP:** O *Network Time Protocol (NTP)* e o *PTP* são fundamentais para a sincronização dos relógios nos sistemas. A precisão do tempo é essencial para garantir o funcionamento coordenado de diversos dispositivos e processos em tempo real, como é o caso das PMUs.
- a) **Utilizar criptografia para dados sensíveis:** Protege a integridade e confidencialidade dos dados, prevenindo que informações críticas, como *timestamps*, sejam manipuladas.
 - b) **Harmonizar sistemas temporais *Universal Time Coordinated (UTC)* para facilitar correlação de dados:** Ao utilizar uma base de tempo unificada, como o *UTC (Coordinated Universal Time)*, facilita-se a correlação de dados na rede, o que é fundamental para a deteção de anomalias ou falhas. Caso sistemas diferentes utilizem tempos diferentes poderá dificultar a identificação de eventuais problemas.
 - c) **Utilizar *Access Control Lists (ACLs)*, assim como *firewalls* para filtrar ligações a servidores NTP:** O uso de *ACLs* e *firewalls* ajuda a filtrar e limitar as conexões de rede ao servidor NTP, garantindo que apenas dispositivos autorizados possam solicitar a sincronização de tempo, protegendo contra ataques de *DoS (Denial of Service)*.
 - d) **Proteger o protocolo NTP com vários caminhos entre os relógios *master* e *slave*:** Utilizar múltiplos caminhos entre relógios *master* e *slave* oferece redundância e aumenta a segurança do sistema visto que, se um caminho for comprometido ou sofrer uma falha, a sincronização do tempo pode ser mantida através de outros caminhos, garantindo a precisão e confiabilidade da rede.

A “Recomendação (UE) 2019/553 da Comissão de 3 de abril de 2019 sobre a cibersegurança no setor da energia”, constitui um documento vital na consolidação de recomendações a adotar por parte deste setor e a definir as principais questões relacionadas com a cibersegurança. Este documento considera determinadas realidades³¹⁰:

- 1) o progresso tecnológico de redes (inteligentes) energéticas alavanca exposição a novos riscos;
- 2) a reformulação do Regulamento Mercado Interno da Eletricidade considera agora a adoção de normas técnicas para a eletricidade;
- 3) a importância e necessidade de avaliar continuamente e de modo adequado todos os riscos;
- 4) a priorização do reforço da ciber-resiliência: adoção da Diretiva NIS;
- 5) a comunicação de incidentes como obrigatória nos setores essenciais, como a energia;
- 6) o reforço, pretendido pela Comissão Europeia, de partilha de informação entre partes interessadas através de eventos específicos em matéria de cibersegurança;
- 7) Os Estados-membros são responsáveis por “assegurar que todas as partes interessadas (operadores de redes de energia, fornecedores de tecnologias e OSE identificados pela NIS) aplicam as medidas de preparação que se impõem em matéria de cibersegurança, relacionadas com os requisitos em tempo real”, tais como:
 - a) aplicação das normas de segurança mais atualizadas nas instalações e, caso necessário, aplicação de medidas de segurança física complementares caso medidas de cibersegurança não sejam suficientes;
 - b) aplicar normas internacionais em contexto de cibersegurança;
 - c) aplicar restrições em tempo real, em particular na classificação de ativos;
 - d) garantir o nível de qualidade de serviço requerido pelas restrições em tempo real, através da implementação de redes privadas para sistemas de proteção à distância;
 - e) atribuir diferentes zonas lógicas num sistema global e, para cada zona, atribuir critérios de tempo e processos;
 - f) escolher protocolos de comunicação seguros;
 - g) adotar mecanismos de autenticação adequados para qualquer comunicação.

O documento destaca, também, algumas recomendações que podem mitigar os “efeitos de cascata”. Isto significa que, uma vez que as redes elétricas e gasodutos na Europa se encontram fortemente independentes, deve ser garantida uma comunicação transversal com todas as partes interessadas num momento de crise ou incidentes de cibersegurança - um ciberataque capaz de criar falhas ou perturbações num sistema energético, pode, direta ou indiretamente, ser responsável por provocar efeitos em cascata com grande alcance no restante sistema. Neste contexto, algumas das recomendações a ser seguidas pelos operadores de rede de energia são, por exemplo, as seguintes³¹¹:

- 1) garantir que todos os novos dispositivos IoT têm nível de segurança adequado;
- 2) ponderar efeitos ciberfísicos no momento de revisão periódica dos planos de continuidade;
- 3) estabelecer critérios de conceção e uma arquitetura para uma rede resiliente.

O documento foi redigido considerando que o setor está atualmente exposto a “mudanças como o progresso tecnológico, acoplamento de setores e a digitalização”, tornando as redes elétricas cada vez mais inteligentes.

³¹⁰ Comissão Europeia, Direção-Geral da Energia, Recomendação (UE) 2019/553 da Comissão de 3 de Abril de 2019 sobre a cibersegurança no setor da energia, 2019.

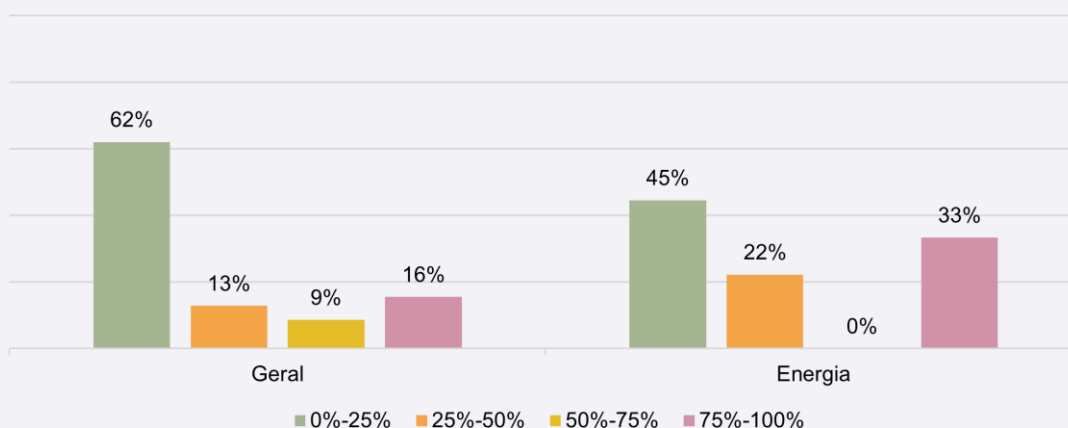
³¹¹ Comissão Europeia, Direção-Geral da Energia, Recomendação (UE) 2019/553 da Comissão de 3 de Abril de 2019 sobre a cibersegurança no setor da energia, 2019.

Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor da energia e subsequentes subsetores, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

A sensibilização para todo o tipo de riscos de cibersegurança e a formação para identificar possíveis tentativas de ataques de segurança são essenciais para impedir que estas se concretizem, pois, a formação leva a que medidas de prevenção, como a realização de *backups*, sejam implementadas. A formação (**Gráfico 33**) nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Podemos verificar que o setor da energia tem uma percentagem maior de trabalhadores com formação básica em cibersegurança comparativamente com o geral. Apesar disso, 45% dos operadores tem uma percentagem aproximada de trabalhadores com formação básica em cibersegurança de 0 a 25%, um valor considerado baixo e que deve ser aumentado.

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor da energia disponibilizarem formação em cibersegurança aos seus colaboradores (**Gráfico 38**), metade das formações são de caráter facultativo, e não obrigatório (**Gráfico 39**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

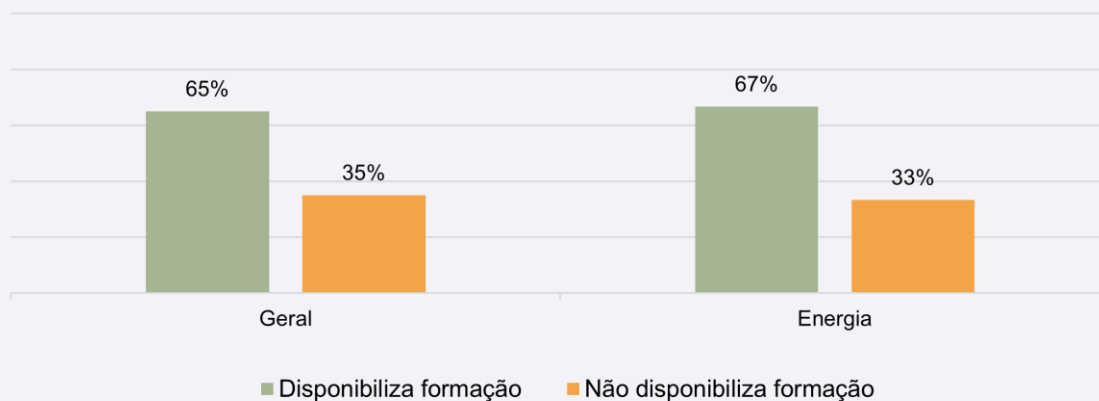
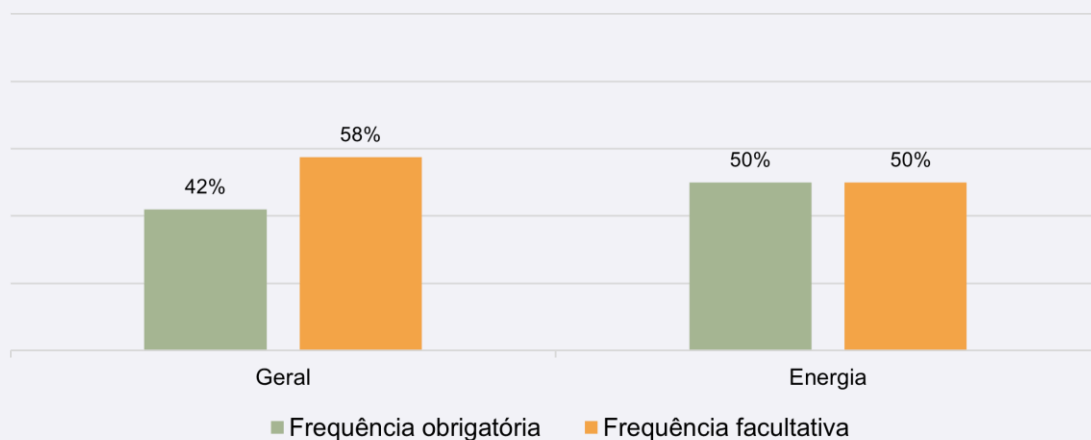
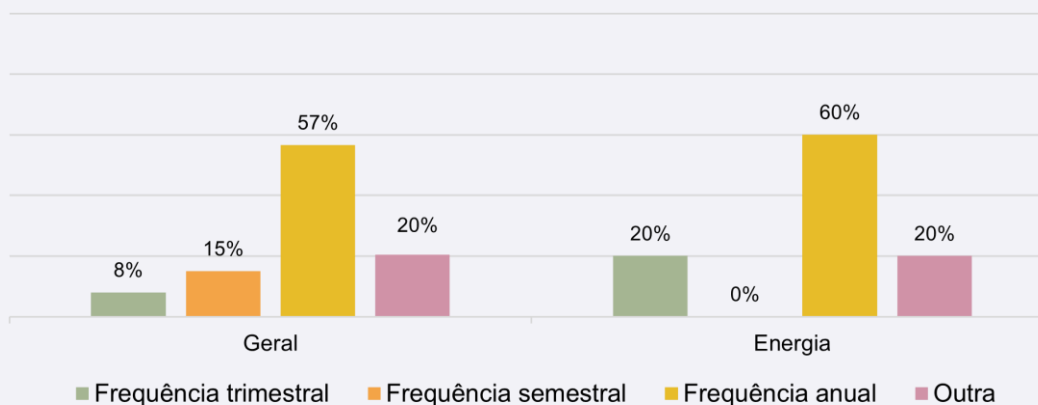


Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



Além disso, na maioria das entidades, os momentos de formação têm frequência anual (**Gráfico 41**), o que no contexto do setor da energia poderá ser insuficiente para assegurar a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória.

Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor da energia, comparativamente com os restantes, é um dos setores onde menos se utiliza sistemas de gestão de *passwords*, a utilização de *browser* que proteja a privacidade, controlos biométricos para identificação e autenticação de utilizadores e *VPN*.

Nesse sentido, recomenda-se aos OSE do setor da energia que:

- Aumentem a equipa de especialistas em cibersegurança;
- Realizem análises de risco com periodicidade mínima anual;
- Implementem sistemas de gestão de *passwords*;
- Implementem *VPN* em, pelo menos, acessos remotos;
- Implementem, onde possível, métodos de autenticação multifator.

Medidas como estas auxiliam a impedir acessos iniciais por parte dos agentes de ameaça e a que os mesmos não sejam capazes de progredir na exploração dos dados, sistemas e ficheiros quando um primeiro acesso é obtido.

Políticas, procedimentos e planos de cibersegurança

De acordo com os dados obtidos no questionário, todos os OSE do setor tinham documentado e implementado políticas e procedimentos de cibersegurança. Adicionalmente, apenas 67% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Diante desta situação, apesar de todos OSE do setor terem uma política de segurança, é importante que a mesma verse sobre:

- Os diversos papéis e responsabilidades dos vários colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, como os controlos de acesso (lógico e físico);
- A gestão de incidentes, incluindo a elaboração de um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação, além de um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir, que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização periódica da política (pelo menos anualmente), para manter a mesma atualizada conforme a evolução das ameaças de cibersegurança e as mudanças na organização.

Análise de vulnerabilidades e realização de testes de intrusão (*pentesting*)

Todos os OSE do setor da energia realizam procedimentos de deteção e gestão de vulnerabilidades, sendo este ponto importante tendo em vista a diminuição e antecipação de possíveis ataques. A deteção e análise, e correção de vulnerabilidades é uma prática importante para a proteção proativa e preventiva dos sistemas e aplicações em utilização em qualquer setor de atividade.

Quanto à realização de testes de intrusão, 72% dos OSE realizam os mesmos, estando a percentagem acima do geral (72% vs 50%). É importante a realização deste tipo de testes, pois é mais uma maneira de identificar vulnerabilidades, corrigi-las e tornar os OSE mais resilientes em matéria de cibersegurança.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de intrusão e exercícios de *Red Team*³¹².

³¹² Hassanzadeh et al., "A Review of Cybersecurity Incidents", 4.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo CIS, assim como a respetiva categoria dos mesmos³¹³:

Tabela 12 - Controlos de Segurança da CIS (Energia)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: CIS, “The 18 CIS Critical Security Controls”, <https://www.cisecurity.org/controls/cis-controls-list>)

³¹³ Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 6.

Recomendações Subsetor da Eletricidade

Um relatório da Comissão Europeia em conjunto com a ENISA dá conta de quatro recomendações para o subsetor da eletricidade:

1. A postura de cibersegurança e a resiliência podem ser melhoradas através de boas práticas para mitigar o *ransomware*, monitorizar possíveis vulnerabilidades, garantir a segurança dos recursos humanos e gerir ativos. É, também, necessário reforçar a cooperação com a rede técnica dos Estados-Membros, as CSIRTs, as autoridades policiais e parceiros internacionais. Adicionalmente, os Estados-Membros devem realizar autoavaliações para o subsetor da eletricidade, de acordo com a Diretiva 2022/2555³¹⁴ e a Diretiva relativa à resiliência das entidades críticas³¹⁵;
2. É necessário melhorar a consistência de cibersegurança e a partilha de informações entre entidades;
3. É necessário criar um plano de contingência, de gestão de crise e de colaboração operacional em caso de incidente de cibersegurança;
4. Deve ser reforçada a cibersegurança das cadeias de abastecimento com avaliações das dependências dos fornecedores de alto risco³¹⁶.

³¹⁴ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555>.

³¹⁵ Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2557>.

³¹⁶ European Commission, "Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors", 24 de julho de 2024, <https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors>.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsetor. Tais cenários são indicados na seguinte tabela:

Tabela 13 - Cenários de risco (Eletricidade)

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços WEB, através de um <i>URL</i> malicioso ou <i>script</i> malicioso que direciona um colaborador da entidade para um website falso e instala <i>software</i> malicioso (ataques <i>Watering Hole</i> , ataques <i>Drive-By</i>), permitindo o furto de dados.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de <i>login</i> ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de APLICAÇÃO WEB (SQL Injection ou Cross-site Scripting).
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em <i>bitcoins</i> , sob a ameaça da sua destruição ou exposição ao público.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 21 de outubro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf>)

Recomendações Subsetor do Petróleo

Um estudo sobre a cibersegurança dos sistemas físicos nos subsectores do petróleo e gás indica que a implementação da *IoT* e de sistemas controlados remotamente têm aumentado as vulnerabilidades nestes subsectores. Para mitigar estes riscos, é fundamental aprimorar determinadas situações, tais como:

- Melhorar os sistemas de deteção de intrusões (*IDS*) para atender melhor às necessidades específicas dos subsectores do petróleo e gás, pois os sistemas existentes são limitados;
- Substituir os protocolos *ModbusRTU* e *ModbusTCP* que são considerados inseguros;
- Melhorar a consistência de cibersegurança e a partilha de informações entre entidades;
- É necessário criar um plano de contingência, de gestão de crise e de colaboração operacional em caso de incidente de cibersegurança³¹⁷.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsector. Tais cenários são indicados na seguinte tabela:

Tabela 14 - Cenários de risco (Petróleo)

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de <i>login</i> ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de APLICAÇÃO WEB (SQL Injection ou Cross-site Scripting).
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
Infeção com software malicioso que conecta os dispositivos da entidade a uma BOTNET, tornando-os zombies, fornecendo poder computacional a ataques de DDoS e de criptomineração, ou comprometendo os sistemas e/ou serviços (ex: RDP, FTP) através de tentativa de força-bruta.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em <i>bitcoins</i> , sob a ameaça da sua destruição ou exposição ao público.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 21 de outubro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

³¹⁷ Abubakar Sadiq Mohammed et al, “Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective”, setembro de 2022, 22.

Recomendações Subsetor do Gás

Um estudo sobre a cibersegurança dos sistemas físicos nos subsectores do petróleo e gás indica que a implementação da *IoT* e de sistemas controlados remotamente têm aumentado as vulnerabilidades nestes subsectores. Para mitigar estes riscos, é fundamental aprimorar determinadas situações, tais como:

- Melhorar os sistemas de deteção de intrusões (*IDS*) para atender melhor às necessidades específicas dos subsectores do petróleo e gás, pois os sistemas existentes são limitados;
- Substituir os protocolos *ModbusRTU* e *ModbusTCP* que são considerados inseguros;
- Melhorar a consistência de cibersegurança e a partilha de informações entre entidades;
- É necessário criar um plano de contingência, de gestão de crise e de colaboração operacional em caso de incidente de cibersegurança³¹⁸.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsector. Tais cenários são indicados na seguinte tabela:

Tabela 15 - Cenários de risco (Gás).

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de <i>login</i> ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de APLICAÇÃO WEB (SQL Injection ou Cross-site Scripting).
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em <i>bitcoins</i> , sob a ameaça da sua destruição ou exposição ao público.
Desenvolvimento de ações de CIBERESPIONAGEM, através de malware ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 21 de outubro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>).

³¹⁸ Abubakar Sadiq Mohammed et al, “Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective”, setembro de 2022, 22.

2. Transportes

2.1. Contextualização setorial

Geral

No âmbito da Diretiva 2016/1148³¹⁹ (NIS) e Lei n.º 46/2018³²⁰, que transpõe a Diretiva e estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), o setor dos transportes abrange quatro subsectores: o transporte aéreo, o transporte marítimo, o transporte ferroviário e o transporte rodoviário. O setor dos transportes, bem como os quatro subsectores que o compõem, tal como são hoje conhecidos, devem o seu desenvolvimento à Revolução Industrial do século XIX, período em que foram desenvolvidas as máquinas a vapor mais capazes, introduzidas nos comboios e nos navios, em que se iniciou mais seriamente o desenvolvimento da ferrovia, em que se inventou o motor de combustão interna, mais tarde introduzido nos automóveis, e período em que se iniciaram os desenvolvimentos na aviação.

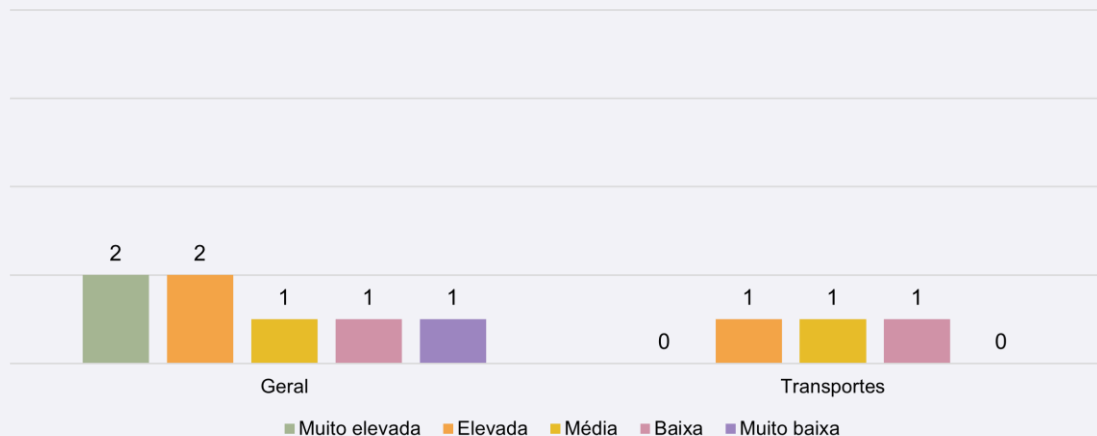
Todos estes transportes foram alvo de grande evolução ao longo de mais de um século, sendo-lhes integrados outros sistemas e mecanismos cada vez mais inteligentes, como por exemplo os de navegação. O crescimento e adaptação do **setor dos transportes** a processos e mecanismos inteligentes aumenta significativamente a exposição a ameaças de cibersegurança que não só poderão ter impactos negativos neste setor, como na economia no seu global, podendo afetar inclusivamente a segurança dos cidadãos. O setor dos transportes torna-se um setor de grande importância e preocupação quando se verifica o seu crescimento enquanto setor inteligente: o aumento relevante de interligações entre transportes e entre setores torna o contexto de cibersegurança muito mais exposto e sobre o qual se deve ter a maior atenção.

³¹⁹ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, Anexo I, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148>

³²⁰ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

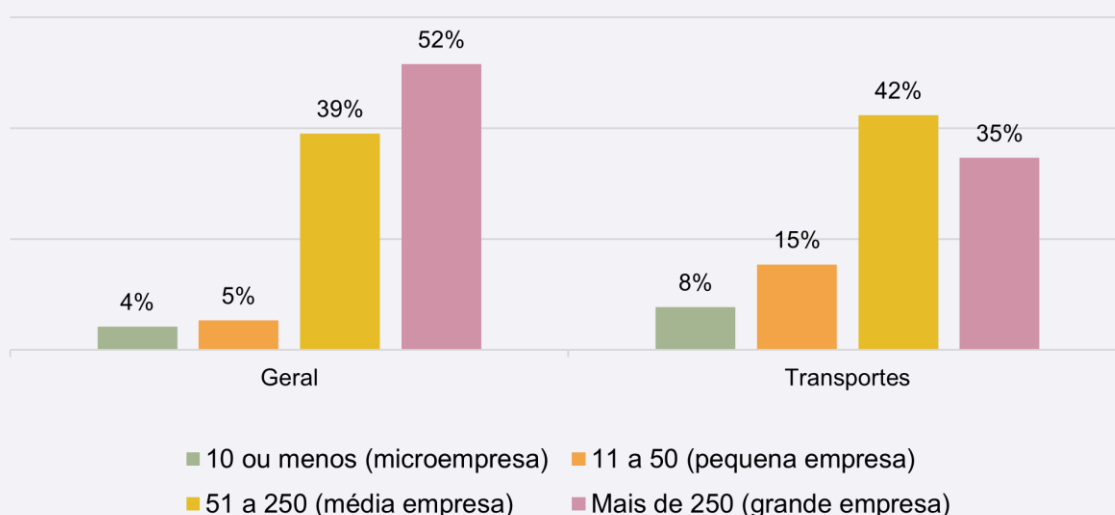
De acordo com o questionário realizado, os três reguladores inquiridos tiveram opiniões diferentes sobre a maturidade em cibersegurança entre baixa, média e elevada (**Gráfico 9**).

Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores



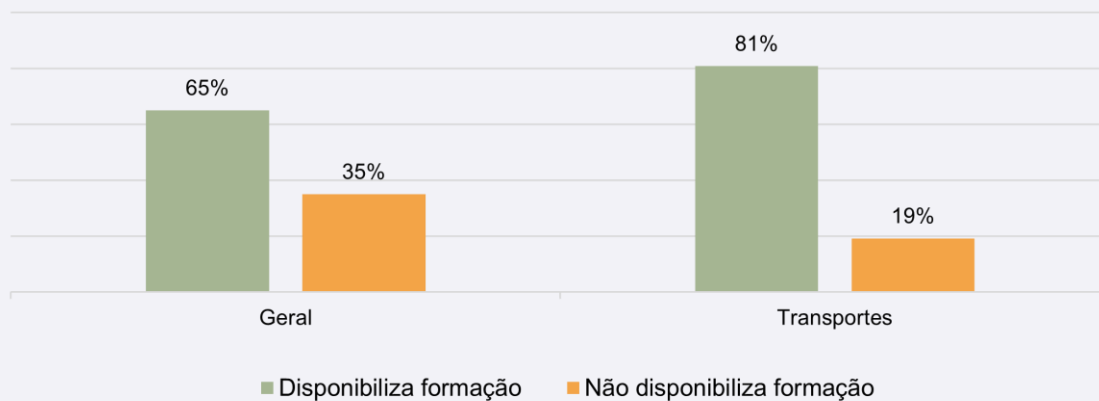
O tecido empresarial dos OSE do setor dos transportes é sobretudo composto por médias empresas, representando 42% dos operadores do setor, seguidas de grandes empresas com 35% e por fim pequenas e microempresas constituindo 23% dos operadores inquiridos. No âmbito geral, 52% dos OSE são grandes empresas, 39% são médias empresas e 9% são pequenas e microempresas (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



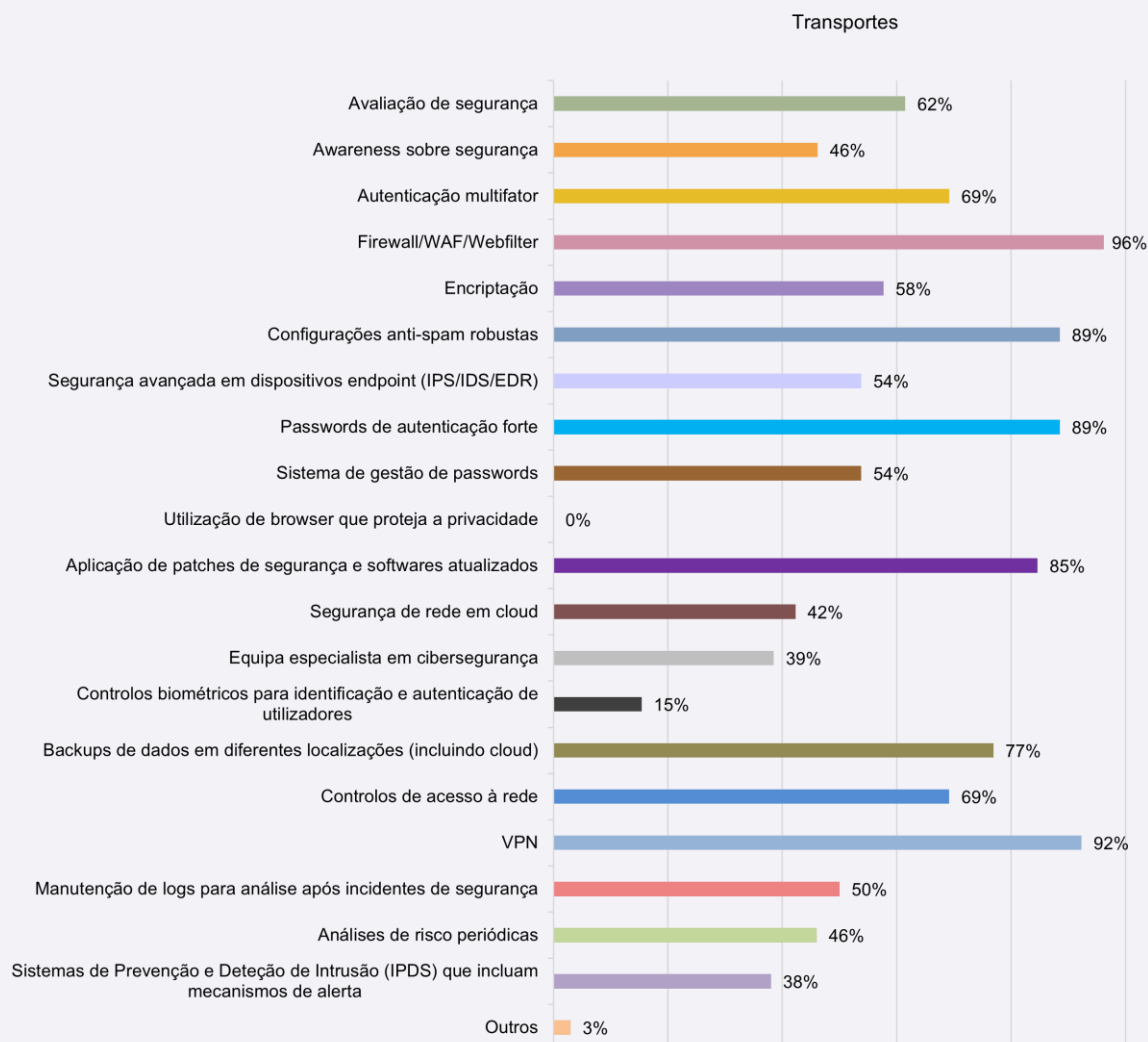
Esta perceção que pode ser suportada pelos 81% dos operadores que disponibiliza formação em cibersegurança aos seus colaboradores (vide **Gráfico 38**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



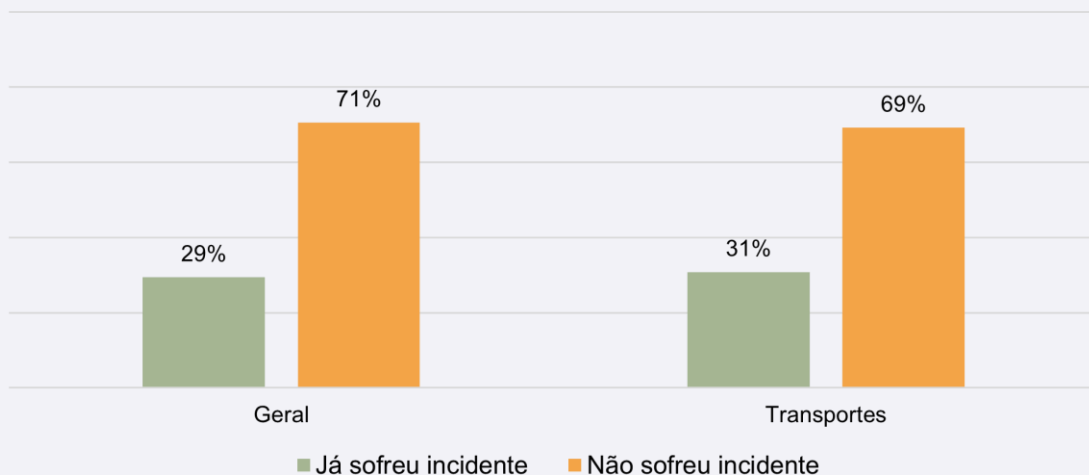
As medidas menos adotadas foram: Segurança de rede em *cloud* com 42%, Equipa especialista em cibersegurança com 39%, a implementação de controlos biométricos para identificação e autenticação com 15%, Análise de risco periódicas e *awareness* sobre segurança com 46% e Sistemas de Prevenção e Detecção de Intrusão (IPDS) com 38% (**Gráfico 66.2**).

Gráfico 66.2 - Medidas de proteção contra ameaças de cibersegurança



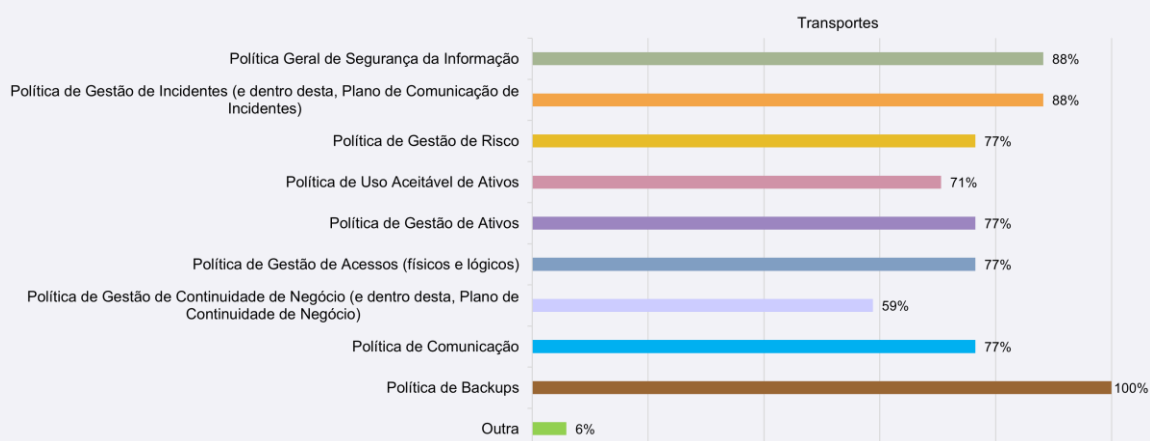
A taxa de incidência de incidentes de cibersegurança é apenas 2 p.p superior à média geral, onde 31% dos OSE sofreram incidentes em contexto TIC.

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



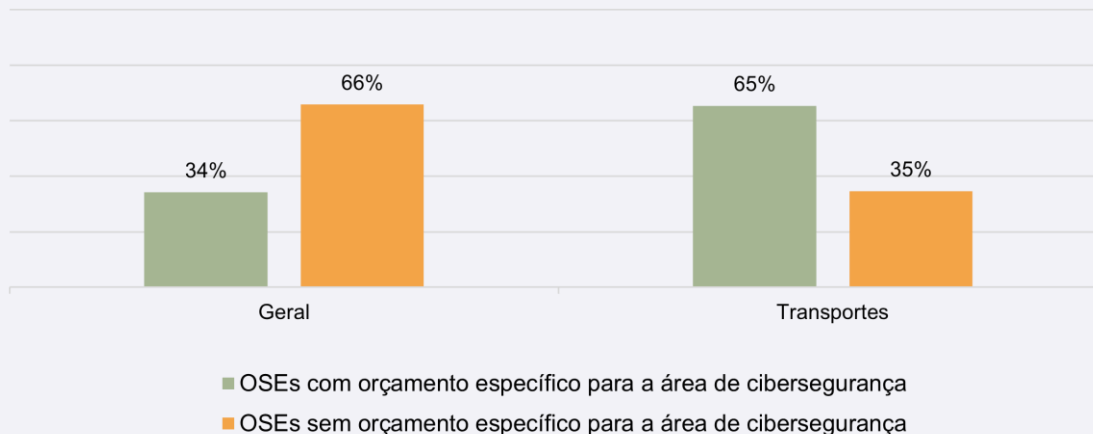
As políticas de cibersegurança e relacionadas menos implementadas foram: a política de gestão de continuidade de negócio com 59% e a política de uso aceitável de ativos com 71% (**Gráfico 79.2**).

Gráfico 79.2 - Políticas incluídas no Plano de Segurança



Relativamente a orçamentos específicos da área de cibersegurança, cerca de 65% dos operadores já possuem um, ficando dentro da média no âmbito geral (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Transporte Aéreo

A história do transporte aéreo em Portugal começou a escrever-se com a realização do primeiro voo bem-sucedido no país, a 27 de abril de 1910, protagonizado pelo piloto Julien Mamet a bordo de uma aeronave Blériot XI, já famosa por ter sido a primeira a atravessar o Canal da Mancha, cerca de um ano antes³²¹. No ano seguinte, 1911, deu-se o primeiro voo bem-sucedido com um piloto português, Alberto Sanches de Castro, ao comando (de uma aeronave Voisin Antoinette)³²². Durante a primeira metade da década de 1910, a aviação e o transporte aéreo eram ainda mais vistos como uma forma de espetáculo e de entretenimento do que um meio de transporte prático, embora os espetáculos aéreos atraíssem grandes multidões nos Estados Unidos da América e na Europa³²³. Não obstante, a tecnologia aeronáutica foi evoluindo e sendo seguida de perto pelo mundo militar, tendo depois desempenhado um importante papel durante a Primeira Guerra Mundial, para funções de observação e reconhecimento, durante o primeiro ano da Guerra (1914) e, depois, para combate aéreo, quando os aviões começaram a ser equipados com armas de fogo (1915-1918)³²⁴.

Passados quatro anos de guerra na Europa em que a aviação fora sobretudo orientada para o uso militar, a aviação civil teve necessidade de se afirmar. Em Portugal, essa afirmação veio por meio da criação de órgãos nacionais destinados à regulamentação do transporte aéreo civil. Em 1929, surge o Conselho Nacional do Ar, através do Decreto-lei n.º 16:424, de 26 de janeiro³²⁵. O Conselho Nacional do Ar foi a primeira estrutura formal e independente de regulação do setor do transporte aéreo no país³²⁶. A década de 30 via a aviação civil e comercial desenvolver-se.

³²¹ “Blériot XI”, Museu do Ar, <https://museudoar.pt/pagina-001.003.002.005-bl-riot-xi>.

³²² Graça Ramos, “A Escola de Aviação de Vila Nova da Rainha”, RTP Ensina, 2016, <https://ensina.rtp.pt/artigo/a-escola-de-aviacao-de-vila-nova-da-rainha/>.

³²³ David Onkst, “The First U.S. Airshows – the Air Meets of 1910”, U.S. Centennial of Flight Commission, https://www.centennialofflight.net/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.

³²⁴ Dave Roos, “How Airplanes Were Used in World War I”, History, 10 de fevereiro de 2022, atualizado a 10 de maio de 2024, <https://www.history.com/news/world-war-i-aviation-airplanes>.

³²⁵ Decreto-lei n.º 16:424, *Diário do Governo*, 26 de janeiro de 1929, <https://files.diariodarepublica.pt/1s/1929/01/02200/02890290.pdf>.

³²⁶ “A nossa história”, Autoridade Nacional da Aviação Civil (ANAC), <https://www.anac.pt/vPT/Generico/ANAC/QuemSomos/Historia/Paginas/Historia.aspx>.

Na década seguinte, de 1940, assinalaram-se importantes marcas no desenvolvimento da aviação. Foi durante esta que foram construídos e abertos ao tráfego os aeroportos de Lisboa (1942) e do Porto (1945). Foi também durante a década de 40 que foi criado o Secretariado da Aeronáutica Civil, através do Decreto-lei n.º 33:967, de 22 de setembro 1944³²⁷ ³²⁸. Foi sob alçada deste órgão que surgiu, a 14 de março de 1945, a Secção de Transportes Aéreos, dirigida por Humberto Delgado. A Secção de Transportes Aéreos foi a precursora do que é hoje a principal companhia aérea portuguesa – a TAP Air Portugal (cuja sigla TAP significa Transportes Aéreos Portugueses)³²⁹. Em contraste com a década de 1910, em que as primeiras aeronaves foram adaptadas para a utilização militar, agora, no pós-Segunda Guerra Mundial, eram as aeronaves militares a serem adaptadas para o transporte aéreo civil. Os dois primeiros aviões da companhia são prova disso: eram dois Dakota DC-3, aviões militares, agora adaptados para a utilização civil e comercial³³⁰.

A primeira linha aérea comercial da companhia foi estabelecida entre Lisboa e Madrid, tendo sido inaugurada em setembro de 1946. No final do mesmo ano, foi inaugurada a “Linha Aérea Imperial”, ligando Lisboa às províncias ultramarinas através da rota Lisboa-Luanda-Lourenço Marques (atualmente Maputo). Ainda durante esta década, a companhia abriu a sua ligação Lisboa-Porto (1947), bem como ligações a Sevilha e Paris, em 1948, e a Londres, em 1949³³¹.

Após o impulso da década de 40, as décadas seguintes continuaram a registar avanços significativos na aviação civil e comercial. A década de 50 viu serem introduzidos os aviões a jato, novas rotas para Marrocos (Casablanca e Tânger), ser realizado o primeiro voo experimental entre Lisboa e o Rio de Janeiro, no Brasil, e serem reduzidos os tempos de voo entre destinos. Nos anos 60, foram iniciados os voos entre Lisboa e o Oriente, com destino a Goa. Surgiam também novas ligações na Europa, como Genebra, Munique e Frankfurt, e era inaugurada a rota do Funchal. Na década seguinte, de 70, é aumentada a rota atlântica, com ligações às ilhas de São Miguel e Terceira, nos Açores, e à América do Norte, com ligações a Boston nos EUA e a Montréal, no Canadá. Os anos 70 marcam também o início do uso de um sistema computadorizado para reservas, *load-control* e *check-in* pela TAP – o TAPMATIC. Na década de 80, surgem ligações a Barcelona, Roma e Caracas. Teresa Carvalho torna-se a primeira mulher a entrar para o quadro de pilotos da TAP. A companhia portuguesa é primeira a estabelecer ligações terra-ar via satélite. Nos anos 90, observa-se uma expansão dos destinos possíveis a partir do Porto. A TAP passa a ter presença na Internet, sendo lançado o primeiro *website* da companhia em 1996³³².

³²⁷ “A nossa história”, ANAC.

³²⁸ Decreto-lei n.º 33:967, *Diário do Governo*, 22 de setembro de 1944, <https://files.diariodarepublica.pt/1s/1944/09/20800/09290931.pdf>.

³²⁹ “Cronologia”, A Nossa História, TAP Air Portugal, <https://www.tapairportugal.com/pt/a-nossa-historia/cronologia>.

³³⁰ “Cronologia”, A Nossa História, TAP.

³³¹ “Cronologia”, A Nossa História, TAP.

³³² “Cronologia”, A Nossa História, TAP.

Seria então nos anos de 2000 que um evento do outro lado do Atlântico mudaria para sempre o setor da aviação. O atentado de 11 de setembro às Torres Gémeas do *World Trade Center*, em Nova Iorque, com dois aviões sequestrados, foi o ataque terrorista mais mortífero até à data, tendo causado a morte de quase três mil pessoas³³³. Face à tragédia, e para tentar impedir que algo semelhante alguma vez se repetisse, o setor da aviação foi sujeito, em todo o mundo, a uma ampla reforma de segurança, que não se limitou ao setor da aviação, mas que se estendeu a diversos setores de infraestruturas críticas, como centrais de energia, hospitais e a banca. A cibersegurança destas infraestruturas foi também contemplada nesta reforma³³⁴.

O setor do transporte aéreo tem continuado a evoluir e mantém-se, aos dias de hoje, como o meio de transporte mais seguro que existe³³⁵, desempenhando um importante papel como uma força motriz da economia, gerando emprego e facilitando o grande comércio e turismo internacionais³³⁶.

Transporte Marítimo e por vias navegáveis interiores

Os primeiros aglomerados populacionais começaram a fixar-se em áreas próximas a cursos de água, muito devido à fertilidade dos terrenos e à abundância de alimento proveniente da pesca. Desde as antigas civilizações que é realizado o transporte de pessoas recorrendo a embarcações arcaicas que foram melhorando com o tempo e experiência. As primeiras embarcações, assim como as utilizadas pelos portugueses na época dos descobrimentos no longínquo século XV, eram feitas de madeira. No século XVII ocorreu uma revolução na engenharia naval e as embarcações começam a utilizar o metal como material de construção. Esta inovação possibilitou o surgimento de embarcações maiores, aumentando, assim, a capacidade de transporte³³⁷.

No século XIX, a tecnologia do vapor foi adaptada à navegação marítima, impulsionando as trocas comerciais, estimulando globalmente o comércio. A introdução da máquina a vapor acelerou significativamente o transporte marítimo, eliminando a dependência dos ventos para navegar³³⁸. A abertura do canal do Suez, em 1869, viria também a acelerar o comércio marítimo, acabando com a necessidade de contornar o continente africano para as embarcações que navegavam entre a Europa e a Ásia, reduzindo em cerca de 6 mil quilómetros os percursos de navegação entre os dois continentes³³⁹. Atualmente, cerca de 80% do comércio mundial é realizado por transporte marítimo³⁴⁰.

³³³ "The Memorial", 9/11 Memorial and Museum, <https://www.911memorial.org/visit/memorial>.

³³⁴ "Safeguarding and Securing Cyberspace", Press Release, News, CISA, 20 de julho de 2020, <https://www.cisa.gov/news-events/news/safeguarding-and-securing-cyberspace>.

³³⁵ International Air Transport Association (IATA), "IATA Annual Safety Report Executive Summary and Safety Overview - 2023", 2024, 6, <https://www.iata.org/contentassets/a8e49941e8824a058fee3f5ae0c005d9/safety-report-executive-and-safety-overview-2023.pdf>.

³³⁶ Air Transport Action Group (ATAG) "Aviation: Benefits Beyond Borders", setembro de 2020, 4, <https://ataq.org/industry-topics/supporting-economic-social-development>.

³³⁷ José Castro, "Tendências de Evolução dos Transportes Marítimos Internacionais e Implicações nas Infraestruturas Portuárias", junho de 2018, 1, <https://repositorio-aberto.up.pt/bitstream/10216/113509/2/275756.pdf>.

³³⁸ Nuno Pousinho, "A revolução do sistema de transportes", *RTP Ensina*, 2021, <https://ensina.rtp.pt/explicador/a-revolucao-do-sistema-de-transportes-h70/>.

³³⁹ "Geographical Impacts of the Suez and Panama Canals", The Geography of Transport Systems, <https://transportgeography.org/contents/chapter1/emergence-of-mechanized-transportation-systems/suez-panama-canal-geography-impacts/>.

³⁴⁰ ONU, "Transporte marítimo perfaz mais de 80% do comércio global", 24 de setembro de 2020, <https://news.un.org/pt/story/2020/09/1727312>.

Em 1974 foram criadas a Direção-Geral da Marinha de Comércio (DGMC) e a Inspeção-Geral de Navios (IGN). Por sua vez, em 1980, foi estabelecida a Direção-Geral do Pessoal do Mar e Estudos Náuticos. Estas três entidades uniram-se em 1989, formando a Direção-Geral da Navegação e Transportes Marítimos, por meio do Decreto-Lei n.º 317/89³⁴¹, de 22 de setembro. No mesmo ano, também foi criada a Direção-Geral dos Portos (DGP). Em 1993, através do Decreto-Lei n.º 319/93³⁴², de 21 de setembro, ocorreu a fusão das entidades formadas em 1989, resultando na Direção-Geral de Portos, Navegação e Transportes Marítimos (DGPNTM). O Instituto Marítimo-Portuário (IMP) teve a sua criação no ano de 1998, fruto da fusão entre a DGPNTM, o Instituto do Trabalho Portuário (ITP) e o Instituto Nacional de Pilotagem de Portos (INPP)³⁴³.

Através da reestruturação da administração pública na área marítimo-portuária foi criado, em 2002, o Instituto Portuário e dos Transportes Marítimos (IPTM). Por meio do Decreto-Lei n.º 257/2002³⁴⁴, de 22 de novembro, ocorreu a fusão entre o Instituto Marítimo-Portuário (IMP) com os três Institutos Portuários (Norte, Centro e Sul), e com o Instituto da Navegabilidade do Douro, todos criados em 1998. Em 2012, o Decreto-Lei n.º 49-A/2012³⁴⁵, de 29 de fevereiro, resultou na criação da Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM) por meio da fusão entre o Instituto Portuário e dos Transportes Marítimos, I. P. (IPTM) e da Direção-Geral das Pescas e Aquicultura (DGPA).

A DGRM é responsável pela segurança e proteção marítimas, bem como pela certificação de embarcações. Também realiza inspeções em navios no âmbito do controlo pelo Estado nos portos e supervisiona a navegação costeira, gerindo o planeamento e a organização do espaço marítimo³⁴⁶.

Segundo o relatório da ENISA “*Guidelines - Cyber Risk Management for Ports*”, relativo à gestão de riscos de cibersegurança em operadores portuários na UE, este subsetor começou de forma gradual e mais sistémica a preocupar-se com a sua exposição em matéria de cibersegurança muito devido à ocorrência de alguns incidentes de cibersegurança nos últimos anos, nomeadamente ataques de *ransomware*. À semelhança de outros OSE, também os operadores portuários são responsáveis por funções críticas, por exemplo, das suas cadeias de abastecimento, ligando serviços terrestres e marítimos³⁴⁷.

³⁴¹ Decreto-Lei n.º 317/89, de 22 de setembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/317-547635>.

³⁴² Decreto-Lei n.º 319/93, de 21 de setembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/319-1993-655527>.

³⁴³ DGRM, “Breve História”, <https://www.dgrm.pt/breve-historia>.

³⁴⁴ Decreto-Lei n.º 257/2002, de 22 de novembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/257-2002-448755>.

³⁴⁵ Decreto-Lei n.º 49-A/2012, de 29 de fevereiro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/49-a-2012-551446>.

³⁴⁶ DGRM, “Breve História”.

³⁴⁷ ENISA, “*Guidelines - Cyber Risk Management for Ports*”, dezembro de 2020, 13-16, <https://safety4sea.com/wp-content/uploads/2021/12/ENISA-Guidelines-Cyber-Risk-Management-for-Ports.pdf>.

Transporte Ferroviário

O comboio e a ferrovia iniciaram o ciclo de grande progresso dos transportes. Podemos datar os primeiros tipos de transporte ferroviário à idade média. Durante esta altura, este tipo de transporte era utilizado para transportar itens considerados mais pesados e cujo transporte tornava-se complicado sem recorrer a este tipo de sistemas³⁴⁸. Com o desenvolvimento da locomotiva a vapor, iniciou-se, em Inglaterra, a expansão da ferrovia, que seria depois copiada pelos países europeus e levada a outros continentes. A tecnologia do vapor, adaptada também à navegação marítima acelerou as trocas comerciais, estimulando globalmente o comércio³⁴⁹. A industrialização verificada durante o século XIX permitiu um rápido crescimento das linhas de comunicação. O desenvolvimento da ferrovia permitia o transporte de cada vez mais pessoas e mercadorias a ritmos até então nunca vistos, aproximando economias e mercados. Em Portugal, os caminhos de ferro foram inaugurados em 28 de outubro de 1856, onde o projeto inicial seria a criação de uma linha ferroviária do Porto à fronteira de Badajoz.

Em Portugal, Carlos Alberto da Maia, Conselheiro da Junta Consultiva de Obras Públicas e Minas, deslocou-se a Inglaterra, França e Bélgica na primeira metade do século XIX, com o propósito de observar a evolução e as técnicas de construção das redes de transportes destes países. Os caminhos de ferro seriam inaugurados pelo Rei D. Pedro V, em 28 de outubro de 1856. O primeiro troço inaugurado foi entre Lisboa e Carregado com o total de 38 quilómetros. No ano seguinte deu-se início ao transporte de mercadorias em grande velocidade e em novembro de 1858 em pequena velocidade. A 22 dezembro de 1859 a Companhia real dos Caminhos de Ferro Portugueses é criada com os estatutos aprovados através de decreto³⁵⁰ e, em 5 de dezembro de 1860, é publicado o decreto que aprova o Regulamento para a Fiscalização dos Caminhos de Ferro.

Entre 1861 e 1890 ocorreram diversas etapas no desenvolvimento ferroviário em Portugal, incluindo a abertura de novas linhas e troços. Em fevereiro de 1861 começou a exploração na linha do Sul e do Sado. Neste espaço de tempo, as primeiras linhas começaram a operar, incluindo a linha entre Lisboa e Madrid. Em junho de 1860 é inaugurada a estação central do Rossio. Entre 1892 e 1894 começou a ser planeada a construção da estação central do Porto e a Companhia real dos Caminhos de Ferro Portugueses enfrenta dificuldades financeiras assim como greves dos operários. No ano de 1912 é criado o Sindicato Pessoal. A 17 de junho de 1927 é publicado o Decreto-Lei n.º 13:829 que cria a Comissão Administrativa do Fundo Especial de Caminhos de Ferro. A 16 de abril de 1974 é nacionalizada com a publicação do Decreto-Lei n.º 205-B/175³⁵¹, em 1987 dá-se início do serviço Alfa entre Lisboa e Porto e em 1993 é criado o passe combinado da Carris e do Metro.

³⁴⁸ James E. Vance e Thomas Clark Shedd, "Railroad history", outubro de 2024, <https://www.britannica.com/technology/railroad/Railroad-history>.

³⁴⁹ Nuno Pousinho, "A revolução do sistema de transportes", *RTP Ensina*, 2021, <https://ensina.rtp.pt/explicador/a-revolucao-do-sistema-de-transportes-h70/>.

³⁵⁰ Decreto-Lei n.º 143, de 26 de junho, *Diário da República*, <https://legislacaoeregia.parlamento.pt/V/1/35/9/p232>.

³⁵¹ Decreto-Lei n.º 205-B/75, de 26 de junho, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/205-b-1975-497832>.

Com o Decreto-Lei n.º 299-B³⁵², de 29 de setembro de 1998, é criado o Instituto Nacional de Transporte Ferroviário (INTF) e, dois meses depois, o INFT inicia as suas atividades, incluindo funções de Regulação, Supervisão e Desenvolvimento do setor ferroviário³⁵³. Em 2015 ocorreu a criação das Infraestruturas de Portugal (IP) e, por consequente, a extinção e incorporação por fusão das Estradas de Portugal na Rede Ferroviária Nacional (RFN). Em 2024, a RFN tem linhas e ramais com uma extensão de 2527 km e existem 561 estações e apeadeiros ferroviários em exploração. Destes, cerca de 290 têm serviço exclusivo de passageiros, 8 serviço exclusivo de mercadorias e 245 têm serviço misto³⁵⁴.

Olhando para o futuro, os Caminhos de Ferro estão a ser alvos de uma profunda transformação, nomeadamente com o Projeto da Nova Linha de Alta Velocidade Porto – Lisboa com bitola ibérica. Este projeto irá aumentar a capacidade e competitividade do sistema ferroviário, reforçar a conectividade territorial e aumentar a descarbonização do setor dos transportes. Este projeto irá ter 3 fases³⁵⁵:

- **Fase 1:** Esta fase irá decorrer entre 2024 e 2028 e tem como objetivo concluir a linha da linha de alta velocidade entre o Porto e Soure;
- **Fase 2:** A segunda fase deste projeto irá decorrer entre 2026 e 2030 e tem como objetivo criar a ligação de alta velocidade entre Soure e o Carregado;
- **Fase 3:** Esta última fase irá ocorrer depois de 2030 e o grande objetivo é concluir a ligação entre o Carregado e Lisboa e, assim, tornar possível a viagem em alta velocidade entre Lisboa e o Porto.

Após o aparecimento da Diretiva NIS em 2016, gestores de infraestruturas e empresas europeias do setor têm cada vez mais atenção e preocupação em abordar de forma consistente e sistemática os riscos de cibersegurança como parte dos processos de gestão. O facto de ser agora uma preocupação mais recente, traz grandes desafios devido à falta de experiência interna das empresas ferroviárias, défice de estrutura organizacional e ausência de processos ou recursos para avaliar e mitigar os riscos de forma correta e eficaz³⁵⁶.

³⁵² Decreto-Lei n.º 299-B/98, de 29 de setembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/299-b-349923>.

³⁵³ Comboios de Portugal, “Cronologia da história dos caminhos de ferro em Portugal”, <https://www.cp.pt/institucional/pt/cultura-ferroviaria/historia-cp/cronologia>.

³⁵⁴ IP Património, “O passado, presente e futuro da Ferrovia que celebra 167 anos”, outubro de 2023, <https://www.ippatrimonio.pt/pt-pt/167-anos-do-caminho-de-ferro-em-portugal>.

³⁵⁵ Infraestruturas de Portugal, “Linha de Alta Velocidade Porto – Lisboa”, <https://www.infraestruturasdeportugal.pt/pt-pt/principais-investimentos/linha-de-alta-velocidade-porto-lisboa>.

³⁵⁶ ENISA, “Railway Cybersecurity”, novembro de 2021, 4, <https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management>.

Transporte Rodoviário

O subsetor do transporte rodoviário, no âmbito da Diretiva n.º 2016/1148 e do RJSC, cinge-se a dois tipos de entidades: autoridades rodoviárias, ou seja, “qualquer autoridade pública responsável pelo planeamento, pelo controlo ou pela gestão das vias abrangidas pelo âmbito da sua competência territorial”³⁵⁷, tal como o Instituto da Mobilidade dos Transportes (IMT) ou as Infraestruturas de Portugal (IP), e operadores de sistemas de transporte inteligentes (STI)³⁵⁸, nos quais se podem incluir detentoras de concessões de estradas (como a Brisa ou a Ascendi), empresas de transportes públicos, operadores de logística, que utilizam STI para seguir e otimizar o transporte de mercadorias e até mesmo entidades de gestão de estacionamento inteligente, como sistemas de parquímetros. Sendo este o âmbito de aplicação do RJSC, a história deste subsetor prende-se essencialmente com a crescente utilização do automóvel, a evolução das autoridades rodoviárias portuguesas, da rede de estradas e das empresas detentoras das suas concessões e da rede de transportes públicos.

O primeiro automóvel chegou a Portugal em 1895, cerca de nove anos depois da sua invenção e registo de patente (1886), pela mão do Conde Jorge de Avilez, que adquirira um automóvel da marca Panhard et Levassor, em Paris³⁵⁹. Cerca de seis anos mais tarde, a 3 de outubro de 1901, era publicado o primeiro Regulamento sobre circulação de automóveis, que impunha os primeiros limites de velocidade, obrigações de provas e inspeções, bem como a necessidade de se obter licença de circulação³⁶⁰. As estradas portuguesas, no entanto, preparadas essencialmente para os pedestres e veículos de tração animal, não eram adequadas para a circulação automóvel, que exigia vias mais largas e pisos mais firmes e regulares. A reforma das estradas portuguesas iniciara-se já na década de 20, após o início da ditadura militar (1926). Em 1927, foi criada a Junta Autónoma de Estradas (JAE), responsável pela “construção de modernas pavimentações e a reconstrução das antigas em grandes troços, a reparação e construção das obras de arte mais importantes, e o estudo e construção das grandes extensões de estradas que faltam para concluir a rede do Estado”³⁶¹. É também de notar que, por esta data, circulavam já em Portugal cerca de 12 mil automóveis, pelo que se começava a tornar urgente a reforma das estradas³⁶². Também por esta altura começavam a surgir os primeiros transportes rodoviários coletivos, tendo, todavia, merecido menos atenção do Estado português nesta fase³⁶³.

³⁵⁷ Diretiva (UE) 2016/1148, Anexo II, 28.

³⁵⁸ Diretiva (UE) 2016/1148, Anexo II, 28.

³⁵⁹ Ana Laura, “Os primeiros automóveis em Portugal”, *RTP Ensina*, 1990, <https://ensina.rtp.pt/artigo/os-primeiros-automoveis-em-portugal/>.

³⁶⁰ “Regulamento sobre circulação de automóveis”, Coleção Oficial de Legislação Portuguesa: Ano de 1901 (Lisboa: Imprensa Nacional, 1902), 701, in Parlamento: Legislação Régia, <https://legislacao regia.parlamento.pt/V/1/86/133/p733>.

³⁶¹ Decreto n.º 13:969, de 20 de julho, *Diário do Governo*, 20 de julho de 1927, 1394, <https://files.diariodarepublica.pt/1s/1927/07/15300/13921396.pdf>.

³⁶² Florbela Maré, “História das Infraestruturas Rodoviárias” (diss. mestrado, Universidade do Porto, 2011), 17, <https://repositorio-aberto.up.pt/bitstream/10216/61562/1/000148960.pdf>.

³⁶³ Raul Esteves, “O Problema Nacional dos Caminhos de Ferro”, *Gazeta dos Caminhos de Ferro* n.º 1208 (16 de abril de 1938): 181, in Hemeroteca Digital de Lisboa, https://hemerotecadigital.cm-lisboa.pt/obras/gazetacf/1938/N1208/N1208_master/GazetaCFN1208.pdf.

Os anos seguintes, nomeadamente os da década de 30, foram anos em que os esforços de melhoria da infraestrutura rodoviária se concentraram nos caminhos rurais, sobretudo ao nível do embelezamento das estradas e da distribuição de sinalética nas mesmas³⁶⁴. O valor destas melhorias foi amplamente reconhecido. O aumento do tráfego de automóveis, passageiros e mercadorias, as facilidades de escoamento dos produtos agrícolas das zonas rurais para as urbanas, entre outras, levaram o Estado a elaborar, na década seguinte, um Plano Nacional Rodoviário (1945), que estabelecia as diretrizes para o desenvolvimento da rodovia no país, desde as classificações das diferentes vias até às suas dimensões, e que procurava melhorar os acessos às zonas menos bem servidas de estrada, bem como continuar a aumentar a rede rodoviária na ligação entre concelhos³⁶⁵. Foi também na década de 40 que a Carris, em Lisboa, e o Serviço de Transportes Coletivos do Porto (STCP), passaram a prestar o serviço de autocarros nas respetivas cidades^{366 367}. O desenvolvimento da rodovia foi progredindo a bom ritmo, e, fazendo um balanço do Plano Nacional Rodoviário, foi possível concluir que entre 1937 e 1957 a rede de estrada alcatroada tinha mais do que duplicado, passando de 3564 km a 7495 km de estrada³⁶⁸.

Chegados à década de 60, viam-se novas iniciativas ganhar força na rodovia. Foi nesta década que se iniciou a construção da primeira autoestrada do país, a A1, que hoje liga Lisboa e Porto, e foi também nesta década que se iniciou e concluiu a construção da Ponte 25 de Abril³⁶⁹, que atualmente liga por rodovia e ferrovia Lisboa e Almada (à data de inauguração, em 1966, a ponte possuía apenas o tabuleiro rodoviário). Apesar destes dois marcos, esta foi uma década em que se realizaram poucas obras dignas de registo, em parte porque a década foi marcada por uma migração da população das zonas rurais para as cidades do litoral, reduzindo a urgência da melhoria das estradas do interior.

A década de 70, por sua vez, não foi extraordinariamente diferente da anterior em matéria de evolução da infraestrutura rodoviária. Marcada pela Revolução de Abril em 1974, que punha fim ao regime ditatorial e dava início ao regime democrático, e pela instabilidade política decorrente da mudança de regime, a década de 70 foi um período em que se produziram mais documentos críticos sobre o sistema rodoviário português deixado pelo Estado Novo do que se realizaram obras no terreno³⁷⁰. Não obstante, foi ainda nesta década, antes da Revolução, que foi constituída a Brisa e que se assinou o primeiro contrato de concessão para o financiamento, construção e manutenção da principal rede de autoestradas em Portugal, no ano de 1972³⁷¹. O abrandamento dos trabalhos na modernização da infraestrutura rodoviária nas décadas de 60 e 70 coincidiu também com uma fase de proliferação do automóvel em Portugal. Entre 1969 e 1973, a cada ano havia cerca de mais 10 mil automóveis em circulação nas estradas portuguesas³⁷².

³⁶⁴ Elsa Pacheco “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte: expectativas, intervenções e resultantes” (tese de doutoramento, Universidade do Porto, 2001), 123-124, https://www.academia.edu/10413987/Alteracao%20da%20Acessibilidade_e_dinamicas_territoriais_na_Regiao_Norte_expectativas_intervencao_e_resultantes?auto=download.

³⁶⁵ Decreto-lei n.º 34:593: Plano Rodoviário, *Diário do Governo*, 11 de maio de 1945, <https://files.dre.pt/1s/1945/05/10201/03730394.pdf>.

³⁶⁶ “História”, A Carris, Carris, <https://www.carris.pt/a-carris/historia/>.

³⁶⁷ “Origem”, Sobre a STCP, STCP, <https://www.stcp.pt/pt/institucional/sobre-a-stcp/origem/>.

³⁶⁸ Pacheco, “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte”, 126.

³⁶⁹ Pacheco, “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte”, 128.

³⁷⁰ Pacheco, “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte”, 129.

³⁷¹ “História”, Sobre nós, Grupo Brisa, <https://grupobrisa.pt/sobre-nos/historia/>.

³⁷² PORDATA, “Veículos matriculados: total e por tipo de veículo”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Veiculos_matriculados_total_e_por_tipo_de_veiculo.xlsx.

A popularização do automóvel, aliada à falta de construção e modernização da infraestrutura rodoviária durante as últimas duas décadas levaria a duras críticas da JAE em 1977, que afirmava que “a rede rodoviária nacional [se encontrava] numa situação de completo desajustamento perante as necessidades do tráfego. Traçados sinuosos e estreitos, com pavimentos em degradação progressiva a atingirem o colapso”³⁷³. O desajuste da rodovia e as críticas à infraestrutura, bem como a perspetiva de adesão à Comunidade Económica Europeia (CEE), levariam os novos governos democráticos a visitar a infraestrutura rodoviária do país.

Foi na década de 80, depois de diversos estudos realizados, que surgiu, 40 anos depois, um novo Plano Nacional Rodoviário (1985)³⁷⁴. A adesão formal à CEE, em 1986, juntamente com os novos fundos comunitários para o investimento em infraestruturas, terão sido a força motriz para uma nova fase de expansão da rede rodoviária em Portugal³⁷⁵. A Brisa desempenhou um importante papel nesta nova fase, contribuindo significativamente para a expansão da rede de autoestradas no país. É durante estes anos que a Brisa atinge a marca dos 200 km de rede e também nesta década que se conclui a ligação entre Porto e Coimbra e que se inaugura a primeira área de serviço em Portugal³⁷⁶.

Já na década de 90, é finalmente concluída a A1, estabelecendo a ligação de todo o percurso entre Lisboa e Porto por autoestrada. A rede Brisa atinge os 600 km de extensão. É também nesta década que surge a tecnologia Via Verde, inicialmente uma forma de pagamento eletrónico apenas para portagens, sem necessidade de parar na praça de portagens. Portugal era o primeiro país do mundo a implementar este tipo de tecnologia. Chegados ao ano de 2000, são concluídas duas ligações a Espanha – a A3 e a A6 e, em 2003, a Via Verde passa também a ser utilizável no acesso a parques de estacionamento³⁷⁷. Em 2014 é lançada a primeira aplicação móvel da Via Verde³⁷⁸ e, nesse mesmo ano, a EMEL (Empresa Municipal de Mobilidade e Estacionamento de Lisboa) lançava uma *app* que permitia o pagamento do parquímetro através do telemóvel³⁷⁹. Em 2016 a Via Verde lançava a aplicação Estacionar³⁸⁰, com valências semelhantes à aplicação da EMEL.

Portugal conta atualmente com cerca de 15 mil km de estrada, nas quais a totalidade dos veículos percorre cerca de 25 mil milhões de km em cada ano³⁸¹. A infraestrutura rodoviária suporta, também o principal modo de transporte em Portugal, tanto de passageiros como de mercadorias, tema que se explora em maior detalhe em 2.1.1. Impacto socioeconómico.

³⁷³ Pacheco, “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte”, 130.

³⁷⁴ Decreto-Lei n.º 380/85, de 26 de setembro, Diário da República, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/380-176998>.

³⁷⁵ Pacheco, “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte”, 135.

³⁷⁶ “História”, Grupo Brisa.

³⁷⁷ “História”, Grupo Brisa.

³⁷⁸ “História”, Grupo Brisa.

³⁷⁹ “ePark – App da Emel para pagamento do estacionamento” *Pplware*, 22 de setembro de 2014, https://pplware.sapo.pt/smartphones-tablets/windows_phone/epark-app-da-emel-para-pagamento-do-estacionamento/

³⁸⁰ “História”, Grupo Brisa.

³⁸¹ “A Rede em Números”, Infraestruturas, Infraestruturas de Portugal, <https://www.infraestruturasdeportugal.pt/pt-pt/rede-rodoviaria-ip>.

2.1.1. Impacto socioeconómico

O setor dos transportes desempenha um papel crucial nos contextos social e económico a nível nacional, facilitando o comércio e a cadeia de abastecimento por meio dos diferentes modos de transporte, como rodoviário, ferroviário, marítimo e aéreo. Estes meios permitem o transporte de pessoas e mercadorias, sem os quais nunca conseguiríamos manter vivo qualquer ciclo económico.

Em Portugal, em 2022, este setor incluía cerca de 24 mil empresas, com uma taxa de variação anual (VVN) na ordem dos 16,5 mil milhões de euros e empregava cerca de 127 mil pessoas. A maior percentagem de empresas (93%) corresponde à fatia de microempresas. No entanto, 0,23% é a percentagem de grandes empresas que gere o maior valor de VVN, de cerca de 47%. O subsetor dos transportes terrestres é o subsetor dominante no que diz respeito ao VVN, com pouco mais de 98% das empresas a gerar cerca de 59% do volume. A tabela seguinte mostra a variação e evolução de alguns dos indicadores económicos e financeiros relevantes, em 2022³⁸²:

Tabela 16 - Variação e evolução dos indicadores financeiros e económicos (Transportes)

Indicador	Ano	Subsetores		
		Transportes Terrestres	Transportes por água	Transportes aéreos
VVN - taxa de variação anual	2021	14,07%	14,59%	30,39%
	2022	19,59%	41,22%	107,83%
EBITDA - taxa de variação anual	2021	31,85%	7,06%	-15,83%
	2022	36,26%	186,44%	120,26%
Rendibilidade dos capitais próprios	2021	2,08%	-3,24%	-45,53%
	2022	6,52%	5,85%	16,29%
Autonomia financeira	2021	38,54%	36,81%	-14,81%
	2022	36,91%	38,79%	7,97%
Pressão financeira	2021	7,45%	29,73%	114,9%
	2022	7,84%	19,08%	55,39%

³⁸² Banco de Portugal, "Análise das empresas do setor dos transportes", 2022, <https://bpstat.bportugal.pt/conteudos/publicacoes/1343>.

Definição:

- 1) **VVN**: valor das vendas e das prestações de serviços realizados pelas empresas durante o exercício económico;
- 2) **EBITDA**: resultado antes de depreciações e amortizações, gastos de financiamento e impostos, corresponde ao resultado das atividades de exploração e das atividades financeiras das empresas;
- 3) **Rentabilidade dos capitais próprios**: quociente entre o resultado líquido do período e os capitais próprios, representa a rentabilidade extraída a partir dos capitais próprios das empresas;
- 4) **Autonomia financeira**: quociente entre o capital próprio e o ativo, expressa a maior ou menor capacidade de as empresas fazerem face aos seus compromissos financeiros através dos capitais próprios.
- 5) **Pressão financeira**: o quociente entre os gastos de financiamento e o EBITDA, indica a proporção do EBITDA gerado pelas empresas durante o período que se destina a cobrir os gastos de financiamento.

No mesmo ano, o VVN do setor de Transportes e Armazenagem teve um crescimento expressivo de 39,6%, totalizando mais de 29 mil milhões de euros. O subsector de empresas de Transportes, representando perto de 58% do VVN, também apresentou um aumento notável (+50,2% em 2022). O número de empresas no setor aumentou para 43 mil em 2022, indicando um crescimento significativo desde 2019 (+37,3%). Este cenário é refletido não apenas no aumento do número de empresas, mas também no crescimento do VVN³⁸³.

Em setembro de 2022, as Infraestruturas de Portugal uniram-se à campanha do Instituto da Mobilidade e dos Transportes (IMT), intitulada “O Futuro é Coletivo”, que tem como objetivo levantar um conjunto de vantagens para o utilizador dos transportes públicos e promovê-las, de modo que o seu uso seja cada vez mais frequente. Esta promoção vem na sequência do Programa de Apoio à Redução Tarifária nos Transportes Públicos (PART) que, graças a ações que provocaram poupanças nas famílias ou simplificação dos sistemas tarifários, levou ao aumento da afluência ao uso dos transportes públicos³⁸⁴.

Dados de 2023 revelam que Portugal se encontra na 17ª posição num total de 30 países no que diz respeito à utilização de transportes públicos. Se nos restringirmos a essa utilização apenas nas capitais, Lisboa ganha duas posições, ficando em 15º lugar de 30. Fatores como o elevado custo, qualidade de serviço em termos de densidade ou a frequência e rapidez de interligação podem justificar o facto de Portugal não se encontrar numa posição mais favorável da tabela³⁸⁵.

O impacto ambiental deste tipo de transportes representa, diretamente, um tipo de impacto societal. Se a sua utilização aumenta, verifica-se uma poupança de cerca de 2200 euros anuais por habitante e uma redução de emissão de gases de efeito de estufa. Naturalmente, os atuais 70% de emissões de gases na Europa que o combustível utilizado pelo setor dos transportes representa também diminuiria³⁸⁶.

³⁸³ Instituto Nacional de Estatística (INE), “Estatística dos Transportes e Comunicações 2022”, novembro de 2023, 5, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=141725&PUBLICACOESmodo=2.

³⁸⁴ “O Futuro é Coletivo: Use os Transportes Públicos”, Infraestruturas de Portugal, 19 de setembro de 2022, <https://www.infraestruturasdeportugal.pt/pt-pt/o-futuro-e-coletivo-use-os-transportes-publicos>

³⁸⁵ Rui Martins, “Aumentar o uso dos transportes públicos”, *Observador*, 2 de outubro de 2023, <https://observador.pt/opiniao/aumentar-o-uso-dos-transportes-publicos/>.

³⁸⁶ Martins, “Aumentar o uso dos transportes públicos”, 2 de outubro de 2023.

Transporte Aéreo

De acordo com dados divulgados pelo INE, em 2022, os operadores nacionais asseguraram 374 linhas aéreas regulares, sobre uma extensão total de quase um milhão de quilómetros (991 mil km) e foram realizados mais de 176 mil voos comerciais e transportados cerca de 16 milhões de passageiros³⁸⁷. Ao nível do transporte de carga e correio pelos operadores aéreos nacionais, foram transportadas, também em 2022, cerca de 103 mil toneladas. Se se contar toda a carga e correio movimentados nos aeroportos nacionais, este valor ascende às 223 mil toneladas³⁸⁸. O subsector do transporte aéreo terá ainda tido, no mesmo ano, um volume de negócios na ordem dos 4,8 mil milhões de euros³⁸⁹. Segundo o Banco de Portugal (2022), o número de empresas de transporte aéreo representaria 0,47% do universo total do setor dos transportes, assim como 9,09% do número de pessoas ao serviço de um total de cerca de 128 mil pessoas empregadas no setor dos transportes, o que se traduz em cerca de 11 mil pessoas empregadas no setor³⁹⁰. Já o movimento total de passageiros nos aeroportos portugueses atingiu os 56,8 milhões. As companhias portuguesas terão sido responsáveis pelo movimento de 19,8 milhões de passageiros. Os restantes 37 milhões foram da responsabilidade das companhias estrangeiras com operações em Portugal³⁹¹.

Um dos principais impactos do transporte aéreo é também a redução dos tempos de viagem. Por exemplo, uma viagem de Lisboa a Madrid levará, atualmente, cerca de seis horas, se feita num automóvel ligeiro. De autocarro ou de comboio, levará cerca de oito horas. De avião, o tempo de viagem reduz-se a cerca de uma hora. A redução dos tempos de viagem, aliada ao facto de haver menos meios aéreos em operação do que, por exemplo, veículos na estrada, reduz também grandemente a probabilidade de acidentes, tornando o transporte aéreo altamente seguro. O transporte aéreo atua também como um dinamizador do turismo, promovendo-o grandemente nas regiões servidas por infraestruturas aeroportuárias.

Apesar das vantagens trazidas pelo transporte aéreo, verificam-se também externalidades negativas. Duas delas são a poluição ambiental e a sonora. Sobre a poluição ambiental, um estudo recentemente publicado pela Federação Europeia de Transportes e Ambiente indica que cerca de 51 milhões de pessoas na Europa podem estar sujeitas a problemas de saúde pela sua proximidade aos aeroportos e exposição a partículas ultrafinas emitidas pelas aeronaves³⁹². No caso do aeroporto de Lisboa, estima-se que o número de pessoas colocadas em risco por residirem próximas do mesmo (num raio até 20 km) atinja um total de dois milhões, das quais 400 mil estarão num nível de risco mais elevado por viverem a 5 km ou menos do aeroporto³⁹³. Segundo o estudo, os principais problemas de saúde que podem advir da exposição prolongada às partículas ultrafinas são problemas do foro respiratório e cardiovascular, e ainda efeitos negativos durante a gravidez³⁹⁴.

Relativamente à poluição sonora, o ruído gerado pelo tráfego aéreo tem sido alvo de diversas críticas nos anos mais recentes. Segundo um estudo da Associação Zero, Lisboa é a segunda capital europeia mais ruidosa devido ao tráfego aéreo, atrás apenas do Luxemburgo³⁹⁵. Cerca de 15% da população estará sujeita a níveis de ruído médios na ordem dos 66,5 dB quando o máximo

³⁸⁷ INE, “Estatísticas dos Transportes e Comunicações 2022”, novembro de 2023, 63.

³⁸⁸ INE, “Estatísticas dos Transportes e Comunicações 2022”, novembro de 2023, 65.

³⁸⁹ PORDATA, “Volume de negócios das empresas de transporte aéreo: total e por área”, Temas em Construção, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Volume_de_negocios_das_empresas_de_transporte_aereo_total_e_por_area.xlsx?gl=1*gu9zqo*up*MQ..*ga*MTI5O TYOOTE3NS4xNzI4OTI1Njk0*ga_HL9EXBCVBZ*MTcyODkyNTY5NC4xLjAuMTcyODkyNTY5NC4wLjAuMA

³⁹⁰ Banco de Portugal, “Análise das empresas do setor dos transportes”, BPstat, <https://bpstat.bportugal.pt/conteudos/publicacoes/1343>.

³⁹¹ INE, “Estatísticas dos Transportes e Comunicações 2022”, novembro de 2023, 65.

³⁹² Daan Seters, Stefan Grebe e Jasper Faber, “Health Impacts of Aviation UFP Emissions in Europe”, CE Delft, maio de 2024, 35, https://www.transportenvironment.org/uploads/files/CEdelft_Final_Study.pdf.

³⁹³ Seters, Grebe e Faber, “Health Impacts of Aviation”, maio de 2024, 36.

³⁹⁴ Seters, Grebe e Faber, “Health Impacts of Aviation”, maio de 2024, 24.

³⁹⁵ Lília Alexandre, “Mobilizar Rumo à Poluição Zero – Ruído”, Associação Zero, janeiro de 2022, 15, https://zero.org/wp-content/uploads/2023/06/Mobilizar-Ruido_.pdf.

permitido por lei está fixado nos 55 dB³⁹⁶. O mesmo estudo indica ainda que a exposição prolongada a níveis de ruído superiores aos recomendáveis podem causar, para além de incómodo, perturbações no sono, provocar efeitos metabólicos e cardiovasculares adversos e até mesmo afetar o desenvolvimento cognitivo em crianças³⁹⁷.

Transporte Marítimo e por vias navegáveis interiores

Entre 2019 e 2021, o transporte marítimo destacou-se como o principal modal de movimentação de mercadorias, totalizando 162,9 milhões de toneladas³⁹⁸. Em 2022, nos portos marítimos nacionais, o movimento de mercadorias cresceu 2,3%, alcançando 85 milhões de toneladas, após um aumento de 4,7% em 2021. Em comparação a 2019, houve uma leve redução de 0,3%. O porto de Sines permaneceu como o mais significativo em Portugal, enquanto se verificaram variações nos volumes dos portos de Leixões e Lisboa, quando comparado com 2019. O transporte de veículos e passageiros por vias navegáveis interiores nacionais assegurou o transporte de 19,3 milhões de passageiros e 330,8 mil veículos, um aumento de 44,6% e 17%, respetivamente, relativamente ao ano anterior³⁹⁹.

De acordo com as estatísticas fornecidas pelo Banco de Portugal, em 2022, as empresas de Transporte Marítimo representavam 1,33% do universo total do setor de transportes, 2,08% do número das pessoas empregadas e 7,79% do volume de negócios. O EBITDA⁴⁰⁰ nestes setores subiu 35,9% em 2022, após um crescimento de 31,85% em 2021⁴⁰¹.

O transporte de passageiros por via fluvial aumentou 8% no primeiro trimestre de 2024 em relação ao mesmo período de 2023, totalizando 5,2 milhões de passageiros. No transporte de mercadorias por via marítima, observou-se um aumento de 2,5% em comparação com o trimestre anterior. Durante o primeiro trimestre de 2024, os portos nacionais receberam 2980 embarcações, havendo assim uma diminuição de 0,9% relativamente ao primeiro trimestre do ano anterior. De realçar que também ocorreu uma redução na dimensão das embarcações de cerca de 1,2%, alcançando assim cerca de 59 milhões de GT⁴⁰². No total, movimentaram-se cerca de 20 milhões de toneladas de mercadorias⁴⁰³.

No que diz respeito aos portos, o porto de Sines movimentou 10,6 milhões de toneladas no primeiro trimestre de 2024, o que correspondeu a um aumento de 14,8% face ao mesmo período do ano anterior. Por outro lado, no porto de Leixões ocorreu uma redução de 6,3% nas mercadorias movimentadas, assim como no porto de Lisboa, Aveiro e Setúbal. Em Lisboa a diminuição foi de 11,1%, em Aveiro foi de 14,2% e, em Setúbal, de 3,4%. No total foram carregadas 8,1 milhões de toneladas de mercadorias o que corresponde a um aumento de 8,5%. Quanto às mercadorias descarregadas ocorreu uma diminuição de 1% totalizando 12,5 milhões de toneladas. Por fim, em tráfego internacional houve um movimento de 17,6 milhões de toneladas de mercadorias (aumento

³⁹⁶ Alexandre, "Mobilizar Rumo à Poluição Zero – Ruído, janeiro de 2022, 15.

³⁹⁷ Alexandre, "Mobilizar Rumo à Poluição Zero – Ruído, janeiro de 2022, 17-18.

³⁹⁸ Graça Sousa e Dulce Vaz, "Os transportes internacionais de mercadorias, em Portugal 2019 a 2021", Gabinete de Estratégia e Estudos - Ministério da Economia e do Mar, junho de 2023, 3.

³⁹⁹ INE, "Estatística dos Transportes e Comunicações 2022", novembro de 2023, 8.

⁴⁰⁰ O EBITDA é o resultado antes de depreciações e amortizações, gastos de financiamento e impostos, corresponde ao resultado das atividades de exploração e das atividades financeiras das empresas. (Fonte: Banco de Portugal, "Análise das empresas do setor dos transportes", <https://bpstat.bportugal.pt/conteudos/publicacoes/1343>).

⁴⁰¹ Banco de Portugal, "Análise das empresas do setor dos transportes".

⁴⁰² Medida do volume total de uma embarcação, determinado em conformidade com a Convenção Internacional de Arqueação de 1969 e expressa num número inteiro sem unidade. (Fonte: INE, "Metainformação", janeiro de 2007, atualização em junho de 2024, https://www.ine.pt/bddXplorer/htdocs/minfo.jsp?var_cd=0002613&lingua=PT).

⁴⁰³ INE, "TRANSPORTE DE PASSAGEIROS CONTINUOU A AUMENTAR NO 1º TRIMESTRE DE 2024", junho de 2024, 1, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=670913041&att_display=n&att_download=y.

de 5,3%) e no tráfego nacional alcançou 2,9 milhões de toneladas diminuindo 11,4%⁴⁰⁴. Podemos dividir as mercadorias carregadas em sete categorias⁴⁰⁵:

- Produtos não energéticos das indústrias extrativas, turfa, urânio e tório;
- Produtos alimentares, bebidas e tabaco;
- Madeira e cortiça e suas obras (exceto mobiliário), obras de espartaria e de cestaria, pasta, papel e cartão e seus artigos, material impresso, suportes gravados;
- Coque e produtos petrolíferos refinados;
- Produtos químicos e fibras sintéticas, artigos de borracha e de matérias plásticas, combustível nuclear;
- Outros produtos minerais não metálicos;
- Metais de base, produtos metálicos transformados, exceto máquinas e equipamento.

Em 2022, no total de mercadorias carregadas por via marítima e por vias navegáveis interiores, destacam-se 2 612 557 toneladas de "Produtos não energéticos das indústrias extrativas, turfa, urânio e tório"; 3 883 307 toneladas de "Produtos alimentares, bebidas e tabaco"; 2 945 372 toneladas de "Madeira e cortiça e suas obras (exceto mobiliário), obras de espartaria e de cestaria, pasta, papel e cartão e seus artigos, material impresso, suportes gravados"; 7 299 971 toneladas de "Coque e produtos petrolíferos refinados"; 2 805 383 toneladas de "Produtos químicos e fibras sintéticas, artigos de borracha e de matérias plásticas, combustível nuclear"; 3 849 269 toneladas de "Outros produtos minerais não metálicos"; e 2 617 592 toneladas de "Metais de base, produtos metálicos transformados, exceto máquinas e equipamento".

Relativamente às mercadorias descarregadas, podemos dividir em 5 categorias⁴⁰⁶:

- Produtos da agricultura, da produção animal, da caça e da silvicultura, peixe e outros produtos da pesca;
- Hulha e lenhite, petróleo bruto e gás natural;
- Produtos alimentares, bebidas e tabaco;
- Coque e produtos petrolíferos refinados;
- Produtos químicos e fibras sintéticas, artigos de borracha e de matérias plásticas, combustível nuclear.

O total de mercadorias descarregadas nos portos por tipo de produto foi: 8 226 228 toneladas de "Produtos da agricultura, da produção animal, da caça e da silvicultura, peixe e outros produtos da pesca"; 14 117 886 toneladas de "Hulha e lenhite, petróleo bruto e gás natural"; 3 739 197 toneladas de "Produtos alimentares, bebidas e tabaco"; 7 125 747 toneladas de "Coque e produtos petrolíferos refinados"; e 5 210 813 toneladas de "Produtos químicos e fibras sintéticas, artigos de borracha e de matérias plásticas, combustível nuclear".

De acordo com o *website* Supply Chain Digital, em julho de 2023, o transporte marítimo de mercadorias do continente asiático para o continente europeu tinha um tempo de transporte estimado em 39 dias, com um tempo real de 40 dias. Já em junho de 2024, o tempo estimado é de 44 dias e o tempo real de 49 dias, resultando num acréscimo superior a 22% no tempo de transporte. A principal causa são os ataques perpetuados pelo movimento lénen aos navios mercantes que passam no Mar Vermelho. Em decorrência desta crise, a rota entre a Ásia e a América do Norte teve um aumento significativo de tráfego. Em relação à rota entre a América do

⁴⁰⁴ INE, "TRANSPORTE DE PASSAGEIROS CONTINUOU A AUMENTAR NO 1º TRIMESTRE DE 2024", 1.

⁴⁰⁵ PORDATA, "Mercadorias transportadas no sistema ferroviário: total e por principais mercadorias - Continente (2008-)", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_transportadas_no_sistema_ferrovioario_total_e_por_principais_mercadorias_-_Continente_%282008-%29.xlsx.

⁴⁰⁶ PORDATA, "Mercadorias descarregadas por via marítima: total e por principais mercadorias", julho de 2024, https://www.pordata.pt/sites/default/files/2024-09/PORTUGAL_601.xlsx.

Norte e a Europa, houve um aumento de 26% no tempo de trânsito, sendo a principal causa o colapso da ponte Francis Scott Key⁴⁰⁷.

A proteção do transporte marítimo é assegurada globalmente por meio de normas estabelecidas no Decreto-lei n.º 226/2006⁴⁰⁸, que define a estrutura básica de organização nacional necessária. Os principais objetivos incluem garantir a segurança dos trabalhadores; visitantes e das instalações; carga e navios; designar um Oficial de Proteção responsável por todas as questões relacionadas com a segurança; realizar avaliações de proteção e desenvolver planos de proteção específicos, além de promover a formação e organizar testes e simulacros⁴⁰⁹.

Transporte Ferroviário

No ano de 2022, 76,6% dos serviços de transporte da rede ferroviária eram de passageiros e mercadorias, 9% eram exclusivos de mercadorias e 14,4% eram exclusivos de transporte de passageiros⁴¹⁰. No mesmo ano, o transporte ferroviário de passageiros teve um aumento significativo em relação ao ano anterior, representando uma variação anual de 42,2% no caso do comboio e de 58,6% no caso do metropolitano, indicando uma procura crescente por esta modalidade⁴¹¹. No mesmo ano, a rede ferroviária permaneceu inalterada, mantendo a sua extensão de mais de 3.600 km, cerca de 546 estações de comboio e 820 passagens de nível⁴¹².

O transporte de passageiros por comboio ou metropolitano apresentou um notável aumento de 42,2%, alcançando perto de 172 milhões de passageiros - valor muito superior ao verificado em 2020, por motivos de restrições da pandemia Covid-19. Existem 13 linhas de metropolitano (metro de Lisboa, metro do Porto e metro do Sul do Tejo) e, no total, as linhas totalizadas têm uma extensão de 122 956 km⁴¹³. O metro de Lisboa teve uma receita de 114 mil euros, o do Porto de 58 mil euros e o metro do Sul do Tejo de quase 12 mil euros⁴¹⁴.

Em 2022, o transporte ferroviário de mercadorias apresentou uma redução de 3,5% na quantidade de toneladas de mercadorias transportadas face ao ano anterior. O transporte de mercadorias em meio ferroviário foi mais reduzido em contexto de tráfego nacional e superior no âmbito internacional⁴¹⁵. No total, no ano de 2022, foram transportadas cerca de 9,3 milhões de toneladas

⁴⁰⁷ Nidhi Gupta, "Analysing Transit Time Delays Along Key Global Trade Routes", *SupplyChain Digital*, Agosto de 2024, <https://supplychaindigital.com/logistics/analysing-transit-time-delays-along-key-global-trade-routes>.

⁴⁰⁸ Decreto-Lei n.º 226/2006, de 15 de novembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/226-2006-544783>.

⁴⁰⁹ Manuel Dias, "Segurança dos Transportes Marítimos e Portos – Visão Prospetiva", abril de 2022, 7 e 9, https://pianc.pt/wp-content/uploads/2022/05/6-Seguranc%CC%A7a_dos_Transportes_Mari%CC%81timos_e_Portos_Visa%CC%83o_Prospetiva_Dinis-Dias-PIANC-2022.pdf.

⁴¹⁰ AMT, "Transporte Ferroviário em Portugal – 2022", dezembro de 2023, 2, <https://observatorio.amt-autoridade.pt/storage/100/8jtMIB1Gfmvaf20hBO1DofNpYQ1DxF-metaRmVycm92aWFfMjAyMI9Ob3RhX2VzdGF0aXN0aWNhLnBkZg==-.pdf>.

⁴¹¹ INE, "Transportes e Comunicações 2022", novembro de 2023, https://www.ine.pt/xportal/xmain?xpgid=ine_inst_infografia&INST=637341691&xpid=INE.

⁴¹² PORDATA, "Estações de comboio e passagens de nível – Continente", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Estacoes_de_comboio_e_passagens_de_nivel_-_Continente.xlsx.

⁴¹³ PORDATA, "Número de linhas e extensão da rede de transporte metropolitano - Continente", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Numero_de_linhas_e_extensao_da_rede_de_transporte_metropolitano_-_Continente.xlsx.

⁴¹⁴ PORDATA, "Receitas do transporte metropolitano – Continente", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Receitas_do_transporte_metropolitano_-_Continente.xlsx.

⁴¹⁵ INE, "Estatística dos Transportes e Comunicações 2022", 6.

de mercadoria no transporte ferroviário, dos quais cerca de 6,6 milhões de toneladas é referente a tráfego nacional⁴¹⁶. Podemos dividir as mercadorias transportadas em cinco categorias⁴¹⁷:

- Produtos da agricultura, da produção animal, da caça e a silvicultura, peixe e outros produtos da pesca;
- Produtos não energéticos das indústrias extrativas, turfa, urânio e tório;
- Coque e produtos petrolíferos refinados;
- Outros produtos minerais não metálicos;
- Metais de base, produtos metálicos transformados, exceto máquinas e equipamento.

No total de mercadorias transportadas por via ferroviária, em 2022, destacam-se 808 851 toneladas de "Produtos da agricultura, produção animal, caça, silvicultura, peixe e outros produtos da pesca"; 1 099 734 toneladas de "Produtos não energéticos das indústrias extrativas, turfa, urânio e tório"; 151 042 toneladas de "Coque e produtos petrolíferos refinados"; 782 088 toneladas de "Outros produtos minerais não metálicos"; e 1 201 250 toneladas de "Metais de base, produtos metálicos transformados, exceto máquinas e equipamentos".

A Diretiva n.º 2016/798⁴¹⁸ foi criada pela UE e tem como objetivo reforçar a segurança do sistema ferroviário através da revisão do papel das autoridades nacionais de segurança. Esta diretiva estabelece uma série de medidas para garantir a promoção e o reforço da segurança, incluindo⁴¹⁹:

- Definir as responsabilidades dos organismos intervenientes no sistema ferroviário da UE;
- Criar objetivos e métodos comuns de segurança, de forma a eliminar as regras nacionais que são um obstáculo ao desenvolvimento de um espaço ferroviário europeu único;
- Estabelecer princípios relativos à emissão, renovação, alteração e limitação dos certificados e autorizações de segurança;
- Criar uma autoridade nacional de segurança e de um organismo de inquérito a acidentes e incidentes para cada Estado-Membro;
- Definir os princípios comuns de gestão, regulamentação e supervisão da segurança ferroviária.

Esta Diretiva deveria ter sido transposta até dia 16 de junho de 2020, mas a Diretiva n.º 2020/700⁴²⁰ veio prorrogar esse prazo até dia 31 de outubro de 2020, devido à pandemia do Covid-19. A 30 de março de 2021, ocorreu uma reunião informal com todos os ministros dos transportes dos países Estados-Membros da UE. O objetivo desta reunião foi fazer um balanço das iniciativas políticas e reavaliar o papel deste modo de transporte devido à necessidade urgente de descarbonização. Esta reunião teve algumas conclusões importantes, tais como⁴²¹:

- O quadro regulamentar é muito complexo e, devido a isso, é necessário colocar para esforços de forma a garantir os benefícios económicos e operacionais;

⁴¹⁶ IMT, "Anuário Estatístico da Mobilidade e dos Transportes - 2022", maio de 2024, <https://www.imt-ip.pt/sites/IMTT/Portugues/Noticias/Paginas/Anuario-Estatistico-Mob-Transp2022.aspx>.

⁴¹⁷ PORDATA, "Mercadorias transportadas no sistema ferroviário: total e por principais mercadorias - Continente (2008-)", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_transportadas_no_sistema_ferrovioario_total_e_por_principais_mercadorias_-_Continente_%282008-%29.xlsx.

⁴¹⁸ Diretiva (UE) 2016/798 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, <https://eur-lex.europa.eu/legal-content/PT/AUTO/?uri=celex:32016L0798>.

⁴¹⁹ Eur-Lex, "Segurança ferroviária à escala da União Europeia", https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:320305_1.

⁴²⁰ Diretiva (UE) 2020/700 do Parlamento Europeu e do Conselho de 25 de maio de 2020, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32020L0700>.

⁴²¹ Conselho da União Europeia, "Conclusões do Conselho sobre 'Impulsionar o transporte ferroviário para a vanguarda da mobilidade sustentável e inteligente'" maio de 2021, <https://data.consilium.europa.eu/doc/document/ST-8790-2021-INIT/pt/pdf>.

- Foi reconhecido que alguns Estados-Membros não conseguem garantir a conectividade por meio ferroviário. Como causa disto a mobilidade inteligente e sustentável só pode ser conseguida utilizando outros meios de transportes;
- Constatou-se grandes variações no desenvolvimento de serviços, infraestruturas e redes internacionais de transporte ferroviário de passageiros;
- Foi observado que a rede transeuropeia de transportes (RTE-T) tem sido muito importante no desenvolvimento de uma rede ferroviária interoperável e com elevada capacidade. Esta rede também permitiu aos Estados-Membros com menor capacidade de investimento modernizar as redes de forma lenta, mas constante.

Em 2022 registaram-se 34 acidentes ferroviários, dos quais resultaram 13 feridos graves e 12 mortos. Um dos episódios mais trágicos ocorreu no dia 11 de setembro de 1985, perto do apeadeiro de Moimenta-Alcáçache, e é considerado o pior acidente ferroviário de que há memória em Portugal, tendo um grande impacto social.

Neste acidente, o comboio internacional Sud-Express e o comboio regional 1324, com destino a Coimbra, tiveram um choque frontal. O Sud-Express, com destino a França, partiu com um atraso de 17 minutos, o qual não foi comunicado ao comboio regional. Como a linha em questão só tinha uma via, o comboio regional deveria ter aguardado pela passagem do comboio regional, mas essa informação não chegou a ser transmitida.

Esta catástrofe trouxe um aprofundamento do estudo e implementação de técnicas de prevenção e de socorro. Como consequência, todo o serviço ferroviário foi reestruturado, com a instalação de sistemas de comunicação e sinalização do tráfego mais avançados, controlo de velocidade e a introdução de sistemas de rádio no solo, que permitem que os maquinistas comuniquem entre si e com as centrais de controlo⁴²².

Transporte Rodoviário

Em 2021, o transporte rodoviário registou um aumento significativo de 30,9% no número de passageiros, totalizando mais 497 milhões. No entanto, em comparação com 2019, houve uma diminuição de 12,1% no número total de passageiros transportados por meios rodoviários. Por exemplo, o tráfego na Ponte 25 de Abril cresceu 13,8%, superando os níveis pré-pandemia. Houve um aumento no número de novas matrículas de veículos, enquanto o consumo de combustíveis e energia no transporte rodoviário aumentou em 6,1%. Em 2022, no transporte rodoviário de mercadorias, observou-se uma redução no transporte através de veículos nacionais (143,4 milhões de toneladas de mercadorias, representando -2,3% face a 2021) e um aumento no transporte de mercadorias em veículos estrangeiros (17,3 milhões de toneladas, +10,7%)⁴²³.

Em 2023, Portugal Continental contava com aproximadamente 3 mil km de autoestradas⁴²⁴, totalizando 14 339 km de estradas⁴²⁵. No ano anterior, 2022, foram exportadas 6 957 mil toneladas de cargas, sendo que Espanha foi o principal destino, recebendo 4 367 mil toneladas⁴²⁶. Quanto às importações, o volume total atingiu 7 767 mil toneladas, com a Espanha novamente em destaque,

⁴²² Luciano Lourenço, "Alcáçache: 30 anos depois", maio de 2017, 102-115, https://www.riscos.pt/wp-content/uploads/2018/SRC_V/Ebook_Alcaface_30_anos_depois.pdf.

⁴²³ INE, "Estatística dos Transportes e Comunicações 2022", novembro de 2023, 6-7.

⁴²⁴ PORDATA, "Extensão da rede de autoestradas - Continente", agosto de 2024, https://www.pordata.pt/sites/default/files/2024-08/Portugal_Extensao-da-rede-de-autoestradas.xlsx.

⁴²⁵ PORDATA, "Extensão da rede rodoviária nacional em Portugal Continental", agosto de 2024, https://www.pordata.pt/sites/default/files/2024-08/Portugal_Extensao-da-rede-rodoviaria-nacional.xlsx.

⁴²⁶ PORDATA, "Mercadorias carregadas pelas empresas de transporte rodoviário: total e por principais países de destino - Continente", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_carregadas_pelas_empresas_de_transporte_rodoviario_total_e_por_principais_paises_de_destino_-_Continente.xlsx.

enviando 5 488 mil toneladas⁴²⁷. Em 2022, o número de veículos matriculados era de cerca de 363 201, dos quais quase 296 mil são automóveis ligeiros, 4 930 são automóveis pesados, 42 455 motociclos e 12 514 tratores⁴²⁸.

Em 2023, registaram-se 34 974 acidentes de viação em Portugal, resultando em 43 495 feridos e 467 mortos⁴²⁹. No mesmo ano, ocorreram 4 873 atropelamentos de peões, dos quais 57 resultaram em mortos⁴³⁰. Um dos acidentes de viação mais aparatosos da história rodoviária em Portugal aconteceu no ano 2000, ao quilómetro 75 da A1, no sentido Norte-Sul. Este acidente resultou em dez quilómetros de sucata, 170 viaturas envolvidas, 72 feridos e quatro mortos⁴³¹.

Os acidentes de viação geram anualmente elevados custos económicos, sociais e humanos, sendo crucial quantificá-los para informar políticas de segurança rodoviária em Portugal⁴³². O custo económico e social dos acidentes rodoviários pode ser dividido em dois componentes:

- **Danos patrimoniais:** Inclui prejuízos nos bens dos envolvidos e terceiros, como custos de reparação de veículos e infraestruturas, despesas médicas e assistência aos sinistrados;
- **Dados morais ou não patrimoniais:** Abrange o valor das vidas afetadas por acidentes de viação, dor física, impacto emocional, perda de qualidade de vida, danos à aparência e as consequências na afirmação pessoal e social das vítimas⁴³³.

2.1.2. Especificidades tecnológicas

Os transportes de todos os setores estão equipados com tecnologia que auxilia a navegação de quem os opera e que transmite informação a diversos sistemas, permitindo saber onde estão em cada momento. A implementação destas tecnologias nos meios de transporte permite aos operadores do setor recolher informação em tempo real, saber onde os seus meios de transporte se encontram durante os períodos de trabalho, se houve avarias ou acidentes, se há vias congestionadas e se há vias alternativas, e fazer a gestão das frotas. Estas tecnologias contribuem para tráfegos mais fluídos e mais seguros em todos os setores, bem como viagens mais ecológicas, ao evitar-se a permanência prolongada dos meios de transporte nas vias utilizadas devido a congestionamentos⁴³⁴.

A crescente integração de tecnologia digital e conectividade nos transportes, apesar de proporcionar mais segurança e conforto na maioria dos casos, acarreta também riscos. Devido às múltiplas camadas de segurança de que se revestem sobretudo os meios de transporte aéreos ou marítimos, ciberataques que permitam ganhar o controlo total de um meio de transporte do género são, apesar de possíveis, improváveis. No entanto, obter o controlo de um sistema em

⁴²⁷ PORDATA, “Mercadorias descarregadas pelas empresas de transporte rodoviário: total e por principais países de origem - Continente”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_descarregadas_pelas_empresas_de_transporte_rodoviario_total_e_por_principais_paises_de_origem_-_Continente.xlsx.

⁴²⁸ PORDATA, “Veículos matriculados: total e por tipo de veículo”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Veiculos_matriculados_total_e_por_tipo_de_veiculo.xlsx.

⁴²⁹ PORDATA, “Acidentes de viação com vítimas: total e por tipo de acidente - Continente”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Acidentes_de_viacao_com_vitimas_total_e_por_tipo_de_acidente_-_Continente.xlsx.

⁴³⁰ PORDATA, “Peões atropelados: total e mortos - Continente”, maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Peoes_atropelados_total_e_mortos_-_Continente.xlsx.

⁴³¹ Ricardo Felner, “Maior choque de sempre”, *Público*, fevereiro de 2000, <https://www.publico.pt/2000/02/22/jornal/maior-choque-de-sempre-140333>.

⁴³² ANSR, “O Impacto Económico e Social da Sinistralidade Rodoviária em Portugal”, outubro de 2021, 4, http://www.ansr.pt/Documents/Impacto_Economico_Social_Sinistralidade_Rodoviaria.pdf.

⁴³³ ANSR, “O Impacto Económico e Social da Sinistralidade Rodoviária em Portugal”, outubro de 2021, 18.

⁴³⁴ “Sistemas de Transporte Inteligentes”, Infracontrol, <https://www.infracontrol.com/pt-pt/sistemas-de-transporte-inteligentes-its/>.

concreto, bloquear o acesso a determinadas funcionalidades ou inserir no sistema de navegação dados falsos são cenários mais plausíveis e até mesmo já concretizados em mais do que uma ocasião. Explorar-se-ão alguns desses cenários em

2.2. Ameaças.

Transporte Aéreo

A European Union Aviation Safety Agency (EASA) iniciou um programa de aviação sustentável que tem as seguintes prioridades:

- Promover novas tecnologias mais ecológicas;
- Facilitar a descarbonização do transporte aéreo;
- Promover ganhos de eficiência nos domínios da formação, manutenção e gestão do tráfego aéreo.

Apesar das significativas dificuldades na implementação de fontes de energia sustentáveis neste setor, em junho de 2019, a EASA e a CAA Noruega firmaram um acordo para acelerar os esforços de eletrificação da aviação⁴³⁵.

As aeronaves e os veículos do aeroportuários transmitem a sua posição e identidade através do *ADS-B (Automatic dependent surveillance – broadcast)*. Este sinal pode ser utilizado para fins de vigilância em terra ou a bordo de outras aeronaves, aprimorando a consciência situacional do tráfego aéreo. O *ADS-B* opera de forma automática, sem necessidade de estímulos externos, embora dependa dos sistemas a bordo para fornecer informações de vigilância a outras entidades⁴³⁶.

Utilizando a tecnologia *ADS-B*, o *website Flightradar24* mostra, em tempo real, todo o tráfego aéreo global. Para que uma aeronave apareça neste *tracker*, é necessário que o *transponder* esteja ligado; o mesmo irá enviar o sinal da localização da aeronave, que será recebido por um recetor conectado à rede do *website*. O *Flightradar24* conta com uma rede com mais de 40 mil recetores *ADS-B* distribuídos ao redor do mundo⁴³⁷.

Devido ao aumento significativo do número de voos e de passageiros, os aeroportos estão a adotar novas tecnologias para enfrentar os desafios operacionais e melhorar a experiência dos passageiros. Um exemplo é a tecnologia *Beacon*, criada pela *Apple* em 2013. Esta tecnologia utiliza *Bluetooth* de baixo consumo (*BLE*) para transmitir, de forma unidirecional, um sinal de curto alcance que pode ser detetado por aplicações móveis nas proximidades, acionando ações específicas, como o envio de mensagens ou cupões em lojas próximas. Os *beacons* não se conectam aos dispositivos ao seu redor e, portanto, não recolhem dados. Esta tecnologia está a começar a ser implementada nos aeroportos, ajudando os passageiros ao enviar informações sobre produtos, descontos, preços e até especificações enquanto se deslocam pelo aeroporto. Também podem auxiliar na orientação, guiando assim os passageiros até à porta do embarque e informando o horário de embarque, o que contribui para uma experiência mais satisfatória⁴³⁸.

⁴³⁵ EASA, “Aviação sustentável: rumo a uma aviação com emissões zero”, <https://www.easa.europa.eu/pt/light/topics/sustainable-aviation-towards-zero-emission-aviation>.

⁴³⁶ EuroControl, “Automatic dependent surveillance – broadcast”, <https://www.eurocontrol.int/service/automatic-dependent-surveillance-broadcast>.

⁴³⁷ Flightradar24, “How flight tracking works”, <https://www.flightradar24.com/how-it-works>.

⁴³⁸ Airport Technology, “New Technologies for Smarter Airports: Beacon Technology”, <https://www.airport-technology.com/contractors/data/pressreleases/smarter-airports-beacon-technology>.

A IA está a ter um papel cada vez mais proeminente no subsetor do transporte aéreo. Esta tecnologia tem como objetivo otimizar processos e apoiar os profissionais da aviação, ajudando na tarefa da descarbonização. A IA possui uma notável capacidade de processar grandes volumes de dados e de aprender com os mesmos, permitindo a deteção de padrões, o desenvolvimento de previsões e a antecipação de riscos. Isto pode ter um impacto em diversas áreas deste subsetor:

- **Operações de voo:** A IA pode ajudar a aconselhar a tripulação em algumas tarefas, melhorando a eficiência do voo. Também é capaz de prever alguns problemas como turbulências e condições meteorológicas;
- **Manutenção:** A manutenção preventiva baseada em IA pode otimizar os cronogramas da manutenção, prever a restante vida útil das peças e, assim, prevenir possíveis falhas;
- **Ambiente:** Com a otimização das trajetórias de voo, é possível reduzir as emissões de carbono nas operações aéreas, e a IA pode desempenhar um papel fundamental neste processo. Além disso, a tecnologia pode ajudar a minimizar o ruído nas proximidades dos aeroportos e apoiar a EASA na análise de dados sobre os impactos ambientais deste subsetor;
- **Gestão de tráfego:** A IA ao otimizar rotas de voo, consegue reduzir o consumo de combustível e o tempo de voo, reduzindo assim a gestão do tráfego aéreo e os possíveis atrasos;
- **Aeroportos:** A IA pode ser utilizada na triagem de segurança, na deteção de mercadorias perigosas e proibidas ou até na vigilância, contribuindo para um aumento significativo da segurança nos aeroportos;
- **Cibersegurança:** Com a IA, podem ser criados sistemas mais eficazes para prevenir incidentes de cibersegurança, permitindo a deteção automática e correção de vulnerabilidades, assim como a identificação de ameaças com base no comportamento⁴³⁹.

Em 2020, a EASA publicou um *roadmap* sobre a IA, apresentando a sua visão inicial tanto em termos de segurança, como em ética. Uma nova versão foi lançada em 2023 e destaca alguns desafios na implementação desta tecnologia neste subsetor⁴⁴⁰.

⁴³⁹ EASA, “Artificial Intelligence and Aviation”, <https://www.easa.europa.eu/en/light/topics/artificial-intelligence-and-aviation-0>.

⁴⁴⁰ EASA, “EASA Artificial Intelligence Roadmap 2.0”, maio de 2023, <https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20>.

Transporte Marítimo e por vias navegáveis interiores

O Transporte Marítimo, assim como outros setores, tem vindo a modernizar-se com a introdução de novas tecnologias. Um exemplo notável desta transformação é a aplicação *MarineTraffic*⁴⁴¹, cuja missão principal é fornecer, quase em tempo real, as localizações dos navios e iates, utilizando uma rede de recetores *Automatic Identification System*⁴⁴² (AIS). Além disso, numa entrevista ao Jornal de Negócios em 2023, uma das empresas operadores no transporte marítimo, a Ocean Network Express (ONE) Portugal, destacou que a transição digital tem sido uma aposta crescente da empresa desde a pandemia de COVID-19 e respetivos períodos de confinamento. Desde então, a empresa tem investido na implementação de serviços *cloud* e *software* CRM, visando aprimorar a forma como acompanha e gere as interações com os seus clientes⁴⁴³.

Existe um sistema de monitorização do tráfego marítimo, semelhante ao controlo de tráfego aéreo, denominado *Vessel Traffic Service* (VTS). Este sistema utiliza tecnologias como o radar, radio telefonia VHF e o já mencionado AIS. Em Portugal, a gestão do VTS costeiro é da responsabilidade da DGRM, atuando como Autoridade Nacional de Controlo de Tráfego Marítimo (ANCTM), conforme estabelecido no Decreto-Lei n.º 49-A/2012⁴⁴⁴, publicado a 29 de fevereiro de 2012.

O VTS opera a partir dos Centros de Controlo de Tráfego Marítimo (CCTM), que estão estrategicamente situados em duas áreas distintas do continente. Além disso, o programa Compete 2020 desenvolveu um projeto inovador denominado MareCom, com o objetivo de garantir alta disponibilidade a um baixo custo, beneficiando assim as comunidades que operam no ambiente marítimo. Este projeto implementou uma nova arquitetura de comunicações MIMO, além de antenas multi-banda, e desenvolveu um protocolo de acesso adaptado ao meio, garantindo assim a fiabilidade e a disponibilidade necessárias para um tráfego marítimo seguro e eficiente⁴⁴⁵.

Os navios, sejam de carga ou de cruzeiro, estão a passar por um período de evolução. Um exemplo pioneiro é o Pyxis Ocean, que em agosto de 2023 se tornou o primeiro navio a completar uma viagem de quase 25 mil quilómetros, combinando o uso de combustível fóssil com a energia eólica. Este navio é equipado com velas dobráveis de aço e fibra de vidro, denominadas por *WindWings*, que com 37,5 metros de altura, conseguem capturar a força do vento e impulsionar a embarcação de forma eficiente. Outro tipo de energia que está a ser explorada é a energia das ondas. Inspirado nos movimentos das baleias e dos golfinhos na água, uma asa artificial foi fixada na parte frontal de um navio com 10 metros de comprimento. Estas asas absorvem a energia das ondas e empurram o navio para a frente. Estas tecnologias visam a descarbonização do setor marítimo, com o ambicioso objetivo de reduzir a sua pegada atual em 50% até 2050⁴⁴⁶.

⁴⁴¹ MarineTraffic, <https://www.marinetraffic.com/>.

⁴⁴² É um Sistema de rastreio automático e autónomo amplamente utilizado no mundo marítimo para a troca de informações de navegação entre terminais equipados com AIS (Fonte: Vasilis Kontas, "What is the Automatic Identification System (AIS)?", MarineTraffic, <https://support.marinetraffic.com/en/articles/9552859-what-is-the-automatic-identification-system-ais>).

⁴⁴³ "Setor do transporte marítimo é barómetro da economia mundial", *Jornal de Negócios*, 29 de março de 2023, <https://www.jornaldenegocios.pt/negocios-em-rede/detalhe/setor-do-transporte-maritimo-e-barometro-da-economia-mundial>.

⁴⁴⁴ Decreto-Lei n.º 49-A/2012, de 29 de fevereiro, *Diário da República*, <https://dre.pt/application/file/a/551481>.

⁴⁴⁵ DGRM, "Sistema VTS", <https://www.dgrm.pt/sistema-vts>.

⁴⁴⁶ Tom Cassauwers, "Winds of change – the new tech steering commercial shipping towards a more sustainable future", *Horizon*, <https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine/winds-change-new-tech-steering-commercial-shipping-towards-more-sustainable-future>.

Os portos marítimos também estão em mudança e inovação. Na esfera logística, surgem soluções que pretendem automatizar diversas tarefas que, anteriormente, eram realizadas de forma manual. Um exemplo é o *Warehouse Management System (WMS)*, que integra e centraliza os processos de gestão e operação do funcionamento de um porto marítimo, como a gestão do pátio, armazém, entre outras. Ao eliminar tarefas repetitivas, que são propensas a falhas e à redução da produtividade, estes sistemas aumentam a eficiência e a fiabilidade das operações portuárias. Outra tecnologia que está a começar a ser utilizada nos portos é a Internet das Coisas (IoT). Estes dispositivos inteligentes são capazes de medir, monitorizar e processar dados sem necessidade de intervenção humana, passando a ser possível rastrear cargas e acompanhar toda a movimentação do porto em tempo real⁴⁴⁷.

A Inteligência Artificial (IA) e o *Machine Learning (ML)* são ferramentas fundamentais na gestão do vasto volume de dados gerados nos portos marítimos. Com a implementação destas tecnologias, passa a ser possível desenvolver algoritmos que processem estes dados, gerando relatórios cruciais para as tomadas de decisão. O ML adquire, com o tempo, a capacidade de compreender as ações necessárias para bom funcionamento dos portos e, com isso, promovendo uma otimização dos processos e uma reorganização do espaço portuário⁴⁴⁸.

Atualmente, os portos marítimos, estão a incorporar a realidade aumentada no treino de profissionais, especialmente quando envolvem situações riscos para pessoas ou património. Este risco está particularmente evidente nas operações de logística, mais concretamente nas movimentações portuárias. Além disso, a utilização de *drones* nos portos marítimos tornou-se uma realidade consolidada graças ao avanço da tecnologia e à crescente autonomia destes dispositivos. O seu uso é importante para o controlo do tráfego dos navios, para a gestão da posição das cargas e equipamentos, e para monitorizar a eficiência dos embarques e desembarques. Com estas inovações, os portos não só aumentam a segurança, mas também melhoram a eficiência nas suas operações, tornando-se mais ágeis e eficazes⁴⁴⁹.

A introdução do piloto automático representa uma inovação que impacta diretamente a atuação dos pilotos marítimos. Atualmente, já existem ferramentas avançadas que possibilitam que os navios sigam rotas pré-definidas de forma totalmente autónoma. Estas ferramentas não apenas garantem a manutenção da direção da embarcação, mas também permitem a programação para a execução de manobras complexas como ziguezagues, círculos temporizados, inversão de marcha, entre muitas outras. Com estas capacidades o setor marítimo aumenta a segurança nas operações em alto-mar, assim como uma maior precisão e eficiência na navegação⁴⁵⁰.

⁴⁴⁷ Luca Braidotti et al., "On the Automation of Ports and Logistics Chains in the Adriatic Region", setembro de 2020, 99, https://link.springer.com/chapter/10.1007/978-3-030-58820-5_8.

⁴⁴⁸ Luca Braidotti et al., "On the Automation of Ports and Logistics Chains in the Adriatic Region", setembro de 2020, 104-105.

⁴⁴⁹ Luca Braidotti et al., "On the Automation of Ports and Logistics Chains in the Adriatic Region", setembro de 2020, 99.

⁴⁵⁰ Garmin, "Funcionalidades úteis que distinguem os pilotos automáticos garmin", <https://www.garmin.com/pt-PT/garmin-technology/marine-technology/autopilot/advanced-autopilot-features/>.

Transporte Ferroviário

O subsetor do transporte ferroviário tem procurado modernizar-se e ser mais competitivo e sustentável de modo a estabelecer-se como um meio de transporte preferencial. A própria União Europeia tem adotado algumas medidas nesse sentido. Uma delas foi a publicação da Diretiva n.º 2016/797⁴⁵¹, que define a Interoperabilidade Ferroviária Europeia, promovendo o tráfego ferroviário entre os países da UE, ao eliminar barreiras tecnológicas e padronizando o modo de operação da rede. Esta Diretiva deu origem ao *standard European Rail Traffic Management (ERTMS)* e este *standard* proporciona uma sinalização sem barreiras, podendo assim os comboios atravessar diversos países sem enfrentar atrasos e problemas relacionados com a sinalização, garantindo um sistema ferroviário europeu seguro e interoperável. O *standard ERTMS* é composto por dois subsistemas:

- **European Train Control System (ETCS)**: é um sistema de proteção automática dos comboios, com o propósito de substituir os sistemas *ATP* existentes nos comboios nacionais;
- **GSM-R**: é um sistema de rádio para voz e aplicações ferroviárias⁴⁵².

O *ETCS* é comumente conhecido como *Automatic Train Protection (ATP)* e tem como objetivo supervisionar os comboios em relação à autorização de movimento, velocidade e regras de sinalização. Caso estas regras não sejam respeitadas, este sistema é capaz de acionar automaticamente os freios do comboio. O *ETCS* tem 3 níveis e cada rede ferroviária pode optar por um ou por uma combinação destes níveis⁴⁵³:

- **Nível 1**: Este nível funciona em conjunto com a sinalização convencional transmitindo a autorização do movimento através de balizas. Estas informações são mostradas no ecrã do comboio ao condutor, incluindo o itinerário e a velocidade máxima. Este sistema monitoriza a velocidade e calcula as curvas de friagem, garantindo assim uma paragem segura antes da próxima estação, caso o condutor não intervenha;
- **Nível 2**: Neste nível, a autorização do movimento é comunicada ao sistema embarcado via rádio *GSM-R* pelo *Radio Block Center (RBC)*, que se conecta aos sistemas de sinalização convencionais. As balizas, neste nível, deixam de enviar autorizações, passando apenas a transmitir dados fixos como a localização e os limites de velocidade. Os sinais luminosos paralelos à via passam a ser opcionais neste nível;
- **Nível 3**: Este nível ainda se encontra em desenvolvimento e a principal diferente este e o nível anterior é a dispensa de um sistema de deteção de comboios na sinalização convencional, sendo ainda necessário um sistema que verifique a integridade do comboio. O bloco fixo também é substituído por um bloco móvel que é dinâmico e adapta-se ao comprimento do comboio e à sua velocidade⁴⁵⁴.

⁴⁵¹ Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3AQJ.L.2016.138.01.0044.01.POR>.

⁴⁵² European Union Agency for Railways, "European Rail Traffic Management System (ERTMS)", https://www.era.europa.eu/domains/infrastructure/european-rail-traffic-management-system-ertms_en.

⁴⁵³ European Commission, "ETCS Levels and Modes", https://transport.ec.europa.eu/transport-modes/rail/ertms/what-ertms-and-how-does-it-work/etcs-levels-and-modes_en.

⁴⁵⁴ European Union Agency for Railways, "TSI Revision Package 2023: Key Changes Part I – Rolling stock and CCS", junho de 2023, 39 e 41, <https://www.era.europa.eu/system/files/2023-06/15%2006%2023%20Webinar%20Slides.pdf>.

Em 2021, foi instalado na Estação Ferroviária de Elvas o Piloto do nível 2 da ETCS. A instalação deste Piloto permitirá a consolidação e verificação da conformidade deste novo sistema aos parâmetros da RFN. O novo canal ferroviário em construção entre Évora e a Linha do Leste foi criado com o objetivo de aprimorar das ligações ferroviárias portuguesas a Espanha, em conformidade com o RTE-T, garantindo assim a ligação ferroviária de mercadorias entre os portos portugueses e a UE⁴⁵⁵.

Existe um sistema de assistência ao condutor, conhecido como *Connected Driver Advisor System* (C-DAS) que oferece recomendações sobre as melhores opções em relação à velocidade e aceleração dos comboios. Este sistema utiliza algoritmos avançados para calcular estas decisões em tempo real e está conectado ao Centro de Comando Operacional, permitindo obter, instantaneamente, informações sobre o estado dos itinerários e do tráfego ferroviário. Com a implementação destes novos sistemas, é essencial normalizar as interfaces entre os Centros de Controlo de Tráfego, utilizando a *Big Data* e a IA nas decisões a tomar, sendo estas informações depois partilhadas com as estações e os comboios em tempo real. Devido ao alto volume de trocas de informação, o GSM-R terá de ser descontinuado e outra solução deverá ser adaptada⁴⁵⁶. Esta nova solução, o *Future Radio Mobile Communication System* (FRMCS), está previsto ficar totalmente implementado até 2030 e tem como principais objetivos permitir e ajudar a digitalização da ferrovia, substituir o GSM-R e permitir a utilização do 5G, LTE, entre outros⁴⁵⁷.

Outro sistema importante no transporte ferroviário é o *Advanced Train Positioning System* (ATPS), que permite a deteção segura dos comboios por meio de tecnologia instalada nos carris. Esta tecnologia pretende que os cantões de bloco fixo ou os virtuais passem a ser calculados por algoritmos, passando assim a ser possível obter a maior capacidade possível da infraestrutura. A implementação desta tecnologia representa um grande avanço em direção à autonomia dos comboios⁴⁵⁸.

Em direção à descarbonização do setor ferroviário, foi criado o projeto europeu FCH2RAIL que resultou no desenvolvimento de um comboio bimodal equipado com pilhas de combustível a hidrogénio. Este comboio foi testado com sucesso entre os dias 3 e 6 de abril de 2024 em Portugal e recebeu autorização para circular noutros países europeus. Após os testes realizados em Portugal, o comboio de demonstração já percorreu mais de 8500km utilizando hidrogénio como combustível⁴⁵⁹.

O Metropolitano de Lisboa está a implementar uma atualização no sistema de sinalização ferroviária, que estará completamente funcional em 2025. O novo sistema, denominado Communication-Based Train Control (CBTC) promete aumentar a fiabilidade e a eficiência do transporte. Além disso, permitirá um controlo contínuo do movimento dos comboios, aumentando a sua frequência, melhorando a acessibilidade para clientes com mobilidade reduzida e proporcionando uma maior velocidade de circulação⁴⁶⁰.

⁴⁵⁵ Ferrovia Geral Inovação Investimentos, "Apresentação da instalação de Piloto ETCS L2", Infraestruturas de Portugal, novembro de 2021, <http://www.infraestruturasdeportugal.pt/pt-pt/apresentacao-da-instalacao-de-piloto-etcs-l2>.

⁴⁵⁶ Siemens, "Connected Driver Advisory System (C-DAS)", <https://www.mobility.siemens.com/uk/en/portfolio/rail-infrastructure/connected-driver-advisory-system.html>.

⁴⁵⁷ UIC, "FRMCS: Future Railway Mobile Communication System", setembro de 2023, <https://uic.org/rail-system/telecoms-signalling/frmcs>.

⁴⁵⁸ Ikuo Watanabe e Tetsuo Takashige, "Advanced ATP System for Improving Train Traffic Density and Control Efficiency", 1991, 1, <https://onlinepubs.trb.org/Onlinepubs/trr/1991/1314/1314-023.pdf>.

⁴⁵⁹ Ferrovia Inovação, "Primeiro comboio a Hidrogénio realiza testes na rede ferroviária portuguesa", Infraestruturas de Portugal, abril de 2024, <https://www.infraestruturasdeportugal.pt/pt-pt/primeiro-comboio-hidrogenio-realiza-testes-na-rede-ferroviaria-portuguesa>.

⁴⁶⁰ Metropolitano de Lisboa, "Novo sistema de sinalização do Metropolitano de Lisboa entra em fase final de testes", maio de 2024, <https://www.metrolisboa.pt/institucional/2024/05/10/novo-sistema-de-sinalizacao-do-metropolitano-de-lisboa-entra-em-fase-final-de-testes/>.

Transporte Rodoviário

O aumento do número de automóveis e transportes urbanos nas grandes cidades tem causado congestionamentos e um maior risco de acidentes. Para enfrentar estes desafios, foram desenvolvidos sistemas de controlo de tráfego com o objetivo de melhorar a fluidez, reduzir as emissões e melhorar o desempenho do transporte público. Atualmente, a cidade de Lisboa possui um sistema de gestão e controlo de tráfego denominado de SIM.Lx. Os principais objetivos deste sistema são aprimorar a fluidez do tráfego, melhorar o desempenho dos transportes coletivos e controlar a poluição atmosférica. Este sistema utiliza IA para prever situações de congestionamento e prioriza veículos de emergência⁴⁶¹.

Os veículos totalmente autónomos estão a aproximar-se rapidamente da realidade e trarão implicações significativas em diversas áreas. Estes veículos apresentam vários níveis de automatização, que vão de 0 a 6, onde 0 representa a ausência de automatização e 5 automatização total⁴⁶². A automatização dos veículos pode aumentar a eficiência do tráfego, assim como reduzir as emissões poluentes e o consumo de energia. Espera-se que a adoção de veículos elétricos cresça juntamente com a dos veículos autónomos, apesar da atual escassez de postos de carregamento e da limitada autonomia em comparação com os combustíveis fósseis. Fatores como incentivos públicos, menores custos de manutenção e as restrições de acesso a veículos de combustão são fatores que podem impulsionar o aumento de veículos elétricos⁴⁶³.

O sistema ADAS (Sistemas Avançados de Assistência ao Condutor) utiliza câmaras, sensores e radares para monitorizar o ambiente em redor do carro, ajudando a evitar acidentes através de sistemas como o ABS, ESP, controlo adaptativo de velocidade e travagem automática. Estes sistemas auxiliam o condutor a manter a trajetória, ajustar a velocidade e evitar colisões⁴⁶⁴.

A IoT (*Internet of Things*) possibilita transformar o subsetor do transporte num sistema mais conectado, sustentável e eficiente na gestão de tráfego. Estão a começar a ser construídas estradas mais inteligentes, capazes de se adaptar às necessidades de um transporte mais sustentável. Graças às tecnologias integradas, é possível analisar dados quase em tempo real, o que contribui para a melhoria do fluxo dos veículos. Com estas informações, torna-se viável utilizar a IA para processar os dados e enviá-los aos sistemas de gestão e controlo de tráfego⁴⁶⁵.

⁴⁶¹ LPP, "Semáforos em Lisboa começam a ser ligados ao novo sistema inteligente", Lisboa para pessoas, novembro de 2021, <https://lisboaparapessoas.pt/2021/11/02/semaforos-lisboa-sistema-inteligente/>.

⁴⁶² Jun Wang et al., "Safety of Autonomous Vehicles", Journal of Advanced Transportation, outubro de 2020, <https://onlinelibrary.wiley.com/doi/full/10.1155/2020/8867757>.

⁴⁶³ Margarita Martínez-Díaz e Francesc Soriguera, "Autonomous Vehicles: theoretical and practical challenges", Transportation Research Procedia, 2018, <https://www.sciencedirect.com/science/article/pii/S2352146518302606>.

⁴⁶⁴ Dr. Bassim Abdulbaqi Jumaa et al., "Advanced Driver Assistance System (ADAS): A Review of Systems and Technologies", junho 2019, 1, https://www.academia.edu/42907359/Advanced_Driver_Assistance_System_ADAS_A_Review_of_Systems_and_Technologies.

⁴⁶⁵ Intel, "Estradas Inteligentes Começam com Infraestrutura Inteligente", <https://www.intel.com.br/content/www/br/pt/transportation/smart-road-infrastructure.html>.

Os sistemas *ITS* (*Intelligent Transport Systems*) são aplicações avançadas com o objetivo de proporcionar serviços inovadores relacionados com vários modos de transporte, tornando a rede de transportes mais segura, mais coordenada e mais inteligente⁴⁶⁶. Estes sistemas incluem todos os tipos de comunicações em veículos, como a tecnologia *V2X* (*Vehicle-to-Everything*). A tecnologia *V2X* permite a comunicação entre veículos e o ambiente em redor, utilizando a tecnologia de *IoT* para conectar veículos a infraestruturas, peões, sistemas de gestão de trânsito e até mesmo outros veículos. Esta inovação melhora a segurança e a eficiência do tráfego, previne acidentes e otimiza rotas. Esta tecnologia tem várias subcategorias, como *V2V* (veículo a veículo) e *V2I* (veículo a infraestrutura). A evolução do 5G será crucial para expandir o potencial desta tecnologia, permitindo aos veículos comunicar entre si sem intermediários. Com estas tecnologias torna-se possível geolocalizar veículos em tempo real e gerir eficazmente a frota de uma empresa, permitindo às empresas otimizar as rotas e melhorar a eficiência operacional⁴⁶⁷.

Como mencionado anteriormente, a congestão do tráfego é um problema comum em grandes cidades. Esta situação resulta não apenas na perda de tempo e combustível, mas também contribui para o aumento da poluição. Para mitigar estes efeitos, estão a ser implementados sistemas de estacionamento inteligentes. Uma gestão eficiente do estacionamento pode reduzir significativamente a congestão e os atrasos. Investigadores dos EUA analisaram o tempo médio que os condutores passam à procura de um lugar para estacionar e descobriram que esse tempo varia entre 3 e 14 minutos, sendo que cerca de 30% do volume total de tráfego corresponde a condutores à procura de um lugar de estacionamento.

Este problema pode ser abordado de duas maneiras: aumentando o preço dos parques de estacionamento ou indicando aos condutores onde estão os lugares disponíveis. Os estacionamentos inteligentes enquadram-se nesta última abordagem. Com a utilização de sensores em cada lugar de estacionamento, é possível informar, em tempo real, os condutores sobre a disponibilidade de lugares⁴⁶⁸.

⁴⁶⁶ European Commission, "Smart Mobility", https://transport.ec.europa.eu/transport-themes/smart-mobility_en.

⁴⁶⁷ Haibo Zhou et al., "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities", Janeiro de 2020, 1-2, <https://ieeexplore.ieee.org/abstract/document/8967260>.

⁴⁶⁸ Mohammed Rezwanul Islam et al., "Smart Parking Management System to Reduce Congestion In Urban Area", novembro de 2020, 1-3, <https://ieeexplore.ieee.org/abstract/document/9309546>.

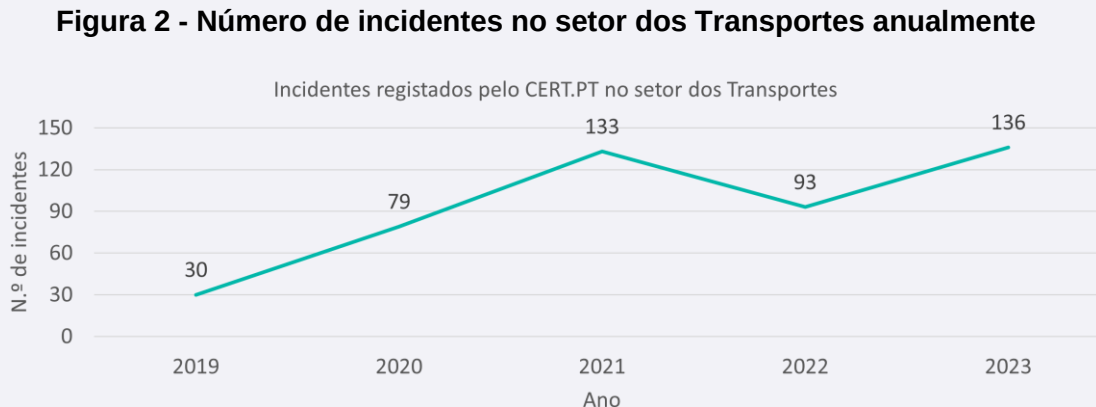
2.2. Ameaças

Quando se analisa as ameaças a que o **setor dos transportes** se encontra exposto, as consequências podem ir muito além de perdas financeiras ou materiais, podendo interferir na segurança humana. Esta é uma das principais razões que deve servir de base para que seja dada a devida importância e atenção à análise de ameaças, vulnerabilidades e implementação de medidas que as possam mitigar, neste setor.

Não obstante, ataques que procurem atingir diretamente os transportes, são, apesar de menos prováveis, possíveis. Tal como referido em **2.1.2. Especificidades tecnológicas**, obter o controlo total de um meio transporte, embora possível, é improvável devido à complexidade que tal ataque exigiria, mas obter o controlo ou mesmo bloquear o controlo sobre sistema específico que comprometa a segurança ou a operacionalidade de um meio de transporte é já mais plausível.

Embora o contexto de ciberameaças esteja em constante evolução e seja consequente do crescimento da tecnologia nos transportes, é possível identificar alguns cenários de ciberameaças nos diferentes setores. Qualquer vulnerabilidade a que os transportes possam estar sujeitos, podem causar acidentes, afetar serviços e pôr em causa fatores como a segurança, reputação, proteção ou atividade. Qualquer ator de ameaça como infiltrados, cibercriminosos, Estados-nação, grupos paraestatais ou *hacktivistas* podem explorar as vulnerabilidades do setor.

Segundo dados do CERT.PT, registaram-se em Portugal, entre 2019 e 2023, 471 ataques, no setor dos transportes⁴⁶⁹.



(Fonte: CNCS, “Incidentes e Setores: 2019-2023”, Conhecimento Situacional: Estatísticas, Obtido a 10 de outubro de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

⁴⁶⁹ CNCS, “Incidentes e Setores”, Conhecimento Situacional: Estatísticas, obtido a 10 de outubro de 2024, <https://www.cncs.gov.pt/pt/estatistica/#cert.pt>.

A cadeia de abastecimento, devido à sua complexidade, pode ser um foco de ameaças críticas à cibersegurança no setor dos transportes, afetando os subsectores do transporte aéreo, marítimo, ferroviário e rodoviário. Cada um destes subsectores enfrenta desafios específicos devido à complexidade das operações e à diversidade de atores e tecnologias envolvidas. No caso do transporte aéreo, a cadeia de abastecimento é extremamente complexa, o que gera múltiplos pontos vulneráveis que podem ser explorados por agentes maliciosos, tanto internos como externos. A cibersegurança deste subsector é essencial, pois um incidente pode comprometer toda a cadeia, afetando desde os dados utilizados no desenvolvimento das infraestruturas até aos componentes eletrónicos das aeronaves⁴⁷⁰.

Relativamente ao subsector do transporte marítimo, a cadeia de abastecimento abrange o transporte de mercadorias por mar e envolve operações portuárias e de transporte interno, conectando diferentes portos em diversos países e continentes. Esta interligação inclui uma vasta rede de intervenientes, como embarcadores, transportadoras e autoridades aduaneiras. Este subsector enfrenta alguns riscos como greves, desastres naturais e falhas nos equipamentos, onde qualquer interrupção no transporte marítimo pode ter consequências catastróficas, considerando que mais de 80% do comércio global é realizado por via marítima. Assim, a cibersegurança é essencial, especialmente no que se refere à monitorização dos fornecedores de equipamentos fundamentais para os sistemas náuticos, uma vez que uma vulnerabilidade num destes fornecedores pode comprometer a segurança dos sistemas marítimos⁴⁷¹.

Nos subsectores do transporte ferroviário e rodoviário, a cadeia de abastecimento também é uma preocupação crescente devido à forte interligação entre os sistemas e à dependência da tecnologia nas operações diárias. Nestes subsectores, os fornecedores e parceiros têm um papel crucial, pois uma falha de segurança pode afetar as operações e comprometer a integridade e eficiência dos sistemas.

⁴⁷⁰ Civil Aviation Cybersecurity Subcommittee, "Civil Aviation Supply Chain Cybersecurity Recommendations Report", Aerospace Industries Association, outubro de 2023, 1, <https://www.aia-aerospace.org/wp-content/uploads/Supply-Chain-Cybersecurity-Recommendations-Report.pdf>.

⁴⁷¹ Meixuan Li et al., "Maritime Cybersecurity: A Comprehensive Review", *Journal of the ACM*, vol. 1, n.º 1 (janeiro de 2024): 6-7, <https://arxiv.org/pdf/2409.11417v1>.

De forma geral, os componentes da cadeia de abastecimento do setor dos transportes mais suscetíveis de serem impactados são:

- **Hardware e peças estruturais:** Podem ocorrer ataques de cibersegurança com o intuito de comprometer os equipamentos utilizados na fabricação ou na projeção dos componentes. Outro risco é a contrafação, que pode resultar na inserção de componentes falsificados na cadeia de abastecimento⁴⁷²;
- **Processos de fabricação:** Podem ocorrer ataques de *ransomware* com o objetivo de interromper os processos de fabricação. Além disso, há a possibilidade de espionagem industrial ou até mesmo o furto de propriedade intelectual⁴⁷³;
- **Software:** O *software* pode ser modificado de maneira a comprometer a segurança dos sistemas do transporte aéreo, gerando vulnerabilidades na cadeia de abastecimento;
- **Componentes eletrónicos complexos (CEH):** Estes componentes, com um *design* externo, podem introduzir vulnerabilidades indesejadas no *hardware* se forem projetados de forma inadequada⁴⁷⁴.

⁴⁷² Civil Aviation Cybersecurity Subcommittee, "Civil Aviation Supply Chain", 6-7.

⁴⁷³ Civil Aviation Cybersecurity Subcommittee, "Civil Aviation Supply Chain", 13-14.

⁴⁷⁴ Civil Aviation Cybersecurity Subcommittee, "Civil Aviation Supply Chain", 15-16.

Transporte Aéreo

Segundo a ENISA, em 2022, as ameaças mais comuns no setor incluíram ataques relacionados com dados, *ransomware*, *malware*, ataques *DDoS*, vulnerabilidades nas cadeias de abastecimento, além de fraudes e *phishing*. As ameaças associadas a dados tiveram um peso de 24% no total das ameaças, enquanto o *ransomware* foi a maior ameaça, com 32%. As demais ameaças apresentaram um valor entre 4 e 16%⁴⁷⁵. Como mencionado anteriormente, este setor enfrenta ameaças constantes, tornando essencial a análise dos impactos de ataques passados para compreender possíveis incidentes futuros. Entre os ataques mais significativos dos últimos anos, destacam-se:

- Em abril de 2020, o aeroporto de Praga foi vítima de um incidente onde os atacantes tentaram injetar *malware* no sistema, com o objetivo de comprometer as estações de trabalho. Felizmente, o incidente foi detetado precocemente, permitindo que a propagação fosse evitada⁴⁷⁶;
- Um incidente de cibersegurança afetou a EasyJet em abril de 2020, este incidente comprometeu aproximadamente 9 milhões de clientes. Durante este incidente, foram furtados e-mails e detalhes de viagens, além de dados bancários de 2208 clientes⁴⁷⁷;
- Em março de 2021, a empresa SITA, que desenvolve *software* para diversos aeroportos foi alvo de um incidente de segurança. De acordo com a Singapore Airlines, este incidente afetou 580 mil membros da companhia. Estima-se que o incidente resultou no furto de mais de 4,5 milhões de dados dos passageiros de companhias indianas⁴⁷⁸;
- Em fevereiro de 2022, o aeroporto internacional da Suíça foi alvo de um incidente de *ransomware*, o que impactou as suas operações, resultando em atrasos em alguns voos. Nos dias seguintes, os atacantes divulgaram dados sensíveis, incluindo documentos empresariais, declarações de impostos, imagens de passaportes e cartões de identificação⁴⁷⁹;
- Um ciberataque à TAP ocorrido na noite de 25 de agosto de 2022. Os resultados do ataque não foram logo conhecidos, mas cerca de um mês depois soube-se que os atacantes conseguiram os dados de cerca de 1,5 milhões de clientes da companhia aérea, incluindo nomes, moradas e até alegados acordos comerciais. A companhia sempre manteve que os atacantes não conseguiram aceder a dados de pagamento dos clientes⁴⁸⁰.

⁴⁷⁵ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 26, <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>.

⁴⁷⁶ "Prague Airport says thwarted several cyber attacks; hospitals also targeted", *Reuters*, 18 de abril de 2020, <https://www.reuters.com/article/us-czech-cyber/prague-airport-says-thwarted-several-cyber-attacks-hospitals-also-targeted-idUSKBN2200GW/>.

⁴⁷⁷ Jane Wakefield, "EasyJet admits data of nine million hacked", *BBC*, 19 de maio de 2020, <https://www.bbc.com/news/technology-52722626>.

⁴⁷⁸ Campbell Kwan, "Air India discloses data of 4.5m passengers were stolen in SITA cyber attack", *ZdNet*, maio de 2021, <https://www.zdnet.com/article/air-india-discloses-data-of-4-5m-passengers-were-stolen-in-sita-cyber-attack/>

⁴⁷⁹ Pierluigi Paganini, "BlackCat Gang Claimed Responsibility for Swissport Ransomware Attack", *SecurityAffairs*, fevereiro de 2022, <https://securityaffairs.com/128039/cyber-crime/blackcat-swissport-ransomware-attack.html>.

⁴⁸⁰ Flávio Nunes, "Ciberataque à TAP: o que disse a empresa (e o que aconteceu depois)", *Eco*, 22 de setembro de 2022, <https://eco.sapo.pt/2022/09/22/ciberataque-a-tap-o-que-disse-a-empresa-e-o-que-aconteceu-depois/>.

Segundo o mesmo relatório da ENISA, os ataques *DDoS* começaram a ser mais prevalentes em 2022 e estão, principalmente, associados a atividades ativistas, como por exemplo:

- Em maio de 2022, um grupo pró-russo lançou um ataque contra alguns *websites* italianos, nomeadamente contra aeroportos;
- Outro grupo pró-russo, em junho de 2022, lançou um ataque *DDoS* aos aeroportos da Lituânia;
- Em outubro de 2022, os *websites* dos maiores aeroportos dos Estados Unidos da América (EUA) foram alvos de um ataque massivo que deixou os *websites offline*. Este ataque foi lançado, mais uma vez, por grupo pró-Russo⁴⁸¹.

Durante o ano de 2023, surgiram mais de 50 casos em que as coordenadas de GPS foram alteradas remotamente durante voos de aeronaves. Estes casos foram sobretudo registados em voos no Médio Oriente, particularmente em aeronaves que sobrevoaram os territórios de Israel, do Egito e do Iraque. Os incidentes foram classificados como “falhas de navegação críticas” e a este método de ataque deu-se o nome de “*GPS spoofing*”. Num dos casos, ocorrido a 25 de outubro de 2023, num voo que partira de Tel Aviv, a aeronave foi desviada 417 quilómetros do seu curso. Num outro, a 16 de outubro, um outro ataque fazia parecer nos sistemas que a aeronave estava parada em terra, quando na verdade estava a sobrevoar o Cairo⁴⁸².

A maioria destes incidentes tem, na maior parte das ocorrências, uma motivação financeira. Neste setor, aproximadamente 31% das ocorrências têm como alvo as companhias aéreas. Em segundo lugar, com 21%, estão os operadores aéreos, seguidos dos provedores de serviços que representam 15%. Os demais alvos incluem autoridades, a cadeia de abastecimento e os operadores de transporte terrestre⁴⁸³.

⁴⁸¹ ENISA, “ENISA Threat Landscape: Transport Sector”, março de 2023, 28.

⁴⁸² Alex Mitchell, “Hackers are taking over planes’ GPS — experts are lost on how to fix it”, *New York Post*, 20 de novembro de 2023, <https://nypost.com/2023/11/20/lifestyle/hackers-are-taking-over-planes-gps-experts-are-lost-on-how-to-fix-it/>.

⁴⁸³ ENISA, “ENISA Threat Landscape: Transport Sector”, março de 2023, 29.

A tabela seguinte faz uma breve apresentação das principais ameaças para o subsetor do transporte aéreo, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos⁴⁸⁴, de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal⁴⁸⁵.
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa⁴⁸⁶.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável⁴⁸⁷.
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso⁴⁸⁸. No caso, consideraram-se os colaboradores internos maliciosos.

⁴⁸⁴ CNCS, "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.

⁴⁸⁵ CNCS, "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021", maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>.

⁴⁸⁶ CNCS, "Relatório Riscos & Conflitos 2021", maio de 2021, 75.

⁴⁸⁷ CNCS, "Relatório Riscos & Conflitos 2021", maio de 2021, 75-76.

⁴⁸⁸ CNCS, "Relatório Riscos & Conflitos 2021", maio de 2021, 76-77.

Tabela 17 - Agentes de ameaça mais prováveis (Transporte Aéreo)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>				
<i>Malware</i>				
Vulnerabilidades				
<i>Phishing</i>				
Acesso indevido a dados pessoais				
<i>DDoS</i>				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:



- Agente de ameaça provável

Transporte Marítimo e por vias navegáveis interiores

Relativamente ao setor de transporte marítimo e por vias navegáveis, em 2022, as ameaças mais comuns no setor incluíram ataques de *ransomware*, ataques relacionados com dados, *malware*, *phishing*, intrusões, furto de credenciais, ataques *DDoS*, *spoofing*, vulnerabilidades nas cadeias de abastecimento e no geral⁴⁸⁹.

A ENISA também propõe uma taxonomia detalhada de ameaças, relacionando-as com os principais impactos de incidentes que podem ocorrer em ativos e serviços portuários⁴⁹⁰:

Tabela 18 - Principais ameaças (Transporte Marítimo)

Ameaças de alto nível	Possíveis impactos de alto nível
• Espionagem, interseção ou sequestro; • Atividades maliciosas e abuso; • Desastres; • Interrupções; • Danos não intencionais; • Ataques físicos; • Falhas técnicas e avarias.	• Roubo de dados críticos ou sensíveis; • Roubo de cargas e mercadorias; • Tráfico; • Perdas financeiras; • Fraude e furto monetário; • Danos de sistemas ou destruição (parcial ou total); • Danos reputacionais ou perda de competitividade; • Desastres ambientais; • Encerramento de operações; • Lesões humanas, morte ou sequestro.

Ainda de acordo com a ENISA, foi observado, principalmente, ataques de *ransomware*, *malware* e *phishing* e, estes ataques, tiveram como alvos as autoridades dos portos marítimos, operadores dos portos ou os fabricantes pertencentes à cadeia de abastecimento. Os operadores dos portos marítimos foram alvo de 48% dos ataques, as autoridades de 41%, os integrantes da cadeia de abastecimento de 7% e os provedores de serviço de 4%⁴⁹¹.

Os ataques de cibersegurança no setor marítimo têm frequentemente motivações políticas e são executados por agentes patrocinados por estados. Entre 2021 e 2022, vários casos foram reportados: no início de 2021, dois portos marítimos indianos foram alvo de atacantes chineses com intenções políticas. Em outubro do mesmo ano, a Microsoft informou que *hackers* associados ao Irão atacaram setores marítimos nos EUA, na UE e em Israel. Em maio de 2022, Israel foi implicado num incidente de cibersegurança num porto iraniano, o qual causou significativas interrupções nas operações.

⁴⁸⁹ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 30.

⁴⁹⁰ ENISA, "Cyber Risk Management for ports - Guidelines for Cybersecurity in the Maritime Sector", dezembro de 2020, 17.

⁴⁹¹ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 32.

Além destes incidentes com motivações políticas, outros ataques que se destacaram nos últimos anos foram:

- Em 2017, o Grupo A.P, Moller-Maersk sofreu um ataque que utilizou o *malware* NotPetya. Este incidente fez com que o grupo interrompesse as suas operações por 10 dias, resultando num prejuízo de 300 milhões de dólares em receitas⁴⁹²;
- Em 2018, o governo chinês foi suspeito de ter orquestrado um ataque de *ransomware* conta um fabricante da Marinha dos EUA. Como resulta deste incidente, foram furtados dados extremamente sensíveis, incluindo planos para um projeto de um míssil supersónico⁴⁹³;
- Em março de 2019, a empresa de navegação Norsk Hydro foi vítima do *ransomware* LockerGoga. Estima-se que os atacantes estiveram na rede da empresa durante duas a três semanas antes de serem descobertos. As perdas económicas foram estimadas em 71 milhões de dólares⁴⁹⁴;
- Em abril de 2020, ocorreu um ataque de *malware* à Mediterranean Shipping Company (MSC). Os servidores da MSC foram desligados para evitar a propagação do *malware* e proteger os dados da empresa⁴⁹⁵;
- Em fevereiro de 2022, um ataque de *ransomware* desativou o sistema de informação do Terminal de contentores na Índia, levando ao desvio de um navio para outro terminal. Esta interrupção obrigou os funcionários do porto a processassem a carga em formato papel, o que gerou sérios problema no tráfego do terminal e impactou outros terminais na proximidade⁴⁹⁶.

A maioria dos navios utiliza sistemas de TI e TO que já apresentam alguma antiguidade, o que os torna mais vulneráveis a incidentes de cibersegurança. Por meio destes sistemas, é possível controlar remotamente diversas funcionalidades do navio como: manipular os motores, falsificar os sistemas de navegação, interferir com os radares, desligar sistemas de carga ou de deteção de incêndios e até mesmo assumir o controlo do leme⁴⁹⁷.

⁴⁹² Port Economics, Management and Policy, “Petya Ransomware Cyber-Attack on Maersk”, <https://porteconomicsmanagement.org/pemp/contents/part2/digital-transformation/petya-ransomware-cyber-attack-maersk/>.

⁴⁹³ Ellen Nakashima e Paul Sonne, “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare”, *The Washington Post*, 8 de junho de 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

⁴⁹⁴ Hydro, “Cyber-attack on Hydro”, março de 2019, <https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/>.

⁴⁹⁵ Maritime Cybersecurity, “Mediterranean Shipping Company (MSC) hit by a malware attack in Geneva, Switzerland”, abril de 2020, <https://maritimecybersecurity.nl/incident/KPgm1rZz5r>.

⁴⁹⁶ Abhishek Sharma, “Maritime Cybersecurity: An Emerging Area of Concern for India”, *The Diplomat*, 9 de fevereiro de 2024, <https://thediplomat.com/2024/02/maritime-cybersecurity-an-emerging-area-of-concern-for-india/>.

⁴⁹⁷ Nineta Polemi e Christophe Maele, “Cibersegurança na Infraestrutura Marítima Crítica: Reflexão dos portos africanos”, Comissão Europeia, 20 de abril de 2023, 28, <https://rusieurope.eu/wp-content/uploads/2024/02/cybersecurity-in-maritime-critical-infrastructure-crimson-report-portuguese.pdf>

Tal como para o subsetor do transporte aéreo, volta-se a apresentar uma tabela que compila as principais ameaças do setor e dos agentes de ameaça mais prováveis de as concretizar.

Tabela 19 - Agentes de ameaça mais prováveis (Transporte Marítimo)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Malware				
Vulnerabilidades				
Phishing				
Acesso indevido a dados pessoais				
DDoS				
Spoofing				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:

 - Agente de ameaça provável

Transporte Ferroviário

Em 2022, as ameaças mais comuns no setor incluíram ataques de *ransomware*, ataques relacionados com dados, *malware*, intrusões, fraude, ataques *DDoS*, *spoofing* e vulnerabilidades nas cadeias de abastecimento⁴⁹⁸. As ameaças associadas a dados são de cerca 5%, enquanto o *ransomware* é a maior ameaça, com 25%, os ataques de *DDoS* foram de 20% e as intrusões 10%. As demais ameaças apresentaram um valor de 5%⁴⁹⁹.

Conforme o relatório da ENISA, relativo à gestão de riscos de cibersegurança do setor ferroviário na UE, a maioria dos ataques direcionados foca os sistemas de TI, especialmente os serviços de bilheteria, aplicações e ecrãs de serviço. É importante destacar que os ataques aos sistemas de TO geralmente ocorrem apenas quando os sistemas de TI estão indisponíveis⁵⁰⁰.

⁴⁹⁸ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 33.

⁴⁹⁹ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 34.

⁵⁰⁰ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 33.

A ENISA também propõe uma taxonomia detalhada de ameaças, relacionando-as com os principais impactos de incidentes que podem ocorrer em ativos e serviços ferroviários⁵⁰¹:

Tabela 20 - Principais ameaças (Transporte Ferroviário)

Ameaças de alto nível	Possíveis impactos de alto nível
• Espionagem, interseção ou sequestro; • Atividades maliciosas e abuso; • Desastres; • Interrupções; • Danos não intencionais; • Ataques físicos; • Falhas técnicas e avarias.	• Perdas financeiras; • Fraude e furto monetário; • Danos de sistemas ou destruição (parcial ou total); • Desastres ambientais; • Encerramento de operações; • Lesões humanas, morte ou sequestro.

Alguns cenários maliciosos que podem comprometer este setor vão desde o furto de dados pessoais de utilizadores de plataformas *online* (como compra de bilhetes) até contextos de quebra de energia ou ataques maliciosos que comprometam, por exemplo, sistemas de sinalização que podem originar acidentes físicos, levando, no pior dos cenários, a consequências de segurança humana.

Neste setor, cerca de 72% das ocorrências visam as infraestruturas do transporte ferroviário. Em segundo lugar, com 24%, estão as autoridades. Por fim, os provedores de serviços representam 4%⁵⁰². Em 2022, os ataques DDoS aumentaram, alcançando o quinto lugar, com 20%. O principal motivo para este crescimento foi a atividade *hacktivista* gerada depois da invasão da Rússia à Ucrânia, resultando em diversos incidentes de segurança por parte de grupos pró-Rússia e anti-NATO, especialmente direcionados às companhias de transporte ferroviário. Alguns exemplos são:

- Em abril de 2022, um grupo pró-Rússia lançou um ataque contra a operadora de transportes CFR Calatori, derrubando o *website* da companhia⁵⁰³;
- Em junho do mesmo ano, o *website* da Lithuanian railways fica fora do ar, sendo o incidente reivindicado por atacantes russos⁵⁰⁴;
- Em agosto de 2022, a companhia de transporte ferroviário da Estónia sofreu um incidente de cibersegurança após a remoção de um monumento soviético. O ataque foi reivindicado pelo grupo de piratas informáticos russo Killnet⁵⁰⁵.

⁵⁰¹ ENISA, "Railway Cybersecurity", novembro de 2021, 20.

⁵⁰² ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 34.

⁵⁰³ Andra Timu, "Pro-Russian Hacking Group Killnet Attacks Romanian Websites", *Bloomberg*, abril de 2022, <https://www.bloomberg.com/news/articles/2022-04-29/romanian-government-border-police-websites-hit-by-ddos-attack>.

⁵⁰⁴ Andrius Sytas, "Russian group claims hack of Lithuanian sites in retaliation for transit ban", *Reuters*, 27 de junho de 2022, <https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27/>.

⁵⁰⁵ Vera Novais, "Estónia alvo de maior ciberataque desde 2007. Grupo russo reivindica ataque", *Observador*, 18 de agosto de 2022, <https://observador.pt/2022/08/18/estonia-alvo-de-maior-ciberataque-desde-2007-grupo-russo-reivindica-ataque/>.

Além destes incidentes com motivações políticas, outros ataques que se destacaram nos últimos anos foram:

- Em 2015, a Polónia enfrentou um incidente de cibersegurança nas operações ferroviárias, quando os atacantes tiveram como alvo os sistemas de controlo dos comboios. Este ataque resultou em atrasos e falhas no funcionamento nos comboios⁵⁰⁶;
- No mesmo ano, a ferrovia de São Francisco, nos EUA, enfrentou um incidente de *ransomware* que paralisou os sistemas de pagamento e de bilhética. Os criminosos exigiram um resgate em *bitcoin*, mas, felizmente, foi possível restaurar os sistemas sem pagar nenhum resgate⁵⁰⁷;
- A Ucrânia, em 2017, sofreu um ataque aos seus sistemas do setor ferroviário, resultando na interrupção das operações, causando alguns atrasos nos comboios⁵⁰⁸;
- Em 2020, o operador de ferrovias alemão Deutsche Bahn enfrentou um incidente de cibersegurança que impactou a amostragem das chegadas e partidas dos comboios. Apesar deste contratempo, os sistemas de segurança permaneceram intactos, resultando apenas em inconvenientes para os passageiros⁵⁰⁹;
- A infraestrutura ferroviária belga foi alvo de um incidente de cibersegurança em 2021, este incidente afetou os sistemas dos comboios, levando a atrasos nos mesmos⁵¹⁰;
- Em março de 2022, a companhia estatal ferroviária italiana foi vítima de um ataque aos seus sistemas de TI. Este ataque levou a que os passageiros não conseguissem comprar bilhetes de comboio⁵¹¹.

⁵⁰⁶ Carles Llorach, "Cyber-attacks received in the railway sector", Phoenix, 2024, <https://phoeni2x.eu/2024/02/29/cyber-attacks-received-in-the-railway-sector/>.

⁵⁰⁷ Établissement Public de Sécurité Ferroviaire, "Taking cybersecurity challenges into account in railway safety", 2021, 4, https://www.era.europa.eu/system/files/2022-11/enr135-taking_cybersecurity_challenges_into_account_in_railway_safety_en.pdf.

⁵⁰⁸ Tyler Wall, "Throwback Attack: Ukrainian railway hit by cyberattack, stranding passengers", *Industrial Cybersecurity Pulse*, 24 de março de 2023, <https://www.industrialcybersecuritypulse.com/hacks-attacks/throwback-attack-ukrainian-railway-hit-by-cyberattack-stranding-passengers/>.

⁵⁰⁹ "German rail operator affected by global cyber attack", *Reuters*, 13 de maio de 2017, <https://www.reuters.com/article/technology/german-rail-operator-affected-by-global-cyber-attack-idUSKBN1890DM/>.

⁵¹⁰ Georgi Gotev, "Belgium suffers major cyberattack", *Euractiv*, 5 de maio de 2021, https://www.euractiv.com/section/politics/short_news/belgium-suffers-major-cyber-attack/.

⁵¹¹ "Cybersecurity training for the Railway Sector", *Railway Cybersecurity*, https://www.railway-cybersecurity.com/Railway_Cybersecurity_Training.html.

Tal como para os subsetores do transporte aéreo e marítimo, volta-se a apresentar uma tabela que compila as principais ameaças do setor e dos agentes de ameaça mais prováveis de as concretizar.

Tabela 21 - Agentes de ameaça mais prováveis (Transporte Ferroviário)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>				
<i>Malware</i>				
Vulnerabilidades				
<i>Phishing</i>				
<i>DDoS</i>				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:



- Agente de ameaça provável

Transporte Rodoviário

Relativamente ao setor rodoviário, em 2022, destacam-se ataques de *ransomware*, ataques relacionados com dados, *malware*, *phishing*, intrusões, ataques *DDoS* e vulnerabilidades nas cadeias de abastecimento⁵¹².

Transversalmente a todos os setores, também o dos **transportes rodoviários** está sujeito a ciberameaças como *DDoS*, furto de dados, difusão de programas maliciosos, manipulação de *software* e *hardware*, acesso não autorizado, entre outros⁵¹³.

⁵¹² ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 36.

⁵¹³ Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, "Conjunto de ferramentas de cibersegurança para o setor dos transportes", 9.

Tabela 22 - Principais ameaças (Transporte Rodoviário)

Ameaças de alto nível	Possíveis impactos de alto nível
Programas maliciosos	Afetar indivíduos ou organizações nos diferentes modos de transporte.
DoS ou DDoS	Impedir os indivíduos ou as organizações de aceder a recursos ou serviços de transporte importantes.
Acesso não autorizado e furto	Acesso não autorizado, apropriação e exploração de ativos críticos.
Manipulação de <i>software</i>	Modificação do comportamento do <i>software</i> para realizar ataques específicos.

Através das listas apresentadas das principais ameaças no setor, é possível verificar que os principais ciberataques no setor não são dirigidos aos transportes em si, mas sim aos sistemas informáticos das organizações, procurando, por exemplo, obter dados sensíveis sobre as organizações e os seus clientes.

Neste setor, cerca de 30% das ocorrências visam os fabricantes dos componentes dos veículos. Em segundo lugar, com 27%, estão as autoridades. De seguida, com 23%, estão os operadores de transporte público. Por fim, estão os provedores de serviços e os fornecedores diretos⁵¹⁴. A maior fonte de ataque foi o *ransomware*, dirigido em particular aos fabricantes dos componentes e aos fornecedores diretos tendo, em alguns casos, parado a produção dos veículos. Entre 2021 e 2022 ocorreram alguns casos notáveis:

- Em setembro de 2021, a empresa holandesa Bochane sofreu um incidente de cibersegurança que resultou no bloqueio de vários computadores por um dia;
- A Toyota, em fevereiro de 2022, suspendeu as suas operações durante um dia, após um incidente de cibersegurança que afetou um dos seus fornecedores de peças plásticas, resultando na perda de aproximadamente 13 mil carros destinados à exportação;
- Neste mês, a Kia também enfrentou um incidente de cibersegurança, no qual os atacantes exigiram 20 milhões de dólares para não divulgarem os dados obtidos;
- Em abril de 2022, a empresa de aluguer de veículos alemã Sixt sofreu um incidente de cibersegurança e todos os serviços não essenciais foram desligados;
- Em junho do mesmo ano, a empresa japonesa Nichirin enfrentou um incidente que a levou a desligar alguns sistemas de controlo de produção, obrigando-a a substituir estes sistemas por processos manuais⁵¹⁵;
- A 1 de setembro de 2022, ocorreu um ciberataque à empresa russa Yandex Taxi, no qual os atacantes obtiveram o controlo do sistema de gestão de frota da empresa e enviaram dezenas de táxis para o mesmo local em Moscovo, paralisando o trânsito durante cerca de duas horas no local e imediações⁵¹⁶. Este tipo de ataque pode ser repetido noutras entidades, enviando os veículos para locais onde estejam, por exemplo, grupos armados prontos a roubar os bens transportados⁵¹⁷.

As ameaças relacionadas com o furto de dados tiveram como alvo, principalmente, sistemas de TI, com o objetivo de adquirir informações de clientes, funcionários e dados proprietários. Em fevereiro de 2021, foram divulgados mais de 3,2 milhões de dados de clientes da DriveSure, uma empresa dos EUA de serviços para concessionárias de automóveis. Os casos mais notáveis neste quesito foram os incidentes de cibersegurança que afetaram a Tesla e a Volvo. Em setembro de 2021, foi tornado público o *software* de inteligência artificial da Tesla e, em dezembro de 2021, a Volvo anunciou que no incidente de cibersegurança que foi vítima, foram furtadas informações de pesquisa e de desenvolvimento⁵¹⁸.

⁵¹⁴ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 38.

⁵¹⁵ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 36-37.

⁵¹⁶ Matthew Holroyd, "Gridlock as hackers order hundreds of taxis to same place in Moscow", *Euronews*, 2 de setembro de 2022, <https://www.euronews.com/my-europe/2022/09/02/gridlock-as-hackers-order-hundreds-of-taxis-to-same-place-in-moscow>.

⁵¹⁷ James Menzies, "Under Attack: Trucking industry increasingly at risk of cyberattacks", *Trucknews*, 10 de novembro de 2023, <https://www.trucknews.com/features/under-attack-trucking-industry-increasingly-at-risk-of-cyberattacks/>.

⁵¹⁸ ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 38.

Tal como para os subsetores do transporte aéreo, marítimo e ferroviário, volta-se a apresentar uma tabela que compila as principais ameaças do setor e dos agentes de ameaça mais prováveis de as concretizar.

Tabela 23 - Agentes de ameaça mais prováveis (Transporte Rodoviário)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Malware				
Vulnerabilidades				
Phishing				
Acesso indevido a dados pessoais				
DDoS				
Manipulação de Sistemas (TI)				
Manipulação de Sistemas (TO)				

Legenda:



- Agente de ameaça provável

2.3. Capacitação

O setor dos transportes tem procurado capacitar-se ao nível da cibersegurança ao longo dos últimos anos. Parte dessa capacitação tem passado pela assinatura de protocolos de cooperação com entidades como o CNCS e pela realização de sessões de formação sobre o tema. Em maio de 2017, a Autoridade da Mobilidade e dos Transportes (AMT) e o Gabinete Nacional de Segurança (GNS)/CNCS assinaram um protocolo que permite “estabelecer formas de cooperação no desenvolvimento estratégico e técnico e aprofundar competências de Cibersegurança entre as partes”⁵¹⁹, enquadrado na Estratégia Nacional de Segurança do Ciberespaço (ENSC) de 2015 aprovada pela Resolução do Conselho de Ministros nº36/2015, 12 de junho⁵²⁰.

Em janeiro de 2022, a AMT participou no evento “Inovação na Era Digital”, onde foram apresentadas Zonas Livres Tecnológicas (“espaços físicos e virtuais para testes, em ambiente real ou quase-real, destinadas à realização, pelos seus promotores, de testes de tecnologias, produtos, serviços e processos inovadores de base tecnológica, de forma segura”). Esta presença revela a preocupação da AMT em manter-se próxima da importância da inovação numa era digital como aquela em que vivemos⁵²¹.

Em novembro de 2022, a AMT promoveu um evento sobre o mote “Transição Digital, Ambiental e Energética - Impacto na Gestão dos Modelos de Concessão”. Esta mesa-redonda surge do encontro entre a AMT e a Agência Nacional dos Transportes Terrestres do Brasil (ANTT). Ambas as entidades estabeleceram um Protocolo de Cooperação, em 2018, na sequência da promoção e aumento de formação de colaboradores no que diz respeito à transição digital no setor⁵²².

No dia 11 de dezembro de 2023, a AMT organizou uma formação interna sobre cibersegurança, cujo principal objetivo era sensibilizar os seus colaboradores acerca da necessidade de adoção de comportamentos seguros relacionados com a cibersegurança, mais concretamente no que respeita aos riscos decorrentes do dia a dia⁵²³.

Outra forma de capacitação no setor surge através do programa de formação C-Academy, promovido pelo CNCS, que oferece formação avançada em cibersegurança, tendo como objetivo capacitar profissionais das principais entidades abrangidas pelo RJSC. Assim sendo, os destinatários prioritários da C-Academy são as entidades da Administração Pública, os operadores de infraestrutura crítica, os prestadores de serviços digitais e os operadores de serviços essenciais em estudo no presente relatório. A C-Academy tem como objetivo abranger 9,8 mil formandos até ao primeiro trimestre de 2026⁵²⁴.

⁵¹⁹ AMT, “AMT assina protocolo com Centro Nacional de Cibersegurança”, 1 de junho de 2017, <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-assina-protocolo-com-centro-nacional-de-ciberseguran%C3%A7a/>.

⁵²⁰ Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/36-2015-67468089>.

⁵²¹ Autoridade da Mobilidade e dos Transportes (AMT), “Inovação na Era Digital: Zonas Livres Tecnológicas (ZLT) e Digital Innovation Hubs (DIH)”, 25 de janeiro de 2022, <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/inova%C3%A7%C3%A3o-na-era-digital-zonas-livres-tecnol%C3%B3gicas-zlt-e-digital-innovation-hubs-dih/>.

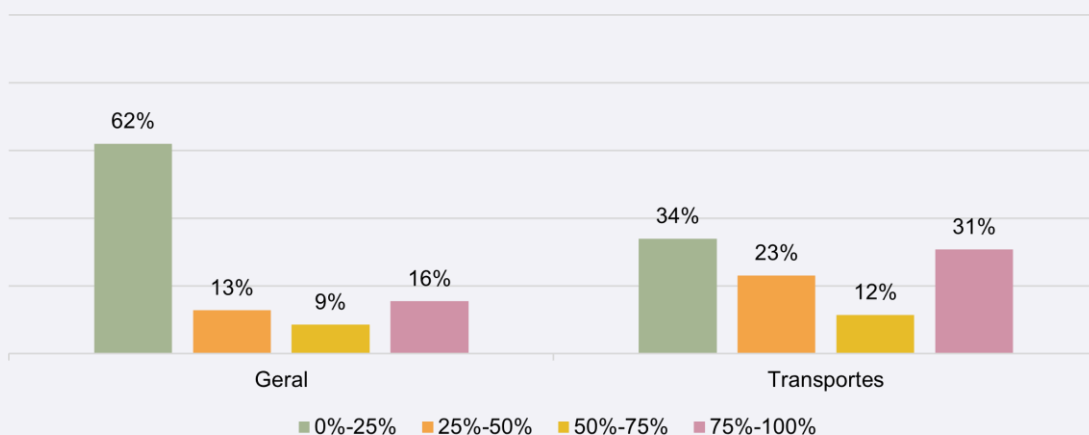
⁵²² AMT, “AMT promoveu debate sobre “Transição digital, ambiental e energética - impacto na gestão dos modelos de concessão””, 22 de novembro de 2022, <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-promoveu-debate-sobre-transi%C3%A7%C3%A3o-digital-ambiental-e-energ%C3%A9tica-impacto-na-gest%C3%A3o-dos-modelos-de-concess%C3%A3o/>.

⁵²³ AMT, “AMT promoveu ação de formação interna sobre cibersegurança”, 12 de dezembro de 2023, <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-promoveu-a%C3%A7%C3%A3o-de-forma%C3%A7%C3%A3o-interna-sobre-ciberseguran%C3%A7a/>.

⁵²⁴ “C-Academy”, Sensibilização e Formação, CNCS, <https://www.cncs.gov.pt/pt/c-academy/>.

No entanto, segundo o questionário realizado, em seguida podemos observar a percentagem de aproximada de trabalhadores do setor dos transportes com formação básica em cibersegurança. A sensibilização para todo o tipo de riscos de cibersegurança e a formação para identificar possíveis tentativas de ataques de segurança são essenciais para impedir que estas se concretizem, pois, a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação (**Gráfico 33**) nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Podemos verificar que o setor dos transportes tem uma percentagem maior de trabalhadores com formação básica em cibersegurança comparativamente com o geral.

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Transporte Aéreo

Os riscos associados à segurança da informação na operação das aeronaves são uma preocupação significativa da TAP. Isto inclui tanto os sistemas de informação a bordo quando os de solo. Na TAP, os processos empresariais dependem amplamente da tecnologia da informação, o que gera riscos à estabilidade destes processos, bem como à disponibilidade, confidencialidade e integridade das informações e dos dados. É importante capacitar-se para tentar reduzir ao máximo estes riscos. Desta forma, a TAP tem uma monitorização contínua da segurança informática e adota e implementa cada vez mais medidas para reforçar a segurança dos sistemas de informação, como ferramentas para prevenir e responder rapidamente a ciberataques, adaptar processos a cenários de risco e dar formação de sensibilização regularmente. A TAP também implementa autenticação multifator (MFA) e mantém uma equipa de gestão de incidentes disponível 24 horas, focada em detetar e responder a ameaças⁵²⁵.

⁵²⁵ TAP, "Apresentação de resultados 2023", março de 2024, 23-24, <https://www.tapairportugal.com/pt/sobre-nos/investidores/informacao-financeira?accordionid=12943eea-2400-4b17-ad20-487d8c4f8635>.

A TAP tem em funcionamento, desde o primeiro semestre de 2023, a aplicação *Cybercomm*. A *Microsoft* e a *Devscope*, responsáveis pelo desenvolvimento desta aplicação, em parceria com o CNCS, acreditam que venha a impactar “mais de 100 mil profissionais no sector público e privado para capacitação no reforço do profissional e cidadão ciberseguro”. O principal foco desta aplicação é o de divulgação de conteúdos de formação que permita que os colaboradores fiquem alerta para casos de *phishing*, *ransomware*, desinformação, entre outros, e possam preparar-se para uma melhor identificação de ameaças ou comunicação entre todos em caso de incidentes de cibersegurança⁵²⁶.

Transporte Marítimo e por vias navegáveis interiores

Os portos marítimos com a crescente modernização a que têm estado sujeitos, são altamente dependentes de sistemas de informação, tornando a cibersegurança crucial. No entanto, muito dos portos marítimos apresentam deficiências nesta área, apesar de serem alvos de incidentes de cibersegurança que podem comprometer o bom funcionamento das operações.

O Porto de Sines participou, em abril de 2022, num exercício de cibersegurança integrado na Singapore Maritime Week. Este exercício foi organizado pela Autoridade Marítima e Portuária de Singapura e envolveu outros portos como o de Hamburgo, Tanger Med, Los Angeles e Seattle. O principal objetivo deste exercício foi aumentar a consciencialização sobre as ameaças de cibersegurança no setor marítimo, através de simulações de cenários reais. Esta iniciativa também promoveu a colaboração e partilha de informação entre as autoridades portuárias, dentro da rede PACC-Net, fortalecendo assim a resiliência de cibersegurança⁵²⁷.

A aliança ISAC Portos, coordenada pelo CNCS, visa fortalecer a ciberresiliência dos portos marítimos nacionais. Esta iniciativa promove a colaboração entre portos e facilita a partilha de informação sobre ameaças, vulnerabilidades e incidentes de cibersegurança. O grande objetivo é criar um ambiente de confiança entre os mesmos para proteger as operações portuárias e mitigar riscos que possam afetar a cadeia de abastecimento marítima e o comércio internacional⁵²⁸.

⁵²⁶ Security Magazine, “App Cybercomm já está em funcionamento na TAP”, junho de 2023, <https://www.securitymagazine.pt/2023/06/07/ciberseguranca-app-cybercomm-ja-esta-em-funcionamento-na-tap-e-ctt/>.

⁵²⁷ APS, “Porto de Sines integra exercício de cibersegurança enquadrado na Singapore Maritime Week”, abril de 2024, <https://www.apsinesalgarve.pt/noticias/2024/porto-de-sines-integra-exerc%C3%ADcio-de-ciberseguran%C3%A7a-enquadrado-na-singapore-maritime-week/>.

⁵²⁸ “ISAC Portos”, Comunidades de Cibersegurança, CNCS, última atualização em abril de 2024, <https://www.cncs.gov.pt/pt/comunidades-ciberseguranca/isacs/portos/>.

Transporte Ferroviário

No Relatório de Governo Societário de 2023, a CP identifica como um dos riscos operacionais a perda de informações decorrente da indisponibilidade dos sistemas de informação. Este risco está associado à escassez de recursos humanos especializados necessários para garantir as atividades de cibersegurança num contexto cada vez mais exigente. Para cumprir o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE, foram adotadas diversas medidas, incluindo a criação de um regulamento interno. Este documento incorpora orientações da CNPD e do CNCS, estabelecendo práticas e condutas essenciais para a gestão segura de documentos e sistemas de informação⁵²⁹. No relatório de contas de 2023 da CP, verificou-se um aumento de 2 milhões de euros nos investimentos em tecnologias da informação. Estes recursos foram aplicados na aquisição e atualização de *software*, renovação de licenças, e na implementação de novas plataformas informáticas⁵³⁰.

Transporte Rodoviário

Assim como no setor ferroviário, os OSE do transporte rodoviário são também destinatários prioritários do programa de formação C-Academy. Para além deste aspeto, a Infraestruturas de Portugal realizou, em 2019, ao longo do Mês Europeu da Cibersegurança (outubro), diversas ações de divulgação e sensibilização. As ações desenvolvidas ao longo desse mês tiveram como linha condutora a sensibilização dos diversos públicos sobre a importância da segurança no ciberespaço. A IP, enquanto operadora de infraestrutura crítica, operadora de serviços essenciais e prestadora de serviços digitais, tinha como objetivos aumentar o seu grau de maturidade nas capacidades mínimas de resposta a incidentes de cibersegurança e aplicar o Quadro Nacional de Referência para a Cibersegurança (QNRCS), preparando-se assim para as ameaças existentes e emergentes⁵³¹. Além destas ações, os relatórios anuais divulgados pela Infraestruturas de Portugal revelam também uma crescente aposta no aumento das capacidades digitais através da aquisição e manutenção de soluções tecnológicas, como soluções de Enterprise Resource Management (ERM), Customer Relationship Management (CRM), ciberdefesa e cibersegurança. Em 2023, os gastos com esta capacitação terão totalizado 10 milhões de euros⁵³².

Em 2022, a Carris (Lisboa), com o objetivo de mitigar os riscos de gestão onde se incluem os riscos de corrupção, infrações conexas e conflitos de interesses, foram implementados alguns controlos dos quais se destaca a formação em cibersegurança, o curso “cidadão Ciberseguro” para todos os colaboradores⁵³³. Tanto a Carris como a STCP pertencem à OPT (Optimização e Planeamento de Transportes, SA), que realiza “Desenvolvimento de projetos de I&D na área dos transportes, desenvolvendo soluções informáticas avançadas para a gestão e otimização de sistemas de transportes”⁵³⁴.

⁵²⁹ CP, “Relatório do Governo Societário 2023”, 16 de maio de 2024, 59, https://www.cp.pt/StaticFiles/Institucional/1_a_empresa/3_Relatorio_Contas/2023/relatorio-governo-societario-2023.pdf.

⁵³⁰ CP, “Relatório do Governo Societário 2023”, 145.

⁵³¹ Infraestruturas de Portugal, “A IP promove ações sobre Cibersegurança”, outubro de 2019, <https://www.infraestruturasdeportugal.pt/pt-pt/ip-promove-aco-es-sobre-ciberseguran-ca>.

⁵³² AMT, “Relatório de Atividades, Gestão e Contas de 2023”, 16 de abril de 2024, 108, https://www.amt-autoridade.pt/media/4423/relatorio_de-atividades_2023_16042024.pdf.

⁵³³ Carris, “Plano de Prevenção de Riscos de Corrupção e Infrações Conexas 2022”, 2023, 28, <https://www.carris.pt/media/22uhz5qn/plano-de-preven%C3%A7%C3%A3o-de-riscos-de-corrup%C3%A7%C3%A3o-e-infra%C3%A7%C3%B5es-conexas-2022.pdf>.

⁵³⁴ OPT, “Empresa”, <https://www.opt.pt/empresa/>.

2.4. Investimento em cibersegurança

O relatório de atividades, gestão e contas da AMT de 2023, revela também que a oito de agosto de 2019 foi celebrado um contrato de prestação de serviços com a empresa Warpcom Services S.A, com preço contratual de 78 388€ e prazo de execução 36 meses, que visa a manutenção, suporte e gestão da infraestrutura e segurança da rede informática local⁵³⁵.

O programa “Horizonte 2020”⁵³⁶ é um programa-quadro comunitário para a investigação e inovação, onde se incluem ações de desenvolvimento e teste a novas soluções de transporte. Com base neste programa e nas necessidades do setor, a Comissão Europeia prosseguirá com apoios no período 2021-2027, e implementará e desenvolverá as seguintes iniciativas:

- Contribuição de 500 milhões de euros para a parceria Horizonte Europa “Mobilidade conectada, cooperativa e automatizada” que consiste na investigação e inovação com o objetivo de tornar a Europa um líder mundial em sistemas e serviços de Mobilidade conectada e automatizada (CAM). Esta implementação depende fortemente dos sistemas cooperativos de transportes inteligentes, responsáveis por intercâmbio de informações entre os veículos e entre veículos e infraestruturas rodoviárias;
- Alcance de uma cobertura 5G ininterrupta das principais vias de transporte em toda a Europa, para viagens cada vez mais seguras e conectadas. Também financiado pelo Horizonte 2020, o projeto 5G-Carmen tem como objetivo, através do 5G, desenvolver transportes mais seguros, ecológicos e inteligentes⁵³⁷;

Consequentemente a todas estas iniciativas, projetos e implementações, cresce a relevância e preocupação relativamente à cibersegurança. Como já foi referido, a evolução tecnológica é acompanhada de crescimento de atividade maliciosa que pode resultar no efeito contrário ao pretendido pela implementação de sistemas de transportes inteligentes - a segurança dos passageiros. Neste sentido, a Diretiva da UE relativa à segurança das redes e da informação (Diretiva SRI) tem a preocupação de garantir um forte nível comum de cibersegurança em toda a UE⁵³⁸.

Existe a necessidade de apoiar as empresas de mobilidade e transportes na caminhada de transformação digital dos seus serviços. Neste sentido, os Polos Europeus de Inovação Digital (PEID) apoiam empresas de mobilidade e transportes através de conhecimentos técnicos, formação de competências, inovação de serviços e sensibilização para questões ambientais⁵³⁹. Em 2022, a UE adotou uma Diretiva SRI revista (SRI 2) para substituir a diretiva de 2016. As novas regras garantem um elevado nível comum de cibersegurança na União, respondendo à evolução do cenário de ameaças e tendo em conta a transformação digital, acelerada pela pandemia de COVID-19⁵⁴⁰.

⁵³⁵ AMT, “Relatório de Atividades, Gestão e Contas de 2023”, 16 de abril de 2024, 116, https://www.amt-autoridade.pt/media/4423/relatorio_de-atividades_2023_16042024.pdf.

⁵³⁶ IAPMEI, “Horizonte 2020”, última atualização a 10 de maio de 2024, <https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Empreendedorismo-Inovacao/Inovacao-e-Competitividade/Incentivos-e-financiamento/Horizonte-2020.aspx>.

⁵³⁷ Comissão Europeia, “Tecnologias-chave para impulsionar a digitalização dos transportes”, <https://digital-strategy.ec.europa.eu/pt/policies/technologies-digitalisation-transport>.

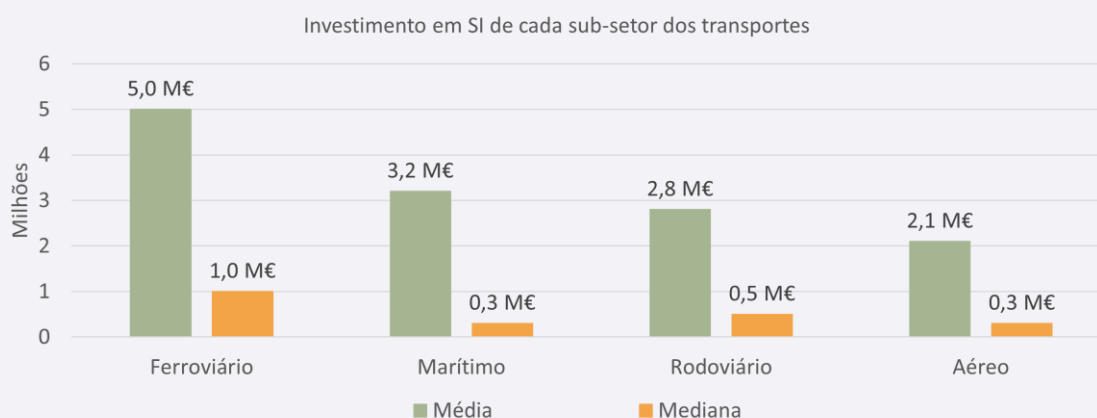
⁵³⁸ Comissão Europeia, “Tecnologias-chave para impulsionar a digitalização dos transportes”.

⁵³⁹ Comissão Europeia, “European Digital Innovation Hubs”, <https://digital-strategy.ec.europa.eu/en/activities/edihs>.

⁵⁴⁰ Conselho Europeu, “Cibersegurança: Como combate a UE as ciberameaças”, <https://www.consilium.europa.eu/pt/policies/cybersecurity/>.

O relatório anual “NIS Investments” de 2023, elaborado pela ENISA, mostra que o setor ferroviário tem a maior despesa em Segurança da Informação (SI) entre os subsetores dos transportes, com 5 milhões de euros de despesa, em média. Segue-se o Marítimo com 3.2 M€ de gastos em SI, o rodoviário com 2.8 M€ e por último aéreo com 2.1 M€, em média. Essas médias são muito superiores aos valores medianos, indicando que as maiores organizações têm um orçamento de SI muito maior do que as mais pequenas. Os valores medianos destacam os operadores ferroviários como aqueles com despesas de SI significativamente mais elevadas, com 1 M€. Os outros três subsectores apresentam valores entre 300 mil e 500 mil euros de gastos com SI⁵⁴¹.

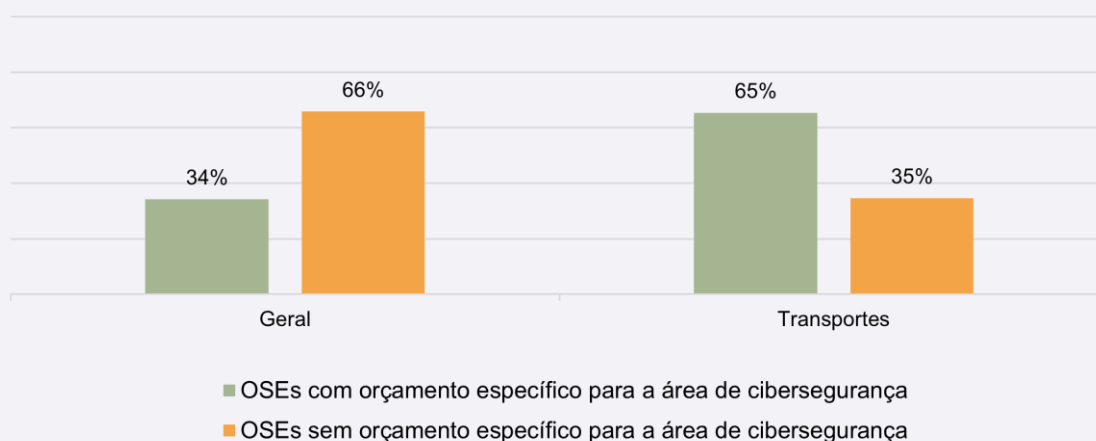
Figura 3 - Investimento em SI de cada subsector dos transportes



(Fonte: ENISA, “NIS Investments 2023”, última atualização em novembro de 2023, <https://www.enisa.europa.eu/publications/nis-investments-2023>)

Deste setor, cerca de 65% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



⁵⁴¹ ENISA, “NIS Investments”, novembro de 2023, 66.

Em relação às áreas de aplicação do orçamento de cibersegurança, segundo os inquiridos do questionário, 88% é destinado à formação e análise de segurança, 82% à segurança das redes e à gestão de vulnerabilidades, e 77% à aquisição de *software* e *hardware*. Nas demais áreas, os investimentos variam entre 35% e 65%. (**Gráfico 110.2**). Comparativamente ao geral, os valores são mais elevados em algumas áreas do setor dos transportes, havendo um valor mais baixo nas áreas de capacitação em tecnologia, *governance*, *risk & compliance*, segurança das redes e aquisição de *software* e *hardware* (**Gráfico 110**).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

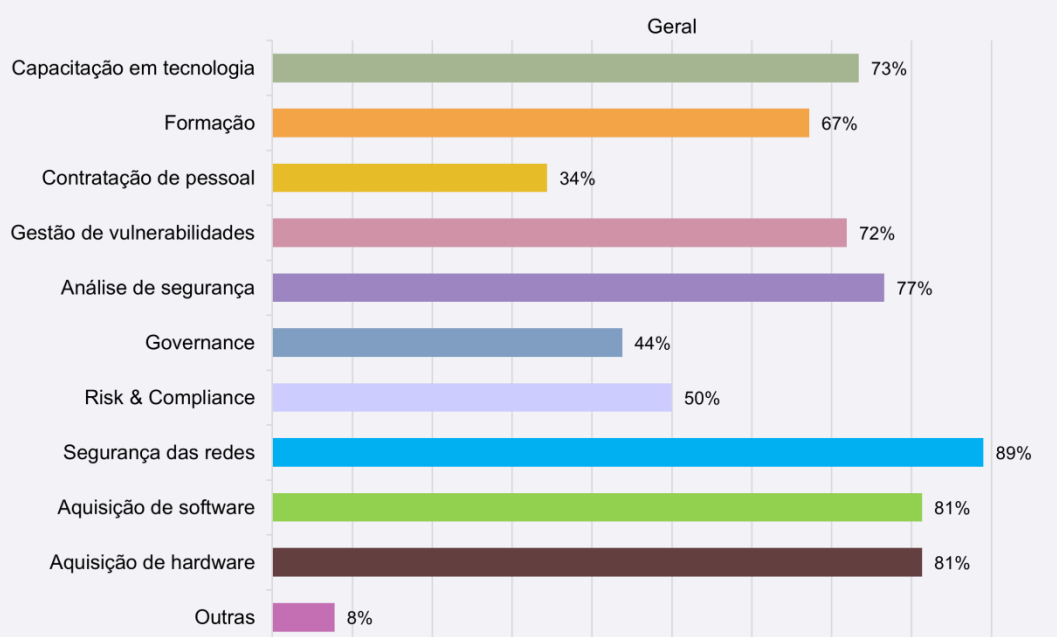
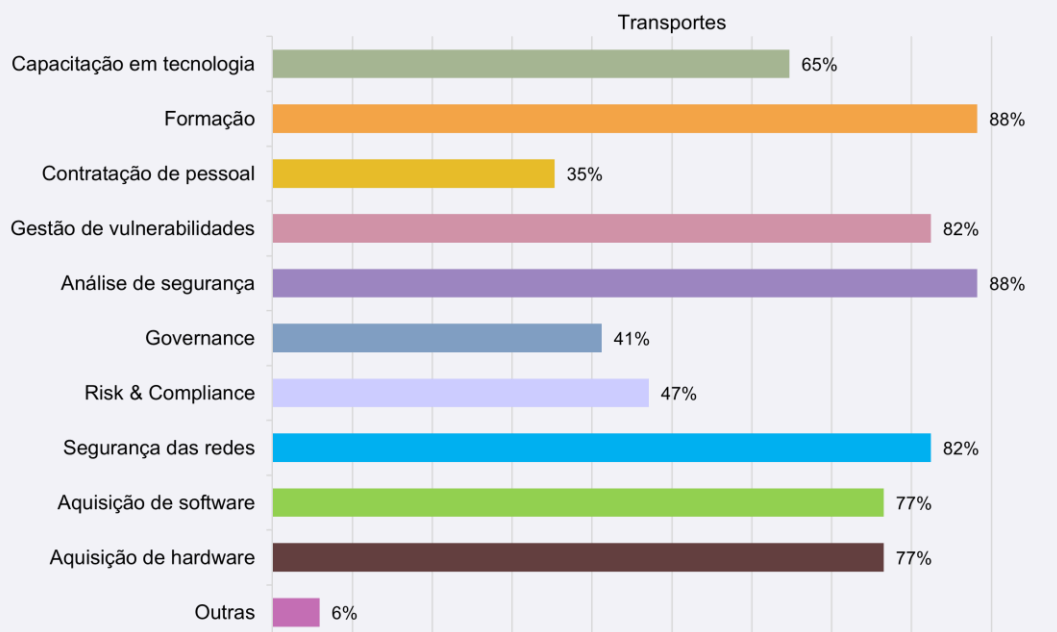
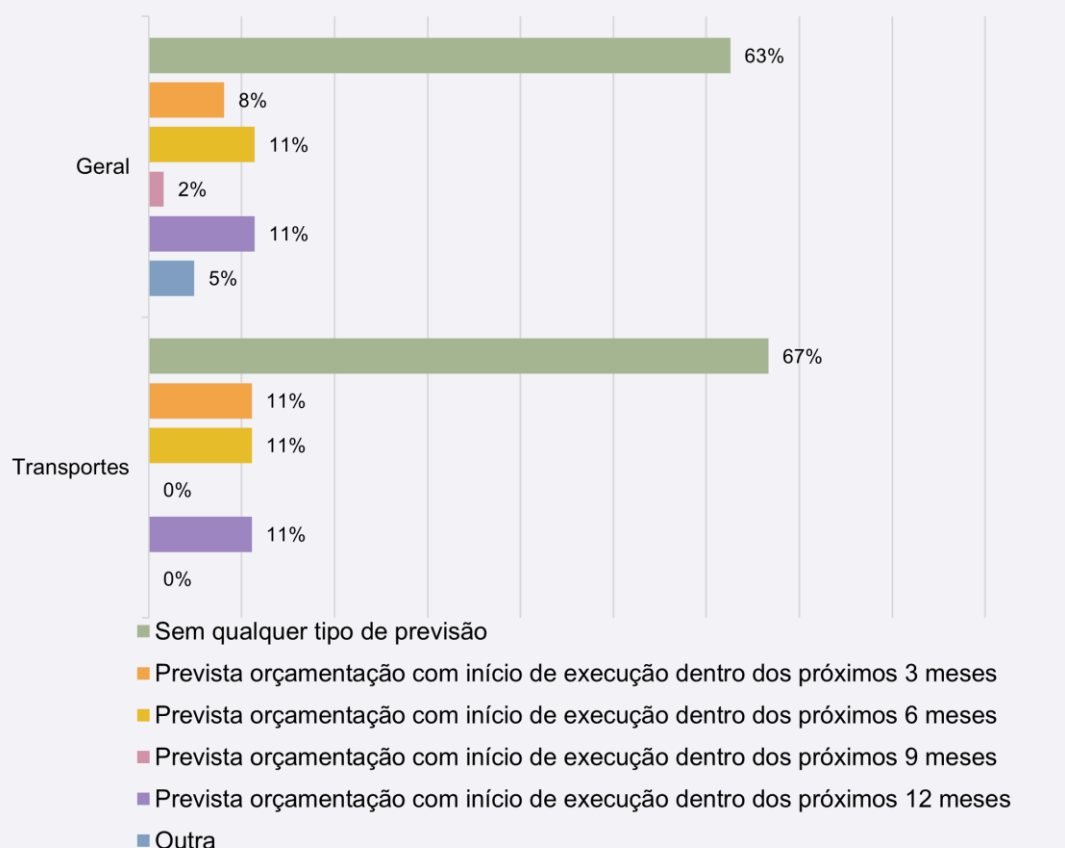


Gráfico 110.2 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 67% não tem qualquer previsão para a orçamentação, 11% tem previsto a orçamentação dentro dos próximos 3,6,9 ou 12 meses (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Transporte Aéreo

De acordo com o Relatório de Sustentabilidade de 2023 da TAP, foram dados cerca de oito temas relacionados com cibersegurança aos colaboradores através de formação *e-learning*. A TAP recebeu a aprovação da ANAC para a implementação de um novo dispositivo eletrónico que substituirá os antigos. Este sistema, que funciona como um *tablet* para os pilotos, facilitará a gestão do plano de voo, cálculos de desempenho e acesso a documentação operacional. Esta inovação impulsionará a transformação digital da empresa, permitindo a eliminação do papel, reduzindo o peso a bordo e, consequentemente, o consumo de combustível. Estes novos equipamentos serão gradualmente integrados, aumentando a resiliência, a fiabilidade e a cibersegurança das operações⁵⁴².

⁵⁴² TAP, "Relatório de Sustentabilidade de 2023", 48 e 64-65, <https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais>.

Durante 2023, a TAP lançou diversas iniciativas para transformar e aprimorar a cibersegurança com foco na redução da exposição a riscos externos e internos. No âmbito externo, a empresa restringiu o número de ativos disponíveis na internet e ampliou a implementação de MFA para o acesso a plataformas e aplicações. Em relação aos riscos internos, continuou o programa de combate à obsolescência que abrange aplicações, sistemas operacionais e plataformas. Foi ainda introduzido um processo mais rigoroso de verificação de identidades e houve um aumento gradual das configurações de segurança dos ativos⁵⁴³.

Transporte Marítimo e por vias navegáveis interiores

De acordo com o Plano de Formação para 2024 da DGRM irá existir uma formação de Cibersegurança com o total de sete horas e é destinado a chefes de divisão, inspetores de navios, coordenadores e assistentes técnicos, assim como uma formação em *Cloud Computing* com o total de três horas e destinado a técnicos superior e inspetores de navios⁵⁴⁴.

Segundo o Plano de Atividade de 2023 da DGRM, uma das principais iniciativas consiste em garantir, em colaboração com as áreas de informática e comunicação, a segurança e arquitetura das redes, assegurando que os serviços online estejam disponíveis 24 horas por dia, todos os dias⁵⁴⁵.

Transporte Ferroviário

O Relatório de Governo Societário de 2023 estabelece como diretriz a ampliação da eficiência, segurança e sustentabilidade dos processos. Isto inclui a otimização de processos críticos e o fortalecimento dos níveis de segurança. Além disso, a CP visa evoluir os seus sistemas e promover a transformação digital, modernizando as áreas mais estratégicas. Para alcançar estes objetivos, é essencial evoluir os sistemas *core*, reforçar a capacidade de captação e análise inteligente de dados, além de melhorar a experiência digital tanto para clientes como para colaboradores. No programa estratégico de 2022-2030, são destacados diversos projetos de transformação digital, como Produção Digital, Oficina Digital, CP *Digital Train*, Comboio 360, CP Segurança 360 e CP *NextGen*. Aproximadamente 2% do total de investimentos realizados pela CP em 2023 foram direcionados à informatização dos sistemas. No Plano de Atividades, estava previsto um investimento de cerca de 5,6 milhões de euros, dos quais foram aplicados 1 milhão⁵⁴⁶.

No Relatório de Contas Consolidado de 2023, é possível observar que o Metropolitano de Lisboa, ao reconhecer a crescente importância da cibersegurança, implementou melhorias nas suas condições de segurança digital e desenvolveu iniciativas destinadas a promover a cultura de segurança da informação dentro da empresa⁵⁴⁷.

⁵⁴³ TAP, "Relatório de Sustentabilidade 2023", 2024, 97, <https://www.tapairportugal.com/pt/-/media/Institucional/PDFs/Relatorios/2023/Relatorio-de-Sustentabilidade-TAP-2023.pdf?la=pt-PT&hash=A15B2D9DA1DBF21D101AFE8F24258F5DB60BAE98>.

⁵⁴⁴ DGRM, "Plano de Formação 2024", janeiro de 2024, 7, <https://www.dgrm.pt/documents/20143/714947/PlanoForma%C3%A7%C3%A3o2024.pdf/5a6f158d-257e-4aeb-68a7-9d5f8c46c329>.

⁵⁴⁵ DGRM, "Plano de Atividades 2023", 60, <https://www.dgrm.pt/documents/20143/714947/Plano+de+Atividades+da+DGRM+2023.pdf/53fb147c-46be-7094-77f5-af80a530dcad>.

⁵⁴⁶ Comboios de Portugal, "Relatório do Governo Societário 2023", maio de 2024, 48 e 56, https://www.cp.pt/StaticFiles/Institucional/1_a_empresa/3_Relatorio_Contas/2023/relatorio-governo-societario-2023.pdf.

⁵⁴⁷ Metropolitano de Lisboa, "Relatório Consolidado 2023", junho de 2024, 8, https://www.metrolisboa.pt/institucional/wp-content/uploads/sites/2/2024/08/Relatorio_Consolidado_2023.pdf.

Transporte Rodoviário

No relatório do Governo Societário de 2023, observamos a contratação de serviços de consultoria em informática⁵⁴⁸. O Relatório e Contas de 2023 revelou um aumento no licenciamento de *software*, com um total aproximado de 2 milhões de euros⁵⁴⁹. De acordo com o Plano de Atividades de 2024, irá ocorrer um investimento de cerca de 3,5 milhões de euros em 2024 e 5 milhões de euros até 2027. Estes recursos serão alocados especificamente em três projetos⁵⁵⁰:

- Projeto «C-Streets» – Contagem de passageiros, paragens digitais e prioridade semafórica;
- Desenvolvimento de software;
- Adição de novos meios de pagamento.

Segundo o Relatório e Contas da Companhia Carris de Ferro de Lisboa, E.M., S.A., em 2022 foi realizado um investimento de 368 mil euros com o objetivo de melhorar os sistemas informáticos⁵⁵¹.

De acordo com o plano de atividades e orçamento para os anos de 2024 a 2027 da mesma entidade, estão previstos para a área de informática os seguintes valores⁵⁵².

- 3 521 500€ para 2024;
- 910 000€ para 2025;
- 290 000€ para 2026;
- 490 000€ para 2027.

Para além da Carris, também a STCP, EIM, SA previu investir, em equipamento informático, entre 2021 e 2027, 2,382 milhões de euros⁵⁵³.

⁵⁴⁸ Carris, “Relatório Governo Societário 2023”, março 2024, 87, <https://www.carris.pt/media/3g1lrm01/relatorio-governo-societario-2023.pdf>.

⁵⁴⁹ Carris, “Relatório e Contas 2023”, 116, <https://www.carris.pt/media/lwsixqty/relatorio-e-contas-2023.pdf>.

⁵⁵⁰ Carris, “Plano de Atividades e Orçamento 2024”, 20-22, https://www.carris.pt/media/4duh1ymp/carris_pao-2024-2027.pdf.

⁵⁵¹ Carris, “Relatório e Contas 2022”, 61.

⁵⁵² Carris, “Plano de Atividades e Orçamento 2024”, 20.

⁵⁵³ Sociedade de Transportes Colectivos do Porto (STCP) “Instrumentos Previsionais de Gestão 2023-2027”, 12 de setembro de 2022, 11.

2.5. RJSC e legislação setorial

Os OSE dos quatro subsectores do setor transportes estão sujeitos a diversos diplomas legais europeus e nacionais que impõem obrigações em matéria de cibersegurança para além do RJSC. Ver-se-á, de seguida, qual a legislação relevante nesta matéria para cada um dos subsectores abrangidos.

Transporte aéreo

Tal como referido na contextualização setorial, o setor da aviação e do transporte aéreo viria a ser alvo de uma profunda reforma ao nível da segurança após o ataque de 11 de setembro de 2001 nos EUA. Foi no seguimento desse ataque que o Parlamento e Conselho Europeu publicaram, a 16 de dezembro de 2002, o Regulamento (CE) n.º 2320/2002, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil⁵⁵⁴. Embora este Regulamento não versasse sobre cibersegurança, assumiu um papel pioneiro na segurança da aviação civil e dos aeroportos, abrangendo o controlo dos passageiros, carga, formação e controlo do pessoal envolvido, desde os trabalhadores nos aeroportos ao pessoal de cabine dos voos⁵⁵⁵.

Este regulamento viria a ser revogado pelo Regulamento (CE) n.º 300/2008, de 11 de março⁵⁵⁶ e, este, posteriormente revogado pelo Regulamento (UE) n.º 185/2010, de 4 de março⁵⁵⁷, ambos ainda sem menções específicas à cibersegurança, segurança informática ou outras expressões associadas. Seria apenas com o Regulamento de Execução (UE) 2015/1998, de 5 de novembro de 2015, que já se veriam menções à proteção contra ciberameaças e ciberataques dos sistemas e dados críticos da informação e das comunicações da aviação civil. Segundo o mesmo, os operadores aeroportuários e as transportadoras aéreas devem identificar e proteger os seus sistemas e dados críticos das tecnologias da informação e das comunicações contra ciberataques que possam afetar a segurança da aviação⁵⁵⁸. Devem também possuir programas de segurança que identifiquem esses sistemas e dados críticos, as medidas destinadas a proteger os mesmos contra ciberataques, bem como para detetar os ataques, e responder e recuperar dos mesmos. Tais medidas devem ser desenvolvidas e aplicadas partindo de uma avaliação dos riscos efetuadas pelas entidades visadas⁵⁵⁹. Embora o Regulamento date de 2015, as provisões relacionadas com cibersegurança foram introduzidas apenas a 25 de setembro de 2019, através daquela que era já a oitava emenda ao Regulamento⁵⁶⁰.

⁵⁵⁴ Regulamento (CE) n.º 2320/2002 do Parlamento Europeu e do Conselho de 16 de dezembro de 2002 relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil, *Jornal Oficial das Comunidades Europeias*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002R2320>.

⁵⁵⁵ Regulamento (CE) n.º 2320/2002, Anexo, 8.

⁵⁵⁶ Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho de 11 de março de 2008 relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002, *Jornal Oficial da União Europeia*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008R0300>.

⁵⁵⁷ Regulamento (UE) n.º 185/2010 da Comissão de 4 de março de 2010 que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação, *Jornal Oficial da União Europeia*, 5 de março de 2010, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02010R0185-20140131>.

⁵⁵⁸ Regulamento de Execução (UE) 2015/1998 da Comissão de 5 de novembro de 2015 que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação, *Jornal Oficial da União Europeia*, versão atualizada a 1 de setembro de 2024, 13, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02015R1998-20240901>.

⁵⁵⁹ Regulamento de Execução (UE) 2019/1583 da Comissão de 25 de setembro de 2019 que altera o Regulamento de Execução (UE) 2015/1998 da Comissão que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação, no que respeita às medidas de cibersegurança, Anexo, *Jornal Oficial da União Europeia*, 26 de setembro de 2019, 17, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R1583>.

⁵⁶⁰ Regulamento de Execução (UE) 2015/1998, 1-2.

O Regulamento foi, até ao momento, alvo de 18 emendas sobre variados temas, desde a harmonização de regras ao reconhecimento de medidas de segurança equivalentes implementadas por países terceiros (não pertencentes à União Europeia)⁵⁶¹.

O Regulamento (UE) n.º 376/2014, de 3 de abril, relativo à comunicação, à análise e ao seguimento de ocorrências na aviação civil, impôs no setor a obrigação da comunicação de ocorrências relacionadas com a operação das aeronaves, com os serviços e as instalações de navegação aérea e com os aeródromos e os serviços de terra, nas quais se incluem o mau funcionamento de sistemas, sejam eles de comunicação, de navegação, ou de outro foro operacional⁵⁶².

A nível nacional, o principal diploma setorial é o Decreto-Lei n.º 142/2019, de 19 de setembro, que aprova o Programa Nacional de Segurança da Aviação Civil (PNSAC). Embora não inclua medidas específicas sobre cibersegurança, o PNSAC determina que “relativamente à área da cibersegurança (...), a regulamentação, pública e não pública, do PNSAC, a emitir é efetuada pelo CNCS, enquanto Autoridade Nacional de Cibersegurança, em articulação com a Autoridade Nacional da Aviação Civil (ANAC)”⁵⁶³. A par do PNSAC, existe ainda o Programa Nacional de Segurança Operacional da Aviação (PNSOA) que, embora não tenha caráter de lei, orienta a atuação dos intervenientes na aviação em Portugal ao nível da segurança. Quanto à cibersegurança, o PNSOA estabelece que “a utilização de meios tecnológicos e dispositivos conectados entre si através da Internet, aumentam a exposição ao risco e a ameaças no ciberespaço, que devem ser endereçadas de forma preventiva, através de uma abordagem de gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam”⁵⁶⁴ e que, por isso, as entidades reguladoras e todos prestadores de serviço devem ser alvo de “workshops ou outros eventos similares para interagir diretamente com as partes interessadas, relativamente às medidas de cibersegurança a adotar na indústria”⁵⁶⁵.

Transporte marítimo e por vias navegáveis interiores

Um importante documento ao nível da segurança no subsector do transporte marítimo é o Código ISPS (International Ships and Ports Security) adotado pela Organização Marítima Internacional em 2002. A sua consulta é, no entanto, restrita, mas diversas disposições do mesmo têm sido acolhidas pelo Direito europeu através de regulamentos e diretivas. Um exemplo desse acolhimento é o Regulamento (CE) n.º 725/2004, de 31 de março, que inclui múltiplas referências ao Código ISPS⁵⁶⁶. Este Regulamento impôs diversas obrigações, como a de realizar avaliações da proteção dos navios e da proteção da instalação portuária, e que estas devem abordar elementos como os “sistemas de rádio e telecomunicações, incluindo os sistemas e redes informáticos”⁵⁶⁷.

⁵⁶¹ “Texto consolidado: Regulamento de Execução (UE) 2015/1998 da Comissão, de 5 de novembro de 2015, que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação”, *Eur-Lex*, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02015R1998-20240901>.

⁵⁶² Regulamento (UE) n.º 376/2014 do Parlamento Europeu e do Conselho de 3 de abril de 2014 relativo à comunicação, à análise e ao seguimento de ocorrências na aviação civil, que altera o Regulamento (UE) n.º 996/2010 do Parlamento Europeu e do Conselho e revoga a Diretiva 2003/42/CE do Parlamento Europeu e do Conselho, e os Regulamentos (CE) n.º 1321/2007 e (CE) n.º 1330/2007 da Comissão, artigo 4.º, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0376&qid=1691222818840>.

⁵⁶³ Decreto-Lei n.º 142/2019, de 19 de setembro, artigo 2.º, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/142-2019-124831327>.

⁵⁶⁴ ANAC, “Plano Nacional de Segurança Operacional da Aviação 2022-2024: Revisão 1”, março de 2024, 50, https://www.anac.pt/SiteCollectionDocuments/PNSO/PNSOA_2022_2024_rev_1.pdf.

⁵⁶⁵ ANAC, “Plano Nacional de Segurança”, 49.

⁵⁶⁶ Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho de 31 de março de 2004 relativo ao reforço da proteção dos navios e das instalações portuárias, *Jornal Oficial da União Europeia*, 29 de abril de 2004, 6-7, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:PT:PDF>.

⁵⁶⁷ Regulamento (CE) n.º 725/2004, Apêndice 2, 8.3.5.

Das avaliações realizadas devem depois resultar planos de proteção dos navios e das instalações portuárias, que devem também versar sobre as medidas adotadas para a proteção desses mesmos sistemas⁵⁶⁸.

Em 2005, foi publicada a Diretiva 2005/65/CE, de 26 de outubro, relativa ao reforço da segurança nos portos⁵⁶⁹. Esta Diretiva voltava a impor a obrigação de realizar avaliações de segurança dos portos, e previa ainda a ligação com os sistemas de informação das autoridades responsáveis pelo controlo da carga, das bagagens e dos passageiros⁵⁷⁰. Seria depois transposta para o ordenamento jurídico português através do Decreto-Lei n.º 226/2006, de 15 de novembro⁵⁷¹.

Mais recentemente, foi publicado o Regulamento (UE) 2019/1239, de 20 de junho de 2019, que estabelece um ambiente europeu de plataforma única para o setor marítimo, revogando a Diretiva que vigorava desde 2010, relativa às formalidades de declaração exigidas aos navios à chegada e/ou à partida dos portos dos Estados-Membros⁵⁷². De forma resumida, o Regulamento de 2019 veio criar uma plataforma única para a transmissão dessas informações à chegada e à partida dos portos dentro da União. O Regulamento inclui provisões de segurança no que diz respeito ao registo e à gestão dos acessos dos utilizadores à plataforma, ao tratamento dos dados armazenados, alinhados com o Regulamento Geral sobre a Proteção de Dados, bem como requisitos sobre a harmonização das interfaces de acesso à plataforma entre os diferentes portos e Estados-membros⁵⁷³.

O subsetor do transporte marítimo conta ainda com o Decreto-Lei n.º 93/2020, de 3 de novembro, que estabelece regras de segurança aplicáveis a navios de passageiros e regras de tratamento de dados pessoais dos passageiros e que transpõe a Diretiva (UE) 2017/2108, a Diretiva (UE) 2017/2109 e a Diretiva (UE) 2017/2110⁵⁷⁴. Embora não se trate de um diploma dedicado à cibersegurança, o Decreto-Lei inclui algumas disposições relacionadas com essa matéria. Por exemplo, é exigido que os navios possuam mecanismos de reposição das configurações iniciais em caso de avaria dos sistemas elétricos, eletrónicos e informáticos provocada por incêndios, e, a nível do tratamento de dados pessoais, é imposto que os sistemas de registo desses dados sejam aprovados e certificados pela Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM)⁵⁷⁵. A DGRM deve ainda proceder a verificações periódicas e aleatórias do correto funcionamento dos sistemas de registo de dados⁵⁷⁶.

⁵⁶⁸ Regulamento (CE) n.º 725/2004, Artigo 3.º, n.º 8.

⁵⁶⁹ Diretiva 2005/65/CE do Parlamento Europeu e do Conselho de 26 de outubro de 2005 relativa ao reforço da segurança nos portos, *Jornal Oficial da União Europeia*, 25 de novembro de 2005, 28, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:PT:PDF>.

⁵⁷⁰ Diretiva 2005/65/CE, Anexo II, 36.

⁵⁷¹ Decreto-Lei n.º 226/2006, de 15 de novembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/226-2006-544783>.

⁵⁷² Regulamento (UE) 2019/1239 do Parlamento Europeu e do Conselho de 20 de junho de 2019 que estabelece um ambiente europeu de plataforma única para o setor marítimo e que revoga a Diretiva 2010/65/UE, *Jornal Oficial da União Europeia*, 25 de julho de 2019, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R1239>.

⁵⁷³ Regulamento (UE) 2019/1239, artigos 5.º, 10.º e 12.º.

⁵⁷⁴ Decreto-Lei n.º 93/2020, de 3 de novembro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/93-2020-147432950>.

⁵⁷⁵ Decreto-Lei n.º 93/2020, artigo 29.º, n.º 2 e Capítulo II, Parte A, ponto 9.1.15.

⁵⁷⁶ Decreto-Lei n.º 93/2020, artigo 29.º, n.º 3.

Transporte ferroviário

O transporte ferroviário, tal como o rodoviário, tem como base legal a Lei de Bases do Sistema de Transportes Terrestres (Lei n.º 10/90, de 17 de março)⁵⁷⁷. Embora não haja referências específicas à cibersegurança na Lei de Bases, esta estipula que “a organização e funcionamento do sistema de transportes deverão ter (...) em conta (...) as necessidades de segurança da circulação dos transportes”⁵⁷⁸, nas quais se incluem as necessidades de cibersegurança, que é atualmente um aspeto incontornável da segurança dos transportes.

Mais tarde, no ano de 2001, foram publicadas três diretivas europeias relativas ao setor ferroviário: Diretiva 2001/12/CE, a Diretiva 2001/13/CE e a Diretiva 2001/14/CE. A mais relevante em termos de cibersegurança terá sido a Diretiva 2001/14/CE, que versava sobre a certificação de segurança das empresas de transporte ferroviário⁵⁷⁹. As três diretivas foram depois transpostas através do Decreto-Lei n.º 270/2003, de 28 de outubro, que especificava que para obter a certificação de segurança as empresas tinham de apresentar os “procedimentos, sistemas e equipamentos afetos em permanência para a realização, a monitorização e o controlo da execução da atividade de prestação de serviços de transporte ferroviário”⁵⁸⁰, bem como demonstrar a “forma como a empresa executa e mantém o sistema de gestão da segurança”⁵⁸¹ e demonstrar a “forma como a empresa controla a aplicação de regras técnicas de segurança e procedimentos para situações de emergência”⁵⁸².

Existe ainda o Regulamento de Execução (UE) 2023/1695 relativo à especificação técnica de interoperabilidade para os subsistemas de controlo-comando e sinalização do sistema ferroviário da União Europeia⁵⁸³, que serve de base legal a uma das tecnologias utilizadas pelo setor ferroviário – o ETCS (Sistema Europeu de Controlo dos Comboios e principal sistema de sinalização utilizado) – que inclui requisitos de segurança a adotar por parte dos operadores do sistema. Por exemplo, deve ser realizada “uma avaliação da integração segura de todos os componentes e interfaces internos e externos que constituem a arquitetura do subsistema ETCS ou do componente de interoperabilidade ETCS”⁵⁸⁴.

⁵⁷⁷ Lei n.º 10/90, de 17 de março, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/10-1990-333167>.

⁵⁷⁸ Lei n.º 10/90, artigo 2.º, n.º 3.

⁵⁷⁹ Diretiva 2001/14/CE do Parlamento Europeu e do Conselho de 26 de fevereiro de 2001 relativa à repartição de capacidade da infraestrutura ferroviária, à aplicação de taxas de utilização da infraestrutura ferroviária e à certificação da segurança, *Jornal Oficial das Comunidades Europeias*, 15 de março de 2001, 29, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001L0014>.

⁵⁸⁰ Decreto-Lei n.º 270/2003, de 28 de outubro, *Diário da República*, artigo 14.º, alínea l).

⁵⁸¹ Decreto-Lei n.º 270/2003, artigo 14.º, n.º 2, alínea n).

⁵⁸² Decreto-Lei n.º 270/2003, artigo 14.º, n.º 2, alínea o).

⁵⁸³ Regulamento de Execução (UE) 2023/1695 da Comissão de 10 de agosto de 2023 relativo à especificação técnica de interoperabilidade para os subsistemas de controlo-comando e sinalização do sistema ferroviário da União Europeia e que revoga o Regulamento (UE) 2016/919, *Jornal Oficial da União Europeia*, L, 8 de setembro de 2023, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023R1695>.

⁵⁸⁴ Regulamento de Execução (UE) 2023/1695, Anexo I, 4.2.1.1. Segurança, 399.

Transporte rodoviário

No subsetor do transporte rodoviário, a legislação específica do setor em matéria de cibersegurança incide principalmente sobre os sistemas de transportes inteligentes (STI). Foi nesse âmbito que surgiu, em 2010, a Diretiva 2010/40/UE⁵⁸⁵, que estabeleceu o quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário. Apesar de não se verificarem menções específicas à cibersegurança, a Diretiva incluía provisões dedicadas à necessidade de os Estados-membros protegerem, através da anonimização, os dados utilizados no quadro das aplicações e serviços STI, bem como provisões relativas à segurança dos sistemas de comunicações a bordo dos veículos⁵⁸⁶.

Anos mais tarde, em 2019, foi publicado o Regulamento (UE) 2019/2144, que incide sobre os requisitos de homologação dos veículos, componentes unidades técnicas e à sua segurança geral⁵⁸⁷. O Regulamento estipula que os fabricantes devem assegurar que “os veículos, sistemas componentes e unidades técnicas cumprem os requisitos aplicáveis relativos a (...) instrumentos de bordo, sistema elétrico, iluminação do veículo e proteção contra a utilização não autorizada, incluindo ataques cibernéticos”⁵⁸⁸. É também este Regulamento que estabelece requisitos aplicáveis aos veículos automatizados e veículos totalmente automatizados, devendo estes possuir:

- “a) Sistemas destinados a substituir o condutor no controlo do veículo, incluindo a sinalização, a direção, a aceleração e a travagem;
- b) Sistemas destinados a fornecer ao veículo informação em tempo real sobre o estado do veículo e a zona circundante;
- c) Sistemas de controlo da disponibilidade do condutor;
- d) Aparelhos de registo de eventos para veículos automatizados;
- e) Formato harmonizado para o intercâmbio de dados destinados, por exemplo, a um comboio de veículos de diferentes marcas;
- f) Sistemas destinados a fornecer informações de segurança aos outros utentes da estrada”⁵⁸⁹.

⁵⁸⁵ Diretiva 2010/40/UE do Parlamento Europeu e do Conselho de 7 de Julho de 2010 que estabelece um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte, *Jornal Oficial da União Europeia*, 6 de agosto de 2010, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010L0040>.

⁵⁸⁶ Diretiva 2010/40/EU, artigos 10.º, Anexo 1, 4.1.

⁵⁸⁷ Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho de 27 de novembro de 2019 relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) n.º 2015/166 da Comissão, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R2144>.

⁵⁸⁸ Regulamento (UE) 2019/2144, artigo 4.º, n.º 5, alínea d).

⁵⁸⁹ Regulamento (UE) n.º 2019/2144, artigo 11.º.

Âmbito geral

Para além dos diplomas setoriais, existe ainda legislação transversal aplicável ao setor dos transportes, tal como é o caso da Diretiva (UE) 2016/1148, ou Diretiva NIS, cuja transposição é feita através da Lei n.º 46/2018⁵⁹⁰, que a transpõe e que estabelece o RJSC, e o Decreto-Lei n.º 65/2021, que regulamenta Regime Jurídico da Segurança do Ciberespaço (RJSC)⁵⁹¹.

A par destes diplomas, é ainda de referir o Decreto-Lei n.º 20/2022, de 28 de janeiro, que veio atualizar o Regime Jurídico das Infraestruturas Críticas, estabelecido pelo Decreto-Lei n.º 62/2011, de 9 de maio e que visa os quatro subsectores de transportes no âmbito deste relatório. O diploma estabelece que “cada infraestrutura crítica nacional deve dispor de um plano de segurança”, que deve incluir, “a identificação dos elementos críticos; (...) uma análise do risco baseada em cenários de ameaça grave, na vulnerabilidade de cada elemento e nos impactos potenciais; a identificação, seleção e prioridade de contramedidas e procedimentos de segurança permanentes”, contramedidas essas que devem incluir “procedimentos de alerta e gestão de crises; normas de controlo de acesso e de verificação de segurança; ações de comunicação, sensibilização e formação (...) [e] soluções em matéria de cibersegurança, nos termos previstos do Decreto-Lei n.º 65/2021”⁵⁹², entre outros elementos.

Passados seis anos sobre a publicação da Diretiva NIS, foi publicada a Diretiva (UE) 2022/2555⁵⁹³, ou NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: “setores de importância crítica”⁵⁹⁴ e “outros setores críticos”⁵⁹⁵. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsectores. São também introduzidas novas obrigações.

Apesar da abrangência alargada da Diretiva NIS 2, o setor dos transportes não vê alargada essa abrangência. Continuam a ser visadas as mesmas entidades já abrangidas pela NIS 1. Quanto às novas obrigações decorrentes do diploma, a Diretiva NIS 2 reforça a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos⁵⁹⁶. Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto⁵⁹⁷.

⁵⁹⁰ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

⁵⁹¹ Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

⁵⁹² Decreto-Lei n.º 20/2022, de 28 de janeiro, Artigo n.º 13, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/20-2022-178264070>.

⁵⁹³ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

⁵⁹⁴ Diretiva (UE) 2022/2555, Anexo I.

⁵⁹⁵ Diretiva (UE) 2022/2555, Anexo II.

⁵⁹⁶ Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

⁵⁹⁷ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

A nova Diretiva encoraja ainda a que as entidades abrangidas estabeleçam, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como as relacionadas com “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”⁵⁹⁸.

⁵⁹⁸ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

2.6. Standards e boas práticas aplicáveis

De forma a combater a desinformação relativamente às ciberameaças no setor dos transportes, a Direção-Geral da Mobilidade e dos Transportes (DG MOVE) da Comissão Europeia procedeu à elaboração e publicação de um “conjunto de ferramentas para reforçar a sensibilização e preparação das partes interessadas do setor dos transportes para as ciberameaças”⁵⁹⁹. O objetivo principal deste documento é que diferentes intervenientes do setor - todo o pessoal envolvido nos transportes e decisores em matéria de cibersegurança nos diferentes modos de transporte - possam compreender as ciberameaças a que o setor se encontra exposto e reduzir o seu impacto através da formação e ação de todos.

Standards e boas práticas do setor de transporte aéreo

Aeroportos, companhias aéreas e fornecedores de serviços de navegação aérea recorrem principalmente a uma abordagem de segurança baseada em risco e confiam sobre *standards* internacionais de segurança da informação, como a ISO 27001 e NIST *Cybersecurity Framework*.

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor aéreo⁶⁰⁰:

Tabela 24 - Standards e Boas Práticas (Transportes Aéreo)

<i>Standards</i>	<i>Boas práticas</i>
• ICAO Aviation Security Manual - Document 8973 (Restricted Access); • ARINC 811 Commercial aircraft information security concepts of operations and process framework; • EUROCAE ED-201-204 Aeronautical Information System Security (AISS) Framework; • RTCA DO-326 Airworthiness security process specifications; • ISO 4170:1995; • ISO 6772:2012; • ISO 24113:2023.	• AIAA (The American institute of Aeronautics and Astronautics) The Connectivity Challenge: Protecting Critical Assets in a Networked World; • Information Security Certification and Accreditation (C&A) Handbook - FAA; • FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorized External Access; • FAA Aircraft systems information security protection overview.

⁵⁹⁹ Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, “Conjunto de ferramentas de cibersegurança para o setor dos transportes”, 2.

⁶⁰⁰ ENISA, “Mapping of OES Security Requirements to Specific Sectors”, 18 de janeiro de 2018, 20.

Na tabela anterior estão os *standards* e boas práticas referentes ao transporte aéreo. De seguida, apresenta-se um breve sumário de cada um:

- **ICAO Aviation Security Manual - Document 8973 (Restricted Access):** Fornece diretrizes para garantir a segurança da aviação civil, abordando avaliação de riscos, medidas preventivas e formação dos colaboradores⁶⁰¹;
- **ARINC 811 Commercial aircraft information security concepts of operations and process framework:** Aborda conceitos de operações e de processos para a segurança da informação em aeronaves comerciais⁶⁰².
- **EUROCAE ED-201-204 Aeronautical Information System Security (AISS) Framework:** É uma *framework* para a segurança dos Sistemas de Informação de Aeronáutica e aborda requisitos e práticas para proteger os dados e sistemas críticos⁶⁰³;
- **RTCA DO-326 Airworthiness security process specifications:** Estabelece especificações para processos de segurança relacionados com a aeronavegabilidade⁶⁰⁴;
- **ISO 4170:1995:** Conjunto de normas que definem métodos de teste para determinar a resistência à corrosão de materiais metálicos utilizados nas estruturas das aeronaves⁶⁰⁵;
- **ISO 6772:2012:** Conjunto de normas que definem métodos de teste para avaliar a resistência de materiais a produtos químicos, mais concretamente em relação à durabilidade e desempenho⁶⁰⁶;
- **ISO 24113:2023:** Fornece diretrizes para a avaliação e gestão de riscos relacionados com a segurança dos sistemas de informações aeronáuticos⁶⁰⁷;
- **AIAA (The American institute of Aeronautics and Astronautics) The Connectivity Challenge: Protecting Critical Assets in a Networked World:** Orientações de segurança num ambiente cada vez mais conectado. Estas orientações são focadas na proteção de ativos críticos na aviação e na exploração espacial⁶⁰⁸;
- **Information Security Certification and Accreditation (C&A) Handbook - FAA:** Guia para a certificação e acreditação de sistemas de informação neste setor. Este documento aborda processos e práticas necessárias para garantir que os sistemas são seguros⁶⁰⁹;
- **FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorized External Access:** Aborda a importância da segurança nos sistemas eletrónicos e tem como foco a proteção contra acessos não autorizados⁶¹⁰;
- **FAA Aircraft systems information security protection overview:** Aborda as práticas necessárias para proteger dados críticos, assim como a identificação de vulnerabilidades e a implementação de medidas de proteção⁶¹¹.

⁶⁰¹ ICAO, "Aviation Security Manual (Doc 8973 – Restricted)", <https://www.icao.int/security/sfp/pages/securitymanual.aspx>.

⁶⁰² SAE International, "COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK ARINC811", dezembro de 2005, <https://www.sae.org/standards/content/arinc811/>.

⁶⁰³ EUROCAE, "ED-201A - Aeronautical Information System Security (AISS) Framework Guidance", dezembro de 2021, <https://www.eurocae.net/news/posts/2021/december/ed-201a-aeronautical-information-system-security-aiiss-framework-guidance/>.

⁶⁰⁴ RTCA, "Introducing RTCA's Security Standards and Training Partnership", <https://www.rtca.org/security/>.

⁶⁰⁵ ISO, "ISO 4170:1995", <https://www.iso.org/standard/20263.html>.

⁶⁰⁶ ISO, "ISO 6772:2012", <https://www.iso.org/standard/54516.html>.

⁶⁰⁷ ISO, "ISO 24113:2023", <https://www.iso.org/standard/83494.html>.

⁶⁰⁸ AIAA, "A Framework for Aviation Cybersecurity", agosto de 2013, 7, https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/aiaa-cyber-framework-final.pdf?sfvrsn=7bd09ec9_0.

⁶⁰⁹ United States Department of Education, "Handbook OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures", março de 2006, <https://www.ed.gov/media/document/acshbocio05doc>.

⁶¹⁰ Department of Transportation FAA, "Aviation Rulemaking Advisory Committee-New Task", fevereiro de 2015, https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf.

⁶¹¹ Peter Skaves, "FAA Aircraft Systems Information Security Protection (ASISP) Overview", Federal Aviation Administration, abril de 2015, <https://ieeexplore.ieee.org/iel7/7118533/7121207/07121273.pdf>.

Standards e boas práticas do setor de transporte ferroviário

A principal preocupação neste setor concentra-se na segurança física e mecânica, em vez de lidar diretamente com os aspetos de cibersegurança que possam interferir diretamente na segurança e proteção de sistemas de sinalização e/ou controlo destes transportes.

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor dos transportes ferroviários⁶¹².

Tabela 25 - Standards e Boas Práticas (Transportes Ferroviário)

Standards	Boas práticas
• ISO 27001: Information technology - Security techniques - Information security management systems – Requirements; • ANSI/ISA, Series “ISA-62443: Security for industrial automation and control system”; • ISO 20138-2:2019; • ISO 22163:2023; • ISO 22888:2020; • ISO 27002 e 27005; • ISA/IEC 62443; • CLC/TS 50701.	• UK Rail Cyber Security Guidance to Industry; • NIS Directive Cooperation Group guidelines.

⁶¹² ENISA, “Mapping of OES Security Requirements”, 23.

Na tabela anterior estão os *standards* e boas práticas referentes ao transporte ferroviário. De seguida, apresenta-se um breve sumário de cada um:

- **ISO 27001: Information technology - Security techniques - Information security management systems – Requirements:** Conjunto de normas e requisitos para um Sistema de gestão de segurança. Estas normas têm como objetivo proteger a integridade, disponibilidade e confidencialidades das informações⁶¹³;
- **ANSI/ISA, Series “ISA-62443: Security for industrial automation and control system”:** Fornece diretrizes para a segurança dos sistemas de automatização industrial e aborda a proteção contra incidentes de cibersegurança assim como estabelece uma *framework* para identificar e mitigar os riscos⁶¹⁴.
- **ISO 20138-2:2019:** Conjunto de normas que definem métodos para a gestão de informações em projetos de construção ferroviária, com foco na interoperabilidade e troca de dados entre as diferentes partes interessadas⁶¹⁵;
- **ISO 22163:2023:** Específica os requisitos para os sistemas de gestão da qualidade nos transportes ferroviários e tem como objetivo aumentar a eficiência e a confiabilidade das operações⁶¹⁶;
- **ISO 22888:2020:** Específica os requisitos para a gestão de risco em projetos de construção ferroviária⁶¹⁷;
- **ISO 27002 e 27005:** A ISO 27002 é focada em estabelecer, implementar, manter e melhorar a gestão da informação e a ISO 27005 é focada na gestão de risco⁶¹⁸;
- **ISA/IEC 62443:** É uma norma que aborda a cibersegurança nos sistemas de controlo e fornece diretrizes para proteger a rede e os sistemas contra ameaças⁶¹⁹;
- **CLC/TS 50701:** É uma norma técnica que fornece informações de cibersegurança nos sistemas do transporte ferroviário⁶²⁰;
- **UK Rail Cyber Security Guidance to Industry:** Estabelece orientações sobre cibersegurança para a indústria ferroviária, assim como proteger sistemas e dados contra ameaças de cibersegurança⁶²¹;
- **NIS Directive Cooperation Group guidelines:** Documento que resume as principais descobertas sobre medidas de cibersegurança para OSE⁶²².

⁶¹³ ISO, “ISO/IEC 27001:2022”, <https://www.iso.org/standard/27001>.

⁶¹⁴ ISA, “ISA/IEC 62443 Series of Standards”, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.

⁶¹⁵ ISO, “ISO 20138-2:2019”, <https://www.iso.org/standard/68443.html>.

⁶¹⁶ ISO, “ISO 22163:2023”, <https://www.iso.org/standard/79427.html>.

⁶¹⁷ ISO, “ISO 22888:2020”, <https://www.iso.org/standard/74080.html>.

⁶¹⁸ ENISA, “Railway Cybersecurity”, 11.

⁶¹⁹ ISA, “ISA/IEC 62443 Series of Standards”, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.

⁶²⁰ European Standards, “CLC/TS 50701:2023”, <https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/?srsltid=AfmBOorDKQDhbsSznI-J4WKrvDMc6xbxHRStGpKIGvUiP344XdenbQwR>.

⁶²¹ Department of Transport, “Rail Cyber Security Guidance to Industry”, fevereiro 2016,

<https://assets.publishing.service.gov.uk/media/5efcace9e90e075c52d05a94/rail-cyber-security-guidance-to-industry-document.pdf>.

⁶²² ENISA, “Railway Cybersecurity”, 11.

Standards e boas práticas do setor de transporte marítimo e por vias navegáveis interiores

A elevada complexidade dos sistemas de TIC que suportam as operações marítimas, desde a gestão portuária até a comunicação do navio, e a aplicabilidade de várias tecnologias de TIC, exigem uma maior consideração holística em matéria de cibersegurança que ainda não é assegurada.

A tabela seguinte sumariza os *standards* e boas práticas aplicados ao setor marítimo⁶²³:

Tabela 26 - Standards e Boas Práticas (Transporte Marítimo)

Standards	Boas práticas
• International Safety Management (ISM) Code; • IMO interim guidelines on maritime cyber risk management; • International Ship and Port Facility Security (ISPS) Code; • ISO 27001— Information security management systems; • ANSI/ISA, Series “ISA-62443: Security for industrial automation and control system; • IEC 62351:2017 SER - Power systems management and associated information exchange - Data and communications security; • IEC 61162 - Digital interfaces for navigational equipment within a ship; • ISO 13613:2011 - Ships and marine technology - Maintenance and testing to reduce losses in critical systems for propulsion; • ISO 14885:2014 - Large yachts - Diesel engines for main propulsion and essential auxiliaries - Safety requirements.	• BIMCO Guidelines on Cyber Security on board Ships - The Guidelines on Cyber security on board ships; • DNVGL-RP-0496 (DNV-GL, 2016): Cybersecurity resilience management for ships and mobile offshore units in operation; • Cyber-enabled ships: ShipRight procedure – autonomous ships; • Cyber-enabled ships: Deploying information and communications technology in shipping – Lloyd’s Register’s approach to assurance: • United States coast guard – Cyber Strategy Draft guidelines on maritime cyber risk management; • Tanker Management and Self Assessment 3 - OCIMF.

⁶²³ ENISA, “Mapping of OES Security Requirements”, 23-24.

Na tabela anterior estão os *standards* e boas práticas referentes ao transporte marítimo e por vias navegáveis interiores. De seguida, apresenta-se um breve sumário de cada um:

- **International Safety Management (ISM) Code:** Estabelece diretrizes para garantir a segurança operacional e a proteção ambiental nos navios e nas empresas marítimas⁶²⁴;
- **IMO interim guidelines on maritime cyber risk management:** É uma *framework* onde é possível os operadores marítimos identificarem, avaliarem e gerirem os riscos relacionados com a cibersegurança⁶²⁵.
- **International Ship and Port Facility Security (ISPS) Code:** Estabelece medidas de segurança para proteger navios e portos contra atos de interferência ilícita⁶²⁶;
- **ISO 27001— Information security management systems:** Conjunto de normas e requisitos para um Sistema de gestão de segurança. Estas normas têm como objetivo proteger a integridade, disponibilidade e confidencialidades das informações⁶²⁷;
- **ANSI/ISA, Series “ISA-62443: Security for industrial automation and control system”:** Fornece diretrizes para a segurança dos sistemas de automatização industrial e aborda a proteção contra incidentes de cibersegurança assim como estabelece uma *framework* para identificar e mitigar os riscos⁶²⁸;
- **IEC 62351:2017 SER - Power systems management and associated information exchange - Data and communications security:** Aborda a segurança dos dados e comunicações nos sistemas de gestão de energia e estabelece os requisitos para proteger a integridade, confidencialidade e disponibilidade das informações⁶²⁹;
- **IEC 61162 - Digital interfaces for navigational equipment within a ship:** Define padrões para as interfaces digitais nos equipamentos de navegação a bordo de navios⁶³⁰;
- **ISO 13613:2011 - Ships and marine technology - Maintenance and testing to reduce losses in critical systems for propulsion:** Orientações para a manutenção e testes de sistemas críticos de propulsão em navios⁶³¹;
- **ISO 14885:2014 - Large yachts - Diesel engines for main propulsion and essential auxiliaries - Safety requirements:** Define requisitos de segurança para motores a diesel utilizados em grandes iates, tanto para propulsão principal como para auxiliar⁶³²;
- **BIMCO Guidelines on Cyber Security on board Ships - The Guidelines on Cyber security on board ships:** É uma *framework* sobre cibersegurança a bordo de navios e enfatiza a importância estratégica de uma gestão de riscos de cibersegurança⁶³³;
- **DNVGL-RP-0496 (DNV-GL, 2016): Cybersecurity resilience management for ships and mobile offshore units in operation:** Aborda a gestão da resiliência de cibersegurança para navios e unidades móveis *offshore*⁶³⁴;
- **Cyber-enabled ships: ShipRight procedure – autonomous ships:** Aborda as diretrizes de segurança para embarcações autónomas, focando-se na integração de tecnologias de cibersegurança⁶³⁵;

⁶²⁴ Clarksons, “What is the International Safety Management Code?”, <https://www.clarksons.com/glossary/international-safety-management-code>.

⁶²⁵ IMO, “Maritime cyber risk”, <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>.

⁶²⁶ LR, “ISPS Code”, <https://www.lr.org/en/services/statutory-compliance/isps-code>.

⁶²⁷ ISO, “ISO/IEC 27001:2022”.

⁶²⁸ ISA, “ISA/IEC 62443 Series of Standards”.

⁶²⁹ IEC, “IEC 62351-7”, <https://webstore.iec.ch/en/publication/30593>.

⁶³⁰ IEC, “IEC 61162-1:2024”, <https://webstore.iec.ch/en/publication/72729>.

⁶³¹ ISO, “ISO 13613:2011”, <https://www.iso.org/standard/54090.html>.

⁶³² ISO, “ISO 14885:2014”, <https://www.iso.org/standard/55259.html>.

⁶³³ BIMCO, “The Guidelines on Cyber Security Onboard Ships”, <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>.

⁶³⁴ DNV GL, “Cyber security resilience management for ships and mobile offshore units in operation”, setembro de 2016, <https://www.dnv.com/siteassets/images/pdf-documents/dnv-gl-rp-0496.pdf>.

⁶³⁵ LR, “Out of the box – Implementing autonomy and assuring AI”, <https://www.lr.org/en/knowledge/research-reports/2023/ai-and-autonomy/?creative=708188340864>.

- **Cyber-enabled ships: Deploying information and communications technology in shipping – Lloyd’s Register’s approach to assurance:** Discute a implementação de tecnologias de informação e comunicação no setor marítimo⁶³⁶;
- **United States coast guard – Cyber Strategy Draft guidelines on maritime cyber risk management:** Aborda a gestão de riscos de cibersegurança no setor marítimo⁶³⁷;
- **Tanker Management and Self Assessment 3 – OCIMF:** É uma *framework* com o objetivo de melhorar a gestão de navios *tank*⁶³⁸;

Standards e boas práticas do setor de transporte rodoviário

Várias iniciativas levaram à definição de diretrizes ou regras para implementar a segurança na indústria automóvel. As considerações de segurança e proteção têm como responsável o comité TC22/SC3/WG16 sob o desenvolvimento da ISO 26262.

⁶³⁶ LR, “Revised update of LR’s Cyber-enabled ships ShipRight procedure”, dezembro de 2017, <https://www.lr.org/en/knowledge/press-room/press-listing/press-release/2017/early-adopters-and-innovators-in-connected-assets-on-ships/>.

⁶³⁷ DCO, “Cyber Risk Management in the Maritime Transportation System”, <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Commercial-Regulations-standards-CG-5PS/Design-Engineering-Standards/Systems-Engineering-Division/Cyber-Risk-Management/>.

⁶³⁸ OCIMF, “Tanker Management and Self Assessment 3 - A Best Practice Guide”, <https://www.ocimf.org/pt/publications-advocacy-5/publica%C3%A7%C3%B5es/livros/tanker-management-and-self-assessment-3>.

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor dos transportes rodoviários⁶³⁹:

Tabela 27 - Standards e Boas Práticas (Transporte Rodoviário)

<i>Standards</i>	<i>Boas práticas</i>
• SAE J3061 Cybersecurity Guidebook for Cyber - Physical Vehicle Systems; • SAE J3101 - Requirements for Hardware- Protected Security for Ground Vehicle Applications (WiP); • ISO 15031: Road Vehicles - Communication between vehicle and external equipment for emissions-related diagnostics. Part 7: Data link security; • ISO 15764: Road Vehicles - Extended data link security; ISO/AWI 21434 - Road Vehicles - Automotive Security Engineering; • ISO 26262-1:2011 - Road vehicles - Functional safety; • TS 102 940: Intelligent Transport Systems (ITS), Security, ITS communications security; architecture and security management; • TS 103 096-1 to TS 103 096-3: Intelligent Transport Systems (ITS); • TR 103 061-6 Intelligent Transport Systems (ITS), Testing, Conformance test specifications for ITS Security.	• ENISA Cyber Security and Resilience of smart cars; • Auto ISAC, Automotive Information Sharing and Analysis Center, Best Practices; • Five Star Automotive Cyber Safety Program, I Am The Cavalry;

⁶³⁹ ENISA, "Mapping of OES Security Requirements", 27.

Na tabela anterior estão os *standards* e boas práticas referentes ao transporte rodoviário. De seguida, apresenta-se um breve sumário de cada um:

- **SAE J3061 Cybersecurity Guidebook for Cyber - Physical Vehicle Systems:** Guia que aborda a cibersegurança em veículos. O objetivo é garantir a proteção dos sistemas e dos dados⁶⁴⁰;
- **SAE J3101 - Requirements for Hardware- Protected Security for Ground Vehicle Applications (WiP):** Estabelece requisitos para a segurança no *hardware* dos veículos⁶⁴¹;
- **ISO 15031: Road Vehicles - Communication between vehicle and external equipment for emissions-related diagnostics. Part 7: Data link security:** Aborda a comunicação entre os veículos e os equipamentos externos para diagnósticos relacionados com as emissões⁶⁴²;
- **ISO 15764: Road Vehicles - Extended data link security:** Define os padrões na segurança da ligação de dados nos veículos rodoviários⁶⁴³;
- **ISO/AWI 21434 - Road Vehicles - Automotive Security Engineering:** Aborda a identificação de riscos, avaliações de segurança e implementação de medidas de proteção ao longo do ciclo de vida do veículo⁶⁴⁴;
- **ISO 26262-1:2011 - Road vehicles - Functional safety:** Aborda a segurança funcional nos veículos rodoviários⁶⁴⁵;
- **TS 102 940: Intelligent Transport Systems (ITS), Security, ITS communications security; architecture and security management:** Norma técnica que aborda a segurança das comunicações dos sistemas dos veículos⁶⁴⁶;
- **TS 103 096-1 to TS 103 096-3: Intelligent Transport Systems (ITS):** Norma que aborda a cibersegurança dos veículos com conectividade à internet, abordando a gestão de riscos e a proteção dos dados⁶⁴⁷;
- **TR 103 061-6 Intelligent Transport Systems (ITS), Testing, Conformance test specifications for ITS Security:** É uma norma técnica que fornece as diretrizes para a implementação das medidas de segurança e a avaliação de vulnerabilidades em sistemas automobilísticos⁶⁴⁸;
- **ENISA Cyber Security and Resilience of smart cars:** Aborda os desafios e riscos associados à conectividade nos veículos modernos⁶⁴⁹;
- **Auto ISAC, Automotive Information Sharing and Analysis Center, Best Practices:** Centro de partilha e análise de informações com o objetivo de fortalecer a cibersegurança na indústria automobilística⁶⁵⁰;
- **Five Star Automotive Cyber Safety Program, I Am The Cavalry:** Tem como objetivo melhorar a cibersegurança na indústria automobilística através de avaliações e certificações de veículos⁶⁵¹;

⁶⁴⁰ SAE International, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", junho de 2016, 13, https://nmi.org.uk/wp-content/uploads/2016/6/4_SAE-J3061-and-friends-for-NMI-Jun-16.pdf.

⁶⁴¹ SAE International, "Hardware Protected Security for Ground Vehicles", https://www.sae.org/standards/content/j3101_202002/.

⁶⁴² ISO, "ISO 15031-7:2013", <https://www.iso.org/standard/62489.html>.

⁶⁴³ ISO, "ISO 15764:2004", <https://www.iso.org/standard/28775.html>.

⁶⁴⁴ ISO, "ISO/SAE 21434:2021", <https://www.iso.org/standard/70918.html>.

⁶⁴⁵ ISO, "ISO 26262-1:2011", <https://www.iso.org/standard/43464.html>.

⁶⁴⁶ ETSI, "Intelligent Transport Systems (ITS)", <https://cdn.standards.iteh.ai/samples/59261/357d2dcaa38c4977b9b395c643b2114c/ETSI-TS-102-940-V2-1-1-2021-07-.pdf>.

⁶⁴⁷ ETSI, "ETSI TS 103 096-3", https://www.etsi.org/deliver/etsi_ts/103000_103099/10309603/01.04.01_60/ts_10309603v010401p.pdf.

⁶⁴⁸ ETSI, "ETSI TR 103 061-6", https://www.etsi.org/deliver/etsi_tr/103000_103099/10306106/01.01.01_60/tr_10306106v010101p.pdf.

⁶⁴⁹ ENISA, "Cyber Security and Resilience of smart cars", <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>.

⁶⁵⁰ ISAC, "Best Practices", <https://automotiveisac.com/best-practices>.

⁶⁵¹ I am the cavalry, "Five Star Automotive Cyber Safety Framework", <https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf>.

2.7. Desafios

Transporte Aéreo

No contexto do subsetor de transporte aéreo, observa-se uma tendência crescente de interconectividade através da tecnologia digital responsável pela otimização de recursos e com o objetivo de aumento de eficiência. Este aumento na dependência dos aeroportos relativamente a serviços de computador ligados à internet faz com que o aumento de exposição a novas ameaças aconteça de forma (muito) mais rápida, tornando-se este controlo o principal desafio para o setor. Outro grande desafio que causa a exposição a mais vulnerabilidades que podem causar ciberataques e, em consequência, colocar em risco a segurança do setor, é a crescente utilização de recursos de comunicação abertas e não criptografadas (tais como comunicação de tráfego aéreo entre postos e aeronaves)⁶⁵².

Atualmente, em alguns aeroportos, ainda persistem práticas inadequadas na gestão de *passwords* como a partilha ou a reutilização da mesma, a ausência de um centro para a gestão de incidentes e um baixo nível na sensibilização relativamente à cibersegurança. Como mencionado anteriormente, o avanço rápido da tecnologia, aliado à lentidão dos processos legislativos, pode resultar em graves lacunas jurídicas nos futuros aeroportos inteligentes⁶⁵³.

Os aeroportos estão a alterar a maneira de como implementam e projetam a infraestrutura de rede e gerem os seus fornecedores. Esta mudança pode comprometer a sua segurança pois resulta em várias redes *ICT (Information and Communications Technology)* a serem operadas, onde algumas destas redes o próprio aeroporto não tem acesso. Isto cria um cenário de cibersegurança com uma superfície de ataque grande e complexa. Esta complexidade e a ausência de modelos de referência da arquitetura de TI indicam uma lacuna nas diretrizes deste setor. Deve ser criado um modelo e, este, deve considerar a crescente transferência de aeroportos para a gestão privada, a fragmentação dos prestadores de serviços e definir uma segregação entre redes críticas e não críticas⁶⁵⁴.

Outro grande desafio é a criação de uma plataforma que permita aos aeroportos partilhar dados com as autoridades aeroportuárias e com os governos nacionais. Esta plataforma de partilha de dados iria possibilitar a troca de informações sobre novos vetores de ataque e alertas precoces sobre vulnerabilidades nos sistemas, promovendo assim melhorias contínuas⁶⁵⁵.

Atualmente, muitas organizações na área da aviação tendem a adotar uma abordagem reativa em relação à cibersegurança, investindo apenas em medidas de proteção quando um incidente de cibersegurança já ocorreu. Algumas destas instituições não têm um Registo de Risco Empresarial, o que dificulta a identificação e gestão de ameaças, assim como têm falta de especialista em cibersegurança, resultando assim numa cultura de cibersegurança fraca⁶⁵⁶.

⁶⁵² ENISA, "Securing Smart Airports", 2016, 25.

⁶⁵³ ENISA, "Securing Smart Airports", 2016, 47

⁶⁵⁴ ENISA, "Securing Smart Airports", 2016, 48

⁶⁵⁵ ENISA, "Securing Smart Airports", 2016, 49

⁶⁵⁶ ICAO, "Aviation Cybersecurity: Emerging Challenges and Solutions", novembro de 2023, 13, <https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/8.4%20MedAire%20-%20Cybersecurity%20Symp%20PPT%20-%20November%202023.pdf>.

Transporte Marítimo e por vias navegáveis interiores

Embora possa ter começado a ser um ponto ao qual foi dada maior atenção, o setor de transporte marítimo e, em particular, os operadores portuários, ainda enfrentam diferentes desafios como a falta de estrutura organizacional e de cultura digital no contexto portuário, défice de experiência interna, falha de processos e/ou recursos de avaliação e mitigação de ameaças e vulnerabilidades, défice de formação e sensibilização em matéria de cibersegurança, falta de tempo e investimento alocados a medidas de proteção e/ou falta de recursos humanos qualificados em cibersegurança específico do setor.

É um setor que exige que todos os operadores envolvidos atinjam e mantenham um nível mínimo de cibersegurança, pela sensibilidade das operações associadas a este setor e respetivas interconectividade e interdependência. Constitui um maior desafio, pela complexidade que o setor apresenta ao nível do seu ecossistema, quantidade e diversidade de *stakeholders* intervenientes em operações portuárias.

Outros desafios enquadrados no setor marítimo focam-se no contexto particular dos portos marítimos: dificuldade em identificar vulnerabilidades em sistemas TI e TO, dificuldade em comparar e manter registos de riscos de sistemas de TI e TO, dificuldade em avaliar ativos e serviços geridos por terceiros, dificuldade na atribuição de todos os ativos, aplicações, sistemas e pessoal que se relacionem com a prestação de serviços específicos e dificuldade em lidar com a gestão de configuração de sistemas TO⁶⁵⁷.

Transporte Ferroviário

No contexto do setor de transporte ferroviário, um dos maiores desafios consiste na categorização de ameaças (qualquer desastre, interrupção ou ataque) enquanto ameaças enquadradas em matéria de cibersegurança. Outro dos desafios é o nível de dificuldade obtida em avaliar a probabilidade de ocorrência de um cenário de ameaça, por esta avaliação implicar que seja avaliado o nível de capacidade exigido para um determinado ataque, o nível de exposição do ativo/sistema ao qual o ataque se dirige e a intenção de um ator malicioso. São fatores com níveis de mensuração e previsão muito complexos⁶⁵⁸.

As *supply chains* também são um dos desafios mais complexos que este setor enfrenta: existe uma forte dificuldade em dimensionar os riscos de segurança a que se encontram expostos os *stakeholders* visto que não existe qualquer visibilidade sobre o nível de maturidade de cibersegurança no contexto de terceiros. Uma solução que pode ajudar a aliviar esta dificuldade será a realização de um inventário que inclua todos os *suppliers* categorizados em termos de criticidade. Esta criticidade é medida por fatores como a forte dependência e conexão entre sistemas, o acesso a sistemas críticos ou funções que impliquem a manipulação de dados sensíveis⁶⁵⁹.

⁶⁵⁷ ENISA, "ENISA Guidelines - Cyber Risk Management for Ports", 2020,16-18.

⁶⁵⁸ ENISA, "Railway Cybersecurity", novembro de 2021, 18.

⁶⁵⁹ ENISA, "Railway Cybersecurity", novembro de 2021, 18.

A crescente digitalização dos sistemas de operações e controlo do transporte ferroviário torna-o um alvo atraente para ameaças de cibersegurança. Muitas redes ferroviárias operam com infraestrutura envelhecida que requer investimentos significativos. É fundamental atualizar trilhos, sinais e, principalmente os próprios sistemas de controlo, para que atendam às exigências atuais. A pressão sobre a sustentabilidade representa, também, um grande desafio. Embora o transporte ferroviário seja uma das opções mais ecológicas em comparação com os outros modos de transporte, ainda há a necessidade de reduzir a pegada de carbono⁶⁶⁰.

Transporte Rodoviário

No caso do setor rodoviário, um dos grandes desafios está nos transportes inteligentes. Embora estes veículos representem uma evolução enorme no setor, são também veículos muito mais sujeitos à exploração de vulnerabilidades informáticas. Esta foi uma questão levantada quando dois *hackers* éticos foram capazes de aceder a um Jeep Cherokee a partir de um computador a uma distância de quilómetros do veículo e assumir o total controlo do mesmo. Depois desta experiência, grandes marcas automóveis (Tesla, grupo Volkswagen, etc) foram forçadas a ter a temática da cibersegurança muito mais presente na evolução tecnológica dos seus veículos⁶⁶¹.

Embora a indústria automóvel tenha-se tornado cada vez mais segura e inteligente, graças aos sistemas de controlo eletrónicos avançados, componentes inteligentes, sistemas incorporados e interfaces *API*, esta dependência crescente da tecnologia também introduz novos riscos para os carros inteligentes, ligados e autónomos que antes não existiam. Muitos destes sistemas resultam de desenvolvimento de código e de *software* que podem ser comprometidos sob diferentes formas: *malware*, ataques *DDoS*, ataques de injeção de código, entre outros. A não atualização de *software* de um veículo por falta de disponibilidade ou problemas na integração de toda a cadeia de fornecimento podem também representar sérios perigos para a segurança automóvel⁶⁶².

Outro desafio, neste subsetor, é a infraestrutura envelhecida. Muitas estradas e pontes não foram projetadas para suportar o aumento de tráfego e peso dos novos veículos, podendo resultar num aumento do risco de acidentes. Segundo a Organização Mundial da Saúde (OMS), a deterioração das estradas é um fator significativo nos acidentes rodoviários⁶⁶³. A sustentabilidade também é uma preocupação crescente, refletida na crescente adoção de veículos elétricos. No entanto, a transição para estas tecnologias enfrenta alguns desafios, como a falta de infraestrutura de carregamento. De acordo com um relatório da Internacional Energy Agency (AIE), a expansão da infraestrutura de carregamento é essencial para impulsionar a adoção de veículos elétricos⁶⁶⁴.

⁶⁶⁰ Claudio Martani, Natalia Papathanasiou, Bryan Adey, "A Review of the State-of-the-Art in Railway Risk Management", outubro de 2016, 9, https://www.researchgate.net/publication/309609809_A_Review_of_the_State-of-the-Art_in_Railway_Risk_Management.

⁶⁶¹ Julio Poblete e Dr. Yoon, "Connected Automobiles and Cybersecurity", março de 2018, 4-5, http://cysecure.org/470/18sp/indiProject/Jpoblete-Project/indiO18JulioPoblete_ConnectedAutomobiles.pdf.

⁶⁶² Holger Schmeken, "Automotive Cyber Security: New mandatory regulations", DQS, 6 de dezembro de 2022, <https://www.dqsglobal.com/intl/learn/blog/automotive-cyber-security-new-mandatory-regulations>.

⁶⁶³ International Transport Forum, "Road Safety: Annual Report 2023", 26, <https://www.itf-oecd.org/sites/default/files/docs/irtad-road-safety-annual-report-2023.pdf>.

⁶⁶⁴ International Energy Agency, "World Energy Outlook 2023", 200, <https://iea.blob.core.windows.net/assets/ed1e4c42-5726-4269-b801-97b3d32e117c/WorldEnergyOutlook2023.pdf>.

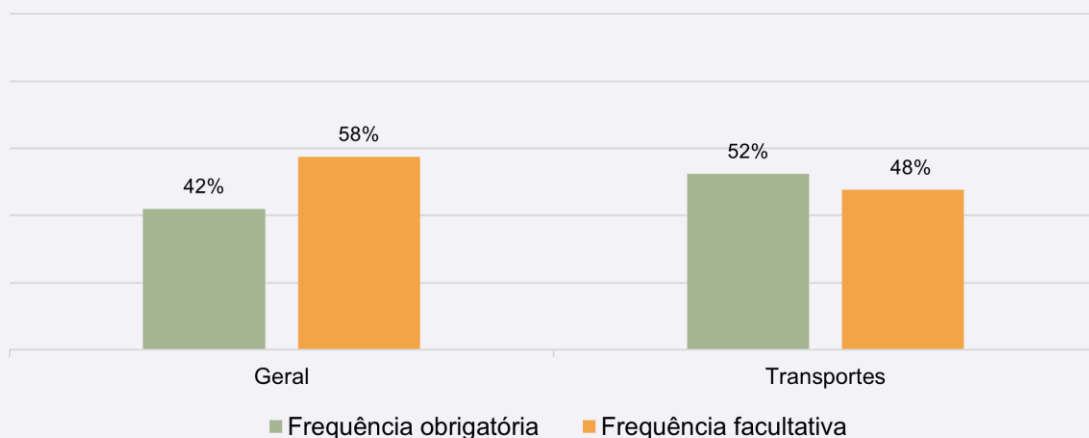
2.8. Recomendações

Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor dos transportes e subsequentes subsectores, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

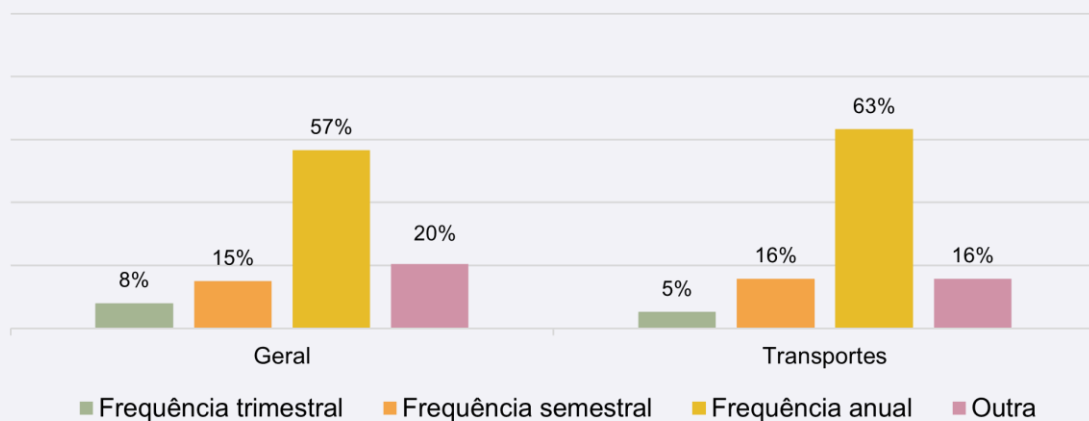
Como abordado inicialmente, os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor dos transportes disponibilizarem formação em cibersegurança aos seus colaboradores, quase metade das formações são de carácter facultativo, e não obrigatório (**Gráfico 39**).

Gráfico 39 - Carácter das formações disponibilizadas - frequência obrigatória ou facultativa



Além disso, na maioria das entidades verificam-se momentos de formação com frequência anual (**Gráfico 41**), o que no contexto do setor dos transportes poderá ser insuficiente para assegurar a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram com maior frequência e que a participação nos mesmos seja obrigatória.

Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor dos transportes, comparativamente com os restantes, é um dos setores onde menos se utiliza segurança avançada em dispositivos *endpoint*, a utilização de *browser* que proteja a privacidade e controlos biométricos para identificação e autenticação de utilizadores.

Nesse sentido, recomenda-se aos OSE do setor dos transportes que:

- Aumentem a equipa de especialistas em cibersegurança;
- Realizem análises de risco com periodicidade mínima anual;
- Implementem segurança avançada nos dispositivos *endpoint*;
- Implementem Sistemas de Prevenção e Detecção de Intrusão (IPDS);
- Aumentem a segurança de rede em *cloud*;
- Implementem, onde possível, métodos de autenticação multifator.

Medidas como estas auxiliam a impedir acessos iniciais por parte dos agentes de ameaça e a que os mesmos não sejam capazes de progredir na exploração dos dados, sistemas e ficheiros quando um primeiro acesso é obtido.

Para mitigar as ameaças de cibersegurança que o setor de transportes enfrenta, a adoção de recomendações específicas para segurança digital e a proteção de sistemas essenciais é fundamental. Estas recomendações são fundamentais tanto para reduzir a exposição aos riscos como para melhorar a capacidade de resposta diante de incidentes. Abaixo, na tabela, seguem tópicos de recomendações que podem ser úteis ao setor e subsetores:

Tabela 28 - Recomendações (Transportes)

Recomendação	Medida
Desenvolvimento de uma Estrutura de Cibersegurança por Subsetor	Cada subsetor (aéreo, marítimo, ferroviário e rodoviário) possui especificidades e deve ter um conjunto próprio de medidas de segurança. Isto inclui padrões de segurança, processos de monitorização de ameaças, e planos de contingência adaptados a cada contexto.
Implementação de Programas de Formação e Sensibilização	Novamente, reforça-se que as formações regulares são essenciais para que colaboradores, especialmente aqueles com acessos a sistemas críticos, saibam identificar e evitar ameaças como <i>phishing</i> , engenharia social, e possíveis armadilhas digitais o que acaba também por minimiza o risco de erros humanos, que é uma das principais vulnerabilidades exploradas.
Segurança na Cadeia de Abastecimento	Fornecedores e parceiros (subcontratações) são pontos vulneráveis significativos, visto que uma falha de segurança num parceiro pode impactar diretamente a organização principal. Realizar auditorias de segurança, exigir certificações de fornecedores e monitorizar os processos de fabricação ajudam a mitigar os riscos de comprometimento de componentes essenciais.
Estabelecer Protocolos de	A monitorização em tempo real de sistemas de TI e TO pode permitir a deteção antecipada de atividades suspeitas. Este tipo de sistemas, especialmente em infraestruturas críticas como

Monitorização Contínua	sistemas de sinalização ferroviária e controlo de tráfego aéreo, aumenta a eficácia de respostas rápidas para evitar danos maiores.
Adoção de Medidas para Prevenção de Ataques de Ransomware	É recomendável manter backups seguros e atualizados dos sistemas, usar técnicas de segmentação de rede para reduzir a propagação de ataques e implementar estratégias de recuperação de sistemas.
Proteção Contra DDoS	Investir em soluções de proteção contra DDoS, que são frequentemente utilizados em ataques ativistas, ajuda a manter os sistemas online e operacionais.
Melhoria na Segurança de Hardware e Software	Realizar a atualização periódica de <i>softwares</i> e sistemas de TI e TO minimiza o risco de exploração de vulnerabilidades conhecidas. Assegurar que componentes de <i>hardware</i> , como sistemas de controlo, estejam protegidos contra falsificação ou alterações maliciosas ajuda a proteger contra ataques na cadeia de suprimentos.
Planos de Recuperação de Desastres e Continuidade de Negócios	É crucial desenvolver e testar regularmente planos de recuperação de desastres que possibilitem a rápida recuperação dos sistemas críticos após um ataque. Isso inclui alternativas de operação manual em casos de falhas em sistemas digitais.
Colaboração com Agências Governamentais e Partilha de Informação	Manter uma comunicação constante com entidades como o CNCS e o CERT.PT bem como participar em redes de partilha de inteligência de ameaças, ajudam as empresas a manterem-se atualizadas sobre novas ameaças e práticas de mitigação, aumentando a resiliência do setor diante de ciberameaças evolutivas.
Realização de Auditorias Regulares e Testes de Penetração	Auditar periodicamente os sistemas e realizar testes de invasão permitem que a organização identifique vulnerabilidades e as corrija proativamente, sendo uma prática eficaz para avaliar a segurança de sistemas complexos, como aqueles utilizados no transporte aéreo e marítimo.

Políticas, procedimentos e planos de cibersegurança

De acordo com os dados obtidos no questionário, 85% dos OSE do setor tinham documentado e implementado políticas e procedimentos de cibersegurança. Adicionalmente, apenas 65% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Face a esta realidade, recomenda-se aos OSE do setor que ainda não o tenham feito que elaborem e implementem uma política de cibersegurança que verse sobre:

- Os diversos papéis e responsabilidades dos colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, tais como os controlos de acesso (lógico e físico);

- A gestão de incidentes, devendo ser elaborados um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação dos mesmos, bem como um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização da política, de forma periódica (no mínimo, anual), de modo a manter atualizada face à evolução das ameaças de cibersegurança e da própria organização.

Face à baixa percentagem de OSE do setor que indicaram possuir uma política de gestão de continuidade de negócio comparativamente às outras políticas (59%), recomenda-se também a elaboração de uma política alinhada com a política de cibersegurança.

A elaboração de políticas, procedimentos e planos de cibersegurança e a comunicação destes aos profissionais, quer dos transportes, quer das áreas tecnológicas, é também uma forma de dar a conhecer a estes o que lhes é permitido ou não fazer em contexto de cibersegurança, como devem tratar ativos de informação, desde dados sensíveis a dispositivos, e como devem atuar perante uma situação suspeita ou de concretização de uma ameaça.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*⁶⁶⁵.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos⁶⁶⁶:

⁶⁶⁵ Hassanzadeh et al., "A Review of Cybersecurity Incidents", 4.

⁶⁶⁶ Hassanzadeh et al., "A Review of Cybersecurity Incidents", 6.

Tabela 29 - Controlos de Segurança da CIS (Transportes)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: CIS, “The 18 CIS Critical Security Controls”, <https://www.cisecurity.org/controls/cis-controls-list>)

Recomendações subsetor do transporte aéreo

A ENISA destaca determinadas recomendações essenciais a seguir pelo setor aéreo. Essas recomendações encontram-se divididas pelos diferentes responsáveis em tomada de decisão: profissionais de segurança de informação aeroportuária, responsáveis pelas políticas e representantes da indústria⁶⁶⁷.

Tabela 30 - Recomendações (Transporte Aéreo)

Destinatários	Boas práticas a aplicar
Profissionais de segurança de informação aeroportuária	• Priorizar a cibersegurança; • Estabelecer contextos claros de cibersegurança no aeroporto e alocar funções e recursos adequados; • Rever políticas e práticas de cibersegurança com base nas melhores práticas; • Implementar políticas e processos de gestão de ameaças e riscos.
Responsáveis pelas políticas	• Monitorizar possíveis ataques nos serviços ou sistemas e detetar se: ○ Consumo anormal da capacidade da rede; ○ Comportamentos inesperados de serviços e sistemas; ○ Desempenho inferior de tarefas; ○ Perdas de ligação inesperadas.
Representantes da indústria	• Colaborar com os principais <i>stakeholders</i> no desenvolvimento de <i>standards</i> específicos para soluções de cibersegurança; • Trabalhar com operadores aeroportuários para desenvolver produtos e/ou soluções alinhados com os requisitos mínimos de cibersegurança.

⁶⁶⁷ ENISA, "Securing smart airports", dezembro de 2016, 50-52.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsetor. Tais cenários são indicados na seguinte tabela:

Tabela 31 - Cenários de risco (Transporte Aéreo)

Cenários de risco

Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.

Comprometimento de serviços WEB, através de um *URL* malicioso ou *script* malicioso que direciona um colaborador da entidade para um website falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.

Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.

Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO WEB** (SQL Injection ou Cross-site Scripting).

Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.

FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.

VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.

RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 15 de outubro de 2024, https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_riscos_conflitos2021.pdf)

Recomendações subsetor do transporte marítimo

Segundo a ENISA, existem algumas recomendações importantes a aplicar no setor, entre elas⁶⁶⁸:

- a) Definir o foco específico da avaliação com base nas características únicas do operador portuário (baseado em ativos ou serviços);
- b) Manter atualizado um inventário de ativos relacionados com matéria de cibersegurança (com respetivas informações de sistema e serviço);
- c) As dependências devem ser identificadas nos requisitos de interface técnica (e/ou troca de dados) com *software* de terceiros, com fornecedores ou entre sistemas TI e TO;
- d) Implementar ferramentas automáticas para identificação, registo e monitorização de ativos;
- e) Incluir responsáveis de cibersegurança na revisão e implementação de políticas e contratos com o objetivo de garantir que a cibersegurança seja abordada e garantida;
- f) Identificar e avaliar os riscos de cibersegurança relacionados com os ativos e serviços identificados neste contexto:
 - i) Contextualizar os riscos, através da adoção de metodologias específicas de identificação e avaliação de riscos;
 - ii) Identificar ameaças, vulnerabilidades associadas a ativos e serviços e dependências internas e externas;
 - iii) Avaliar possíveis probabilidade e impacto de um incidente de cibersegurança;
 - iv) Desenvolver indicadores para avaliar os riscos identificados.

A Comissão Europeia descreveu um conjunto de ferramentas de cibersegurança para o setor dos transportes e destacou, ao nível do transporte marítimo, as seguintes boas práticas e medidas de segurança a adaptar ao setor⁶⁶⁹:

- 1) Definir mecanismos de governação que respondam às obrigações decorrentes de regulamentos e diretivas aplicáveis ao setor, como “o Regulamento (UE) 2019/1239 que estabelece um ambiente europeu de plataforma única para o setor marítimo (EMSW, do inglês European Maritime Single Window environment), o Regulamento (CE) n.º 725/2004 relativo ao reforço da proteção dos navios e das instalações portuárias, a Diretiva 2005/65/CE relativa ao reforço da segurança nos portos e o Regulamento (CE) n.º 336/2006 relativo à aplicação do Código Internacional de Gestão da Segurança (ISM), bem como a Resolução A.741(18) que adota o Código *International Safety Management* (ISM) para a Segurança da Exploração dos Navios e a Prevenção da Poluição.”

⁶⁶⁸ ENISA, “Guidelines - Cyber Risk Management for Ports”, 2016, 14.

⁶⁶⁹ Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, “Conjunto de ferramentas de cibersegurança para o setor dos transportes”.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsetor. Tais cenários são indicados na seguinte tabela:

Tabela 32 - Cenários de risco (Transporte Marítimo)

Cenários de risco

Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.

Comprometimento de serviços WEB, através de um *URL* malicioso ou *script* malicioso que direciona um colaborador da entidade para um website falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.

Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.

Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.

Alguns dispositivos da entidade são infetados por software malicioso que os conecta a uma BOTNET, tornando-os zombies, fornecendo poder computacional a ataques de *DDoS* e de criptomineração, ou comprometendo os sistemas e/ou serviços (ex: RDP, FTP) através de tentativa de força-bruta.

RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 15 de outubro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

Recomendações subsetor do transporte ferroviário

Segundo o relatório da ENISA, muitas das recomendações e medidas a implementar e respetiva priorização foram resultado de uma avaliação do nível de conformidade por parte das organizações conforme os requisitos mínimos nacionais de cibersegurança (sobretudo, segundo a Diretiva NIS)⁶⁷⁰. Algumas das medidas levantadas foram as seguintes:

- 1) Sessões de sensibilização e formação (especialmente contra *ransomware* e *phishing*);
- 2) Proteção de *endpoints*, segregação da rede e controlo de acessos em sistemas críticos;
- 3) Adaptação de sistemas *legacy* (embora seja um grande desafio no que respeita à complexidade de atualização de sistemas com longos ciclos de vida);
- 4) Realização de auditorias técnicas e auditorias de *governance* (ISO compliance);
- 5) Planos de continuidade e recuperação e resposta a incidentes devem ser testados.

De facto, é pela Diretiva NIS que muitos dos operadores se guiam para aplicar as medidas de cibersegurança adequadas aos diferentes domínios por ela identificados. De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsetor.

⁶⁷⁰ ENISA, “Railway Cybersecurity”, 2020, 30.

Tais cenários são indicados na seguinte tabela:

Tabela 33 - Cenários de risco (Transporte Ferroviário)

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços WEB, através de um <i>URL</i> malicioso ou <i>script</i> malicioso que direciona um colaborador para um website falso e instala <i>software</i> malicioso (ataques <i>Watering Hole</i> , ataques <i>Drive-By</i>), permitindo o furto de dados.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de <i>login</i> ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em <i>bitcoins</i> , sob a ameaça de destruição ou exposição ao público.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 15 de outubro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

Recomendações subsetor do transporte rodoviário

As boas práticas e recomendações a adaptar no setor de transporte rodoviário são transversais a todos os setores dos transportes e procuram responder rapidamente e corretamente às ameaças e vulnerabilidades identificadas. Algumas dessas recomendações são as seguintes⁶⁷¹:

Tabela 34 - Recomendações (Transporte Rodoviário)

Ameaça	Boas práticas a aplicar
Programas maliciosos	• Seguir políticas de segurança: processos de deteção de vírus, adotar cuidados na utilização de correio eletrónico, instalar e atualizar <i>software</i> autorizado, outros; • Realizar cópias de segurança dos dados; • Instalar medidas de segurança adequadas à proteção de sistemas (dispositivos móveis e terminais);
DoS ou DDoS	• Monitorizar possíveis ataques nos serviços ou sistemas e detetar se: ○ Consumo anormal da capacidade da rede; ○ Comportamentos inesperados de serviços e sistemas; ○ Desempenho inferior de tarefas; ○ Perdas de ligação inesperadas.
Acesso não autorizado e furto	• Seguir políticas de segurança da organização; • Cuidado na utilização e partilha de dados; • Ativar a autenticação de dois fatores (2FA); • Aplicar as regras de segurança de credenciais e palavras-passe.
Manipulação de <i>software</i>	• Instalar sempre <i>software</i> fidedigno; • Atualizar sempre o <i>software</i> instalado em conformidade com as políticas e práticas de organização.

⁶⁷¹ Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, "Conjunto de ferramentas de cibersegurança para o setor dos transportes".

Existem ainda algumas medidas de segurança adaptadas ao transporte terrestre - transversais a ferroviário e rodoviário. Estas medidas têm em consideração as particularidades dos serviços e sistemas TI e TO deste subsetor. As particularidades de TI são, por exemplo, todos os sistemas e serviços utilizados pelos funcionários (computadores de serviço, por exemplo) e pelos passageiros (Wi-fi públicos, por exemplo). Por outro lado, as TO referem-se a tudo o que diz respeito a tecnologia de vigilância, alarmes, monitorização, sistemas de controlo de dados, ou sistemas de aquecimento e ar condicionado. Neste sentido, algumas das medidas a adotar por organizações integradas neste subsetor são as seguintes⁶⁷²:

Tabela 35 - Medidas de segurança (Transporte Rodoviário)

Âmbito	Medidas de segurança adaptadas
Governança	• Atribuir papéis e responsabilidades de gestão e comunicação em matéria de cibersegurança e segurança TI e TO; • Assegurar a governança da cibersegurança em toda a cadeia de prestação de serviços de segurança; • Definir mecanismos de governança para cumprimento regulamentar e legislativo.
Gestão dos riscos	• Identificar claramente vários sistemas de <i>hardware</i> e <i>software</i> que executam as funções indispensáveis à prestação de serviços; • Realizar avaliações dos riscos de cibersegurança com respetiva identificação de medidas e planos de tratamento dos riscos; • Desenvolver e aplicar um plano de gestão de ativos e planeamento de recursos;
Deteção de ciberameaças	• Monitorização do estado de segurança das redes e dos sistemas de informação de TI e TO; • Deteção e monitorização de atividades maliciosas que possam afetar os contextos TI e TO.
Proteção contra ciberameaças	• Definir e implementar políticas e processos de segurança; • Definir e documentar um processo de gestão de identidades e acessos; • Proteger dados, redes e sistemas de informação críticos; • Definir e implementar um plano de reforço de resiliência de redes e sistemas.
Resposta e Recuperação	• Definir, aplicar e testar procedimentos de gestão de incidentes: ○ colaboração e partilha de informação com autoridades, partes interessadas e fornecedores; ○ exercícios regulares de ciberataque; ○ definição de protocolos operacionais em matéria de segurança.

⁶⁷² Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, "Conjunto de ferramentas de cibersegurança para o setor dos transportes".

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste subsetor. Tais cenários são indicados na seguinte tabela:

Tabela 36 - Cenários de risco (Transporte Rodoviário)

Cenários de risco

Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.

Comprometimento de serviços WEB, através de um *URL* malicioso ou *script* malicioso que direciona um colaborador da entidade para um website falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.

Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.

Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO WEB** (SQL Injection ou Cross-site Scripting).

Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.

VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.

RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 15 de outubro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

3. Bancário

3.1. Contextualização setorial

A criação da banca moderna é largamente atribuída ao Renascimento italiano. O intenso comércio que se verificava nas cidades que mais beneficiavam das trocas marítimas feitas através do Mar Adriático, como Florença, Veneza e Génova, rapidamente passou a exigir muitas das operações ainda hoje praticadas pela banca, de modo a financiar viagens, importações e a produção artística do período renascentista.

Algumas das atividades que ainda hoje se verificam na banca moderna têm uma história de milénios. Por exemplo, relativamente aos depósitos, é possível ler, num texto com cerca de 4000 anos, da Babilónia (hoje Bagdad, Iraque), que “se um homem der a outro prata, ouro, ou qualquer outra coisa para salvar, o que quer que ele dê deverá ser mostrado a testemunhas, e deverá preparar os contratos antes de realizar o depósito”⁶⁷³, e deveriam ser pagos ao depositário um sessenta avos do tesouro depositado por esse serviço.

Na Antiguidade Clássica, gregos e romanos tinham também já implementado mecanismos de depósito de dinheiro e de bens. Em particular, o comércio e a “banca” romanos contavam já com a abertura de contas, emissão de notas de troca, cartas de crédito, empréstimos (com juros), hipotecas, e outras operações idênticas às que ainda hoje se verificam junto das entidades bancárias⁶⁷⁴. Crê-se que algumas destas práticas terão sido perdidas no Ocidente com a queda do Império Romano no século V, mas foram recuperadas e mais bem desenvolvidas durante o Renascimento, que lançaria as bases da banca moderna⁶⁷⁵.

⁶⁷³ Noble Hogsson, *Banking through the Ages* (Nova Iorque: Dodd, Mead & Company, 1926), 33.

⁶⁷⁴ Hogsson, *Banking through the Ages*, 40-41.

⁶⁷⁵ Hogsson, *Banking through the Ages*, 63-64.

No caso de Portugal, o desenvolvimento da atividade bancária ficou também ligado ao comércio e à expansão marítima, iniciada em 1415, com a conquista de Ceuta, conduzindo à exploração da costa ocidental africana, e mais tarde, à descoberta do caminho marítimo para a Índia e ao estabelecimento de relações comerciais com o continente asiático⁶⁷⁶. A necessidade de dinheiro para o financiamento das expedições, a necessidade de adquirir capacidade de navegação, através da compra de instrumentos de navegação e da contratação de astrónomos, engenheiros e cartógrafos estrangeiros e de fazer comércio com outros povos conduziu à criação das primeiras casas de câmbio e bancos em Portugal.

O primeiro banco de que há registo em Portugal é o banco de Mossém Rafael Vivas, fundado em 1465, durante o reinado de D. Afonso V, que “emergia, então, das necessidades cambiais, da exigência de pagamentos devidos à circulação das mercadorias e das pessoas e da vantagem em proceder a pagamentos à distância”⁶⁷⁷.

Outras instituições bancárias foram surgindo ao longo dos anos, mas, ao contrário do que se verificava em repúblicas italianas, como a de Florença, em que os bancos eram essencialmente privados e de iniciativa de grandes famílias, os bancos em Portugal eram sobretudo criados, até finais do século XVIII, por desígnio régio, para responder a necessidades do reino.

Só a 19 de novembro de 1846 foi criado o Banco de Portugal (BdP). Consequência da fusão de outros bancos (Banco de Lisboa e Companhia Confiança Nacional), o BdP foi criado com duas funções: a função banco comercial e a função banco emissor. Até 1974, aquando da sua nacionalização, o BdP era maioritariamente privado e foi fundado com o estatuto de sociedade económica⁶⁷⁸.

Bancos como o Banco Espírito Santo e Caixa Geral de Depósitos são posteriores à criação do BdP, tendo sido fundados em 1869 e 1876, respetivamente. Já bancos como o Banco Português de Investimento (BPI) ou o Banco Comercial Português (Millenium BCP) surgiram apenas na década de 80 do século passado, respetivamente, em 1981 e em 1985. À data da elaboração deste relatório, operavam em Portugal 1373 entidades autorizadas⁶⁷⁹, com cerca de 3852 agências⁶⁸⁰ em funcionamento.

O setor bancário é o principal responsável pela gestão dos depósitos dos seus clientes, pela circulação do dinheiro entre pessoas, empresas e Estado, pela intermediação financeira, pela concessão de crédito e pela disponibilização de meios cómodos e seguros de realizar diversas operações financeiras, como pagamentos, transferências e levantamentos, entre outros.

⁶⁷⁶ António Farinha, “O Primeiro Banco em Portugal (1465)”, *Estudos em Homenagem a Jorge Borges de Macedo*, (Lisboa: Instituto Nacional de Investigação Científica, Centro de Arqueologia e História da Universidade de Lisboa, 1992), 153.

⁶⁷⁷ Farinha, “O Primeiro Banco em Portugal”, 167.

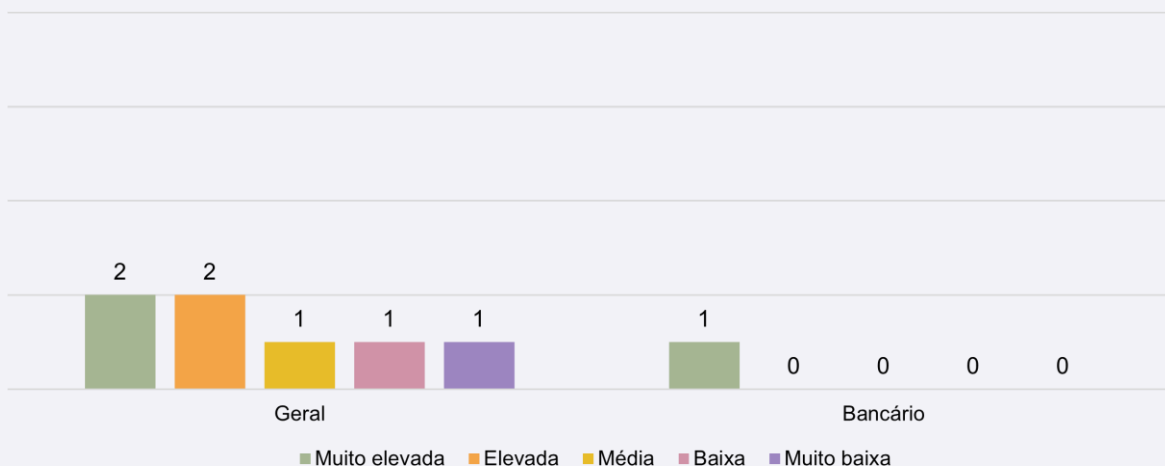
⁶⁷⁸ “História do Banco de Portugal”, Sobre o Banco, Banco de Portugal, <https://www.bportugal.pt/page/historia-do-banco-de-portugal>.

⁶⁷⁹ “Instituições autorizadas”, Banco de Portugal, última atualização em 23 de setembro de 2024, <https://www.bportugal.pt/page/listagem-entidades-autorizadas>.

⁶⁸⁰ “Lista de agências”, Banco de Portugal, agosto de 2024, <https://www.bportugal.pt/sites/default/files/listaagencias.xls>.

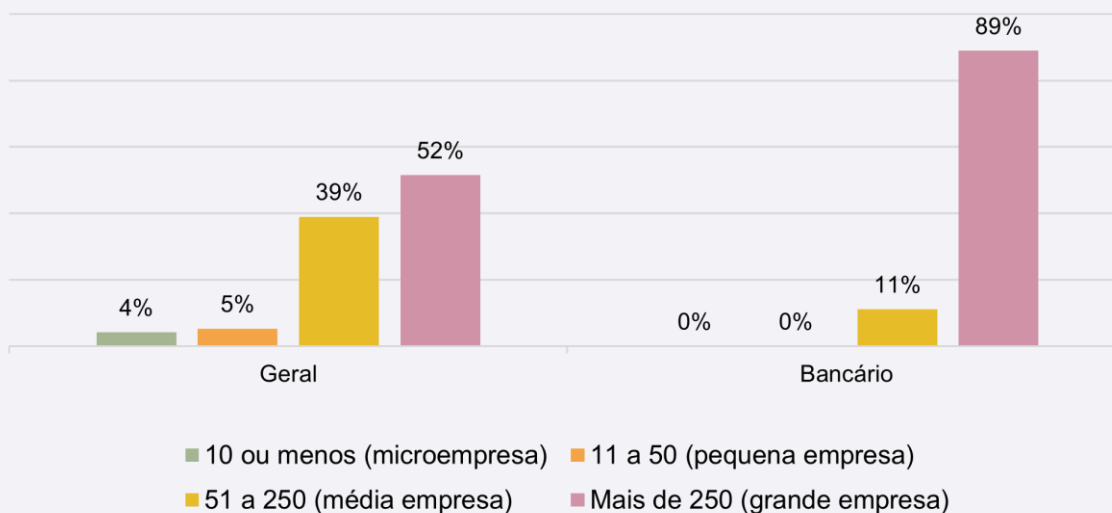
Atualmente, de acordo com o questionário realizado, o regulador do setor considera que a maturidade deste em cibersegurança é muito elevada e, no âmbito geral, não há reguladores com maior percepção de maturidade em cibersegurança (**Gráfico 9**).

Gráfico 9 - Percepção dos reguladores sobre maturidade em cibersegurança nos setores



O tecido empresarial dos OSE do setor bancário é sobretudo composto por grandes empresas, representando estas 90% dos operadores do setor, com os restantes 10% sendo médias empresas. Estes valores são superiores à média geral (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



Esta perceção pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (100% contra 65%) (vide **Gráfico 38**) e pelas medidas de cibersegurança adotadas (**Gráfico 66.3 A** e **Gráfico 66.3 B**). As medidas de proteção menos adotadas são: utilização de *browser* que proteja a privacidade e controlos biométricos para identificação e autenticação de utilizadores.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

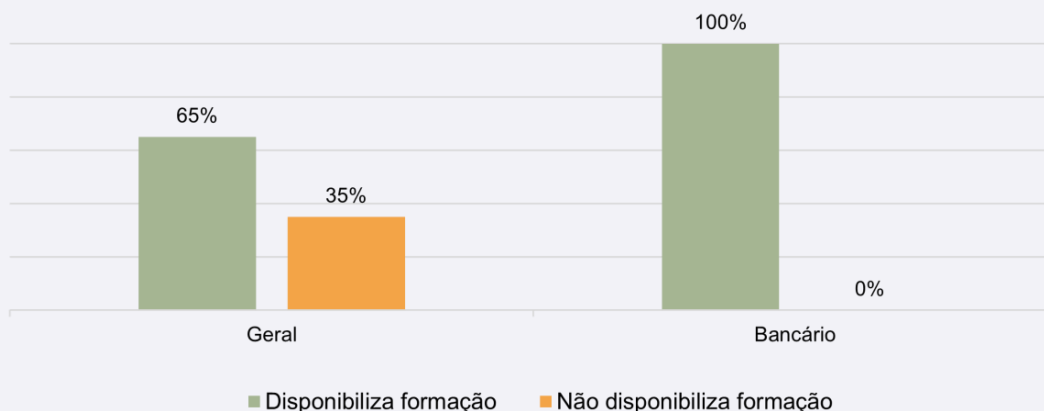
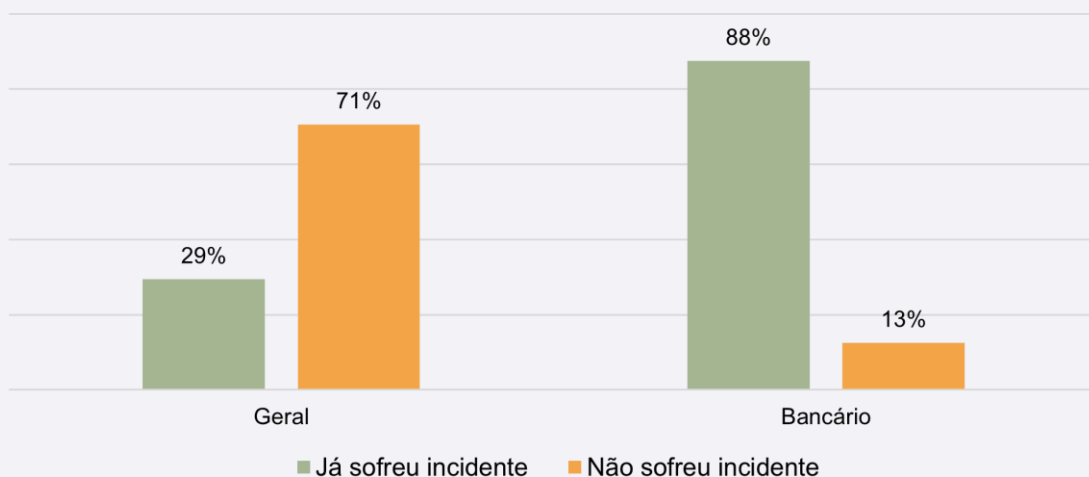


Gráfico 66.3 - Medidas de proteção contra ameaças de cibersegurança



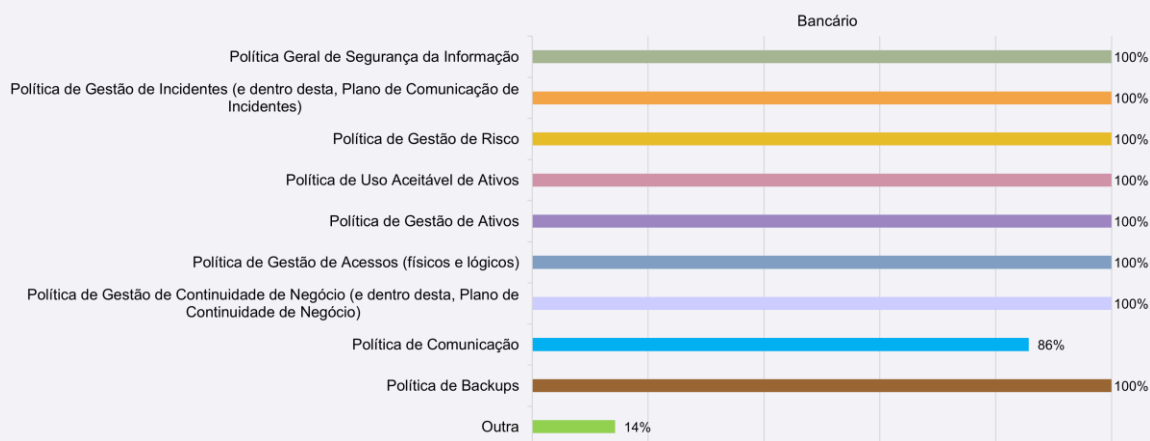
Mesmo sendo este um setor com uma elevada maturidade em cibersegurança, o setor bancário foi o setor onde mais operadores indicaram já ter sofrido incidentes de segurança (88% dos OSE - **Gráfico 68**), evidenciando-o como um alvo preferencial para ciberataques e estando acima dos 71% da média geral.

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



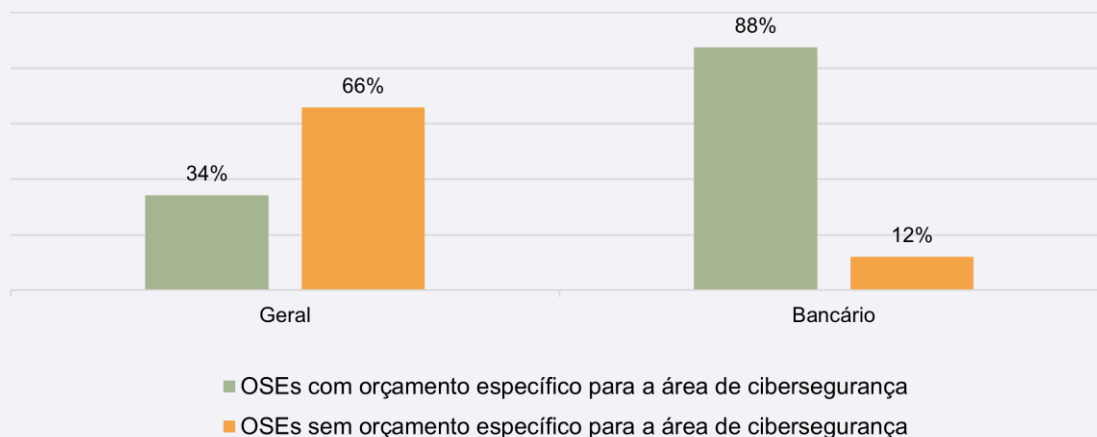
As políticas de cibersegurança e outras políticas relacionadas implementadas (**Gráfico 79.3**) também suportam a afirmação anterior. O plano de segurança tem todas as políticas incluídas, com exceção da política de comunicação que está apenas incluída em 86% dos planos de segurança.

Gráfico 79.3 - Políticas incluídas no Plano de Segurança



Neste setor, cerca de 88% dos OSE têm orçamento específico para a área de cibersegurança, sendo o valor, no geral, situado nos 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



3.1.1. Impacto socioeconómico

O setor bancário desempenha um papel crucial na economia contemporânea, facilitando a intermediação financeira. Um processo de intermediação financeira envolve a captação de recursos, transferindo fundos de agentes económicos com excedente de capital para aqueles com necessidade de financiamento. Neste processo de intermediação financeira, os intermediários financeiros assumem o risco por conta própria pela aquisição de ativos financeiros ou contração de dívidas. Um setor bancário robusto e eficiente promove este tipo de ações que consistem na acumulação de poupança e respetiva alocação em investimentos mais produtivos, impulsionando a inovação e o crescimento económico. Na Europa, os bancos são os principais intermediários financeiros em todos os países do continente⁶⁸¹.

A banca tem também um papel fundamental para a economia portuguesa. Assim como a conjuntura económica de um país tende a afetar o setor bancário, também este setor exerce grande influência no bem-estar económico de um país no seu global.

Os meios de pagamento disponibilizados sobretudo pelo setor bancário, como é o caso dos cartões de débito e crédito e das contas correntes, são o que permite realizar de forma prática e segura um conjunto de operações necessárias no dia a dia, como transferências, pagamentos de bens e serviços, levantamentos ou débitos diretos. Por outro lado, a banca depende da confiança que os depositantes lhe atribuem quando lhes entregam as suas poupanças, para que sejam guardadas de forma segura⁶⁸².

⁶⁸¹ Carlos Costa, "O Sistema Financeiro Português e o Papel do Banco de Portugal", (intervenção no Fórum na Área Financeira, Macau, 10 de outubro de 2012), 1.

⁶⁸² Barroso, "O fundamental papel da banca na saúde das economias", 6 de julho de 2023.

Quer estejamos perante uma recessão ou uma fase de crescimento económico, o banco deverá ter a capacidade de emprestar dinheiro, de garantir que os pagamentos são processados rapidamente, em segurança, a um valor reduzido e que os depósitos estão salvaguardados. A realização segura das diferentes transações financeiras a que todos os cidadãos estão sujeitos diariamente - como transferências, pagamentos de bens ou serviços e débitos diretos - depende diretamente do papel desempenhado pelos meios de pagamento fornecidos pelo setor bancário - como cartões de débito e crédito e contas correntes. Além da segurança destes serviços dever ser garantida pelos bancos, estes também contam com a confiança que os clientes depositam neles ao confiarem as suas poupanças. Por este motivo, e em qualquer contexto nacional, a decisão de deixar um banco falir nunca é tomada por um governo de forma leviana. Levar um banco a uma situação extrema como esta leva a situações de quebra de confiança que “podem provocar corridas aos depósitos, comprometer poupanças de uma vida e inviabilizar os fundos necessários à manutenção do funcionamento de operações de empresas, instituições públicas e tantas outras organizações”⁶⁸³.

O setor bancário tem um papel fundamental na economia nacional e a sua atuação vai muito além da facilitação de transações⁶⁸⁴. Os seus principais papéis, em contexto de facilitação financeira, são os seguintes:

- **Intermediação financeira:** O banco assegura a intermediação financeira através da canalização de fundos dos aforradores para os investidores⁶⁸⁵. Este processo contribui para a estimulação do investimento e consequentemente, do crescimento económico.
- **Disponibilização de crédito bancário:** O banco disponibiliza crédito bancário que é utilizado para financiar as necessidades dos agregados familiares, através da regulação do seu padrão de consumo ao longo do tempo e ajudando-os a investir em bens que impulsionam o desenvolvimento da economia.
- **Contribuição para a estabilidade financeira do país:** Um setor bancário sólido e eficiente incentiva à acumulação de poupança e permite a realização de investimentos mais produtivos, apoiando assim a inovação, o crescimento económico e a estabilidade financeira⁶⁸⁶.

Tendo todas estas valências em conta, o setor bancário é responsável pela movimentação de centenas de milhares de milhões de euros. Segundo o Relatório dos Sistemas de Pagamentos de 2022, publicado pelo BdP, foram transacionados em Portugal, durante esse ano, cerca de 655,5 mil milhões de euros, o equivalente a 1,8 milhões de euros por dia⁶⁸⁷.

O setor bancário tem-se mostrado lucrativo também. Em 2022, os sete maiores Bancos portugueses – CGD, BCP, Novobanco, Santander Totta, BPI, Crédito Agrícola e Banco Montepio – lucraram 2.761 milhões de euros⁶⁸⁸. Em 2023, os lucros da CGD, BCP, Santander Totta, BPI e Novobanco, superaram os 4,4 mil milhões de euros⁶⁸⁹. Em sede de IRC, a banca gerou aproximadamente 1,47 mil milhões de euros para os cofres do Estado no mesmo ano⁶⁹⁰.

⁶⁸³ Barroso, “O fundamental papel da banca na saúde das economias”, 6 de julho de 2023.

⁶⁸⁴ Comissão Europeia, “Ficha temática sobre o semestre europeu: Setor Bancário e estabilidade financeira”, 16 de outubro de 2017, 1, https://commission.europa.eu/system/files/2021-01/european-semester_thematic-factsheet_banking-sector-financial-stability_pt.pdf.

⁶⁸⁵ Comissão Europeia, “Setor Bancário e estabilidade financeira”, 16 de outubro de 2017, 1.

⁶⁸⁶ Comissão Europeia, “Setor Bancário e estabilidade financeira”, 16 de outubro de 2017, 1.

⁶⁸⁷ Banco de Portugal, “Relatório dos Sistemas de Pagamentos 2022”, 11.

⁶⁸⁸ Maria Alves, “Bancos privados com 3,3 mil milhões de lucros em 2023 a subirem 74,2% face ao ano anterior”, *Jornal Económico*, 5 de março de 2024, <https://leitor.jornaleconomico.pt/noticia/bancos-privados-com-3-3-mil-milhoes-de-lucros-em-2023-a-subirem-74-2-face-ao-ano-anterior>.

⁶⁸⁹ Alberto Teixeira, “Banca com lucros recorde em 5 gráficos”, *Eco*, 15 de março de 2024, <https://eco.sapo.pt/2024/03/15/banca-com-lucros-recorde-em-5-graficos/>.

⁶⁹⁰ Mariana Dias, “Cinco maiores bancos pagaram 17% do IRC total arrecadado em 2023”, *Diário de Notícias*, 25 de março de 2023, <https://www.dn.pt/3384889811/cinco-maiores-bancos-pagaram-17-do-irc-total-arrecadado-em-2023/>.

Quanto ao emprego, o setor bancário era responsável, em 2022, por quase 60 mil postos de trabalho. O número de empregos no setor tem, no entanto, vindo a diminuir ao longo dos anos. Ao passo que entre os anos de 2008 e 2014 o setor empregava quase 80 mil pessoas, a empregabilidade reduziu em cerca de 20 mil postos de trabalho desde então⁶⁹¹.

As principais atividades do setor bancário impactam tanto a economia nacional como a vida em sociedade. A disponibilização de formas de transação, permitindo a realização de operações, tais como transferências, pagamentos, de bens, serviços, ou levantamento de dinheiro, de forma prática, rápida e segura geraram a possibilidade de realizar tudo isso sem que seja necessário ir a um balcão ou até mesmo a um terminal multibanco (com exceção dos levantamentos). A maioria das operações referidas podem hoje ser realizadas em praticamente qualquer lugar, desde que se tenha um dispositivo como um computador ou um *smartphone* e acesso à Internet.

A concessão de crédito, como referido, é também o que permite a uma larga porção da população a realização de certos desígnios, como a compra de habitação, de carro, de pagar estudos, ou iniciar um negócio. A melhoria no acesso aos serviços financeiros tem permitido que cada vez mais pessoas tenham acesso a estes, sendo possível observar uma crescente inclusão de cidadãos que eram, até então, ignorados pelos sistemas, o que favorece um movimento de democratização global⁶⁹².

Naturalmente, existe também o “reverso da medalha”. Isto é, quando uma ou várias entidades do setor bancário obtêm maus resultados, esses resultados tendem a refletir-se na economia e na sociedade. O crescimento económico e a criação de riqueza podem abrandar ou até mesmo ser invertidos quando o setor bancário não consegue ter um bom desempenho. Ao nível social, o agravamento de taxas de juro, de prestações de crédito tende a colocar uma pressão económica e financeira sobre aqueles que contraíram empréstimos, podendo mesmo levar ao abandono do objetivo para que o empréstimo foi contraído.

3.1.2. Especificidades tecnológicas

Relativamente ao âmbito tecnológico, têm-se vindo a verificar diversas mudanças no setor financeiro impulsionadas por tecnologias como a IA, IoT, *Cloud*, o 5G ou a computação quântica. Estas inovações tecnológicas têm contribuído para a reformulação dos serviços financeiros, sugerindo novas e diferentes oportunidades quer para empresas, quer para consumidores⁶⁹³.

O setor bancário tem-se reinventado para dar resposta às exigências da era digital, sendo o surgimento das empresas de *fintech* (*Financial Technology*) uma das consequências dessa adaptação⁶⁹⁴. Este termo pode referir-se à tecnologia financeira ou às entidades ou empresas que, a operar no setor financeiro (bancário ou segurador, com o termo *Insurtech*), implementam modelos de negócio baseados naquelas novas tecnologias. O objetivo é agilizar procedimentos e inovar nas suas práticas de negócio com vista a melhorar a experiência do cliente.

⁶⁹¹ “Banco de Portugal atualiza séries longas do setor bancário português”, BPStat, Banco de Portugal, 26 de julho de 2023, <https://bpstat.bportugal.pt/conteudos/noticias/1955>.

⁶⁹² “Inovação e setor financeiro: simplificar é a regra”, *Observador*, 29 de novembro de 2023, <https://observador.pt/2023/11/29/inovacao-e-setor-financeiro-simplificar-e-a-regra/>.

⁶⁹³ “Inovação e setor financeiro: simplificar é a regra”, *Observador*, 29 de novembro de 2023.

⁶⁹⁴ “Inovação e setor financeiro: simplificar é a regra”, *Observador*, 29 de novembro de 2023.

As *fintech* atuam em diferentes áreas como serviços de informação de contas, serviços de pagamento, ativos e moedas virtuais, atividade de intermediação de crédito, entre outros⁶⁹⁵.

O surgimento de inovações tecnológicas como o *homebanking* ou a tecnologia de verificação de identidade (através de biometria, impressão digital ou reconhecimento facial) constituem ferramentas fundamentais para um aumento do conforto dos clientes ao permitirem a realização de um grande número de operações bancárias, quando lhes for mais conveniente e de forma tão segura quanto possível⁶⁹⁶.

Os desenvolvimentos tecnológicos neste setor não se limitam à melhoria da experiência dos utilizadores, passando também por aumentar o nível de proteção dos dados dos clientes e das transações realizadas, considerando a sensibilidade dos dados que estas implicam. Os bancos utilizam, atualmente, soluções de segurança como a criptografia de dados, a 2FA, o 3D Secure ou a monitorização contínua de atividades suspeitas⁶⁹⁷. O 3D Secure reforça a segurança dos serviços de compras na *internet* no momento de utilização de cartão de crédito. Este cenário permite, através de um código de validação que os clientes recebem no seu número de telemóvel, registado no seu banco, que confirmem que são os titulares do cartão. Esta ação diminui a possibilidade de atividade fraudulenta através da confirmação do titular do cartão a ser utilizado na respetiva compra. Consequentemente, aumenta a confiança no serviço prestado no *site* em que a compra está a ser realizada⁶⁹⁸. O 3D Secure acaba por ser um formato de 2FA, uma vez que, de forma a garantir a autenticidade da identificação de um cliente, são mais utilizadas duas combinações de dois fatores: uma palavra-passe juntamente com um código enviado por SMS para um número de telemóvel registado ou utilização de identificação facial ou impressão digital com código enviado para o telemóvel⁶⁹⁹.

Os *chatbots* e os assistentes virtuais são outras tecnologias que têm sido exploradas neste setor permitindo que os clientes obtenham apoio por parte dos bancos e dos serviços durante todo o ano e durante 24 horas por dia⁷⁰⁰.

A utilização de IA é particularmente relevante neste setor ao nível da cibersegurança, onde torna possível identificar ataques e ciberameaças às bases de dados de clientes. Além disso, contribui muito para a transformação digital do setor, através de funções de processamento massivo de dados e algoritmos⁷⁰¹. A IA também desempenha um papel crucial na deteção e prevenção de fraudes no setor bancário. Especialistas explicam que, por meio de análises avançadas de dados e *machine learning*, os sistemas de IA são capazes de identificar padrões suspeitos ou anómalos em transações financeiras. Isso assegura uma abordagem proativa na proteção das contas dos clientes contra fraudes e atividades maliciosas⁷⁰².

⁶⁹⁵ “Fintech: o que são e o que fazem”, Saldo Positivo, Caixa Geral de Depósitos, 4 de abril de 2023, <https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/o-que-sao-fintech.aspx>

⁶⁹⁶ “Inovação e setor financeiro: simplificar é a regra”, *Observador*, 29 de novembro de 2023.

⁶⁹⁷ “Inovação e setor financeiro: simplificar é a regra”, *Observador*, 29 de novembro de 2023.

⁶⁹⁸ “A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor”, *Business IT*, 21 de outubro de 2022, <https://business-it.pt/2022/10/21/a-tecnologia-e-a-banca-as-inovacoes-que-estao-a-permitir-digitalizar-o-setor/>.

⁶⁹⁹ “A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor”, *Business IT*, 21 de outubro de 2022.

⁷⁰⁰ “Inovação e setor financeiro: simplificar é a regra”, *Observador*, 29 de novembro de 2023.

⁷⁰¹ “A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor”, *Business IT*, 21 de outubro de 2022.

⁷⁰² Flávia Magalhães, “IA e o setor financeiro: A revolução da tecnologia”, *Consumidor Moderno*, 29 de fevereiro de 2024, <https://consumidormoderno.com.br/ia-e-o-setor-financeiro-a-revolucao-da-tecnologia/>.

Outra das tecnologias que impactaram de forma significativa o contexto de utilização de IA no setor bancário foi o aumento da utilização de robôs de investimento - “*robo-advisors*”. Esta tecnologia consiste em sistemas automatizados que “utilizam algoritmos complexos para tomar decisões de investimento com base em objetivos, tolerância ao risco e dados do mercado”. Algumas empresas oferecem plataformas que recorrem a IA com capacidade para gerir portfólios de investimentos. Este tipo de serviços permite consultoria financeira personalizada mais acessível que consultoria tradicional humana⁷⁰³.

⁷⁰³ Magalhães, “IA e o setor financeiro”, 29 de fevereiro de 2024.

3.2. Ameaças

As ameaças à cibersegurança são transversais a todo o setor bancário, não havendo correlação entre a dimensão da instituição financeira e as perdas de informação devido a uma ameaça, segundo o relatório “Cyber Risk for the Financial sector: A framework for Quantitative Assessment”, publicado pelo International Monetary Fund (IMF) em 2020. A perda de informação e as possíveis consequências dessas perdas podem ter resultados desastrosos no normal funcionamento da instituição, independentemente da dimensão que a instituição apresente. Ao considerar as ameaças mais comuns direcionadas às instituições bancárias, é possível identificar 3 categorias: **Fraude, Data Breach e Business Disruption**, sendo que cada uma destas ameaças/eventos causa um impacto diferente nas instituições⁷⁰⁴:

- As ameaças integradas no contexto de **Fraude** têm como objetivo aceder a informação confidencial dos clientes, incluindo as credenciais usadas pelos próprios em compras *online*, resultando em transferências de dinheiro não autorizadas e perdas de montantes. De acordo com o BCE, este tipo de eventos desceu 11% em 2021⁷⁰⁵ e o valor total ascendeu a 4 mil milhões de euros em 2022 e a 2 mil milhões na primeira metade de 2023⁷⁰⁶;
- Como já referido, uma **data breach** corresponde a um incidente onde há um ataque intencional por parte de um agente criminoso que lhe permite ganhar acesso não autorizado e divulgar dados sensíveis, confidenciais e protegidos. Este tipo de incidente, por ser mais complexo de detetar, pode ser apenas detetado e reportado meses ou anos após o início do incidente;
- **Business Disruption** é um incidente onde, através de ataques de DDoS, o agente malicioso impede o normal funcionamento das atividades da empresa, danificando a reputação da empresa e de recursos monetários⁷⁰⁷.

Segundo o artigo “Cyber Risk: A Growing Concern for Macrofinancial Stability”, publicado em abril de 2024, em 2020 houve uma estimativa de perdas de 1000 milhões de dólares, já em 2021 este número aumentou para 2500 milhões. Em 2019 o valor tinha sido de quase 2000 milhões. Podemos verificar que entre 2019 e 2020 ocorreu uma diminuição, mas em 2021 ocorreu um grande aumento tendo atingido o máximo nos últimos 4 anos⁷⁰⁸.

De acordo com o *Threat Landscape Report* de 2023 da ENISA, os principais ataques passam pelo comprometimento da disponibilidade dos serviços e da informação (ataques de negação de serviço: “*Denial of Service*”, DoS), ataques de *ransomware*, contando-se ainda ameaças relativas a dados (*data breaches* e furto de dados)⁷⁰⁹.

⁷⁰⁴ Antoine Bouveret, “Cyber Risk for the Financial sector: A framework for Quantitative Assessment”, *Working Paper* do Fundo Monetário Internacional, junho de 2018, 4-5, <https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924>.

⁷⁰⁵ “Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures”, European Central Bank, maio de 2023, <https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html>

⁷⁰⁶ “ECB and EBA publish joint report on payment fraud”, European Central Bank, agosto de 2024, <https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html>

⁷⁰⁷ Bouveret, “Cyber Risk for the Financial sector”, junho de 2018, 4-5.

⁷⁰⁸ “Cyber Risk: A Growing Concern for Macrofinancial Stability”, International Monetary Fund, abril de 2024, 7, <https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3onlineannex.ashx>

⁷⁰⁹ ENISA, “ENISA Threat Landscape 2023”, 19 de outubro de 2023, 14, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@download/fullReport>.

Em fevereiro de 2020, Christine Lagarde, presidente do Banco Central Europeu, veio a público, alertar que um ciberataque poderia originar uma crise financeira, afirmações estas que foram corroboradas pelo FSB (Financial Stability Board)⁷¹⁰. De acordo com o Fórum Económico Mundial, o risco de ciberataques e de perdas monetárias subiu. Em 2017 houve cerca de 8 mil incidentes e em 2021 houve cerca de 11 mil incidentes⁷¹¹.

O artigo "Cybersecurity threats in the banking sector" publicado em maio de 2022 refere que, no primeiro semestre de 2021, os ataques de chantagem aumentaram cerca de 1300 por cento em relação ao ano anterior. Este artigo também refere que os ataques digitais mais comuns no setor bancário são o furto ou o comprometimento de credenciais. Outro ataque muito comum são os ataques de *Phishing*, sendo este tipo de ataque muito complicado de gerir porque, normalmente, tem como alvos funcionários. O terceiro ataque mais comum são os ataques de *Ransomware* e, estes, tem como objetivo bloquear o acesso dos funcionários aos seus e dados aos dados da empresa, pedindo, normalmente, alguma quantia financeira para voltarem a ter acesso a estes⁷¹².

De seguida, é abordado cinco dos maiores ataques de cibersegurança no setor bancário. Estes incidentes não só tiveram um impacto significativo nas instituições financeiras envolvidas, mas também revelaram vulnerabilidades nos seus sistemas:

- O ataque à JPMorgan Chase em 2014 foi um dos maiores comprometimentos de dados na história do setor financeiro. *Hackers* conseguiram invadir a rede da empresa, aceder a informações de cerca de 76 milhões de contas de clientes e 7 milhões de empresas. Foi explorada uma vulnerabilidade de segurança, o que permitiu furtar dados pessoais tais como: nomes, endereços, números de telefone e emails⁷¹³.
- Em fevereiro de 2016, um ciberataque ao Banco Central de Bangladesh resultou no furto de 81 milhões de dólares devido a uma vulnerabilidade no *software* SWIFT. Investigadores descobriram que os atacantes instalaram um *malware* no sistema SWIFT do banco, permitindo-lhes apagar registos de transferências fraudulentas. Embora a maioria das transações tenha sido bloqueada, uma parte significativa dos fundos foi desviada para as Filipinas. A SWIFT lançou uma atualização de *software* para mitigar o ataque e alertou os bancos para reforçar a segurança interna. O ataque foi altamente sofisticado e personalizado para a infraestrutura do Bangladesh Bank, os criminosos utilizaram credenciais administrativas comprometidas.⁷¹⁴
- Cerca de 130 milhões de cartões de crédito e débito foram furtados em janeiro de 2018 do *website* da Heartland, através de um ataque de injeção de *SQL*. Os dados comprometidos no ataque foram: número de cartões de crédito, expiração dos mesmos e o nome dos titulares⁷¹⁵;

⁷¹⁰ Tim Maurer e Arthur Nelson, "The Global Cyber Threat to Financial Systems", FINANCE & DEVELOPMENT, março de 2021, 2, <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>.

⁷¹¹ Johnny Wood, "Global financial stability at risk due to cyber threats, IMF warns. Here's what to know", *World Economic Forum*, 15 de maio de 2024, <https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/>.

⁷¹² Oliver Gulyas e Gabor Kiss, "Cybersecurity threats in the banking sector", junho de 2022, 1070 e 1071, <https://ieeexplore.ieee.org/abstract/document/9804140>.

⁷¹³ Jessica Silver-Greenberg, Matthew Goldstein e Nicole Perlroth, "JPMorgan Chase Hacking Affects 76 Million Households", *The New York Times*, outubro de 2014, <https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>.

⁷¹⁴ "Bangladesh Bank hackers compromised SWIFT software, warning issued", *Reuters*, 25 de abril de 2016, <https://www.reuters.com/article/world/exclusive-bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DW/>.

⁷¹⁵ Julia S. Cheney, "Heartland Payment Systems: Lessons Learned from a Data Breach", janeiro de 2010, 4, <https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/d-2010-january-heartland-payment-systems.pdf?la=en&hash=EEAF5C96513D6E176D6C5312E4007061>.

- Em setembro de 2017 ocorreu um comprometimento de dados na Equifax e cerca de 147 milhões de clientes foram afetados. Este comprometimento deveu-se a uma vulnerabilidade não corrigida no *Apache*. Os dados comprometidos no ataque foram: nome, data de nascimento, número da segurança social, carta de condução e números de cartões de crédito⁷¹⁶;
- Em maio de 2019, mais de 800 milhões de registos financeiros foram furtados devido a um erro no website da First American Financial Corp Data. Os dados comprometidos no ataque foram: nome, email e números de telemóvel dos compradores⁷¹⁷;
- Em 2019, a Capital One sofreu um ataque significativo quando um hacker conseguiu explorar uma falha numa configuração de segurança do servidor na nuvem. Este acesso indevido resultou numa exposição de dados de mais de 100 milhões de clientes, incluindo informações pessoais e financeiras, como números de contas e dados de crédito. A vulnerabilidade foi um erro na configuração da firewall⁷¹⁸;

⁷¹⁶ “Equifax Data Breach Settlement”, Federal Trade Commission, fevereiro de 2024, <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>.

⁷¹⁷ AJ Dellinger, “Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?”, Forbes, maio de 2019, <https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/>.

⁷¹⁸ Shaharyar Khan et al., “A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned”, novembro de 2022, <https://dl.acm.org/doi/10.1145/3546068>

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos⁷¹⁹, de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal⁷²⁰.
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa⁷²¹.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável⁷²².
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso⁷²³. No caso, consideraram-se os colaboradores internos maliciosos.

⁷¹⁹ CNCS, “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.

⁷²⁰ CNCS, “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”, maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>.

⁷²¹ CNCS, “Relatório Riscos & Conflitos 2021”, 75.

⁷²² CNCS, “Relatório Riscos & Conflitos 2021”, 75-76.

⁷²³ CNCS, “Relatório Riscos & Conflitos 2021”, 76-77.

Tabela 37 - Agentes de ameaça mais prováveis (Bancário)

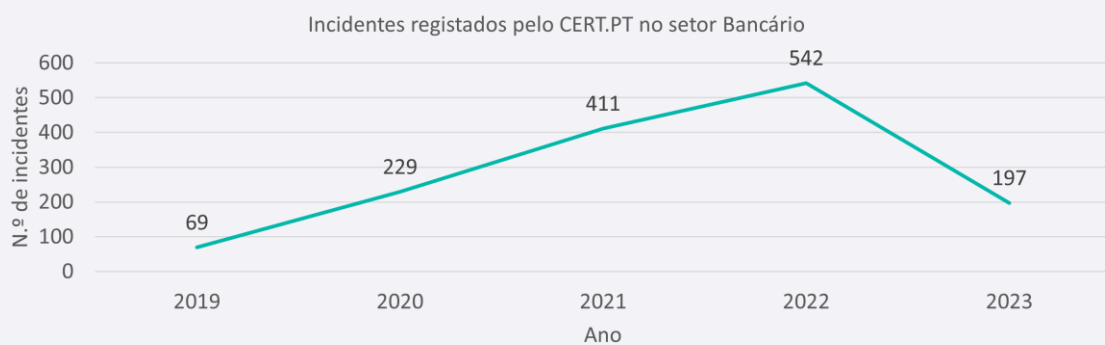
Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>	■	■	■	■
<i>Malware</i>	■	■	■	■
Vulnerabilidades	■	■	■	■
<i>Phishing e Smishing</i>	■	■		
Acesso indevido a dados pessoais	■	■	■	■
<i>DDoS</i>	■	■	■	
Manipulação de Sistemas (TI)	■	■		■

Legenda:

■ - Agente de ameaça provável

A atratividade do setor bancário para ciberataques é comprovada pelo número de ataques que o setor tem sofrido em Portugal. Segundo dados do CERT.PT, registaram-se, entre 2019 e 2023, 1448 ataques, sendo o setor que sofreu mais ataques⁷²⁴.

Figura 4 - Número de incidentes no setor Bancário anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização em 18 de setembro de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

⁷²⁴ CNCS, "Incidentes e Setores", Conhecimento Situacional: Estatísticas, <https://www.cncs.gov.pt/pt/estatistica/#cert.pt>

3.3. Capacitação

No que diz respeito à formação e consciencialização em matéria de cibersegurança no setor bancário, a European Banking Authority (EBA) dinamiza sessões de formação e *workshops* para entidades supervisoras e reguladoras pertencentes aos Estados-Membros. Adicionalmente, inclui nos requisitos para os reportes de riscos exigidos às entidades supervisionadas a inclusão de riscos relacionados com tecnologias de informação e comunicação (TIC) e cibersegurança, tornando-se temáticas abordadas com frequência nos relatórios de avaliação de riscos publicados. O *FinTech Knowledge Hub*, pertencente à EBA, contribui também para a formação das autoridades competentes nestas áreas.

Também a Federação Bancária Europeia (EBF, no inglês) contribui para a formação e sensibilização em contexto de cibersegurança. O seu grupo de trabalho de cibersegurança promove campanhas e iniciativas de sensibilização com o objetivo de melhorar as capacidades de cibersegurança no *staff* das empresas do setor. Promove também eventos e iniciativas de diversos tipos com o objetivo comum de contribuir para uma melhor cibersegurança.

No contexto português, a sensibilização para as questões de cibersegurança no setor bancário tornou-se uma preocupação, principalmente, para o BdP, autoridade supervisora e reguladora do sistema financeiro. Desenvolve mecanismos de sensibilização em conjunto com a EBA. O BdP apresenta na sua página um separador dedicado inteiramente à sensibilização e segurança aquando da utilização dos diferentes canais digitais, nomeadamente quando estes são usados para efetuar pagamentos, transações ou outro tipo de operações bancárias.

Os tópicos abordados neste separador estão descritos mais detalhadamente na tabela seguinte:

Tabela 38 - Capacitação no setor Bancário

Tópico	Descrição
Risco	• <i>Phishing</i> • <i>Pharming</i> • <i>Spyware</i> • <i>SIM card swap</i> • <i>Shoulder surfing</i>
Cuidados a ter	• Cuidados a observar na realização de operações bancárias através de canais digitais • Cuidados especiais a observar no homebanking • Cuidados especiais a observar em pagamentos na internet
<i>Big Data</i>	• Riscos para os consumidores • Precauções a tomar pelos consumidores

A título de exemplo, o BdP lançou, a 7 de fevereiro de 2023, a campanha #ficaadica, que tem como principal objetivo o de sensibilizar o público em geral, nomeadamente a população jovem e adulta, para os riscos de aceder a produtos e serviços bancários digitais. Para tal, o BdP preparou uma brochura e vídeos explicativos dos riscos a evitar durante a navegação online, em especial, assuntos relacionados com os pagamentos e transferências online⁷²⁵.

Na brochura acima mencionada, é possível encontrar tópicos como: conhecer os riscos que podem surgir durante a navegação na Internet; como aceder corretamente e de forma segura a conta bancária online; como abrir uma conta bancária à distância de forma segura e como fazer compras online de forma segura⁷²⁶. Na análise do “Plano Estratégico do BdP 2021-2025”, é possível entender que existe preocupação relativamente à proteção do mercado bancário (leia-se em Orientação Estratégica 2). Nesta orientação, o BdP define várias prioridades estratégicas como acompanhamento da evolução dos modelos de negócio das instituições com foco em dimensões como a transformação digital e resiliência operacional; revisão de modelos de análise de risco de BCFT do setor financeiro ou dinamização de um estratégia médio/longo prazo de literacia financeira digital para Portugal, promovendo a inclusão financeira através da utilização adequada e segura dos canais digitais no acesso a produtos bancários de retalho⁷²⁷.

Em 2021, espelhado no relatório de Atividades e contas do BdP, foram realizadas diferentes atividades em conjunto com as entidades financeiras: um workshop relativo à temática de inovação digital com especialistas e indústria, a criação de um Fórum com a Indústria para a Cibersegurança e Resiliência Operacional - com representantes do setor bancário, do prestador de serviços críticos de pagamento e da autoridade nacional de cibersegurança - e ações de diálogo com as instituições supervisionadas para apresentar as novidades legislativas em matéria de planeamento da resolução. Foi também iniciada a implementação do quadro de referência europeu para a realização de testes de intrusão em Portugal (TIBER-EU)⁷²⁸.

⁷²⁵ Banco de Portugal, “Campanha #ficaadica. Banco de Portugal divulga brochura com conselhos sobre o acesso a produtos e serviços bancários digitais”, 7 de fevereiro de 2023. <https://www.bportugal.pt/comunicado/campanha-ficaadica-banco-de-portugal-divulga-brochura-com-conselhos-sobre-o-acesso>.

⁷²⁶ Banco de Portugal, “Campanha #ficaadica”.

⁷²⁷ Banco de Portugal, “Plano Estratégico 21-25”, 14.

⁷²⁸ Banco de Portugal, “Relatório do Conselho de Administração - Atividade e Contas 2021”, 43.

3.4. Investimento em cibersegurança

O relatório “NIS Investments” de 2023, elaborado pela ENISA, indica que o setor bancário tem sido, a nível europeu, o que mais investe em segurança da informação, em comparação com os restantes setores. Em média, cada OSE do setor bancário europeu tem investido, por ano, cerca de 10 milhões de euros em segurança da informação. A mediana desse investimento, no entanto, ronda os 2 milhões de euros de investimento anual por OSE⁷²⁹. A ENISA opta por apresentar os dois valores (média e mediana) por considerar que a mediana oferece uma visão mais próxima do que é a realidade de investimento da maioria dos OSE, uma vez que o valor da média é de certo modo “deturpado” pelas entidades bancárias de maior dimensão e que realizam investimentos mais avultados⁷³⁰. O mesmo relatório indica ainda que o investimento realizado em segurança da informação por este setor tem representado, de 2020 a 2022, cerca de 7% do investimento global realizado nas TIC⁷³¹.

A nível nacional, as demonstrações financeiras e relatórios de contas tendem a não mencionar o investimento específico em cibersegurança, mas sim os gastos com equipamento ou serviços de informática. Por exemplo, o Relatório de Contas do Novo Banco indica gastos com serviços de informática na ordem de quase 44 milhões de euros em 2022 e de 46,4 milhões de euros em 2023⁷³². O mesmo relatório indica que o valor do equipamento informático enquanto ativo tangível foi avaliado em praticamente 118 milhões de euros em 2022 e em 126 milhões de euros em 2023⁷³³.

No caso do banco Santander Totta, o Relatório Anual de 2023 indica a despesa realizada com a manutenção de *hardware* e de *software*. Em 2022, esta despesa foi de cerca de 74 milhões de euros e, em 2023, de cerca de 88 milhões de euros⁷³⁴.

No relatório de contas do Banco Montepio é referenciada uma rubrica destinada a serviços especializados em informática que totalizou os 13,2 milhões de euros em 2022 e 16,4 milhões de euros em 2023⁷³⁵.

Em relação ao Banco Português de Investimento (BPI), contabilizaram-se 46,7 milhões de euros em 2022 e 65,5 milhões de euros em 2023 destinados a serviços de comunicações e informática⁷³⁶.

No que diz respeito à Caixa Geral de Depósitos, verifica-se que as despesas com serviços de informática totalizaram em 2022, 47,6 milhões de euros e, em 2023, 42,77 milhões de euros⁷³⁷. A estas acrescem ainda as despesas com serviços de informações, que representaram gastos de 4,44 milhões de euros em 2022 e gastos de 4,56 milhões de euros em 2023⁷³⁸.

⁷²⁹ ENISA, “NIS Investments”, novembro de 2023, 21, <https://www.enisa.europa.eu/publications/nis-investments-2023>.

⁷³⁰ ENISA, “NIS Investments”, 16.

⁷³¹ ENISA, “NIS Investments”, 24.

⁷³² Novo Banco, “Relatório e Contas 2023”, 28 de fevereiro de 2024, 349, <https://www.novobanco.pt/content/dam/novobancopublicsites/docs/pdfs/divulga%C3%A7%C3%B5es-financeiras/2023/relat%C3%B3rio-e-contas/RC%20novobanco%202023.pdf.coredownload.inline.pdf>.

⁷³³ Novo Banco, “Relatório e Contas 2023”, 370.

⁷³⁴ Banco Santander Totta, “Annual Report 2023: Proposal”, 17 de maio de 2024, 180, [https://www.santander.pt/pdfs/investor-relations/santander-totta-sa/relatorio-e-contas/2023/BST Annual Report 2023 non official non audited.pdf](https://www.santander.pt/pdfs/investor-relations/santander-totta-sa/relatorio-e-contas/2023/BST%20Annual%20Report%202023%20non%20official%20non%20audited.pdf).

⁷³⁵ Banco Montepio, “Relatório e Contas 2023”, 15 de abril de 2024, 183, <https://www.bancomontepio.pt/content/dam/montepio/pdf/institucional/investor-relations/relatorios-comunicados-e-informacao-financeira/2023/informacao-anual/relatorio-contas-anual-banco-montepio-2023.pdf>.

⁷³⁶ Banco Português de Investimento, “Relatório e Contas 2023”, 368, https://www.bancobpi.pt/content/service/getContent?documentName=PR_UCMS02106736.

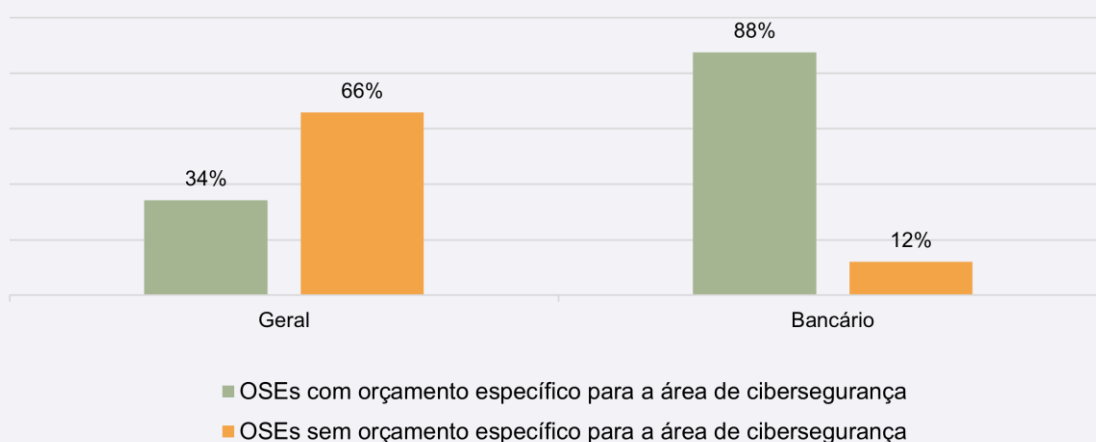
⁷³⁷ Caixa Geral de Depósitos, “Relatório de Gestão e Contas 2023”, 203, <https://www.cgd.pt/Investor-Relations/Informacao-Financeira/CGD/Relatorios-Contas/Pages/Relatorios-Contas-CGD.aspx>.

⁷³⁸ Caixa Geral de Depósitos, “Relatório de Gestão e Contas 2023”, 203.

Apesar de estes relatórios não indicarem os montantes específicos alocados à cibersegurança, é possível verificar que esta tem sido incluída nos objetivos e estratégias definidos para os próximos anos, e que têm sido também realizadas apostas na certificação das entidades bancárias em *standards* internacionais, como a ISO 27001 ou CMMI⁷³⁹, bem como na formação dos colaboradores. Por exemplo, o relatório do Banco Montepio indica terem sido contabilizadas mais de cinco mil horas de formação em cibersegurança e outras mais de cinco mil horas de formação no âmbito da Continuidade de Negócio durante o ano de 2023⁷⁴⁰, e o relatório da CGD indica ter realizado sessões de formação em cibersegurança especialmente dedicadas à temática do *ransomware*, entre outras⁷⁴¹.

De acordo com o questionário realizado, cerca de 88% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



⁷³⁹ Banco Português de Investimento, "Relatório e Contas 2023", 138.

⁷⁴⁰ Banco Montepio, "Relatório e Contas 2023", 34.

⁷⁴¹ Caixa Geral de Depósitos, "Relatório de Gestão e Contas 2023", 710.

Relativamente às áreas de aplicação do orçamento de cibersegurança, 89% aplica na segurança das redes, 81% na aquisição de *hardware* e *software*, 77% na análise de segurança, 73% na capacitação em tecnologia e 72% na gestão de vulnerabilidades (Gráfico 110 e 110.3).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

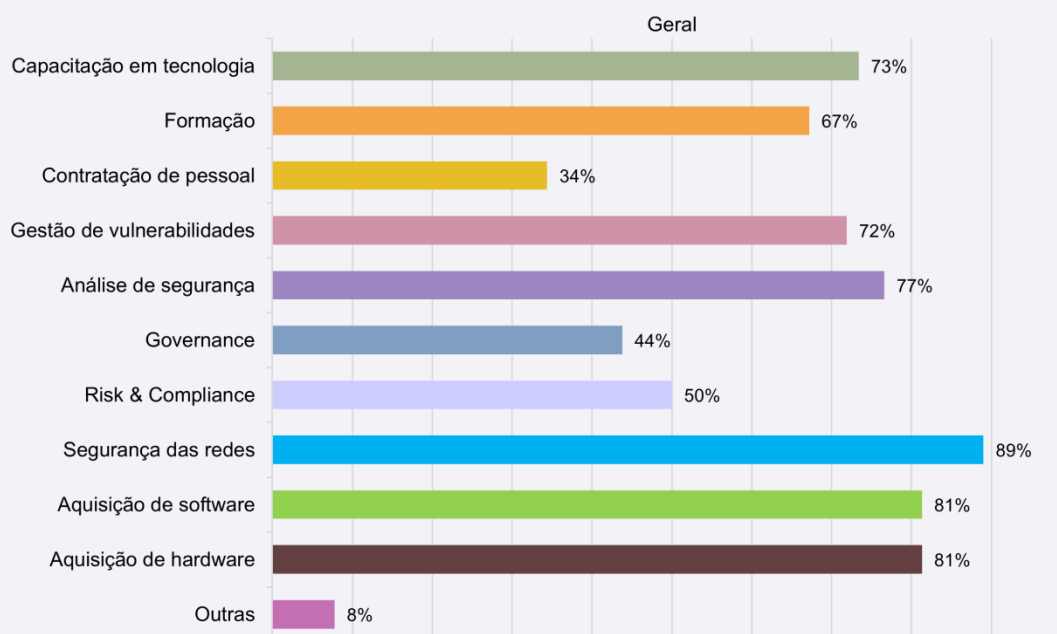
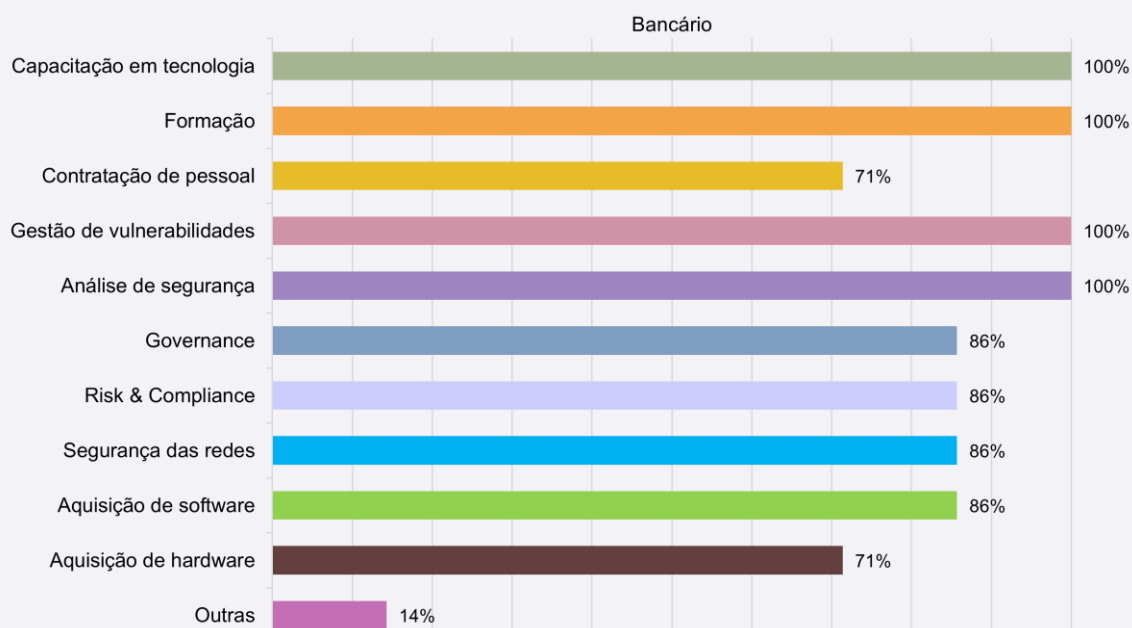
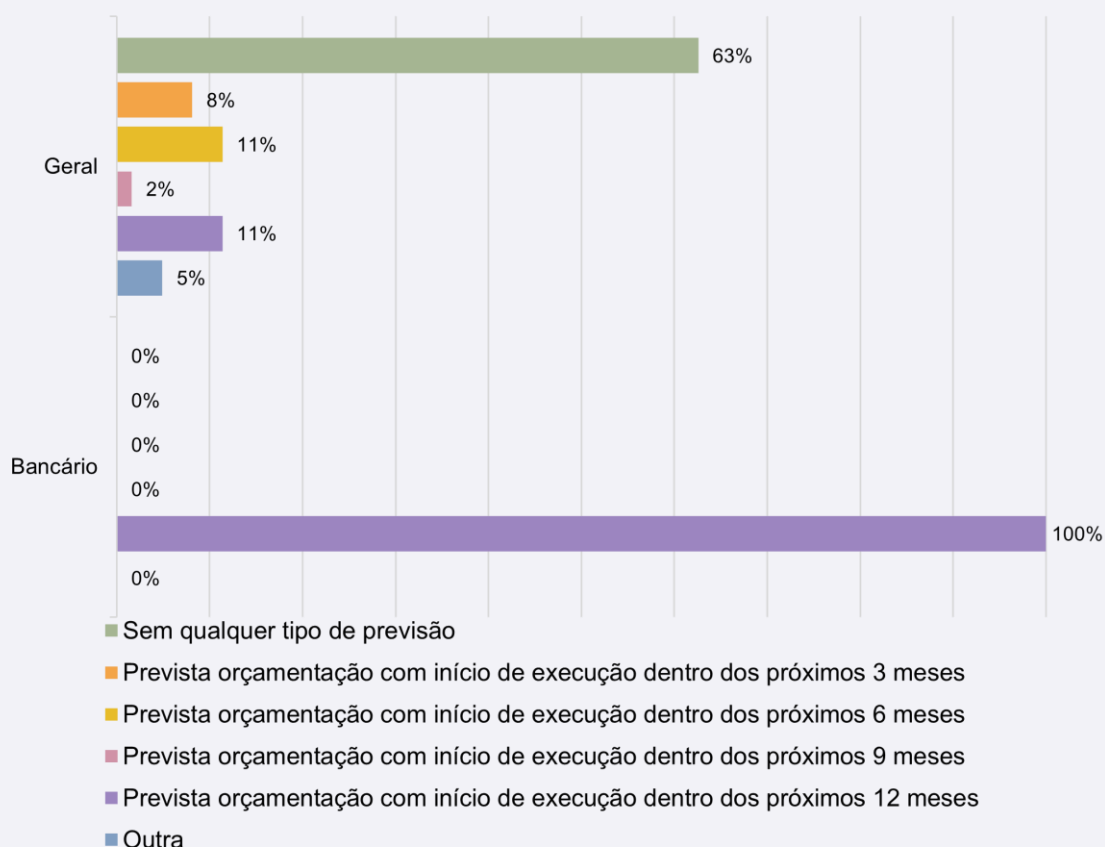


Gráfico 110.3 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 100% tem previsto a orçamentação dentro dos próximos 12 meses (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Embora não se tenham verificado, nos documentos mencionados, rubricas destinadas especificamente à cibersegurança, algumas ações enquadradas na orçamentação de informática contribuem para uma maior resiliência digital e operacional tais como manutenção de sistemas informáticos, atualização de *hardware* e *software*, controlo de acessos, promoção de reportes a autoridades de supervisão, entre outros.

3.5. RJSC e legislação setorial

O setor bancário, pelo papel que desempenha na economia e na sociedade, e pela gestão de avultados volumes de capital e informações sensíveis que realiza, tanto a nível individual como empresarial, tem forçosamente de ser um setor seguro em várias vertentes. O cumprimento de normas de segurança e transparência é essencial para garantir a proteção dos depósitos, a resiliência contra fraudes e ataques, bem como a continuidade dos serviços. O setor obedece assim a um quadro regulatório e legal rigoroso, no qual é contemplada a cibersegurança.

O principal diploma que rege o setor bancário é o Decreto-Lei n.º 298/92, de 31 de dezembro (1992), também conhecido como Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF). Embora o principal foco do diploma seja a supervisão das instituições de crédito e sociedades financeiras, são também incluídas disposições acerca da necessidade de informar o Banco de Portugal sobre os “processos de segurança e controlo no domínio informático”⁷⁴², de manter um inventário “pormenorizado e descrição dos principais sistemas de informação de gestão utilizados (...) incluindo os destinados à gestão de risco, (...) com discriminação por entidades, funções críticas e linhas de negócio estratégicas”⁷⁴³, e ainda “medidas de gestão de risco”, nas quais se incluem as medidas de gestão do risco relacionadas com a cibersegurança.

Em 2007, a Diretiva 2007/64/CE, relativa aos serviços de pagamento no mercado interno (ou Diretiva dos Serviços de Pagamento - PSD), criada para regular os serviços de pagamento na UE, impôs também obrigações de segurança relativamente aos pagamentos, tais como o de garantir formas de autenticação segura, de modo que “apenas o utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento”⁷⁴⁴ o utiliza. Dito de outra forma, a Diretiva impôs obrigações de segurança ao nível da autenticação dos utilizadores.

Em 2015, esta Diretiva foi atualizada através de uma outra, a Diretiva (UE) 2015/2366, de 25 de novembro (PSD 2), de modo a responder às novas realidades digitais, como o crescimento do comércio eletrónico e a emergência de novos atores no setor dos pagamentos, como as *fintechs*. Ao nível da cibersegurança, a Diretiva veio reforçar as obrigações relativas à autenticação segura dos clientes, impondo a necessidade da “autenticação forte do cliente (...) baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é)”⁷⁴⁵, ou seja, autenticação de dois passos ou autenticação multifator (MFA), de modo a prevenir acessos e transações não autorizadas, bem como fraudes.

No ano seguinte, 2016, foi publicada a Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União⁷⁴⁶, também conhecida como Diretiva SRI ou Diretiva NIS, cuja transposição para o ordenamento jurídico nacional, através da Lei n.º 46/2018, de 13 de agosto, estabeleceu o Regime Jurídico da

⁷⁴² Decreto-Lei n.º 298/92, de 31 de dezembro, “Regime Geral das Instituições de Crédito e Sociedades Financeiras - RGICSF”, artigo 120.º, alínea h), *Diário da República*, <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1992-70072322>.

⁷⁴³ Decreto-Lei n.º 298/92, artigo 138.º-AH, alínea, q).

⁷⁴⁴ Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007 relativa aos serviços de pagamento no mercado interno, artigo 57.º, n.º 1, alínea a), *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32007L0064>.

⁷⁴⁵ Diretiva (UE) 2015/2366 do Parlamento europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, artigo 4.º, n.º 30, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366>.

⁷⁴⁶ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, *Jornal Oficial da União Europeia*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148>.

Segurança do Ciberespaço (RJSC)⁷⁴⁷. Foi o RJSC que identificou o setor bancário como um setor de operadores de serviços essenciais e lhe impôs obrigações ao nível do cumprimento de medidas técnicas e organizativas adequadas para a gestão dos riscos relativos à segurança das redes e da informação, bem como de adoção de medidas para evitar incidentes e minimizar os impactos dos mesmos. Esta mesma legislação impôs a obrigatoriedade de reporte de incidentes de impacto relevante ao CNCS⁷⁴⁸. O RJSC viria a ser depois complementado em 2021 através do Decreto-Lei n.º 65/2021, de 30 de julho, que o regulamenta, ou seja, estabelece como determinadas normas do RJSC devem ser cumpridas. Deste Decreto-Lei decorrem obrigações como a designação de um ponto de contacto permanente pelas entidades abrangidas para comunicação com o CNCS, a designação de um responsável de segurança; a necessidade de elaborar e manter atualizado um inventário de ativos; um plano de segurança, que deve incluir a política de segurança e medidas de segurança adotadas; a elaboração de um relatório anual com informações sobre as atividades desenvolvidas ao nível da segurança e estatísticas semestrais de todos os incidentes e análise agregada dos incidentes de segurança com impacto relevante ou substancial⁷⁴⁹. É também imposta a necessidade de realizar análises de risco anuais e são definidos os tempos para a notificação de incidentes de impacto relevante ao CNCS⁷⁵⁰.

Depois, em 2022, foi publicado o Regulamento (UE) 2022/2554, relativo à resiliência operacional digital do setor financeiro, mais conhecido como Regulamento DORA (*Digital Operational Resilience Act*). Este regulamento abrange diversas entidades. Para além das bancárias, o Regulamento DORA abrange ainda entidades como as que compõem as infraestruturas do mercado financeiro (plataformas de negociação e contrapartes centrais), empresas de seguros, instituições de crédito, instituições de pagamento, empresas de investimento, entre várias outras⁷⁵¹. A estas “entidades financeiras”, como são comumente designadas no Regulamento DORA, são impostas diversas obrigações, que passam pela gestão do risco associado às tecnologias da informação e comunicação (TIC), gestão dos serviços e ferramentas TIC prestados por terceiros, gestão de sistemas, protocolos e ferramentas TIC, atividades de proteção e prevenção, deteção, resposta e recuperação em situação de incidente, reporte de incidentes, testes de resiliência operacional (como análises de vulnerabilidades, avaliações da segurança das redes, análises da segurança física, revisões do código fonte, entre outros) e ainda testes de intrusão com base em ameaças (*Threat-Led Penetration Testing - TLPT*), testes que exigem uma ampla recolha de informações sobre ameaças (*Threat Intelligence*) às quais uma entidade financeira possa estar exposta⁷⁵². Essa recolha deverá passar tanto pelas informações sobre ameaças cedidas pelas próprias entidades, como pela investigação, por exemplo, de informações confidenciais, como credenciais de utilizadores, divulgadas ou expostas na *dark web*⁷⁵³. A conformidade com o Regulamento DORA será obrigatória a partir de 17 de janeiro de 2025.

⁷⁴⁷ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

⁷⁴⁸ Lei n.º 46/2018, artigo 13.º.

⁷⁴⁹ Decreto-Lei n.º 65/2021, de 30 de julho, artigos 4.º a 8.º, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

⁷⁵⁰ Decreto-Lei n.º 65/2021, artigo 10.º e artigos 11.º a 15.º.

⁷⁵¹ Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro, artigo 2.º, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554>.

⁷⁵² Regulamento (UE) 2022/2554, artigos 6.º a 27.º.

⁷⁵³ Banco Central Europeu, “TIBER-EU Guidance for Target Threat Intelligence Report”, julho de 2020, 7, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.

Para além desta legislação, verificam-se ainda as recomendações, circulares e instruções das entidades reguladoras para o setor. Embora a autoridade reguladora do setor seja o BdP, podem surgir recomendações conjuntas para todo o setor financeiro, publicadas pelo Conselho Nacional de Supervisores Financeiros (CNSF), composto pelo BdP, pela Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) e pela Comissão do Mercado de Valores Mobiliários (CMVM). A título de exemplo, o CNSF aprovou, em 2021, as Recomendações sobre a Gestão da Continuidade de Negócio, que atualizam as Recomendações aprovadas em 2010. Nestas Recomendações é possível encontrar orientações destinadas à gestão do risco das TIC, à sua resiliência em situações de catástrofes naturais, como incêndios, inundações, falhas graves de energia; às infraestruturas alternativas, aos planos de continuidade de negócio, recuperação de desastres, e de comunicação, bem como à realização de testes, simulações e treinos no âmbito da continuidade de negócio⁷⁵⁴. Depois de seis anos passados desde a publicação da Diretiva NIS, foi publicada em 2022 a Diretiva (UE) 2022/2555⁷⁵⁵, mais comumente conhecida como NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: “setores de importância crítica”⁷⁵⁶ e “outros setores críticos”⁷⁵⁷. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsectores. São também introduzidas novas obrigações.

Apesar de a Diretiva NIS 2 abranger mais entidades nalguns setores, tal não acontece no setor bancário. As entidades visadas continuam a ser as mesmas já abrangidas pela Diretiva anterior. Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos⁷⁵⁸. Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto⁷⁵⁹. A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança. O Regulamento DORA inclui provisões semelhantes incentivando este tipo de acordos para o intercâmbio de “informações específicas e sensíveis relativas a ciberataques, nomeadamente indicadores de comprometimento dos sistemas ou dos dados, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração”⁷⁶⁰. Já a Diretiva NIS 2 estabelece que as informações partilhadas à luz destes acordos podem ser relacionadas com “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”⁷⁶¹.

⁷⁵⁴ Banco de Portugal, “Recomendações sobre Gestão da Continuidade de Negócio”, Carta Circular n.º CC/2021/00000047, 2021, 21, https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/463107899_6.docx.pdf.

⁷⁵⁵ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

⁷⁵⁶ Diretiva (UE) 2022/2555, Anexo I.

⁷⁵⁷ Diretiva (UE) 2022/2555, Anexo II.

⁷⁵⁸ Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

⁷⁵⁹ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

⁷⁶⁰ Regulamento (UE) 2022/2554, artigo 45.º, n.º 1.

⁷⁶¹ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

3.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor bancário, segundo a ENISA⁷⁶²:

Tabela 39 - Standards e Boas Práticas (Bancário)

Standards	Boas práticas
• ISO/TR 13569:2005; • Gramm–Leach–Bliley Act; • Sarbanes–Oxley Act; • Payment services (PSD 2) - Directive (EU) 2015/2366; • EBA on the security of internet payments; • ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services; • American National Standards Institute (ANSI) X9 series.	• Payment Card Industry Data Security Standard (PCI DSS); • Basel II; • Draft Guidelines on the security measures for operational and security risks of payment services under PSD2; • CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure; • SEC OCIE Cybersecurity.

Na tabela anterior estão os *standards* e boas práticas referentes à área do setor bancário. De seguida, apresenta-se um breve sumário de cada um:

- **ISO/TR 13569:2005:** Orientações para o desenvolvimento da segurança da informação das instituições da indústria financeira⁷⁶³;
- **Gramm–Leach–Bliley Act:** Lei dos EUA que exige que instituições financeiras protejam a confidencialidade e a segurança das informações dos clientes⁷⁶⁴;
- **Sarbanes–Oxley Act:** Lei dos EUA com disposições que afetam a governação das empresas, a gestão de riscos, auditorias e os relatórios financeiros das empresas públicas, incluindo disposições destinadas a dissuadir e punir a fraude e a corrupção⁷⁶⁵;
- **Payment services (PSD 2) - Directive (EU) 2015/2366:** Diretiva da UE com o objetivo de modernizar os serviços de pagamento na Europa, promovendo a inovação e aumentando a segurança nas transações⁷⁶⁶;
- **EBA on the security of internet payments:** Orientações da EBA para melhorar a segurança dos pagamentos pela Internet, reduzindo riscos de fraude e aumentando a proteção ao consumidor⁷⁶⁷;

⁷⁶² ENISA, "Mapping of OES Security Requirements", 2.

⁷⁶³ "ISO/TR 13569:2005", ISO, novembro de 2005, <https://www.iso.org/standard/37245.html>

⁷⁶⁴ "Gramm–Leach–Bliley Act", Business Guidance: Privacy and Security, United States Federal Trade Commission, <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>.

⁷⁶⁵ "The Sarbanes–Oxley Act", Sarbanes Oxley Act, <https://sarbanes-oxley-act.com/>.

⁷⁶⁶ Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366>.

⁷⁶⁷ "Orientações definitivas sobre a segurança dos pagamentos efetuados através da internet", EBA, https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/558993c7-c253-472c-bae3-f897f6c6038a/EBA-GL-2014-12_PT_rev1%20GL%20on%20Internet%20Payments.pdf.

- **ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services:** Fornece orientações específicas para a gestão da segurança da informação no setor financeiro. Tem como foco assegurar que as instituições financeiras implementem controlos adequados de forma a proteger dados sensíveis contra ameaças de cibersegurança⁷⁶⁸;
- **American National Standards Institute (ANSI) X9 series:** Conjunto de normas que definem padrões de segurança para transações financeiras, garantindo a integridade e confidencialidade das mesmas⁷⁶⁹;
- **Payment Card Industry Data Security Standard (PCI DSS):** Conjunto de padrões de segurança para proteger as informações dos cartões de pagamento e evitar fraudes⁷⁷⁰;
- **Basel II:** Acordo internacional que estabelece normas para a regulação bancária⁷⁷¹;
- **Draft Guidelines on the security measures for operational and security risks of payment services under PSD2:** Orientações preliminares para medidas de segurança e gestão de riscos operacionais nos serviços de pagamento sob a PSD2⁷⁷²;
- **CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure:** Diretrizes para aumentar a resiliência de cibersegurança das infraestruturas dos mercados financeiros⁷⁷³;
- **SEC OCIE Cybersecurity:** Diretrizes da SEC (Securities and Exchange Commission - EUA) para avaliar a postura de cibersegurança das empresas financeiras⁷⁷⁴.

De forma complementar à legislação aplicável, entidades pertencentes ao setor têm ainda que cumprir com *standards* nacionais e internacionais que fornecem orientações mais específicas e concretas na gestão de temáticas relacionadas com NIS.

A utilização destes *standards* permite melhorar as medidas de segurança nas entidades abrangidas e facilita a supervisão por parte das autoridades supervisoras e regulatórias, permitindo-lhes aferir a efetiva aplicação dos regulamentos e políticas.

⁷⁶⁸ “ISO/TR 27015:2012”, ISO, dezembro de 2012, <https://www.iso.org/standard/43755.html>

⁷⁶⁹ “X9: Accredited Standards Committee X9, Inc.”, ANSI Webstore, American National Standards Institute, https://webstore.ansi.org/sdo/x9?source=blog&_gl=1*v6wen5*_gcl_au*NzI0ODc2NzI1LjE3MjU1NTU5ODc.

⁷⁷⁰ “PCI Data Security Standard (PCI DSS)”, Standards, Security Standards Council, <https://www.pcisecuritystandards.org/standards/pci-dss/>.

⁷⁷¹ “Basel II: Revised international capital framework”, Basel Committee on Banking Supervision, Bank for International Settlements, <https://www.bis.org/publ/bcbsca.htm>.

⁷⁷² “Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)”, EBA, 12 de janeiro de 2018, [https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20\(EBA-GL-2017-17\)_PT.pdf](https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf).

⁷⁷³ “Guidance on cyber resilience for financial market infrastructures”, BIS e IOSCO, junho de 2016, <https://www.bis.org/cpmi/publ/d146.pdf>.

⁷⁷⁴ “OCIE Cybersecurity and Resiliency Observations”, U.S. Securities and Exchange Commission, <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>.

Outros exemplos de *standards* nacionais e internacionais aplicáveis ao setor bancário são os seguintes:

- **Minimum Requirements for Risk Management da German Federal Financial Supervisory Authority:** a Autoridade Supervisora da Alemanha Financeira Federal (*German Federal Financial Supervisory Authority*) fornece uma *framework* para a gestão de riscos em institutos financeiros alemães. A *framework* endereça as responsabilidades da gestão de topo, requisitos gerais para a gestão de riscos e de recursos (incluindo recursos humanos, sistemas, instalações técnicas, processos e planos de contingência)⁷⁷⁵.
- **Banking Act da German Federal Financial Supervisory Authority:** a Autoridade Supervisora da Alemanha Financeira Federal (BaFin) utiliza o *Banking Act* como instrumento de supervisão bancária. O *Banking Act* define as regras que instituições bancárias devem cumprir no decurso da sua operação. As regras são definidas por forma a permitir o funcionamento adequado do sistema bancário, incluindo um conjunto de requisitos alto-nível⁷⁷⁶.
- **National Banking Act do Banco Nacional da Suíça:** o *Banking Act* do Banco Nacional da Suíça obriga a que este supervisione os sistemas que operam compensações, liquidações e outros instrumentos financeiros. A legislação também se aplica a operadores que têm sede no estrangeiro, desde que partes substanciais da operação ou *stakeholders* chave estejam sedeados na Suíça⁷⁷⁷.
- **Management of operational risk, standard da Autoridade de Supervisão Financeira da Finlândia (Finnish Financial Supervisory Authority):** este *standard* define requisitos para a gestão de riscos operacionais em organizações financeiras. Nele são detalhadas instruções como: gestão de processos, recursos humanos, sistemas de informação e pagamentos, segurança da informação, planeamento de continuidade e riscos legais. Preocupa-se com os sistemas e serviços de pagamento, identificando oito controlos que o banco deverá implementar, como caracterização dos sistemas de pagamentos, meios de pagamento, princípios para a transferência de fundos nos sistemas de pagamentos, garantia de controlos internos de eficiência e a segurança dos serviços de pagamentos⁷⁷⁸.

No setor bancário e em todo o setor financeiro, a ENISA tem um papel ativo no apoio aos estados-membro da UE na resposta a crises decorrentes de incidentes de cibersegurança. O apoio prestado passa pela consciencialização e pela estruturação de procedimentos de resposta a incidentes, contribuindo para uma melhor tomada de decisão em momentos de resposta a crises. Adicionalmente, a ENISA gere o programa de exercícios Pan-Europeus denominado *Cyber Europe*⁷⁷⁹.

⁷⁷⁵ "Risk management", Federal Financial Supervisory Authority, dezembro de 2017, https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Risikomanagement/risikomanagement_node_en.html

⁷⁷⁶ "Gesetz über das Kreditwesen", Banking Act of the Federal Republic of Germany, setembro de 1998, <https://www.cftc.gov/sites/default/files/idc/groups/public/@otherif/documents/ifdocs/eurexmcobankingact.pdf>

⁷⁷⁷ "The SNB's legal basis", Swiss National Bank, <https://www.snb.ch/en/the-snb/organisation/legal-framework>

⁷⁷⁸ "Management of operational risk in supervised entities of the financial sector", FIN-FSA, agosto de 2014, https://www.finanssivalvonta.fi/globalassets/en/regulation/fin-fsa-regulations-and-guidelines/2014/08_2014/08_2014.m4_en.pdf

⁷⁷⁹ ENISA, "Cyber Europe Programme", 2024, <https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme>

Para além da ENISA, as seguintes estruturas contribuem também para a gestão de crises de cibersegurança na UE⁷⁸⁰:

- *European Association for Secure Transactions (EAST)*: apoia na identificação de incidentes e na preparação de ações qualificadas de resposta nas várias localizações;
- *Nordic Financial CERT*: apoia os estados-membro na resposta a incidentes e na recuperação dos mesmos;
- *European Payments Council*: promove uma melhor colaboração entre fornecedores de serviços de pagamentos através do grupo de trabalho *Payment Scheme Fraud Prevention Working Group (PSFPWG)*;
- *FS-ISAC*: fornece mecanismos de resposta e comunicação de crises, assim como recursos humanos de suporte, transversais às várias indústrias.

⁷⁸⁰ ENISA, “*Mapping of OES Security Requirements to Specific Sectors*”, 18 de janeiro de 2018, <https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors>

3.7. Desafios

De um modo geral, as grandes instituições bancárias a nível internacional demonstram uma boa capacidade de incorporar a gestão de risco na gestão da segurança dos seus sistemas de informação. Para isso, as entidades do setor seguem Sistemas de Gestão da Segurança da Informação (ISMS) e implementam controlos e *standards* como parte integrante do seu modelo de governo da segurança. Adicionalmente, muitos bancos são certificados em normas internacionais tais como a ISO 27001 e a ISO 22301, que garantem a implementação de boas práticas na área de *IT Governance* e que contribuem para uma melhor gestão de riscos, nomeadamente riscos de cibersegurança.

A gestão de riscos no setor bancário não se foca apenas em temas relacionados com a NIS. A gestão de riscos assenta em três pilares:

- Riscos financeiros: Qualquer tipo de risco associado ao financiamento de empresas, nomeadamente risco de crédito, risco de liquidez e risco operacional;
- Riscos operacionais: Qualquer tipo de risco associado às operações do dia-a-dia de uma determinada empresa;
- Riscos de segurança da informação: Qualquer risco associado à vulnerabilidade de certos ativos de uma empresa e que impacto no negócio caso estes sejam atingidos por um determinado incidente.

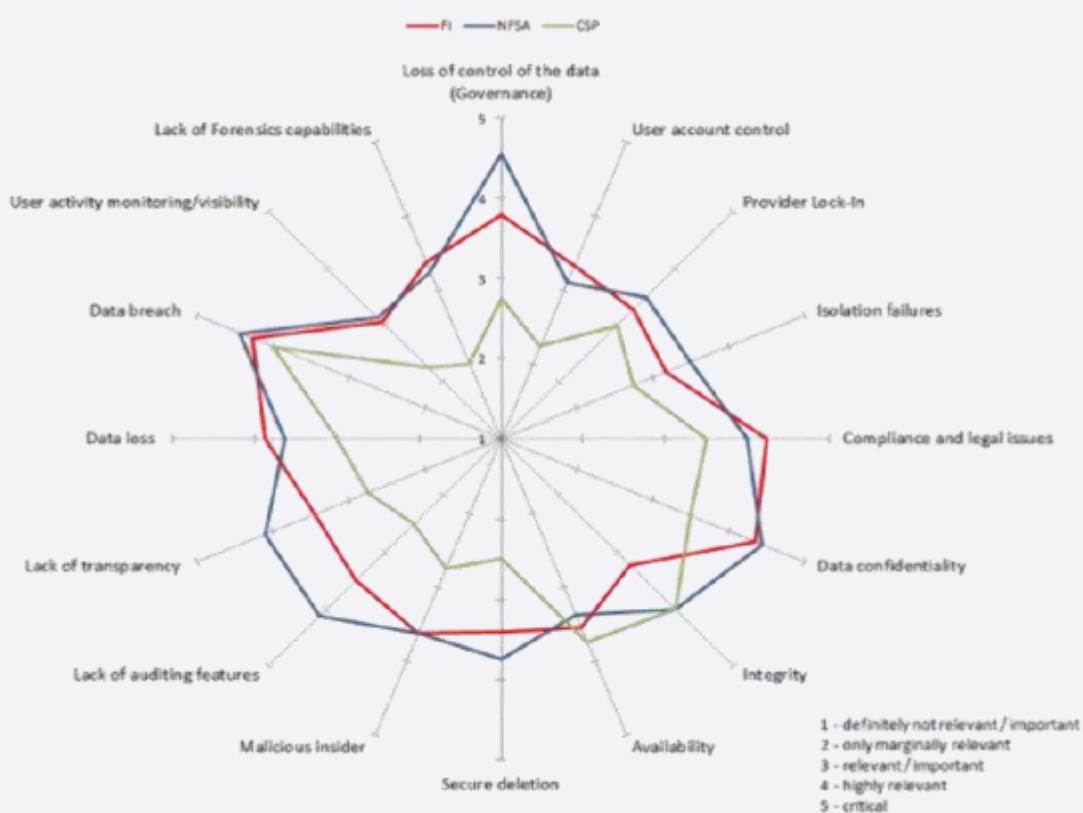
Apesar de os temas da NIS estarem em maior destaque nos riscos de segurança de informação, os restantes riscos, associados a contextos financeiro e operacional, direta ou indiretamente, podem ter impacto também nos próprios riscos de segurança de redes e informação. Isto faz com que a temática da NIS seja considerada transversal aos três pilares de gestão de riscos pelos atores do setor bancário. Uma das maiores vulnerabilidades e desafios neste setor, segundo o FMI, é a confiança colocada em infraestruturas críticas e a dependência do setor de redes altamente interligadas. As infraestruturas críticas do setor bancário abrangem vários sistemas, como sistemas de pagamento e sistemas de liquidação, e várias instituições/plataformas essenciais à infraestrutura como plataformas de *trading* e contrapartes centrais. Esta dependência, juntamente com a centralização de várias atividades numa única infraestrutura, constituem um risco muito elevado, que pode atingir os 3 pilares descritos anteriormente⁷⁸¹.

⁷⁸¹ Bouveret, “Cyber Risk for the Financial sector”, 11, junho de 2018.

No que diz respeito a serviços *cloud*, segundo ENISA, é possível identificar as diferentes preocupações demonstradas pelas instituições financeiras, pelas autoridades nacionais de supervisão financeira (ANSF) e pelos prestadores de serviços de *cloud*. Essas preocupações são as seguintes:

- As instituições financeiras consideram que os principais desafios a que estão sujeitos estão ao nível da confidencialidade dos dados, *data breach*, questões legais e de conformidade.
- No caso das ANSF, consideram a falta de transparência e falta de recursos de auditoria como os principais desafios a superar.
- Considerando os prestadores de serviços *cloud*, os principais desafios a superar estão relacionados com a integridade e disponibilidade dos dados e *data breach*⁷⁸².

Figura 5 - Perda de controlo de informação no setor Bancário



(Fonte: ENISA, "Secure Use of Cloud Computing in the Finance Sector", 7 de dezembro de 2015, 26, <https://www.enisa.europa.eu/publications/cloud-in-finance>)

⁷⁸² ENISA, "Secure Use of Cloud Computing in the Finance sector", 7 de dezembro de 2015, 26.

De acordo com o documento “Desafios da transformação digital para o Setor Bancário”, um dos grandes desafios é a criação de uma *API* denominada por *Open Banking* e, esta, tem como grande objetivo evoluir o setor para plataformas mais ágeis, distribuídas e escaláveis. Com o *Open Banking*, as contas passam a ser possíveis de serem acedidas por outras entidades, sendo assim possível, por exemplo, levantar montantes em qualquer país da UE apenas utilizando uma aplicação. O maior desafio será as *Big Tech*, visto estas fornecerem soluções de pagamento *end-to-end* em concorrência com o banco, alavancando os pagamentos tradicionais. É importante assim adaptar a regulação às *Big Tech* e bancos digitais, garantindo assim um tratamento justo e equilibrado entre os incumbentes e os novos operadores. Outro ponto crucial é remover barreiras à inovação, adaptando os *standards* às novas tecnologias⁷⁸³.

⁷⁸³ Hélder Rosalino, “Desafios da transformação digital para o Setor Bancário”, Fintech House Lisboa, janeiro de 2020, 8-18, <https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20200123.pdf>.

3.8. Recomendações

O relatório mencionado (“*Network and Information Security in the Finance Sector*”, ENISA) resulta na análise ao panorama da cibersegurança no setor financeiro com a formulação das seguintes recomendações:

- **Criação do *European Security Guidebook*:** definição de um conjunto de linhas orientadoras comuns que apresentem uma solução possível para a implementação de medidas uniformizadas de segurança operacional ao invés de regular os níveis de serviço. No contexto dos operadores do setor financeiro, a utilização de *standards* é a medida utilizada com maior frequência para garantir a prevenção, deteção e resposta a incidentes de segurança. Adicionalmente, é crucial definir linhas orientadoras transversais que facilitem a avaliação custo-benefício de investimentos em cibersegurança e o envolvimento da gestão de topo na tomada de decisão relacionada com cibersegurança;
- **Segurança da Cadeia de Abastecimento:** As entidades beneficiaram da implementação de mecanismos de transparência para partilha de riscos identificados.
- **Security Intelligence:** Cooperação internacional entre entidades bancárias é uma das formas mais eficazes para definir um conjunto de indicadores comuns. Esta medida permitiria garantir a consistência técnica dos mesmos e elaborar linhas orientadoras mais intuitivas para aplicação por parte das entidades bancárias. As instâncias de colaboração podiam ainda permitir a realização de *stress-tests* regulares no setor bancário⁷⁸⁴.

No relatório da ENISA mencionado anteriormente, foi também realizada uma avaliação das práticas de segurança em implementação no setor. Das respostas obtidas, foi possível verificar que as práticas implementadas nas entidades do setor estão em linha com os *standards* mencionados. Alguns exemplos de práticas implementadas conforme apresentadas pelas entidades inquiridas são:

- O responsável pela segurança da informação (*Chief Information Security Officer*) define as políticas, estruturas e técnicas a utilizar;
- As avaliações de riscos e respetivo impacto no negócio são feitos com periodicidade no mínimo anual;
- Todos os incidentes de segurança são registados, classificados, analisados e discutidos com equipas de auditoria interna em reuniões periódicas⁷⁸⁵.

⁷⁸⁴ ENISA, “*Network and Information Security in the Finance Sector: Regulatory landscape and Industry priorities*”, 2014, 31.

⁷⁸⁵ ENISA, “*Network and Information Security in the Finance Sector: Regulatory landscape and Industry priorities*”, 2014, 26-27.

Também num relatório elaborado pela ENISA denominado “*EU Cybersecurity Initiatives in the Finance Sector*”, publicado em março de 2021, é reunido um conjunto de ações no âmbito do setor bancário e financeiro que permitem uma maior resiliência em matéria de cibersegurança. Estas iniciativas estão divididas em 6 áreas principais, onde se listam algumas das atividades:

- **Desenvolvimento e implementação de políticas:**

- Estas iniciativas são da responsabilidade da Comissão Europeia (CE). A CE emitiu em 2018 o Plano de Ação “*Fintech*” que se propõe a alcançar uma mais forte ciberresiliência, através da partilha de informação entre operadores do mercado, promover a convergência de supervisão de gestão de riscos de IT, aumentar a coordenação da UE em processos *threat intel* entre EM (como TIBER-EU⁷⁸⁶);
- Em 2020, a *Digital Finance Strategy* definiu linhas gerais sobre como a Europa pode apoiar a transformação digital do setor bancário e financeiro nos próximos anos, regulando os seus riscos;
- O principal papel da EBA é o de contribuir para a criação do *European Single Rulebook*, com o objetivo de fornecer um conjunto único de regras de harmonização para as IF em toda a UE;
- Desenvolvimento e aplicação de Diretrizes da EBA sobre a comunicação de fraude em pagamentos *online* considerando a PSD2. As Diretrizes pretendem contribuir para o aumento da segurança dos pagamentos na UE, exigindo que as instituições de crédito, as instituições de pagamento e instituições de *e-money* colem e relatem dados sobre as transações de pagamento e transações de pagamento fraudulentas.
- Implementação do “TIBER-PT”, quadro de referência para testes de cibersegurança avançados pelas instituições de crédito em Portugal⁷⁸⁷.

- **Partilha de informação e capacitação:**

- O ECRB lançou a *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU) em 27 de fevereiro de 2020. O CIISI-EU reúne uma comunidade de entidades públicas e privadas com o objetivo de compartilhar informações e trocar boas práticas. Os principais objetivos do CIISI-EU são: proteger o sistema financeiro prevenindo, detetando e respondendo a ciberataques; facilitar a partilha de informação, inteligência e boas práticas entre infraestruturas financeiras; aumentar a consciencialização sobre as ameaças à cibersegurança.
- Plataforma e fórum da “CIISI-PT”, o centro para partilha e análise de informação sobre ameaças de cibersegurança do setor bancário. Em atividade desde setembro de 2023, o centro apresenta sinais positivos de crescimento e interação⁷⁸⁸.

⁷⁸⁶ TIBER-EU: estrutura europeia para *red-teaming* ético, baseado em *threat intelligence*. É o primeiro guia da UE sobre como autoridades, entidades e *threat intelligence* e provedores de *red-team* devem trabalhar juntos para testar e melhorar a resiliência em matéria de cibersegurança de entidades, através da realização de ciberataques controlados.

⁷⁸⁷ “Banco de Portugal avança na cooperação para a cibersegurança”, Banco de Portugal, maio de 2024, <https://www.bportugal.pt/comunicado/banco-de-portugal-avanca-na-cooperacao-para-ciberseguranca>.

⁷⁸⁸ “Banco de Portugal avança na cooperação para a cibersegurança”, Banco de Portugal, maio de 2024.

- **Gestão de crises de cibersegurança:**
 - A EBA promove ações de sensibilização em matéria de ciberresiliência através do seu trabalho político e atividades de convergência de supervisão. Isso envolve workshops e formação para entidades supervisoras e reguladores em toda a UE e em algumas jurisdições externas à UE. Do lado da supervisão, a EBA aumenta a sensibilização também incorporando detalhes específicos sobre TIC. Como parte de seu mandato para avaliar riscos e vulnerabilidades no setor bancário da UE, a EBA publica regularmente relatórios de avaliação de riscos de TIC e cibersegurança.
- **Formação e sensibilização:**
 - A Autoridade Bancária Europeia (EBA) promove a consciencialização sobre a ciberresiliência do seu trabalho político e atividades de convergência de supervisão. Isto inclui *workshops*, formações e a incorporação de questões de TIC e cibersegurança na supervisão dos supervisores e reguladores da União Europeia e de algumas jurisdições não pertencentes à UE. A EBA também publica relatórios de avaliação de riscos, que incluem riscos relacionados com a cibersegurança, para avaliar vulnerabilidades no setor bancário da UE.
 - A EBA colabora com partes interessadas externas para promover a partilha de conhecimento sobre cibersegurança. Através do FinTech Knowledge Hub, a EBA oferece formação às autoridades competentes sobre a supervisão de TIC e segurança, promovendo uma compreensão comum e a troca de conhecimentos.
 - A European Banking Federation (EBF) implementa campanhas e iniciativas para aumentar a consciencialização sobre questões de cibersegurança, tanto para colaboradores de entidades bancárias quanto para cidadãos da UE. Através da *Cybersecurity Working Group*, a EBF realiza ações como a campanha *Cyber Scams*, em colaboração com o Centro Europeu de Cibercrime da Europol, além de organizar anualmente a Conferência de Cibersegurança da EBF em Bruxelas, durante o Mês Europeu da Cibersegurança (ECISM).
- **Certificação e padronização**⁷⁸⁹:
 - O BCE publicou a *Cyber Resilience Oversight Expectations (CROE)* para as infraestruturas do mercado financeiro. A *CROE* define as expectativas do regulador do Euro em relação à ciberresiliência com base nas orientações globais;
 - Já o *Cyber Risk Institute (CRI)* promove a cibersegurança no setor financeiro através do *Financial Services Cybersecurity Profile*, que serve como referência para a cibersegurança;
 - A EBA publicou dois padrões técnicos sob a *PSD2*, focada no registo central eletrónico e na estrutura das informações e o FSB criou o *Cyber Lexicon* com o objetivo de padronizar a terminologia relacionada à cibersegurança neste setor, de forma a facilitar a comunicação entre o setor público e o privado;
 - O PCI desenvolve padrões para proteger os dados das contas de pagamentos e garantir a segurança de todos os ciclos de pagamento.

⁷⁸⁹ ENISA, "EU Cybersecurity Initiatives in the Finance Sector", março de 2021, 12-13.

- **Pesquisa e Inovação**⁷⁹⁰:

- O CONCORDIA é uma rede de competência em cibersegurança que reúne lideranças em pesquisa, tecnologia, indústria e competências públicas. O objetivo é estabelecer um ecossistema de cibersegurança integrado na União Europeia e voltado ao utilizador, promovendo soluções inovadoras para vários setores, incluindo o setor financeiro. Além disso, o CONCORDIA oferece laboratórios virtuais, cursos de formação e exercícios de cibersegurança (*cyber ranges*), e fornece experiência aos responsáveis políticos e à indústria europeia.
- O projeto Cybersecurity for Europe visa harmonizar o desenvolvimento de componentes de *software* para enfrentar desafios de cibersegurança em setores críticos, como infraestruturas digitais, finanças, governo, cidades inteligentes, saúde e transportes. Este projeto foca-se na pesquisa, desenvolvimento e inovação em tecnologias de cibersegurança de próxima geração, com especial atenção à cibersegurança em setores essenciais como o financeiro.

⁷⁹⁰ ENISA, “EU Cybersecurity Initiatives in the Finance Sector”, março de 2021, 4-17.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste setor. Tais cenários são indicados na seguinte tabela:

Tabela 40 - Cenários de risco (Bancário)

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços WEB , através de um <i>URL</i> malicioso ou script malicioso que direciona um colaborador da entidade para um website falso e instala software malicioso (ataques <i>Watering Hole</i> , ataques <i>Drive-By</i>), permitindo o furto de dados.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em <i>bitcoins</i> , sob a ameaça da sua destruição ou exposição ao público.

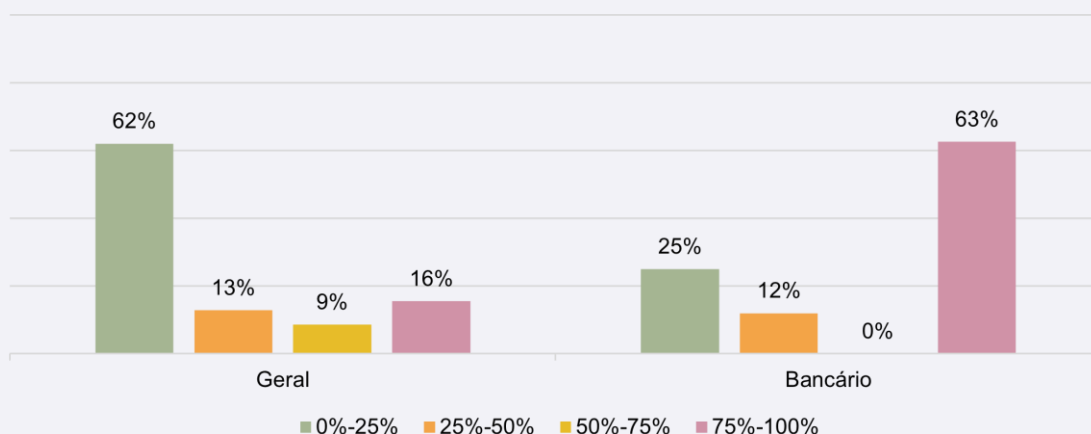
(Fonte: CNCS, “Riscos & Conflitos 2021”, obtido em 19 de setembro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor bancário, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

As ameaças mais prevalentes neste setor são o *ransomware* e as ameaças relativas a dados pessoais dos clientes, sendo estas ameaças concretizadas, normalmente, através de ataques bem-sucedidos de *phishing*. A sensibilização para este tipo de riscos e a formação para identificar estes riscos são essenciais para impedir que estas se concretizem, já que a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Este setor está à frente da média geral, dado que nos OSE, cerca de 63% dos 75%-100% trabalhadores têm formação básica em cibersegurança quando, no âmbito geral, apenas 16% dos setores estão nesse patamar (**Gráfico 33**).

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Os resultados do questionário evidenciam que a totalidade dos OSE do setor disponibiliza formação em cibersegurança aos seus colaboradores (**Gráfico 38**), sendo que 88% são de carácter obrigatório (**Gráfico 39**). No âmbito geral podemos observar que a média da disponibilização de formação em cibersegurança aos colaboradores está nos 65% e apenas 42% tem carácter obrigatório.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

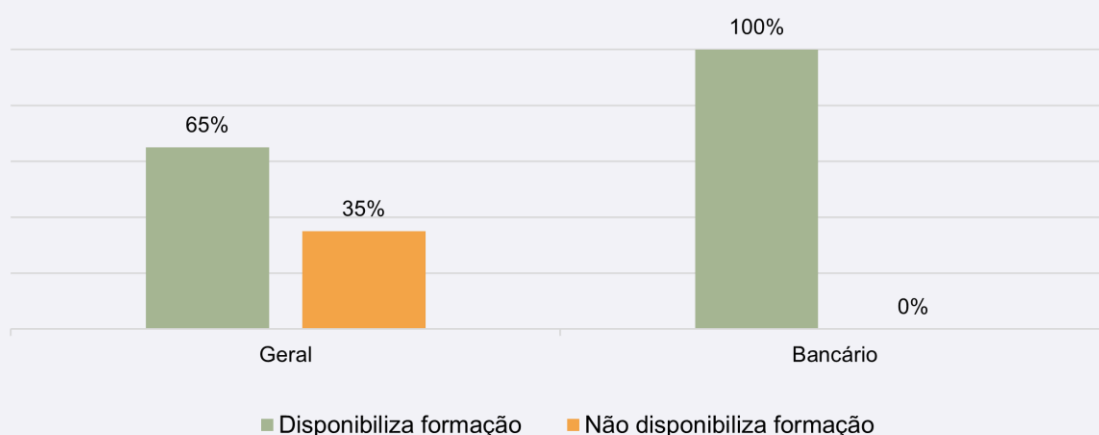
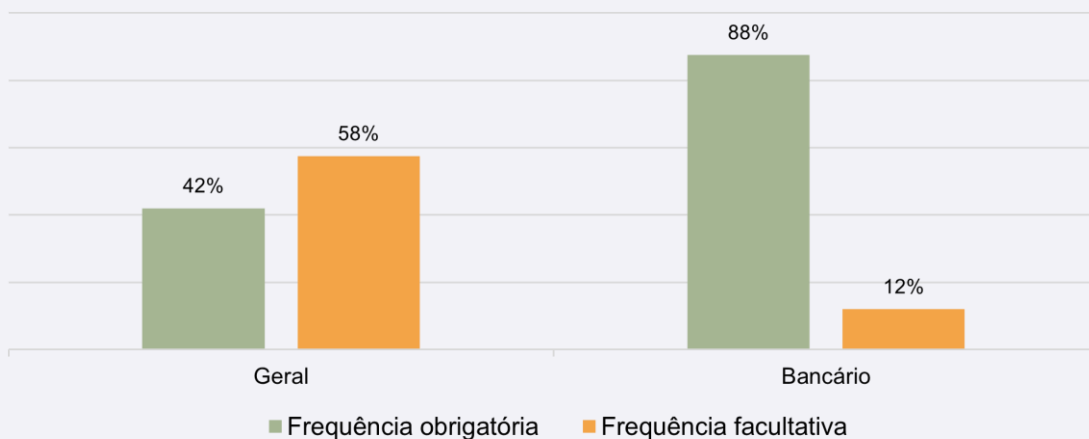
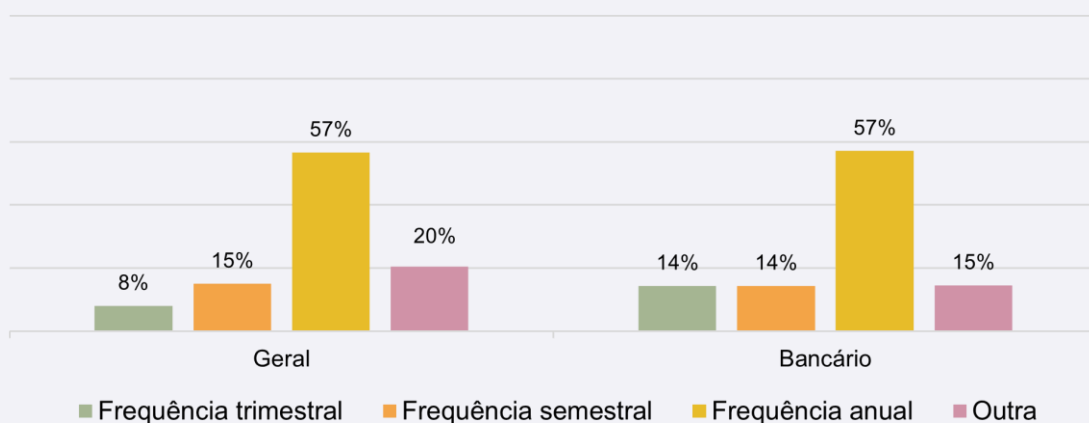


Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



Além disso, a maior parte dos momentos de formação têm frequência anual (**Gráfico 41**), o que no contexto do setor assegura a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores e está na média geral.

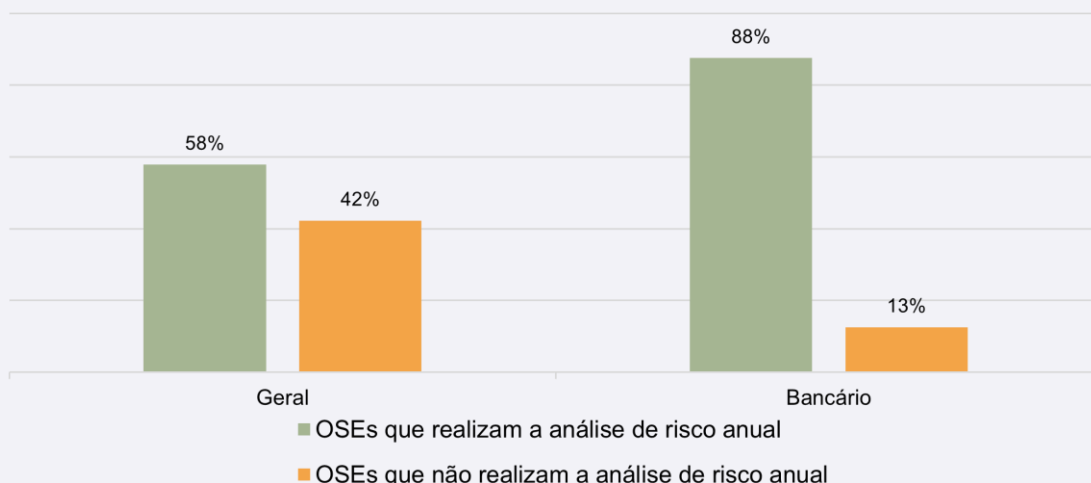
Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que este setor, comparativamente com os restantes, está acima da média, com exceção na *Firewall/WAF/Webfilter*. Este setor está acima da média na realização de avaliações de segurança anuais no âmbito de cibersegurança (**Gráfico 99**).

Gráfico 99 - Realização de análise de riscos anual no âmbito de cibersegurança



Nesse sentido, recomenda-se aos OSE do setor bancário que:

- Realizem avaliações de segurança, em todas as entidades, pelo menos anualmente;
- Realizem análises de risco pelo menos anualmente;
- Implementem, onde possível, *Firewall/WAF/Webfilter*.

Políticas, procedimentos e planos de cibersegurança

Com base nos dados reunidos no questionário, todos os OSE do setor possuíam políticas e procedimentos de cibersegurança documentados e implementados. Este valor é superior à média geral (100% vs 50%).

Diante desta situação, apesar de todos OSE do setor terem uma política de segurança, é importante que a mesma verse sobre:

- Os diversos papéis e responsabilidades dos vários colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, como os controlos de acesso (lógico e físico);
- A gestão de incidentes, incluindo a elaboração de um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação, além de um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização periódica da política (pelo menos anualmente), para manter a mesma atualizada conforme a evolução das ameaças de cibersegurança e as mudanças na organização.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de intrusão e exercícios de *Red Team*⁷⁹¹.

No setor bancário, os controlos fundacionais, que dizem respeito à segurança da rede, assumem um papel especialmente crítico. Infraestruturas bancárias, como sistemas de pagamento e transferência de fundos, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, disponibilidade e continuidade dos serviços financeiros. Qualquer falha ou configuração inadequada pode ser explorada para interromper transações, desviar fundos, ou comprometer a privacidade e segurança dos dados financeiros dos clientes, colocando em risco a estabilidade das operações bancárias.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos⁷⁹²:

⁷⁹¹ Hassanzadeh et al., "A Review of Cybersecurity Incidents", 4.

⁷⁹² Hassanzadeh et al., "A Review of Cybersecurity Incidents", 6.

Tabela 41 - Controlos de Segurança da CIS (Bancário)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de <i>Logs</i> de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: CIS, “The 18 CIS Critical Security Controls”, <https://www.cisecurity.org/controls/cis-controls-list>)

4. Infraestruturas do mercado financeiro

4.1. Contextualização setorial

No âmbito da Diretiva 2016/1148 e do Regime Jurídico da Segurança do Ciberespaço (RJSC, ou Lei n.º 46/2018, de 13 de agosto), que a transpõe, as infraestruturas do mercado financeiro são compostas por dois tipos de entidades: operadores de plataformas de negociação e contrapartes centrais (*Central Counterparties* - CCPs). Os operadores de plataformas de negociação são sociedades/entidades que, através de diferentes plataformas, permitem que um investidor aceda a diferentes mercados e instrumentos financeiros, tal como faz a Euronext Lisbon, mais vulgarmente conhecida por Bolsa de Lisboa. Já as contrapartes centrais, são infraestruturas do mercado financeiro que atuam como a contraparte em ambos os lados de uma transação financeira, efetuando operações de compensação em vários instrumentos financeiros. Um dos papéis principais das CCPs é então o de assegurar que as transações entre duas partes são realmente cumpridas. Estas entidades desempenham assim duas funções principais como intermediárias numa transação: a função de compensação e a função de liquidação. Uma CCP atua como contraparte tanto para os vendedores quanto para os compradores, arrecadando dinheiro de cada um, o que lhe permite garantir os termos de uma negociação. Isto é, uma CCP suporta a maior parte do risco de crédito dos compradores e dos vendedores quando compensam e liquidam transações de mercado. Se um comprador ou vendedor não cumprir a sua parte no processo de transação, a CCP cobre as perdas resultantes da transação falhada. Nesses casos, a CCP compensa a transação falhada com o valor atual de mercado da mesma⁷⁹³. Em Portugal, existem contrapartes centrais dedicadas às operações no mercado de capitais nacional⁷⁹⁴ e contrapartes centrais dedicadas exclusivamente a derivados do setor da energia (eletricidade e gás natural)⁷⁹⁵.

Tanto as plataformas de negociação como as CCPs são reguladas em Portugal pela Comissão do Mercado de Valores Mobiliários - CMVM.

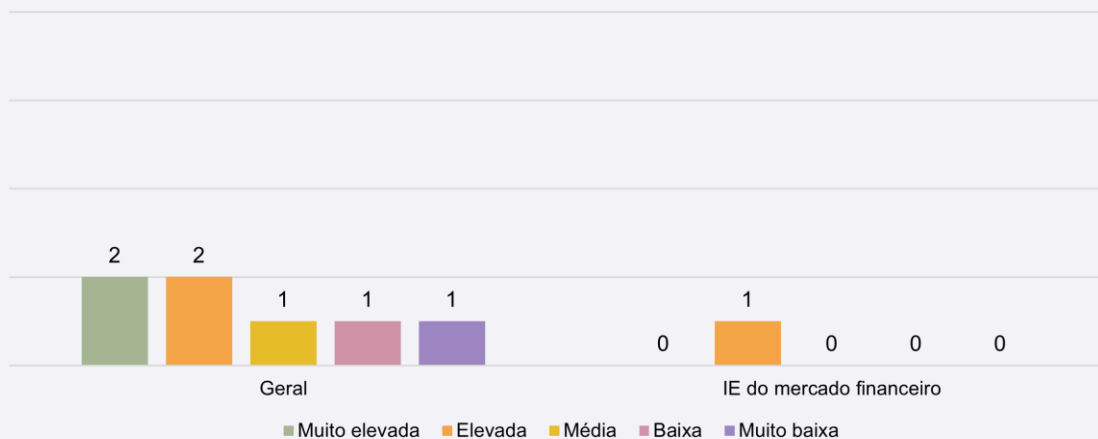
⁷⁹³ Banco Central Europeu, "Central Counterparty Clearing Houses and Financial Stability", *Financial Stability Review*, 2005, 179, https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart200512_06.en.pdf.

⁷⁹⁴ "Outros sistemas de liquidação", Infraestruturas de mercado, Banco de Portugal, <https://www.bportugal.pt/page/outros-sistemas-de-liquidacao>.

⁷⁹⁵ "Quem somos", OMIClear, <https://www.omiclear.pt/pt>.

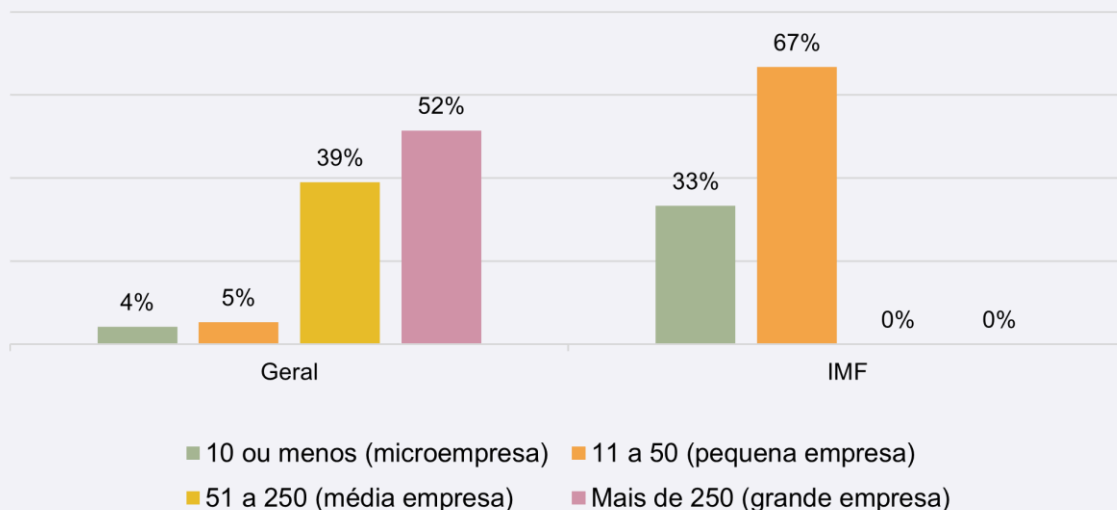
De acordo com o questionário realizado, o regulador do setor considera que a maturidade deste em cibersegurança é elevada e, no âmbito geral, apenas existem dois reguladores com maior perceção de maturidade em cibersegurança (**Gráfico 9**).

Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores



O tecido empresarial dos OSE do setor das infraestruturas do mercado financeiro é sobretudo composto por pequenas empresas, com apenas entre 11 e 50 colaboradores, e as restantes são microempresas com 10 ou menos colaboradores (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



A perceção dos reguladores sobre maturidade em cibersegurança nos setores pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (100% contra 65% no geral) (vide **Gráfico 38**) e pelas medidas cibersegurança adotadas (**Gráfico 66.4**) Todas as medidas de proteção utilizadas têm o mesmo valor.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

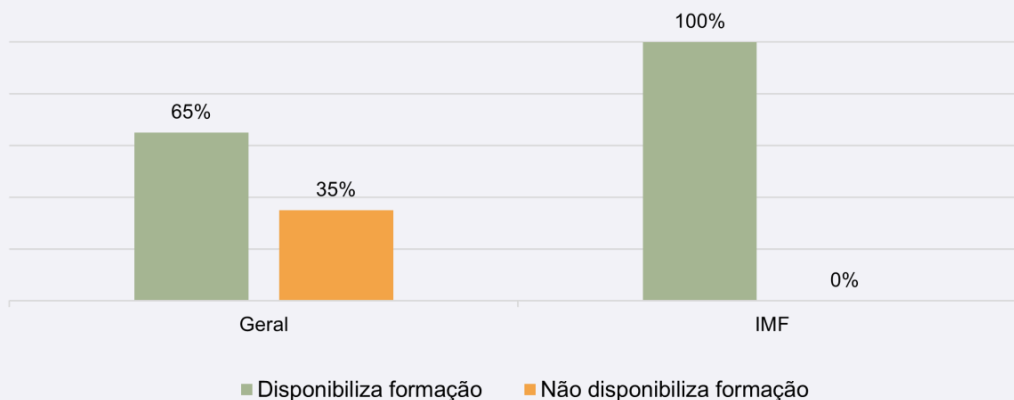
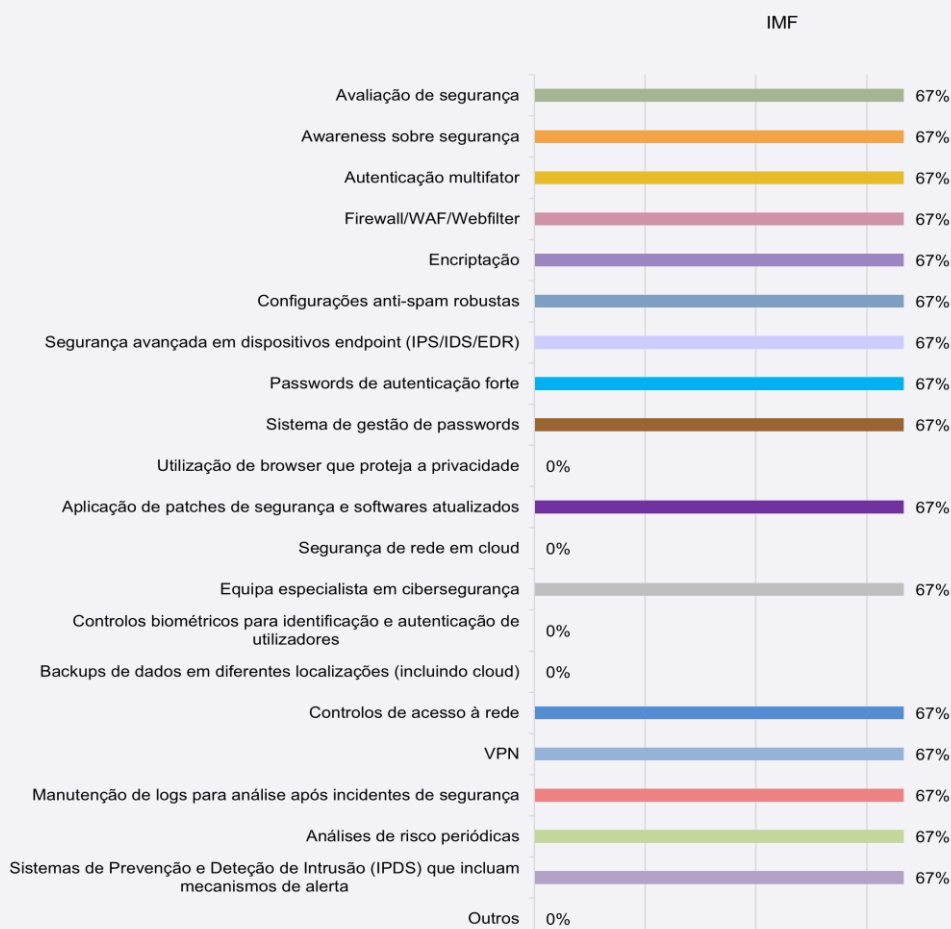
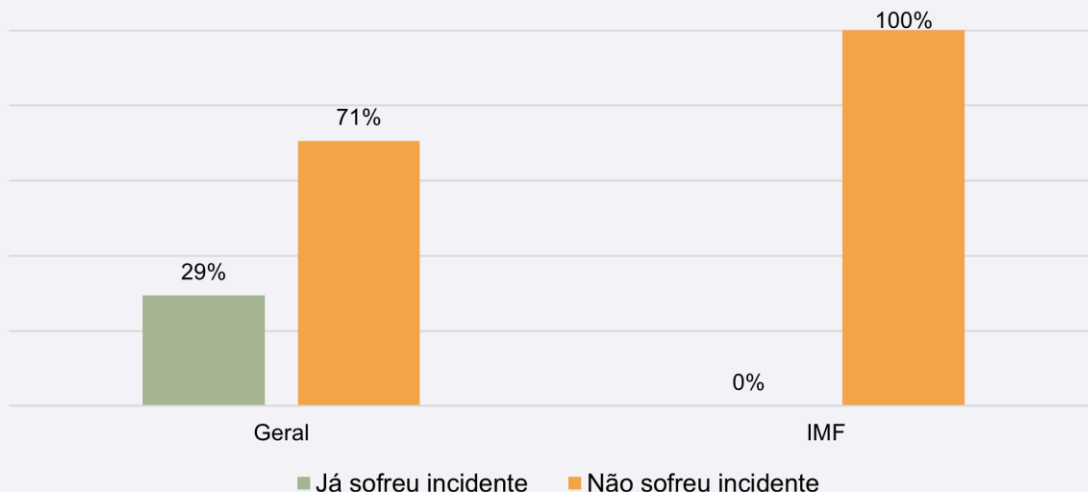


Gráfico 66.4 - Medidas de proteção contra ameaças de cibersegurança



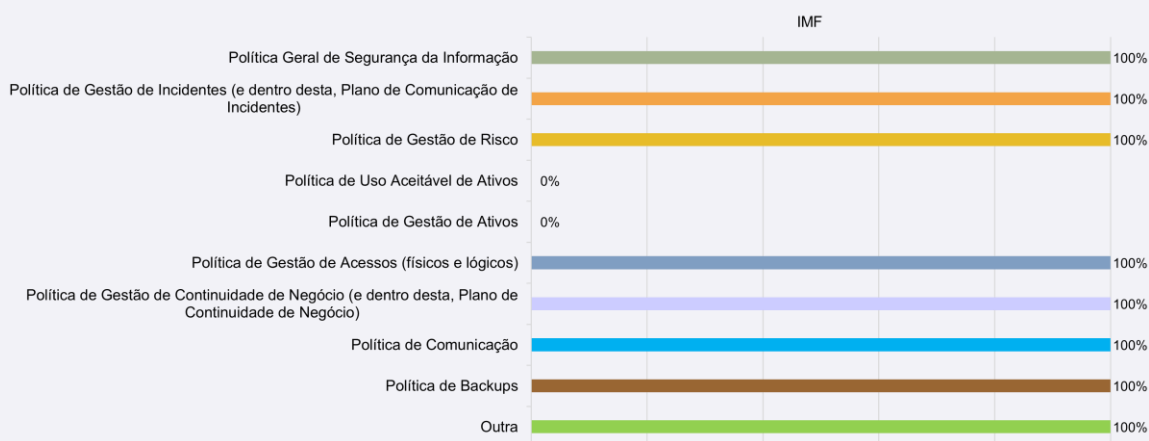
Mesmo não existindo orçamento de cibersegurança, este é o único setor onde não foram registados quaisquer incidentes de cibersegurança, estando assim acima da média geral que fica nos 71% (**Gráfico 68**).

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



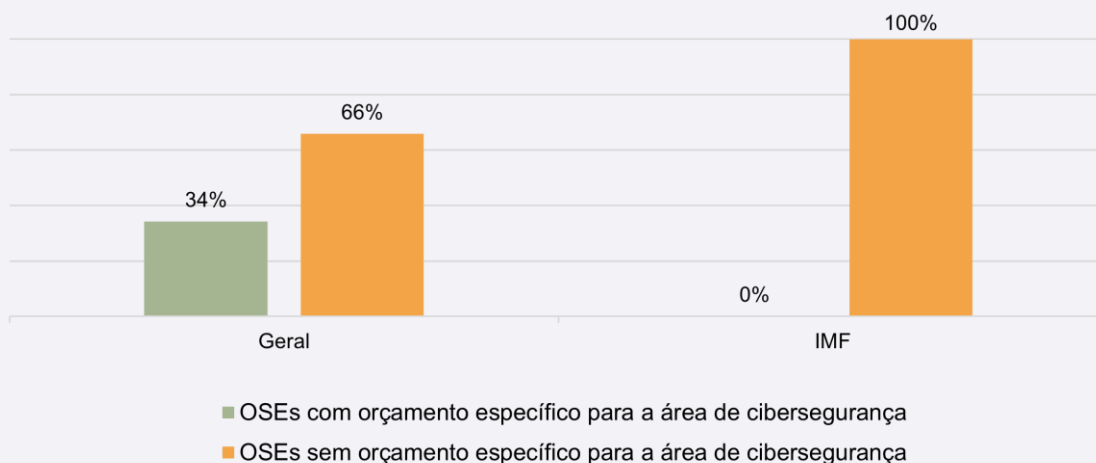
As políticas de cibersegurança e outras políticas relacionadas implementadas também suportam a afirmação anterior. O plano de segurança inclui todas as políticas tradicionalmente associadas à cibersegurança, com exceção de políticas relativas a ativos (**Gráfico 79.4**).

Gráfico 79.4 - Políticas Incluídas no Plano de Segurança



Embora cerca de 34% dos setores tenham um orçamento específico para a área de cibersegurança, não existem OSE neste setor a seguir esta prática (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



4.1.1. Impacto socioeconómico

As infraestruturas do mercado financeiro (as plataformas de negociação e as CCPs) desempenham um papel fundamental na economia nacional. Estas permitem pagamentos, compras, vendas, investimentos e sustentam o funcionamento da economia como um todo. São também estas que, muitas vezes, dão a necessária liquidez de capital a empresas, por exemplo, através da emissão de ações, recebendo as empresas dinheiro por cada ação vendida.

No caso específico das plataformas de negociação, o desempenho das empresas nas mesmas, como na Euronext Lisbon (Bolsa de Lisboa), pode desempenhar um papel crucial na atração de investimentos. Estas informações podem influenciar, impactando o nível de investimento interno e externo das empresas cotadas na bolsa nacional. É importante sublinhar que atrair investimento é importante em qualquer economia, uma vez que este é um impulsionador do crescimento económico e da produtividade⁷⁹⁶.

Em 2019, o volume diário de negócios da Bolsa de Lisboa era de cerca de 86 milhões de euros. Em 2021, esse valor aumentou para os 112 milhões e, em 2022, o volume diário atingiu os 137 milhões de euros, tendo crescido percentualmente mais do que em outras praças europeias⁷⁹⁷. A maior parte do volume de negócios ainda vem de instituições internacionais, com 80% das transações a serem feitas por intermediários dora de Portugal, indicando um investimento estrangeiro. No entanto, o crescimento do volume de negócios deve-se principalmente ao aumento de investidores individuais, que representam 15%, o triplo de 2019. Portugal tem atraído, sobretudo, investidores particulares norte-americanos, brasileiros e franceses⁷⁹⁸.

⁷⁹⁶ Pedro Bação et al., "Investimento Empresarial e o Crescimento da Economia Portuguesa", coord. Fernando Alexandre, *Fundação Calouste Gulbenkian* (2017): 7, https://gulbenkian.pt/wp-content/uploads/2017/11/Estudo_relatorio_Investimento_Empresarial_final_dez2017.pdf.

⁷⁹⁷ Mariana Dias, "Euronext Lisboa cresce em 2022. Foram negociados 137 milhões de euros por dia", *Dinheiro Vivo*, 28 de fevereiro de 2023, <https://www.dinheirovivo.pt/bolsa/euronext-lisboa-cresce-em-2022-foram-negociados-137-milhoes-de-euros-por-dia-15918612.html/>.

⁷⁹⁸ Dias, "Euronext Lisboa cresce em 2022".

Já no caso concreto das contrapartes centrais, estas ganharam particular relevância no seguimento da crise financeira de 2007-2008, iniciada nos Estados Unidos da América. Após o deflagrar dessa crise, a consequente insolvência de várias empresas e a falta de liquidez verificada levaram a uma grave quebra de confiança nas instituições financeiras por parte dos investidores e do público. Perante este cenário, iniciou-se uma profunda reforma das infraestruturas do mercado financeiro, na qual as CCPs desempenharam um importante papel. De forma sucinta, as CCPs passaram a ter um papel mais ativo nos procedimentos de compensação e liquidação⁷⁹⁹, mitigando assim uma porção do risco de contraparte e do risco sistémico. Este novo papel surge no seguimento de desenvolvimentos legislativos na União Europeia tais como o Regulamento (UE) n.º 648/2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (também conhecido como *European Market Infrastructure Regulation* - EMIR), que impõe obrigações ao nível da partilha de dados entre CCPs e plataformas de negociação, ao nível da comunicação de informações sobre transações num repositório dedicado, bem como ao nível do capital mínimo para as CCPs poderem operar (7,5 milhões de euros de capital inicial e de capital permanente)⁸⁰⁰. A nova regulamentação, embora não tenha imposto a necessidade de incluir uma CCP na negociação de todo o tipo de ativos e derivados, impeliu a que mais plataformas de negociação celebrassem acordos com CCPs de modo a realizarem transações mais seguras. Dados do Banco Central Europeu demonstram que o número de transações seguras aumentou, entre 2008 e 2015, de cerca de 60% para praticamente 90% e que o envolvimento de CCPs nas transações aumentou, também, entre 2008 e 2015, de 40% para cerca de 65%⁸⁰¹. A regulação das infraestruturas do mercado financeiro acabou por contribuir para um mercado mais seguro, embora a recuperação da confiança dos consumidores e investidores tenha sido lenta. Não obstante, as CCPs tornaram-se elementos indispensáveis à segurança e integridade dos mercados financeiros⁸⁰². A nova regulamentação, juntamente com outras medidas, tais como as injeções de capital e a redução das taxas de juro, permitiram, lentamente, a recuperação da confiança dos investidores no mercado financeiro⁸⁰³.

As infraestruturas do mercado financeiro são também um garante de igualdade no que diz respeito ao acesso ao mercado financeiro. As infraestruturas do mercado financeiro não são acessíveis apenas a investidores com um alto poder económico ou a grandes empresas. Estas permitem também investimentos de menores valores, alocações de poupanças individuais, com diferentes graus de risco, como por exemplo em fundos para a reforma, planos de poupança-reforma (PPR) e planos de poupança em ações (PPA), entre muitos outros.

⁷⁹⁹ André Barata, "O Regime Europeu de Resolução de Contrapartes Centrais: a peça que faltava ao mercado dos derivados de balcão?", *Revista de Direito Financeiro e dos Mercados de Capitais*, dezembro de 2023, 201, <https://rdmfc.com/wp-content/uploads/2024/01/Revista-de-Direito-Financeiro-e-do-Mercado-de-Capitais-2-20231.pdf>.

⁸⁰⁰ Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, *Jornal Oficial da União Europeia*, 25, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012R0648>.

⁸⁰¹ Florian Heider, "Collateral, central clearing counterparties and regulation", *European Central Bank Research Bulletin* 41, 6 de dezembro de 2017, <https://www.ecb.europa.eu/press/research-publications/resbull/2017/html/ecb.rb171206.en.html>.

⁸⁰² Barata, "O Regime Europeu de Resolução de Contrapartes Centrais", 270-271.

⁸⁰³ International Monetary Fund, "World Economic Outlook: Challenges to Steady Growth", outubro de 2018, 82, <https://www.imf.org/-/media/Files/Publications/WEO/2018/October/English/main-report/Text.ashx>.

As infraestruturas do mercado financeiro são também responsáveis pela promoção de uma maior transparência nos mercados, uma vez que as empresas cotadas em Bolsa são obrigadas a publicar informações financeiras de forma periódica e contínua⁸⁰⁴. A divulgação periódica de relatórios anuais detalhados, como balanços patrimoniais, demonstrações de resultados e de fluxos de caixa, bem como relatórios semestrais e trimestrais, que fornecem atualizações sobre a *performance* financeira e a situação económica das empresas contribuem para a transparência no mercado e para o aumento da confiança no mesmo por parte dos investidores⁸⁰⁵.

4.1.2. Especificidades tecnológicas

As tecnologias utilizadas no setor financeiro, sobretudo as tecnologias inovadoras são comumente designadas como *fintech* (juntando o início das palavras inglesas *financial* e *technology*). Embora a origem do termo possa ser traçada até ao início da década de 90, foi somente nos anos de 2013 e 2014 que este começou a ganhar mais atenção e a ser mais amplamente utilizado⁸⁰⁶.

O termo *fintech* engloba agora qualquer inovação tecnológica do setor financeiro, incluindo avanços em literacia financeira, consultoria e educação, bem como na simplificação da gestão de carteiras de investimentos, empréstimos, banca de retalho, *crowdfunding*, transferências/pagamentos e muito mais. Tecnologias como a *blockchain*, Inteligência Artificial (IA) e automatização de processos robóticos, estão cada vez mais integradas nas infraestruturas do mercado financeiro. Estas inovações impactam diretamente as organizações, pois exigem novas abordagens para garantir a segurança e resiliência das operações financeiras num ambiente cada vez mais digitalizado⁸⁰⁷.

⁸⁰⁴ “Financial Reporting”, Issuer Disclosure, ESMA, <https://www.esma.europa.eu/issuer-disclosure/financial-reporting>.

⁸⁰⁵ Shatha Hussain, Amer Alaya e Thana Azizi, “The impact of financial accounting disclosures on investors’ reactions towards bad news: The moderating role of investors’ sentiments”, *Cogent Economics and Finance*, 16 de julho de 2023, 5, <https://www.tandfonline.com/doi/pdf/10.1080/23322039.2023.2228087?download=true>.

⁸⁰⁶ Douglas Arner, “FinTech: Evolution and Regulation”, Asian Institute of International Financial Law, University of Hong Kong, junho de 2016, https://law.unimelb.edu.au/_data/assets/pdf_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf.

⁸⁰⁷ Maximilian Palmié et al., “The evolution of the financial technology ecosystem: an introduction and agenda for future research on disruptive innovations in ecosystems”, University of Vaasa, 2020, 10 e 21, https://osuva.uwasa.fi/bitstream/handle/10024/10315/Osuva_Palmi%C3%A9_Wincent_Parida_Caglar_2020b.pdf?sequence=2&isAllowed=y.

Descrevem-se, de seguida, algumas das mais relevantes utilizadas no setor:

- ***Distributed Ledger Technology (DLT) e Blockchain***

*Distributed Ledger*⁸⁰⁸ *Technology* (DLT) é uma tecnologia de registo descentralizado que permite o registo de transações de ativos em múltiplos locais simultaneamente. Esta descentralização, ao contrário das bases de dados tradicionais centralizadas, oferece maior resiliência e segurança contra falhas e ataques.

Quanto ao conceito de *blockchain*, este tem origem num artigo publicado em 2008⁸⁰⁹. A *blockchain* é uma rede formada por blocos encadeados onde cada um destes blocos contém uma “impressão digital”, ou *hash* criptográfico, que se conecta ao bloco anterior. Como um tipo específico de DLT, a *blockchain* organiza os dados em blocos que são verificados e adicionados de forma imutável e segura. Este encadeamento por *hashes* criptográficos torna a *blockchain* interligada, permitindo rastrear todas as transações. Além disto, cada transação é visível para todos os envolvidos. Esta natureza descentralizada e distribuída da *blockchain* torna-a menos vulnerável a falhas: se algum bloco for removido, os demais já possuem uma cópia exata das informações, preservando a integridade dos dados. Da mesma forma, quando um novo nó se junta rede, o mesmo recebe uma cópia completa de todas as informações reforçando a confiabilidade e resiliência deste sistema⁸¹⁰.

O modo de funcionamento da tecnologia *blockchain* oferece um elevado nível de segurança às transações. Tentar modificar um bloco obrigaria a mudar o *hash* criptográfico de todos os blocos subsequentes, algo que exigiria um imenso poder computacional e que, mesmo assim, é altamente impraticável. Este modo de funcionamento torna virtualmente impossível a adulteração de dados e oferece uma plataforma segura para o armazenamento de dados sensíveis e para a realização de transações financeiras⁸¹¹. Para as organizações do setor das infraestruturas do mercado financeiro, as DLT podem ser fundamentais na modernização dos sistemas de transações, aumentando a transparência, reduzindo os riscos de manipulação de dados e melhorando a continuidade do negócio em caso de incidentes.

⁸⁰⁸ Na língua inglesa, “*ledger*” é o termo utilizado para se referir a um livro de contas, no qual se registam as transações respeitantes a uma conta específica. Neste registam-se todas as transações de débito, crédito, de venda e de compra realizadas através dessa conta.

⁸⁰⁹ Pornpit Wongthongtham et al., “Blockchain-enabled Peer-to-Peer energy trading”, *Computers & Electrical Engineering* 94 (setembro de 2021): 1-9, <https://doi.org/10.1016/j.compeleceng.2021.107299>.

⁸¹⁰ Dejan Vujičić, Dijana Jagodić e Siniša Randić, “Blockchain technology, bitcoin, and Ethereum: A brief overview”, *paper* apresentado no 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), Sarajevo, Bósnia e Herzegovina, de 21 a 23 de março de 2018, 1-6, <https://ieeexplore.ieee.org/abstract/document/8345547/>.

⁸¹¹ Reza Soltani et al., “Distributed Ledger Technologies and Their Applications: A Review”, *Applied Sciences* 12, 7898 (2022): 4, <https://doi.org/10.3390/app12157898>.

- **IA e robo-advisors**

A Inteligência Artificial (IA) e os *robo-advisors* estão a ser cada vez mais aplicados no setor das infraestruturas do mercado financeiro para otimizar processos e melhorar a tomada de decisões. Embora a IA em si seja uma tecnologia ampla e não exclusiva deste setor, a sua aplicação específica em serviços como os *robo-advisors* tem transformado o modo como todas as instituições financeiras operam e interagem com os clientes. Os *robo-advisors*, que utilizam algoritmos baseados em IA, permitem a gestão automática de carteiras de investimento, oferecendo soluções personalizadas a baixos custos. Segundo um inquérito do Fórum Económico Mundial, em 2020 já 85% dos intervenientes no setor financeiro utilizavam IA e, no questionário realizado no âmbito deste relatório, todos os operadores inquiridos indicaram que utilizam IA. A Inteligência Artificial, segundo o mesmo inquérito, é amplamente utilizada no setor para diversos fins, como a automatização de processos, gestão de riscos, redução de custos, criação de novas fontes de receita, análise de dados, deteção de fraudes e anomalias, além de serviços de comunicação com clientes, como os *chatbots*⁸¹². Os mercados financeiros são, por natureza, intangíveis, e os diversos serviços que neles operam, como a execução de pagamentos, a emissão de ações e a compra e venda de ativos, dependem fundamentalmente do processamento de informação⁸¹³. Este é um setor que emprega há décadas processos automatizados e algoritmos para realizar análises e previsões.

Quando um novo cliente se regista para utilizar serviços deste tipo, são-lhe pedidos diversos dados, tais como idade, género, vencimento, objetivos de investimento, atuais ativos de que disponha e o seu grau de tolerância ao risco. Com base nestes dados, e nas capacidades de análise e de previsão do mercado, como tendências de descidas e subidas de preços, o *robot* procura os melhores ativos onde investir e quais ignorar, em busca do cumprimento dos objetivos do cliente.

⁸¹² Emmanuel Schizas et al., "Transforming Paradigms: A Global AI in Financial Services Survey", *World Economic Forum*, 29 de fevereiro de 2020, 25, https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf.

⁸¹³ Giacomo Calzolari, "Artificial Intelligence market and capital flows: Artificial Intelligence and the financial sector at crossroads", estudo para o Parlamento Europeu, maio de 2021, 25, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU\(2021\)662912_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf).

- **FIX (Financial Information eXchange)**

O setor das infraestruturas do mercado financeiro necessita de ter uma baixa latência nas suas operações de forma a garantir que as ordens são executadas no menor tempo possível. Para ajudar a garantir a menor latência, este setor utiliza o protocolo *FIX (Financial Information eXchange)*. O protocolo *FIX*, foi desenvolvido em 1992 pela Goldman Sachs e pela Fidelity Investments, e é utilizado para facilitar as comunicações entre os diferentes sistemas de *trading* e define uma linguagem padrão que permite que diferentes sistemas comuniquem entre si sem a necessidade de criar interfaces específicas. Este protocolo baseia-se em mensagens pré-definidas que seguem um formato específico. Cada mensagem contém uma sequência de campos denominados por *tags*, onde cada campo transmite um dado específico, como por exemplo o preço de uma ação, a quantidade de ações, entre outros⁸¹⁴. O *FIX* tem alguns benefícios, tais como⁸¹⁵:

- **Velocidade e Eficiência:** O *FIX* facilita a transmissão rápida e precisa das informações, pois é um padrão de comunicação amplamente utilizado;
- **Interoperabilidade:** As empresas financeiras podem integrar os seus sistemas com os outros do mercado, independentemente do *software* ou *hardware* que estão a utilizar;
- **Redução de custos:** Como a comunicação fica padronizada, a necessidade de adaptações fica reduzida, permitindo uma configuração mais eficiente e, consequentemente, uma redução dos custos operacionais;
- **Segurança:** Este protocolo é adaptável às normas de segurança e oferece um suporte para a autenticação, proporcionando um ambiente seguro para as transações mais sensíveis.

Este protocolo é utilizado na gestão de ativos, na bolsa de valores e corretoras. Devido às mudanças regulatórias e ao aumento da complexidade nos mercados financeiros, este protocolo passou por várias atualizações, estando atualmente na versão 5.0 e continua a evoluir de forma a conseguir suportar novos tipos de transações e a aumentar a segurança do mesmo⁸¹⁶.

⁸¹⁴ Hao Jia et al., "A Domain-Specific Accelerator for Ultralow Latency Market Data Distribution System," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, abril de 2023, 5466-5467, <https://ieeexplore.ieee.org/abstract/document/9801674>.

⁸¹⁵ True Tamplin, "Advantages of Financial Information Exchange (FIX)", *Finance Strategists*, 12 de julho de 2023, <https://www.financestrategists.com/wealth-management/investment-management/financial-information-exchange-fix/#advantages-of-financial-information-exchange-fix>.

⁸¹⁶ FIX Trading Community, "FIX 5.0 Specifications", <https://www.fixtrading.org/standards/unsupported/fix-5-0/>.

- **RTGS (Real-Time Gross Settlement)**

Os mercados financeiros utilizam sistemas de liquidação bruta (“*gross settlement*”) para processar e liquidar pagamentos de grande valor entre instituições de forma imediata e em tempo real. Estes sistemas são denominados de *RTGS (Real-Time Gross Settlement)* e, neste tipo de sistemas, as transações são processadas de forma individual e liquidadas de forma irrevogável, garantindo assim que o pagamento é finalizado assim que é executado⁸¹⁷.

Existem vários tipos de sistemas *RTGS*. O *TARGET2 (Trans-European Automated Real-time Gross Settlement Express Transfer System)* é um sistema utilizado pelos países da zona Euro para liquidação em Euros. É operado pelo Banco Central Europeu e bancos centrais nacionais⁸¹⁸. Este sistema tem alguns benefícios, tais como⁸¹⁹:

- **Eficiência:** Este sistema foi desenhado para processar um alto volume de dados em tempo real e, devido a isto, é possível fazer e receber pagamentos mais rápido e de forma eficiente;
- **Risco reduzido:** O sistema utiliza várias ferramentas de segurança para ter em conta que os pagamentos são seguros, reduzindo assim o risco de fraude ou de erro;
- **Transparência:** São fornecidas todas as informações dos pagamentos, incluindo o estado de cada transação;
- **Interoperabilidade:** É possível gerir diferentes tipos de pagamentos, podendo o sistema operar em diferentes regiões;
- **Redução de custos:** As taxas neste sistema são, normalmente, mais baixas em comparação com os sistemas alternativos de pagamentos.

Já o *Fedwire* é um sistema utilizado pelos Estados Unidos da América operado pela Federal Reserve para liquidação em dólares⁸²⁰. Este sistema também tem alguns benefícios⁸²¹:

- **Velocidade:** O *Fedwire* processa as ordens de pagamento em tempo real, garantindo uma rapidez e segurança nas transações críticas;
- **Flexibilidade:** Este sistema oferece várias conexões para o envio e gestão de ordens de pagamento;
- **Segurança:** É garantida a segurança e uma alta disponibilidade, com *backups* regionais e testes regulares.

Por fim, o *CHAPS (Clearing House Automated Payment System)* é um sistema utilizado no Reino Unido, gerido pelo Banco de Inglaterra para liquidação em libras⁸²². Tal como os outros sistemas, existem alguns benefícios na utilização do *CHAPS*. Nomeadamente, pagamentos de valor alto no mesmo dia de forma segura e eficiente, e uma infraestrutura de liquidação bruta que garante a resiliência operacional⁸²³.

⁸¹⁷ Peter Allsopp, Bruce Summers e John Veale, “The Evolution of Real-Time Gross Settlement: Access, Liquidity and Credit, and Pricing”, World Bank, fevereiro de 2009, 7-9, <https://documents1.worldbank.org/curated/en/736521468331852042/pdf/490020WP0TheEv10Box338937B01PUBLIC1.pdf>.

⁸¹⁸ Allsopp, Summers e Veale, “The Evolution of Real-Time Gross Settlement”, 31.

⁸¹⁹ European Merchant Bank, “Target2 Explained: What is Target2?”, 12 de junho de 2023, <https://em.bank/blog/target2-explained-what-is-target2/>.

⁸²⁰ Allsopp, Summers e Veale, “The Evolution of Real-Time Gross Settlement”, 13.

⁸²¹ Fedwire, “Fedwire Funds Service”, <https://www.frb.services.org/binaries/content/assets/crsocms/financial-services/wires/funds.pdf>.

⁸²² Allsopp, Summers e Veale, “The Evolution of Real-Time Gross Settlement”, 13-14.

⁸²³ Bank of England, “CHAPS”, <https://www.bankofengland.co.uk/payment-and-settlement/chaps>.

- **Plataformas de processamento de dados**

Com o crescente volume de dados a ser gerado neste setor, é necessário utilizar plataformas para gerir e processar estes dados. O principal desafio é conseguir extrair valor desta enorme quantidade de dados, pois os mesmos podem estar estruturados, semiestruturados ou não estruturados. A ferramenta mais utilizada para este fim é o Apache Hadoop⁸²⁴. Esta permite que os dados sejam processados e distribuídos por vários computadores utilizando modelos desenhados para serem escaláveis⁸²⁵. Existem outras ferramentas como o HPCC⁸²⁶, o Qubole⁸²⁷, que é uma ferramenta de fonte aberta (“open-source”) que se gere e otimiza sozinha e a HPE⁸²⁸.

Através do uso destes dados, é possível criar modelos analíticos que analisam grandes volumes de informações, tanto históricas como atuais. Estes modelos podem ajudar a antecipar os movimentos do mercado, permitindo que as empresas se ajustem a novas tendências e oportunidades.

A gestão de riscos também beneficia significativamente do uso de análises de dados. Com informações precisas e em tempo real, as organizações podem avaliar e mitigar potenciais riscos, desenvolvendo estratégias proativas. Por fim, a análise de dados pode otimizar vendas e apoiar decisões da equipa de *marketing*, ajudando as empresas a entender melhor o comportamento dos clientes e a personalizar as ofertas, resultando num aumento de receitas. Deste modo, a integração de ferramentas de processamento de dados e de análise torna-se fundamental para a competitividade e a eficiência no setor financeiro⁸²⁹.

⁸²⁴ “Apache Hadoop”, The Apache Software Foundation, <https://hadoop.apache.org/>.

⁸²⁵ Luben Boyanov, “Financial Data Processing in Big Data Platforms”, *Economic Alternatives* 4, (2021): 537, <https://www.unwe.bg/doi/eajournal/2021.4/EA.2021.4.03.pdf>.

⁸²⁶ “Home”, HPCC Systems, <https://hpccsystems.com/>.

⁸²⁷ “Platform”, Qubole, <https://www.qubole.com/platform>.

⁸²⁸ “HPE AI and data transformation services”, Hewlett-Packard Enterprise, <https://www.hpe.com/pt/en/services/consulting/big-data.html>.

⁸²⁹ Boyanov, “Financial Data Processing”, 535.

4.2. Ameaças

Segundo o *Threat Landscape Report de 2023* da ENISA, os setores bancário e financeiro, apesar de não deixarem de ser um alvo, ficam atrás de outros alvos como a Administração Pública, o setor da saúde, as infraestruturas digitais, os transportes e os prestadores de serviços digitais⁸³⁰.

É importante sublinhar que ataques significativos neste setor podem impactar todo o ecossistema financeiro, tanto a nível nacional como internacional, colocando a estabilidade financeira em risco⁸³¹. Nos últimos anos, os ataques de cibersegurança neste setor têm vindo a aumentar, sendo agora mais sofisticados e destrutivos. Segundo o estudo "Impact of cyber-attacks on the financial institutions" a principal causa deste crescimento foi o acréscimo dos serviços remotos devido à pandemia⁸³².

Tanto este setor como o setor bancário estão interconectados com vários outros setores e, por esse motivo, estão suscetíveis a várias ameaças como o cibercrime e a ciberespionagem. Tal como referido anteriormente, os ataques neste setor são maioritariamente motivados pela parte financeira e, de acordo com o *Threat Landscape Report de 2023* da ENISA, os principais ataques passam pelo comprometimento da disponibilidade dos serviços e da informação (ataques de negação de serviço: "Denial of Service", DoS), ataques de *ransomware*, contando-se ainda ameaças relativas a dados (*data breaches* e furto de dados)⁸³³. O ataque predominante foi o *ransomware*, onde 25% dos casos foram operações de um só grupo (*Lockbit*) e 87% dos casos vieram de apenas 20 grupos. Este setor e o setor bancário foram os alvos destes grupos em 6% dos casos⁸³⁴.

Ciberataques em grande escala ameaçam a confiança no sistema financeiro e até mesmo na economia global. Nesses casos, são alvo de ataques os sistemas de pagamento, compensação ou liquidação, como o sistema *SWIFT*⁸³⁵. A interrupção desses serviços pode ter um impacto profundo no funcionamento dos mercados financeiros, comprometendo os fluxos de crédito. No contexto de um ecossistema financeiro cada vez mais interligado, um ataque a uma ou mais instituições ou infraestruturas críticas pode ter efeitos em cascata significativos. O Banco da Índia foi um dos afetados e sofreu um ciberataque em fevereiro de 2015, reportando um prejuízo de cerca de 9 milhões de dólares. Anteriormente, em janeiro do mesmo ano, o Banco del Austro, situado no Equador, sofreu também um ataque reportando também um prejuízo de 9 milhões de dólares⁸³⁶.

⁸³⁰ ENISA, "ENISA Threat Landscape 2023", 13.

⁸³¹ Banco Central Europeu, "Cyber resilience and financial market infrastructures", <https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html>.

⁸³² Olivér Gulyás e Gábor Kiss, "Impact of cyber-attacks on the financial institutions", *Procedia Computer Science* 219 (2023): 85, <https://doi.org/10.1016/j.procs.2023.01.267>.

⁸³³ ENISA, "ENISA Threat Landscape 2023", 14.

⁸³⁴ ENISA, "ENISA Threat Landscape 2023", 16 e 17.

⁸³⁵ SWIFT: Society for Worldwide Interbank Financial Telecommunication, responsável pelo sistema de comunicações entre entidades financeiras para transferências internacionais.

⁸³⁶ Abdul Stanikzai e Munam Shah, "Evaluation of Cyber Security Threats in Banking Systems", *paper* apresentado no 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, EUA, de 5 a 7 de dezembro 2021, 3, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9659862>.

Os ataques a dados, nomeadamente à sua confidencialidade, integridade e disponibilidade, são também uma realidade no setor. As questões de confidencialidade surgem quando informações privadas dentro de uma empresa são divulgadas a terceiros, como no caso de violações de dados. As questões de integridade estão relacionadas com a utilização indevida dos sistemas, como é o caso da fraude, que leva a perdas financeiras diretas. Finalmente, os problemas de disponibilidade estão ligados a interrupções nos negócios que impedem as empresas de operar, resultando em perda de lucros⁸³⁷.

Em 2011, um ataque de Negação de Serviço Distribuída (*"Distributed Denial of Service" - DDoS*) à Bolsa de Hong Kong interrompeu a divulgação de informações de mercado, forçando a paragem das atividades da mesma⁸³⁸. Em 2020, uma série de ataques do mesmo tipo à Bolsa de Valores da Nova Zelândia forçou a paragem das operações durante quatro dias consecutivos⁸³⁹.

Em fevereiro de 2020, Christine Lagarde, presidente do Banco Central Europeu, veio a público, alertar que um ciberataque poderia originar uma crise financeira, afirmações estas que foram corroboradas pelo FSB (Financial Stability Board)⁸⁴⁰. De acordo com o Fórum Económico Mundial, o risco de ciberataques e de perdas monetárias subiu. Em 2017, houve cerca de 500 milhões de dólares em prejuízo no setor, enquanto em 2021 houve 2,5 mil milhões de dólares. Relativamente aos ataques, em 2017 houve cerca de 8 mil incidentes e em 2021 houve cerca de 11 mil incidentes⁸⁴¹.

⁸³⁷ Antoine Bouveret, "Cyber Risk for the Financial sector: A Framework for Quantitative Assessment", *Working Paper* do Fundo Monetário Internacional, junho de 2018, 4, <https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924>.

⁸³⁸ "Hong Kong exchange trading disrupted as hackers target website", *Reuters*, 10 de agosto de 2011, <https://www.reuters.com/article/technology/hong-kong-exchange-trading-disrupted-as-hackers-target-website-idUSTRE7792FT/>.

⁸³⁹ "New Zealand stock exchange disrupted by fourth 'offshore' cyber attack", *The Guardian*, 28 de agosto de 2020, <https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack>.

⁸⁴⁰ Tim Maurer e Arthur Nelson, "The Global Cyber Threat to Financial Systems", *FINANCE & DEVELOPMENT*, março de 2021, 2, <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>.

⁸⁴¹ Johnny Wood, "Global financial stability at risk due to cyber threats, IMF warns. Here's what to know", *World Economic Forum*, 15 de maio de 2024, <https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/>.

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos⁸⁴², de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal⁸⁴³.
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa⁸⁴⁴.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável⁸⁴⁵.
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso⁸⁴⁶. No caso, consideraram-se os colaboradores internos maliciosos.

⁸⁴² CNCS, "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.

⁸⁴³ CNCS, "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021", maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>.

⁸⁴⁴ CNCS, "Relatório Riscos & Conflitos 2021", 75.

⁸⁴⁵ CNCS, "Relatório Riscos & Conflitos 2021", 75-76.

⁸⁴⁶ CNCS, "Relatório Riscos & Conflitos 2021", 76-77.

Tabela 42 - Agentes de ameaça mais prováveis (IMF)

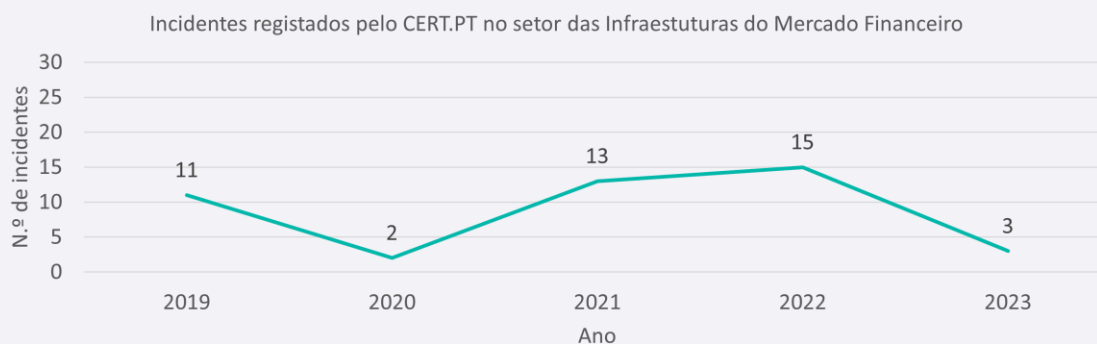
Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>	■	■	■	■
<i>Malware</i>	■	■	■	■
Vulnerabilidades	■	■	■	■
<i>Phishing e Smishing</i>	■	■	■	
Acesso indevido a dados pessoais	■	■	■	■
<i>DDoS</i>	■	■	■	
Manipulação de Sistemas (TI)	■	■		■

Legenda:

■ - Agente de ameaça provável

No questionário realizado, nenhum dos inquiridos indicou ter sofrido qualquer tipo de incidente de segurança. Contudo, esse resultado contraria os números do CNCS e do CERT.PT, que registaram, entre 2019 e 2023, um total de 44 incidentes no setor financeiro⁸⁴⁷.

Figura 6 - Número de incidentes no setor das Infraestruturas do Mercado Financeiro anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização em 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

⁸⁴⁷ CNCS, "Relatório Riscos e Conflitos" (2023), 10.

4.3. Capacitação

As infraestruturas do mercado financeiro, têm, em Portugal, procurado capacitar-se em cibersegurança de duas formas: através da contratação de profissionais, devido à falta de profissionais na área (**Gráfico 44**) e da aquisição de tecnologia para dar resposta às ameaças visto que 100% do setor tem acesso a equipamentos digitais na realização do seu trabalho (**Gráfico 48**) bem como acesso à internet (**Gráfico 50**). Relativamente à média geral, este setor tem maior percentagem no acesso a equipamentos digitais na realização do seu trabalho e à internet, ambos com 100%.

Gráfico 44 - Perceção sobre a falta de profissionais em cibersegurança e áreas relacionadas

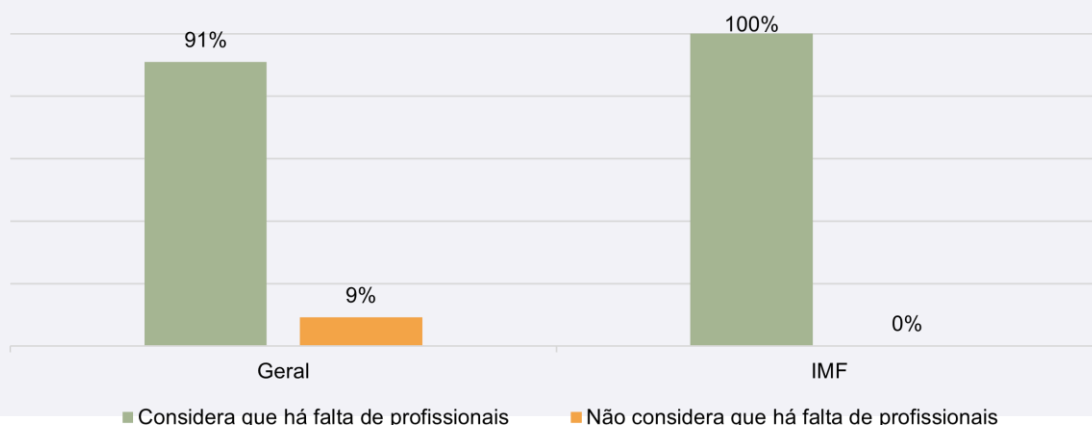


Gráfico 48 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho

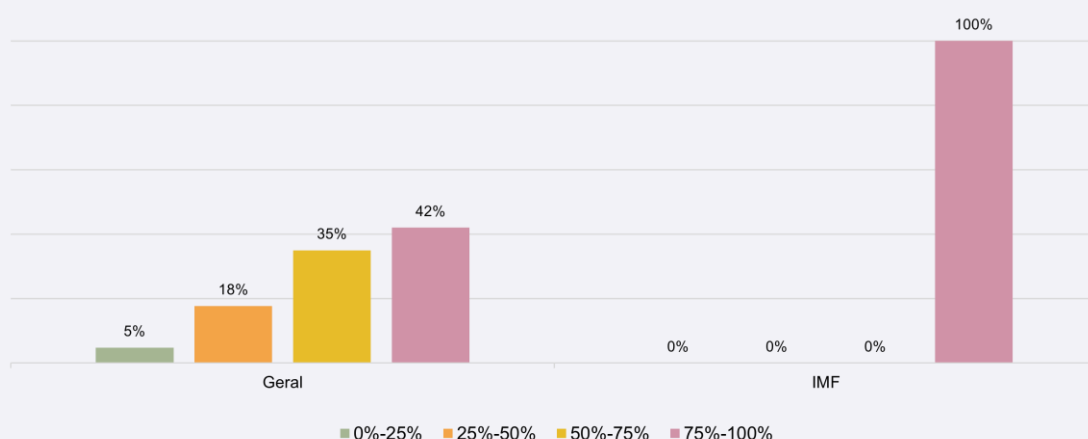
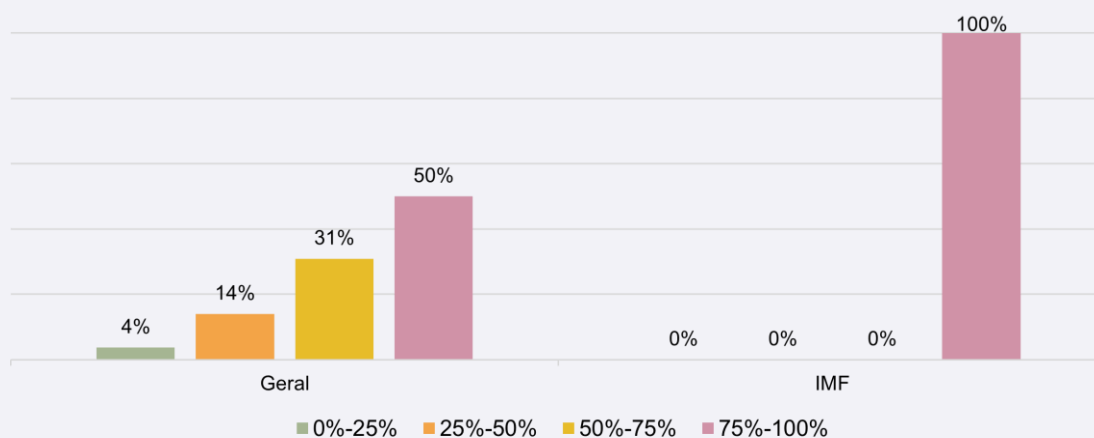


Gráfico 50 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções



Desde 2017, ano em que o Centro Tecnológico da Euronext foi transferido de Belfast para o Porto, a plataforma pan-europeia de Bolsas, que também opera em Portugal, tem aumentado continuamente a equipa dedicada à cibersegurança. Inicialmente, o centro no Porto contava com cerca de 70 profissionais, mas em 2021 esse número já aumentou para aproximadamente 180 trabalhadores. Com o objetivo de fortalecer ainda mais as defesas de cibersegurança, a Euronext planeou contratar mais 50 profissionais em 2022 e pretende adicionar várias dezenas de novos colaboradores até final de 2024⁸⁴⁸.

Quanto à aquisição de tecnologia, também a Euronext conta, desde 2018, com a plataforma “*Cymulate Breach & Attack Simulation*”, da empresa Cymulate, que permite aos profissionais do grupo realizar uma série de testes, nomeadamente simulam ataques cibernéticos (de cibersegurança) reais para identificar vulnerabilidades e melhorar a postura de segurança da organização aos seus próprios mecanismos de segurança e assim melhorar a sua postura face a ciberataques⁸⁴⁹.

⁸⁴⁸ Miguel Nogueira, “Centro tecnológico da Euronext no Porto vai contratar para continuar ‘história de sucesso’”, *Porto*, 12 de novembro de 2021, <https://www.porto.pt/pt/noticia/centro-tecnologico-da-euronext-no-porto-vai-contratar-para-continuar-historia-de-sucesso>.

⁸⁴⁹ “Euronext adota solução da Cymulate para melhorar resposta a ameaças”, *IT Channel*, 28 de novembro de 2019, <https://www.itchannel.pt/news/negocios/euronext-adota-solucao-da-cymulate-para-melhorar-resposta-a-ameacas>.

No caso das câmaras de compensação e CCPs, a capacitação tem, pelo menos desde 2021, passado pela contratualização externa do serviço de *Security Operations Center (SOC)*⁸⁵⁰ e de *Cyber Threat Intelligence (CTI)*⁸⁵¹, bem como pela mitigação de quaisquer vulnerabilidades identificadas pelo CNCS e ainda pela implementação de melhorias nos controlos de segurança (melhorias nos acessos à *cloud*, filtragem dos acessos à Internet, implementação de autenticação multifator, segmentação de redes). Têm também apostado na formação teórica e prática e na realização de exercícios de cibersegurança⁸⁵².

Atualmente, a União Europeia (UE) está a trabalhar num projeto com o objetivo de fortalecer o mercado financeiro, “melhorando assim o acesso ao financiamento a pequenas e médias empresas (PMEs) e os investimentos transfronteiriços. Esta iniciativa, denominada por União dos Mercados de Capitais (UMC)”, é destinada a criar um verdadeiro mercado único de capitais, assegurando o livre fluxo de investimento entre todos os Estados-Membros. Esta iniciativa tem três pilares principais:

- Apoiar a recuperação económica ecológica, digital, resiliente e inclusiva das empresas;
- Tornar a UE um espaço mais seguro para o investimento a longo prazo;
- Assegurar a integração dos mercados num único mercado⁸⁵³.

⁸⁵⁰ Responsável pela deteção, resposta e prevenção às ameaças de cibersegurança de uma organização. (Fonte: <https://www.ibm.com/topics/security-operations-center>)

⁸⁵¹ Informações sobre ameaças que foram agregadas, transformadas, analisadas, interpretadas ou enriquecidas para fornecer o contexto necessário e auxiliar processos de tomada de decisão. (Fonte: “Threat Intelligence”, Glossary, NIST, https://csrc.nist.gov/glossary/term/threat_intelligence)

⁸⁵² OMI, “Relatório Integrado OMI 2022”, maio de 2023, 47, https://www.omie.es/sites/default/files/2023-05/omi_reporting_integrado_2022_PT_4.pdf.

⁸⁵³ Conselho Europeu, “Construção da União dos Mercados de Capitais da UE”, última revisão a 12 junho de 2024, <https://www.consilium.europa.eu/pt/policies/what-the-eu-is-doing-to-deepen-its-capital-markets/>.

4.4. Investimento em cibersegurança

A par do que tem sido feito ao nível da capacitação no setor, é possível verificar, através dos relatórios de atividades, que têm sido realizados outros esforços no âmbito do reforço da cibersegurança. No caso da Euronext, o grupo revalidou, em 2022, as suas certificações na ISO 22301 (sobre Continuidade de Negócio) e ISO 27001 (sobre Sistemas de Gestão de Segurança da Informação). Tem também sido prestada particular atenção dentro do grupo à preparação para a conformidade com legislação europeia como o *Digital Operational Resilience Act* (DORA), destinado aos setores bancário e financeiro, e com o quadro TIBER-EU⁸⁵⁴, um quadro que oferece orientações sobre como as entidades destes dois setores, autoridades e prestadores de serviços de CTI e *Red Team* devem trabalhar em conjunto para testar a sua resiliência num cenário controlado de ciberataque.

Além disso, o Banco de Portugal e a Comissão do Mercado de Valores Mobiliários (CMVM) têm desenvolvido iniciativas para reforçar a resiliência cibernética. Em 2023, o Banco de Portugal publicou o relatório “Relatório de Estabilidade Financeira” em novembro 2023⁸⁵⁵, destacando a importância da cibersegurança na estabilidade financeira e detalhando as medidas implementadas para aumentar a resiliência do sistema financeiro nacional.

Outras iniciativas incluem parcerias entre instituições financeiras e empresas de tecnologia para desenvolver soluções avançadas de cibersegurança. A SIBS, por exemplo, investiu em sistemas de monitorização e deteção de ameaças no ciberespaço, além de participar de exercícios de simulação de ciberataques para testar e aprimorar sua resposta a incidentes. A SIBS participa ativamente em debates e eventos sobre segurança e cibersegurança⁸⁵⁶.

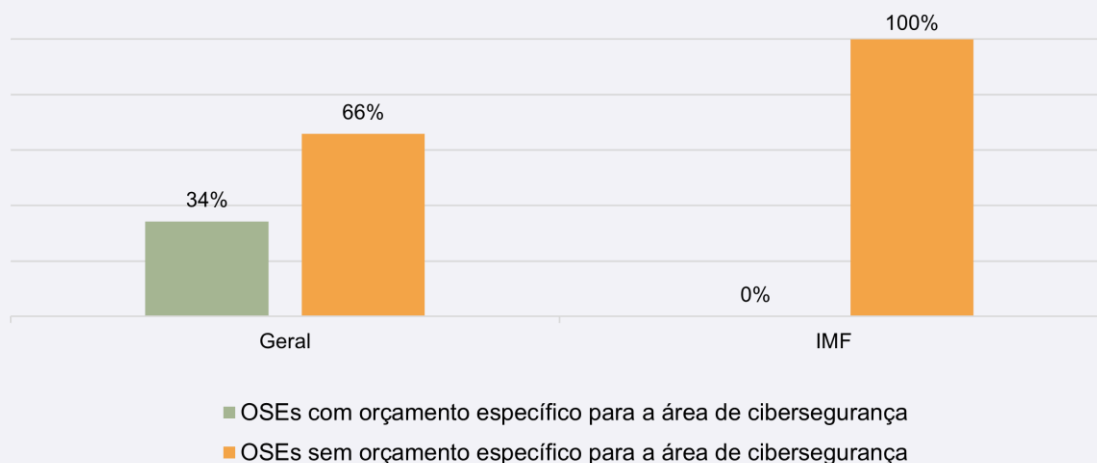
⁸⁵⁴ Euronext, “Financial Statements as of 31 December 2022”, 14, https://www.euronext.com/sites/default/files/2023-06/cassa_di_compensazione_e_garanzia_spa_financial_statement_31.12.2022_eng.pdf.

⁸⁵⁵ Banco de Portugal, “Relatório de Estabilidade Financeira”, novembro de 2023, 50-51, https://www.bportugal.pt/sites/default/files/documents/2024-02/ref_11_2023_pt.pdf.

⁸⁵⁶ SIBS, “Relatório e Contas 2023: Contas Consolidadas”, julho de 2024, 42, https://sibs-sites.sibs.pt/sibs/wp-content/uploads/sites/13/2024/07/RC_2023_SIBS_CONSOLIDADO.pdf

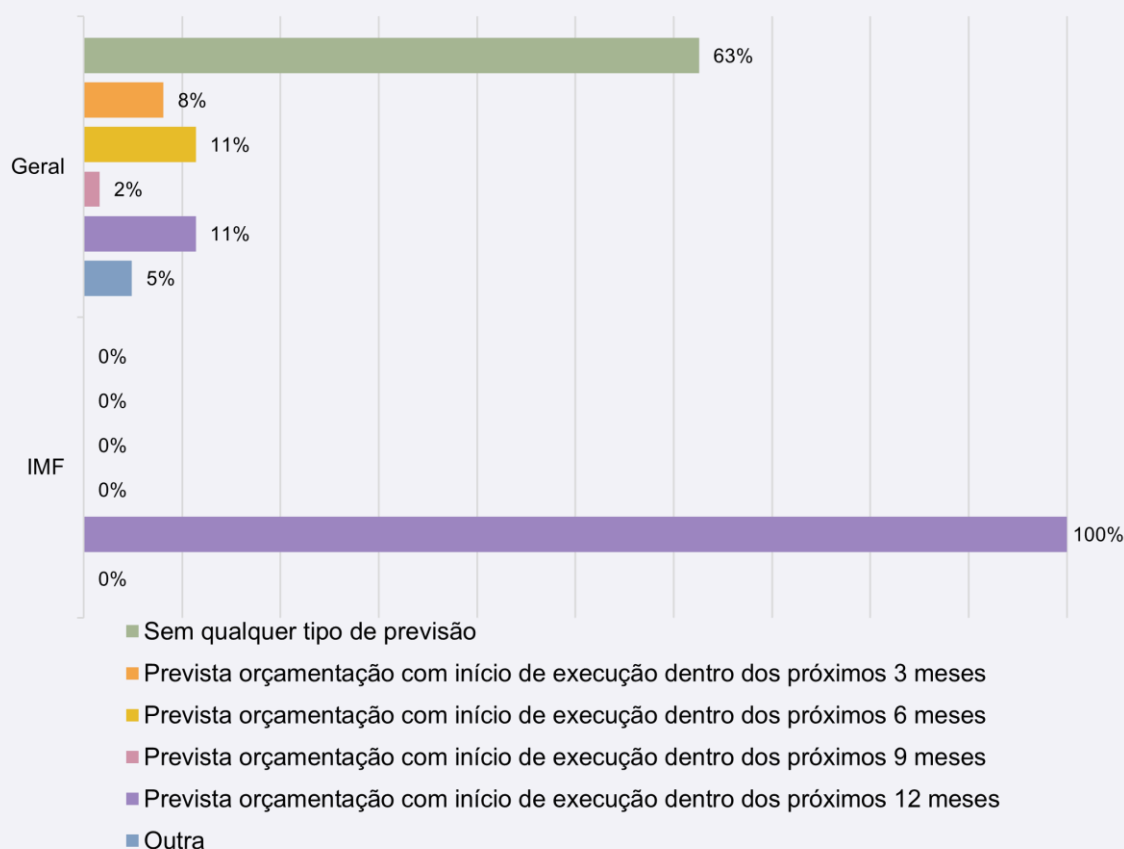
Deste setor, nenhuma das entidades tem um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 66% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Todas as entidades têm previsto a orçamentação dentro dos próximos 12 meses (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Apesar desses esforços, não foram divulgados números concretos sobre os valores investidos em cibersegurança, dificultando uma avaliação precisa do nível de investimento no setor.

4.5. RJSC e legislação setorial

O setor das infraestruturas do mercado financeiro está sujeito a diversas obrigações legais e regulamentares no âmbito da cibersegurança. A legislação existente é maioritariamente de âmbito europeu, mesmo sendo depois transposta para o ordenamento jurídico nacional (como é o caso das diretivas europeias, cuja transposição é obrigatória). A nível nacional, e de forma a complementar a legislação europeia, o setor é sobretudo orientado por regulamentos e circulares produzidos pela entidade reguladora - a CMVM.

Veja-se então primeiro o que tem sido feito a nível europeu. Em 2012, o Regulamento da União Europeia n.º 648/2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, também conhecido como *European Market Infrastructure Regulation* (EMIR), apesar de não versar exclusivamente sobre cibersegurança, impôs às contrapartes centrais o dever de “manter sistemas informáticos adequados para lidar com a complexidade, variedade e tipo de serviços e atividades desenvolvidos, a fim de assegurar elevados padrões de segurança e a integridade e confidencialidade das informações que detêm”⁸⁵⁷.

Por sua vez, em maio de 2014, foi publicada a Diretiva 2014/65/UE, relativa aos mercados de instrumentos financeiros, que impõe às infraestruturas do mercado financeiro a obrigação de “aplicar mecanismos de segurança sólidos para garantir a segurança e a autenticação dos meios de transferência das informações, minimizar o risco de corrupção de dados e de acesso não autorizado e para evitar fugas de informação, mantendo a confidencialidade dos dados em todos os momentos”⁸⁵⁸. Esta diretiva foi transposta para o ordenamento jurídico nacional através da lei n.º 35/2018, de 20 de julho⁸⁵⁹.

Também em 2014, em julho, foi publicado o Regulamento da UE n.º 909/2014, relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs), que impôs às CSDs a obrigação de manter “ferramentas de tecnologias de informação adequadas, que garantam um elevado grau de segurança e fiabilidade operacional e que disponham de capacidade suficiente”⁸⁶⁰, devendo as “ferramentas de tecnologias de informação ser adequadas para lidar com a complexidade, a variedade e o tipo de serviços e atividades desenvolvidas, de modo a garantir normas de segurança elevadas e a integridade e confidencialidade das informações conservadas”⁸⁶¹.

⁸⁵⁷ Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, *Jornal Oficial da União Europeia*, 30, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:201:0001:0059:PT:PDF>.

⁸⁵⁸ Diretiva 2014/65/UE do Parlamento Europeu e do Conselho de 15 de maio de 2014 relativa aos mercados de instrumentos financeiros, *Jornal Oficial da União Europeia*, 173, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014L0065>.

⁸⁵⁹ Lei n.º 35/2018, de 20 de julho, *Procuradoria-Geral Distrital de Lisboa*, https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2920&tabela=leis&so_miolo=.

⁸⁶⁰ Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs), *Jornal Oficial da União Europeia*, 46, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0909>.

⁸⁶¹ Regulamento (UE) n.º 909/2014.

Surgiria depois, em 2016, a Diretiva n.º 2016/1148⁸⁶² (a Diretiva NIS, cuja transposição para o ordenamento jurídico nacional corresponde à Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço⁸⁶³). Foi com esta Diretiva e lei que os operadores do setor das infraestruturas do mercado financeiro foram identificados como Operadores de Serviços Essenciais, sendo-lhes colocadas diversas obrigações ao nível da segurança dos sistemas e redes, bem como ao nível de reporte de incidentes⁸⁶⁴. O RJSC viria a ser complementado pelo Decreto-Lei n.º 65/2021, de 30 de julho, que o regulamenta, e impõe obrigações como a designação de um ponto de contacto permanente, um responsável de segurança, a elaboração e manutenção de um inventário de ativos, a elaboração e implementação de um plano de segurança, a elaboração de um relatório anual que inclua as principais atividades desenvolvidas em matéria de cibersegurança e estatísticas análises agregadas dos incidentes relevantes ocorridos, bem como a realização de uma análise de risco anual⁸⁶⁵.

A nível europeu, surge ainda o Regulamento n.º 2022/2554, relativo à resiliência operacional digital do setor financeiro, mais conhecido por DORA (*Digital Operational Resilience Act*). Este regulamento destina-se a várias entidades financeiras, desde bancos, a empresas de seguros, passando também pelas plataformas de negociação e contrapartes centrais. Deste decorrem diversas obrigações, tais como obrigações afetas à gestão do risco associado às tecnologias da informação e comunicação (TIC), gestão dos serviços e ferramentas TIC prestados por terceiros, obrigações ao nível dos sistemas, protocolos e ferramentas TIC, das atividades de proteção e prevenção, deteção, resposta e recuperação em situação de incidente, reporte de incidentes, testes de resiliência operacional, o que inclui a realização de análises de vulnerabilidades, avaliações da segurança das redes, análises da segurança física, revisões do código fonte, testes baseados em cenários, testes de compatibilidade, testes de desempenho, testes de extremo a extremo e testes de penetração⁸⁶⁶. A aplicação deste regulamento será obrigatória a partir de 17 de janeiro de 2025.

Seis anos depois da publicação da Diretiva NIS, foi publicada em 2022 a Diretiva (UE) 2022/2555⁸⁶⁷, mais amplamente conhecida como NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: “setores de importância crítica”⁸⁶⁸ e “outros setores críticos”⁸⁶⁹. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsectores. São também introduzidas novas obrigações.

Apesar de a Diretiva NIS 2 abranger mais entidades nalguns setores, tal não se verifica no setor das infraestruturas do mercado financeiro. À semelhança do setor bancário, continuam a ser abrangidas as mesmas entidades já visadas pela Diretiva NIS 1. Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos⁸⁷⁰.

⁸⁶² Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148>.

⁸⁶³ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

⁸⁶⁴ Lei n.º 46/2018.

⁸⁶⁵ Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

⁸⁶⁶ Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro, *Jornal Oficial da União Europeia*, 29-51, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554>.

⁸⁶⁷ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>.

⁸⁶⁸ Diretiva (UE) 2022/2555, Anexo I.

⁸⁶⁹ Diretiva (UE) 2022/2555, Anexo II.

⁸⁷⁰ Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto⁸⁷¹.

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança. O Regulamento DORA inclui provisões semelhantes incentivando este tipo de acordos para o intercâmbio de “informações específicas e sensíveis relativas a ciberataques, nomeadamente indicadores de comprometimento dos sistemas ou dos dados, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração”⁸⁷². Já a Diretiva NIS 2 estabelece que as informações partilhadas à luz destes acordos podem ser relacionadas com “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”⁸⁷³.

Como referido, a nível nacional o setor é sobretudo orientado pelos regulamentos, instruções, recomendações e circulares da CMVM. O Regulamento da CMVM n.º 7/2023 sobre a Regulamentação do Regime da Gestão de Ativos, estabelece sobre as entidades reguladas a obrigação de comunicar, no prazo máximo de 24 horas, “a ocorrência de incidentes relacionados com a segurança de informação e comunicação que impactem o normal funcionamento da sua atividade ou que constituam risco elevado para [o seu] funcionamento”⁸⁷⁴. Já circulares como a 005/2023⁸⁷⁵ e a Circular 003/2024 - Circular Anual de Gestão de Ativos 2024⁸⁷⁶ reforçam a importância da cibersegurança, as ações de supervisão executadas nessa matéria por parte da CMVM sobre as entidades reguladas e, simultaneamente, alertam as entidades financeiras para a necessidade de estarem em conformidade com o regulamento DORA a partir de 17 de janeiro de 2025.

⁸⁷¹ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

⁸⁷² Regulamento (UE) 2022/2554, artigo 45.º, n.º 1.

⁸⁷³ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

⁸⁷⁴ Regulamento da CMVM n.º 7/2023 Regulamentação do Regime da Gestão de Ativos, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/regulamento-cmvm/7-2023-835896543>

⁸⁷⁵ Circular 005/2023 - Gestão de Ativos e Empresas de Investimento | Tecnologias da Informação e Comunicação: Cibersegurança - CMVM, <https://www.cmvm.pt/Plnstitucional/Content?Input=C6DE3F376C5004D8E490034ED0FAA70C0A71D3AE04178CDC0170C5EC472B7D19#>.

⁸⁷⁶ Circular 003/2024 - Gestão de Ativos – Circular anual de gestão de ativos 2024 - CMVM, <https://www.cmvm.pt/Plnstitucional/Content?Input=C1B8E11C9FC436AFE660445BDC7E1867050C25D72FD472228ABA2E3FEA4A338B#>.

4.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor de infraestruturas de mercado, segundo a ENISA, que define o setor como “*Financial and Banking*”. Neste sentido, os *standards* e as boas práticas aplicadas a este setor são, muitas vezes, os mesmos seguidos que o setor bancário, por trabalharem em várias circunstâncias com sistemas, ativos e métodos semelhantes⁸⁷⁷.

Tabela 43 - Standards e Boas Práticas (Infraestruturas do Mercado Financeiro)

Standards	Boas práticas
• Gramm–Leach–Bliley Act; • Sarbanes–Oxley Act; • Diretiva (UE) 2015/2366, relativa aos serviços de pagamento no mercado interno (PSD2); • EBA - Orientações definitivas sobre a segurança dos pagamentos efetuados através da Internet; • American National Standards Institute (ANSI) X9 series.	• Payment Card Industry Data Security Standard (PCI DSS); • Basel II; • EBA - Orientações definitivas sobre a segurança dos pagamentos efetuados através da Internet; • CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure; • SEC OCIE Cybersecurity.

Na tabela anterior estão os *standards* e boas práticas referentes à área das infraestruturas do mercado financeiro. De seguida, apresenta-se um breve sumário de cada um:

- **Gramm–Leach–Bliley Act:** Lei dos EUA que exige que instituições financeiras protejam a confidencialidade e a segurança das informações dos clientes⁸⁷⁸;
- **Sarbanes–Oxley Act:** Lei dos EUA com disposições que afetam a governação das empresas, a gestão de riscos, auditorias e os relatórios financeiros das empresas públicas, incluindo disposições destinadas a dissuadir e punir a fraude e a corrupção⁸⁷⁹.
- **Diretiva (UE) 2015/2366, relativa aos serviços de pagamento no mercado interno (PSD2):** Diretiva da UE com o objetivo de modernizar os serviços de pagamento na Europa, promovendo a inovação e aumentando a segurança nas transações⁸⁸⁰;
- **EBA - Orientações definitivas sobre a segurança dos pagamentos efetuados através da Internet:** Orientações da EBA para melhorar a segurança dos pagamentos pela Internet, reduzindo riscos de fraude e aumentando a proteção ao consumidor⁸⁸¹;
- **American National Standards Institute (ANSI) X9 series:** Conjunto de normas que definem padrões de segurança para transações financeiras, garantindo a integridade e confidencialidade das mesmas⁸⁸²;

⁸⁷⁷ ENISA, “Mapping of OES Security Requirements to Specific Sectors”, 18 de janeiro de 2018, 28 <https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors>.

⁸⁷⁸ “Gramm–Leach–Bliley Act”, Business Guidance: Privacy and Security, United States Federal Trade Commission, <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>.

⁸⁷⁹ “The Sarbanes–Oxley Act”, Sarbanes Oxley Act, <https://sarbanes-oxley-act.com/>.

⁸⁸⁰ Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, *Jornal Oficial da União Europeia*, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366>.

⁸⁸¹ “Orientações definitivas sobre a segurança dos pagamentos efetuados através da internet”, EBA, https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/558993c7-c253-472c-bae3-f897f6c6038a/EBA-GL-2014-12_PT_rev1%20GL%20on%20Internet%20Payments.pdf.

⁸⁸² “X9: Accredited Standards Committee X9, Inc.”, ANSI Webstore, American National Standards Institute, https://webstore.ansi.org/sdo/x9?source=blog&_gl=1*v6wen5*_gcl_au*NzI0ODc2NzI1LjE3MjU1NTU5ODc.

- **Payment Card Industry Data Security Standard (PCI DSS):** Conjunto de padrões de segurança para proteger as informações dos cartões de pagamento e evitar fraudes⁸⁸³;
- **Basel II:** Acordo internacional que estabelece normas para a regulação bancária⁸⁸⁴;
- **EBA - Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2):** Orientações preliminares para medidas de segurança e gestão de riscos operacionais nos serviços de pagamento sob a PSD2⁸⁸⁵;
- **CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure:** Diretrizes para aumentar a resiliência de cibersegurança das infraestruturas dos mercados financeiros⁸⁸⁶;
- **SEC OCIE Cybersecurity:** Diretrizes da SEC (Securities and Exchange Commission - EUA) para avaliar a postura de cibersegurança das empresas financeiras⁸⁸⁷.

⁸⁸³ "PCI Data Security Standard (PCI DSS)", Standards, Security Standards Council, <https://www.pcisecuritystandards.org/standards/pci-dss/>.

⁸⁸⁴ "Basel II: Revised international capital framework", Basel Committee on Banking Supervision, Bank for International Settlements, <https://www.bis.org/publ/bcbsca.htm>.

⁸⁸⁵ "Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)", EBA, 12 de janeiro de 2018, [https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20\(EBA-GL-2017-17\)_PT.pdf](https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf).

⁸⁸⁶ "Guidance on cyber resilience for financial market infrastructures", BIS e IOSCO, junho de 2016, <https://www.bis.org/cpmi/publ/d146.pdf>.

⁸⁸⁷ "OCIE Cybersecurity and Resiliency Observations", U.S. Securities and Exchange Commission, <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>.

4.7. Desafios

As infraestruturas do mercado financeiro enfrentam desafios semelhantes aos do setor bancário. São alvos apetecíveis para ciberataques, sobretudo os que podem vir a afetar a disponibilidade dos serviços e da informação, como ataques de *DDoS* e de *ransomware*, bem como os que podem comprometer a segurança e integridade dos dados, como *data breaches*. São também um setor onde os ciberataques podem ter um efeito em cadeia, tornando-se impossível circunscrever os impactos de um ciberataque a uma organização ou a um território, comprometendo assim a estabilidade financeira internacional.

Adicionalmente, são um setor que tem de navegar uma regulamentação extensa e complexa e encetar diversos esforços para estar em conformidade com tudo o que a regulamentação e legislação lhe exige. Por exemplo, o regulamento DORA, em vigor desde janeiro de 2023, e que será de cumprimento obrigatório para as entidades dos setores bancário e financeiro a partir de janeiro de 2025, traz novas exigências ao nível da gestão do risco das TIC, gestão do risco das TIC com terceiros, testes de resiliência operacional digital, incidentes relacionados com as TIC, da partilha de informação e da supervisão dos prestadores de serviços terceiros críticos. Diversas entidades estão já a tomar as medidas necessárias para estarem em conformidade com o regulamento a partir de janeiro de 2025.

4.8. Recomendações

O Conselho Nacional de Supervisores Financeiros (CNSF) destaca a importância da Gestão da Continuidade de Negócio (Business Continuity - BC) no setor financeiro, particularmente para as infraestruturas do mercado financeiro. A continuidade de negócio é essencial para assegurar a manutenção ou rápida recuperação de funções críticas em caso de interrupções operacionais, minimizando impactos nos mercados financeiros. Este enfoque reflete-se nas orientações e normativos do CNSF, que visam fortalecer a resiliência operacional no setor face a riscos como ciberataques ou desastres naturais.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste setor. Tais cenários são indicados na seguinte tabela:

Tabela 44 - Cenários de risco (IMF)

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
COLABORADOR que, por vingança, por razões financeiras ou por negligência, expõe informação sensível da entidade ou instala <i>software</i> malicioso que compromete a organização com <i>spyware</i> , <i>ransomware</i> ou outro tipo de ameaça.
FUGA DE INFORMAÇÃO da organização, causada eventualmente por violação de dados e ação intencional de um colaborador, expondo nos media e ao público em geral dados pessoais, dados financeiros, trocas de emails, propriedade intelectual, entre outras.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em <i>bitcoins</i> , sob a ameaça da sua destruição ou exposição ao público.

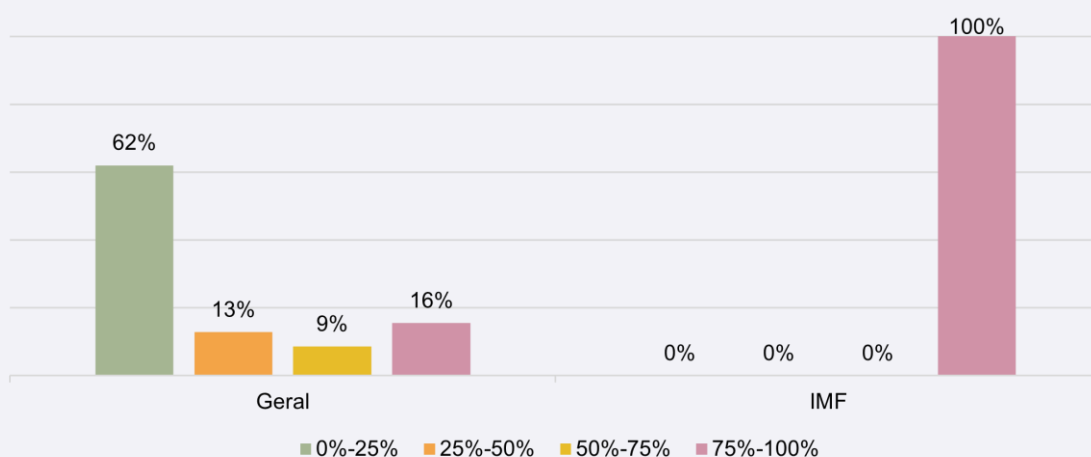
(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 30 de agosto de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor das infraestruturas do mercado financeiro, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

As ameaças mais prevalentes neste setor são o *ransomware* e as ameaças relativas a dados pessoais dos clientes, sendo estas ameaças concretizadas, normalmente, através de ataques bem-sucedidos de *phishing*. A sensibilização para este tipo de riscos e a formação para identificar estes riscos são essenciais para impedir que estas se concretizem, pois a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Este setor está à frente da média geral, dado que em os OSE, 75%-100% trabalhadores têm formação básica em cibersegurança quando, no âmbito geral, apenas 16% dos setores estão nesse patamar (**Gráfico 33**).

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Os resultados do questionário evidenciam que a totalidade dos OSE do setor disponibiliza formação em cibersegurança aos seus colaboradores (**Gráfico 38**), sendo que todas são de carácter obrigatório (**Gráfico 39**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

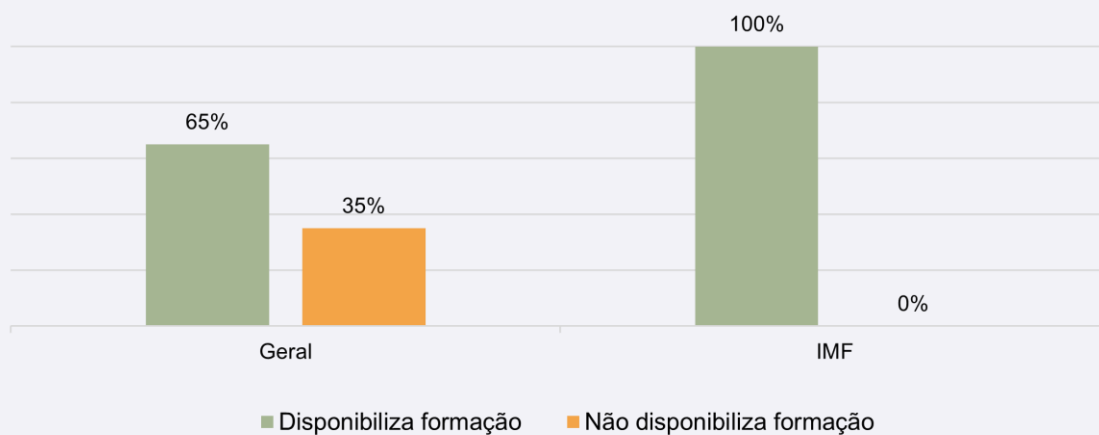
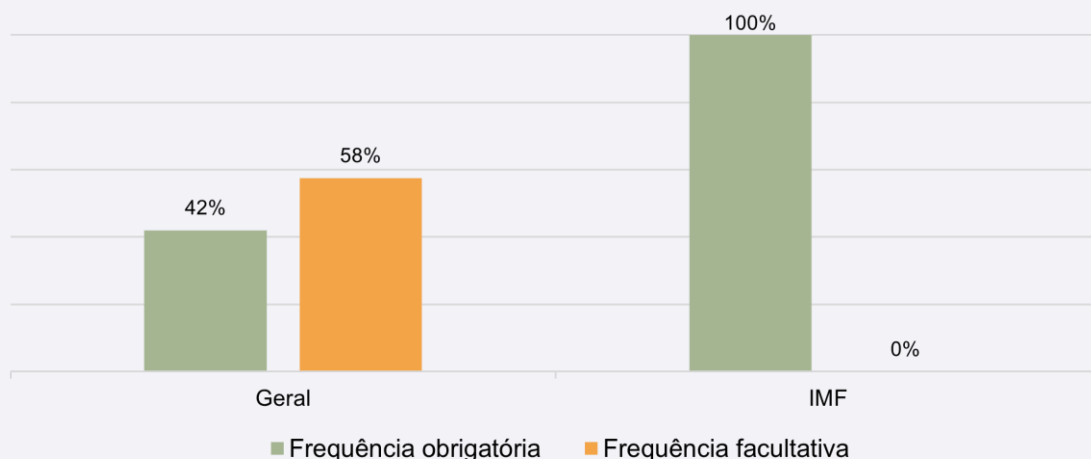
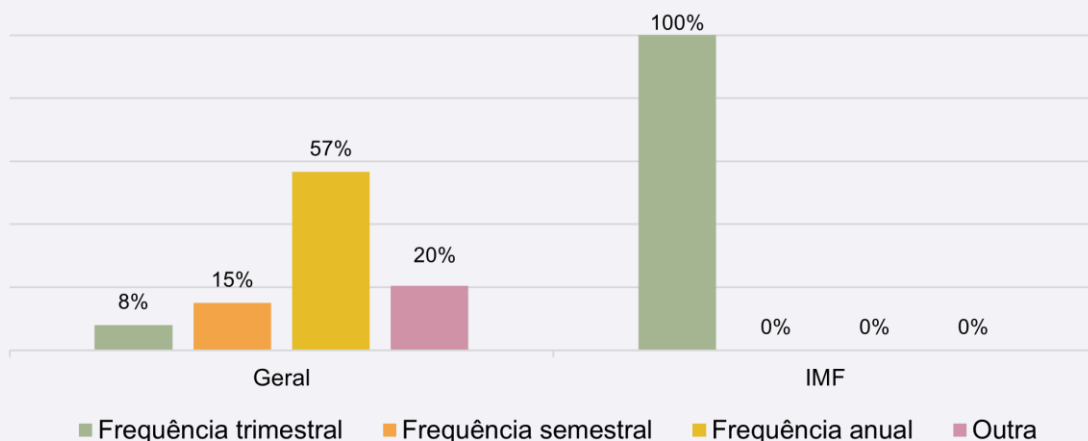


Gráfico 39 - Carácter das formações disponibilizadas - frequência obrigatória ou facultativa



Além disso, em todas as entidades, os momentos de formação têm frequência trimestral (**Gráfico 41**), o que no contexto do setor assegura a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores.

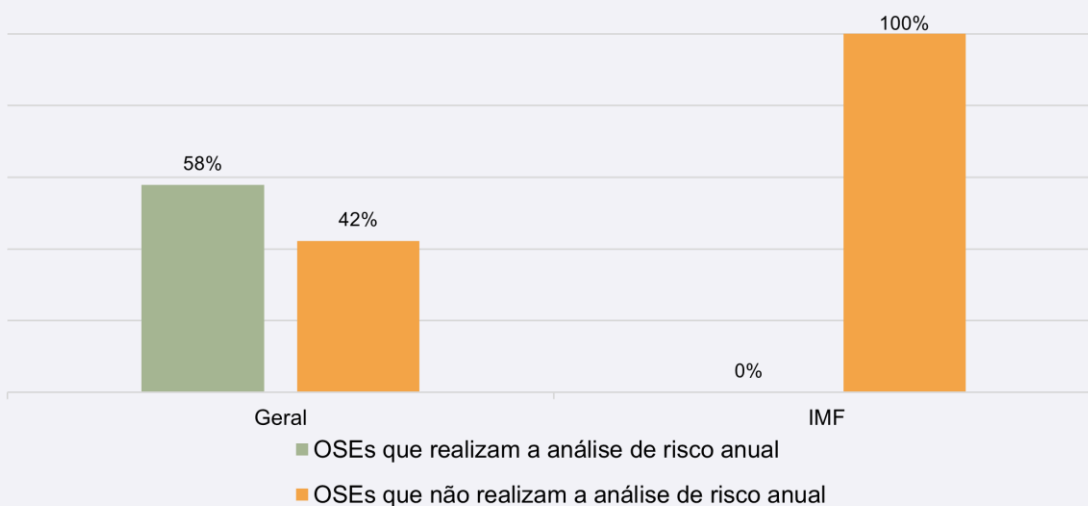
Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que este setor, comparativamente com os restantes, está acima da média, com exceção na utilização de *browser* que proteja a privacidade, segurança de rede em *cloud*, controlos biométricos para identificação e autenticação de utilizadores e *backups* de dados em diferentes localizações. Este setor é o único onde não se realiza avaliações de segurança anuais no âmbito de cibersegurança (**Gráfico 99**).

Gráfico 99 - Realização de análise de riscos anual no âmbito de cibersegurança



Nesse sentido, recomenda-se aos OSE do setor das infraestruturas do mercado financeiro que:

- Realizem avaliações de segurança, em todas as entidades, pelo menos anualmente;
- Realizem análises de risco pelo menos anualmente;
- Implementem, onde possível, controlos biométricos para identificação e autenticação de utilizadores;
- Implementem *backups* de dados em diferentes localizações.

Políticas, procedimentos e planos de cibersegurança

Com base nos dados reunidos no questionário, 100% dos OSE do setor possuíam políticas e procedimentos de cibersegurança documentados e implementados. Todos os inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Diante desta situação, apesar de todos OSE do setor terem uma política de segurança, é importante que a mesma verse sobre:

- Os diversos papéis e responsabilidades dos vários colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, como os controlos de acesso (lógico e físico);
- A gestão de incidentes, incluindo a elaboração de um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação, além de um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir, que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização periódica da política (pelo menos anualmente), para manter a mesma atualizada conforme a evolução das ameaças de cibersegurança e as mudanças na organização.

Considerando que nenhum dos OSE do setor indicaram possuir uma política de uso aceitável de ativos e uma política de gestão de ativos, recomenda-se também a elaboração de uma política de gestão de ativos alinhada com a política de cibersegurança.

Análise de vulnerabilidades e realização de testes de intrusão (*pentesting*)

Todos os OSE do setor das infraestruturas do mercado financeiro realizam procedimentos de deteção e gestão de vulnerabilidades, sendo este ponto importante tendo em vista a diminuição e antecipação de possíveis ataques. A deteção e análise, e correção de vulnerabilidades é uma prática importante para a proteção proativa e preventiva dos sistemas e aplicações em utilização em qualquer setor de atividade.

Quanto à realização de testes de intrusão, todos os OSE realizam os mesmos. É importante a realização deste tipo de testes, pois é mais uma maneira de identificar vulnerabilidades, corrigi-las e tornar os OSE mais resilientes em matéria de cibersegurança.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*⁸⁸⁸.

No setor das infraestruturas de mercado financeiro, os controlos fundacionais, relacionados com a segurança da rede, desempenham um papel particularmente crítico. Infraestruturas essenciais, como sistemas de compensação e liquidação, plataformas de negociação e redes de pagamento, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para assegurar a integridade, disponibilidade e continuidade dos serviços financeiros. Falhas ou configurações inadequadas podem ser exploradas para interromper transações financeiras, comprometer a segurança de dados sensíveis, ou desviar operações críticas, colocando em risco a estabilidade e a confiança nos mercados financeiros.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos⁸⁸⁹:

⁸⁸⁸ “The 18 CIS Critical Security Controls”, CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls-list>.

⁸⁸⁹ “The 18 CIS Critical Security Controls”.

Tabela 45 - Controlos de Segurança da CIS (IMF)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: “The 18 CIS Critical Security Controls”, CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls-list>)

5. Saúde

5.1. Contextualização setorial

Em Portugal, “a saúde constitui matéria de governação política pelo menos desde o século XVI, ainda que o seu financiamento não tenha, durante alguns séculos, sido assumido pelo poder governativo”⁸⁹⁰. Tal só viria a acontecer verdadeiramente depois do 25 de Abril de 1974, com a consagração do direito à proteção da saúde “através de um serviço nacional de saúde [SNS] universal e geral e (...) tendencialmente gratuito”⁸⁹¹ na Constituição de 1976.

Durante o Estado Novo (1933-1974), os cuidados de saúde estavam a cargo das famílias, das instituições privadas ou da previdência⁸⁹² ⁸⁹³. A criação do SNS mudou esse paradigma, transformando o Estado no principal prestador de cuidados de saúde em Portugal.

O SNS foi então formalmente criado em 1979, através da Lei n.º 56/79, de 15 de setembro, enquanto instrumento do Estado para assegurar o direito à saúde, nos termos da Constituição. O acesso é garantido a todos os cidadãos, independentemente da sua condição económica e social, bem como aos estrangeiros, em regime de reciprocidade, apátridas e refugiados políticos, e envolve todos os cuidados integrados de saúde, compreendendo a promoção e vigilância da saúde, a prevenção da doença, o diagnóstico e tratamento dos doentes e a reabilitação médica e social⁸⁹⁴.

⁸⁹⁰ Laurinda Abreu, “Pensar historicamente os cuidados de saúde em Portugal”, *O Referencial: Revista da Associação 25 de Abril*, 12, https://dspace.uevora.pt/rdpc/bitstream/10174/24717/1/REFERENCIAL%20130_bx_12_17.pdf.

⁸⁹¹ Constituição da República Portuguesa, art. 64.º: Saúde, <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>

⁸⁹² A previdência, ou a Previdência Social, era essencialmente composta por instituições corporativas, tais como os sindicatos nacionais obrigatórios, as Casas do Povo ou as Casas de Pescadores, que ofereciam alguma proteção aos trabalhadores em situações de doença ou de invalidez (fonte: BBVA, “História da Segurança Social (parte I)”, 20 de novembro de 2013, <https://www.aminhapensao.pt/blog/historia-da-seguranca-social-parte-i/>).

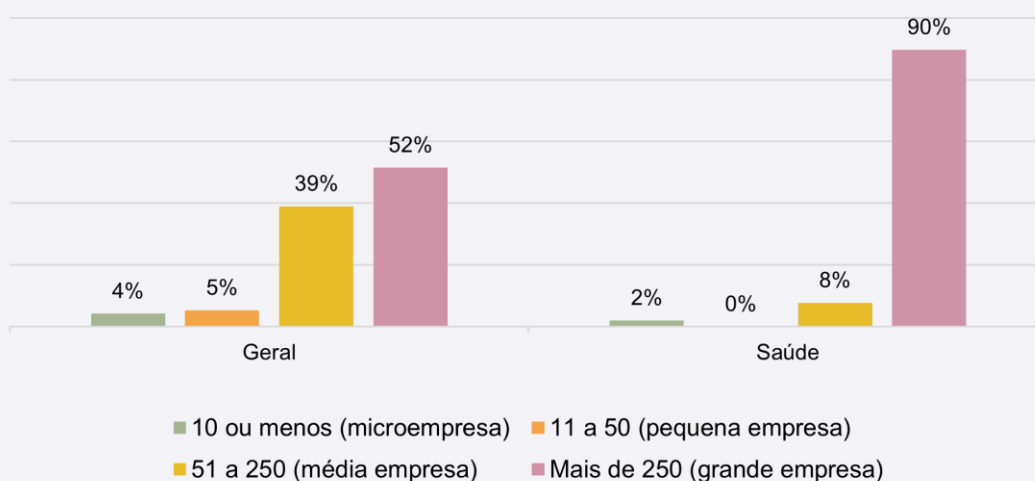
⁸⁹³ Teresa Nicolau, “Da democracia nasceu o Serviço Nacional de Saúde”, *RTP Ensina*, 2014, <https://ensina.rtp.pt/artigo/da-democracia-nasceu-o-servico-nacional-de-saude/>.

⁸⁹⁴ “História do SNS”, SNS, <https://www.sns.gov.pt/sns/servico-nacional-de-saude/historia-do-sns/>.

Segundo os *rankings* mais recentes disponíveis, o SNS é considerado o 13º melhor SNS⁸⁹⁵ entre 35 países europeus⁸⁹⁶ e o 40º melhor entre 104 países do mundo⁸⁹⁷.

De acordo com o questionário realizado, o tecido empresarial dos operadores de serviços essenciais (OSE) do setor da saúde é sobretudo composto por grandes organizações, com mais de 250 colaboradores, e as restantes são médias e micro-organizações (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



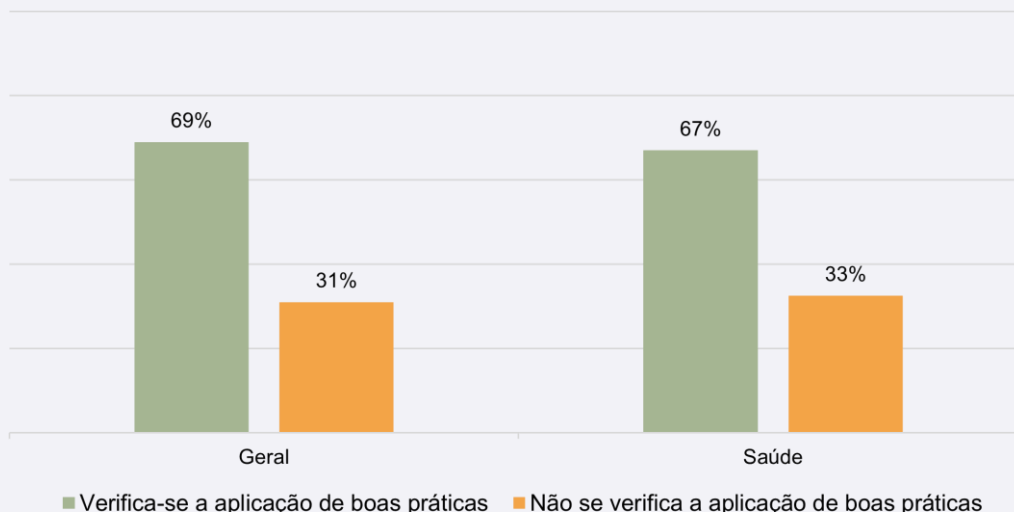
⁸⁹⁵ Arne Björnberg e Ann Phang, "Euro Health Consumer Index 2018", *Health Consumer Powerhouse*, 2019, <https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf>

⁸⁹⁶ "Euro Health Consumer Index by Country 2024", *World Population Review*, <https://worldpopulationreview.com/country-rankings/euro-health-consumer-index-by-country>.

⁸⁹⁷ "The Best Healthcare in the World: Country Rankings", *International Citizens Insurance*, 2024, <https://www.internationalinsurance.com/health/systems/>.

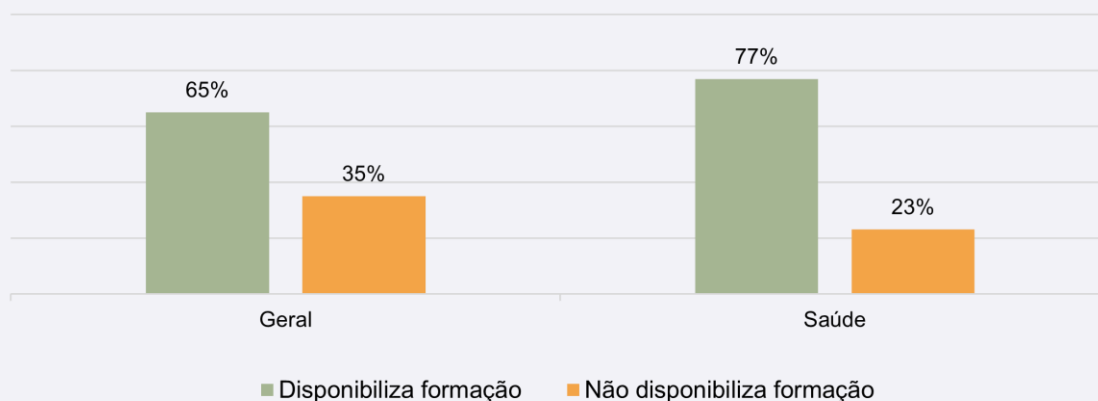
Dois terços dos operadores do setor da saúde referem aplicar boas práticas de segurança (**Gráfico 31**) sendo que o mesmo se verifica na generalidade dos setores.

Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores



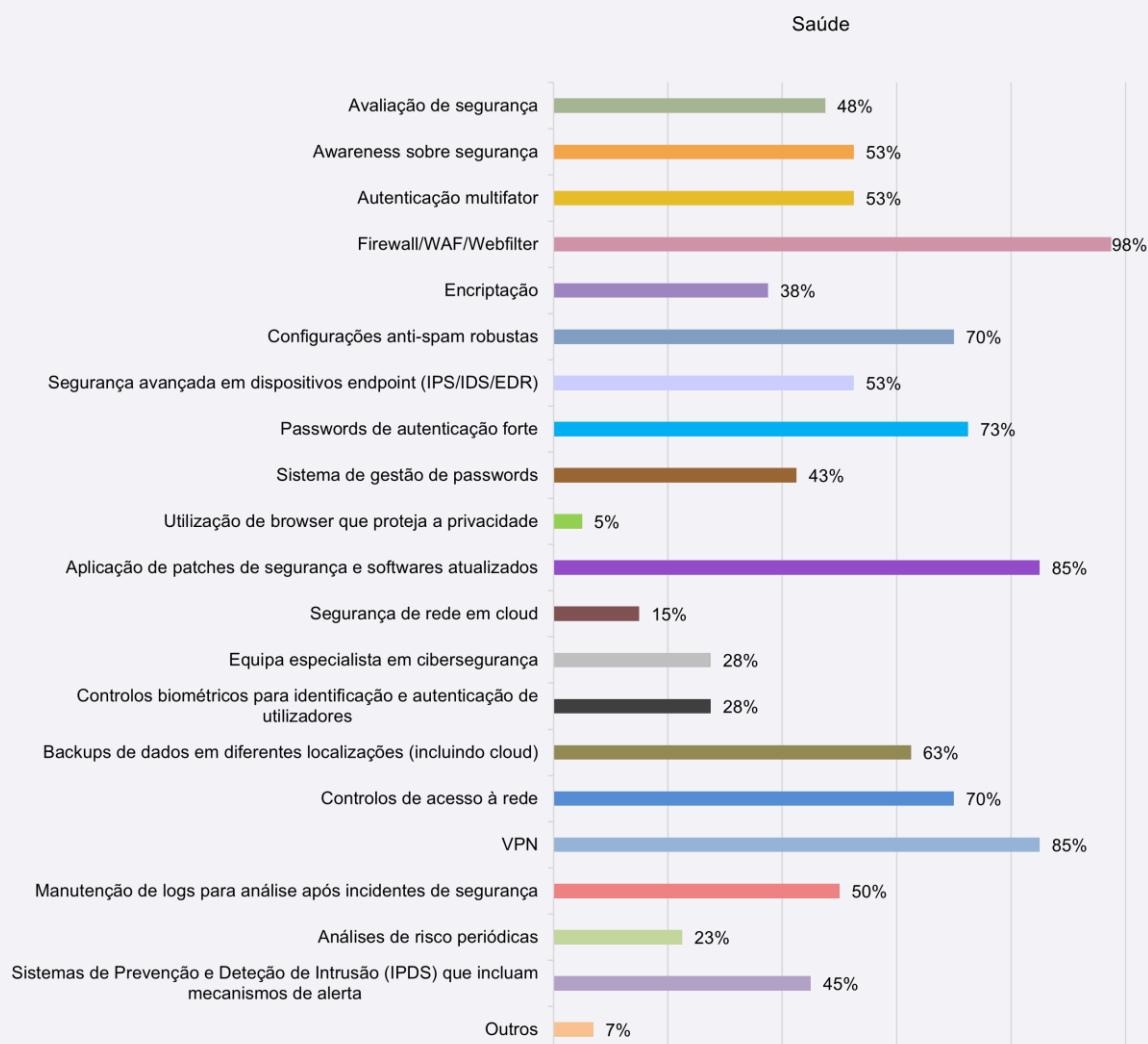
Esta afirmação pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (vide **Gráfico 38**), este número corresponde a cerca de 77%, o que pode ser considerado um número elevado.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



As medidas de proteção contra ameaças de cibersegurança (**Gráfico 66.5**) também suportam a afirmação anterior e, nestas, as mais utilizadas são: A utilização de *Firewall* em cerca de 98% dos casos, a utilização de palavras-passe fortes em 73%, utilização de configurações de *anti-spam* em 70% dos casos, utilização de *VPN* e controlos de acesso à rede com 85% e 70%, respetivamente.

Gráfico 66.5 - Medidas de proteção contra ameaças de cibersegurança



Este é um setor onde a maioria dos operadores (92%) afirma existir falta de profissionais na área da cibersegurança (**Gráfico 44**), no entanto e segundo estes dados, é também um setor que tem demonstrado uma baixa incidência de ciberataques identificados pelos próprios (71% dos inquiridos nunca sofreu um incidente de segurança em contexto TIC) (**Gráfico 68**).

Gráfico 44 - Perceção sobre a falta de profissionais em cibersegurança e áreas relacionadas

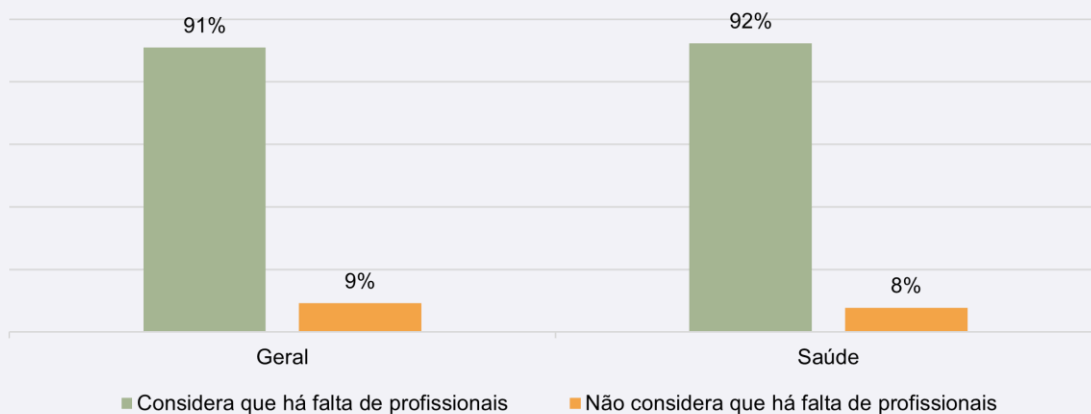
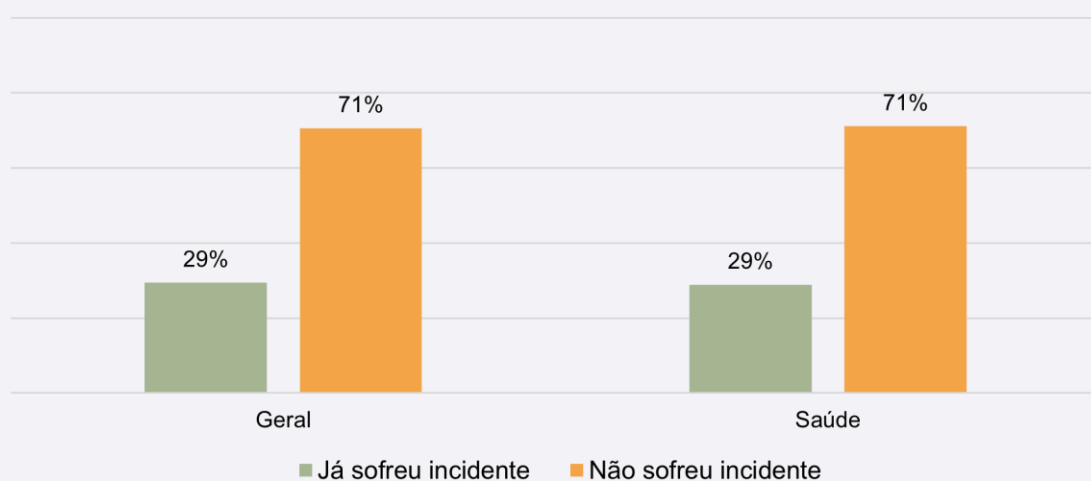


Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



5.1.1. Impacto socioeconómico

O setor da saúde é um dos setores com mais peso na economia do país. A despesa corrente em saúde costuma representar cerca de 10% do Produto Interno Bruto (PIB) nacional, ou seja, mais de 20 mil milhões de euros em cada ano, de um PIB de aproximadamente pelo menos 200 mil milhões de euros desde 2018⁸⁹⁸. Este valor de despesa não se deve apenas ao setor público, mas também à despesa das entidades de saúde privadas. De um modo geral, o setor público costuma representar dois terços desta despesa (cerca de 14-15 mil milhões de euros) e o setor privado o restante terço (cerca de 6-7 mil milhões de euros)⁸⁹⁹. Em termos de Orçamento do Estado, cujo valor total se tem situado acima dos 100 mil milhões de euros (103 mil milhões em 2023 e 123 mil milhões em 2024)⁹⁰⁰, a percentagem alocada à saúde para 2024 é de aproximadamente 12,7% (cerca de 15,5 mil milhões de euros de um orçamento global de 123,6 mil milhões)⁹⁰¹.

Em 2019, a despesa corrente em saúde foi de cerca de 20,4 mil milhões de euros, representando 9,5% do PIB. Em 2020, houve um aumento para 21,1 mil milhões de euros (10,5% do PIB), e em 2021 foi de 23,7 mil milhões de euros (11,2% do PIB), indicando um crescimento de 12,2% face a 2020⁹⁰². Em 2022, a despesa corrente em saúde aumentou 6,3%, atingindo 25,4 mil milhões de euros, representando 10,6% do PIB. O regresso à normalidade nas atividades dos prestadores públicos e privados nas áreas não COVID-19 iniciado em 2021 continuou e, havendo mais entidades a retomar o seu normal funcionamento, houve também um aumento da despesa corrente nesse ano no orçamento. Os efeitos da pandemia persistiram em 2022, mas com impacto inferior na despesa corrente a 2020 e 2021⁹⁰³.

Apesar de a prestação de cuidados de saúde ser em Portugal uma atividade que gera sobretudo despesa, uma vez que o Estado assume o papel de prestador de forma tendencialmente gratuita, o setor da saúde é, noutras vertentes, como a produção de preparações farmacêuticas e o fabrico de material médico-cirúrgico, uma força motriz da economia nacional e um gerador de receita. Agregando estas vertentes, a saúde representa, em Portugal, um volume de negócios anual na ordem dos 34 mil milhões de euros e um valor acrescentado bruto de cerca de 12 mil milhões de euros, envolvendo perto de 105 mil empresas⁹⁰⁴.

Estima-se, também, que o setor da saúde empregue mais de 400 mil pessoas⁹⁰⁵. Cerca de 296 mil pessoas estão ligadas à prestação de cuidados de saúde. Entre médicos, enfermeiros, técnicos auxiliares de saúde e outros, o SNS emprega cerca de 150 mil profissionais⁹⁰⁶, enquanto o setor privado emprega cerca de 146 mil⁹⁰⁷.

⁸⁹⁸ PORDATA, “Produto Interno Bruto (PIB): Quanta riqueza é criada em Portugal”, Estatísticas, <https://www.pordata.pt/pt/estatisticas/economia/crescimento-e-productividade/produto-interno-bruto-pib>.

⁸⁹⁹ INE, “Em 2022, a despesa corrente em saúde aumentou a um ritmo inferior ao do PIB”, Informação à Comunicação Social, 4 de julho de 2023, 3, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=594883237&DESTAQUESmodo=2.

⁹⁰⁰ Ministério das Finanças, “Orçamento do Estado 2024: Relatório - versão consolidada de 16 de outubro de 2023”, 290 e 337, https://www.dgo.gov.pt/politicaorcamental/OrcamentodeEstado/2024/Proposta%20do%20Or%C3%A7amento/Documentos%20do%20OE/OE2024_doc16_Relatorio.pdf

⁹⁰¹ Ministério das Finanças, “Orçamento do Estado 2024: Relatório”, 290.

⁹⁰² INE, “Estatísticas da Saúde - 2022”, edição de 2024, 54, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=660521049&att_display=n&att_download=y.

⁹⁰³ INE, “Em 2022, a despesa corrente em saúde aumentou a um ritmo inferior ao do PIB”, Informação à Comunicação Social, 4 de julho de 2023, 1.

⁹⁰⁴ “Saúde fecha o ano de 2023 a ultrapassar a meta dos 3 mil milhões”, *Health Cluster Portugal*, 27 de fevereiro de 2024, <https://www.healthclusterportugal.pt/pt/noticias/exportacoes-em-saude-2023/>.

⁹⁰⁵ “Saúde fecha o ano de 2023 a ultrapassar a meta dos 3 mil milhões”.

⁹⁰⁶ Ana Ferreira et al., “Os Profissionais do SNS: Retrato e Evolução”, *PLANAPP: Coleção Profissionais da Saúde* - n.º 2, março de 2024, 18, https://www.planapp.gov.pt/wp-content/uploads/2024/03/PlanAPP_ProfissionaisSNS-2.pdf.

⁹⁰⁷ “Empresas privadas do setor da saúde com valor acrescentado acima de 6,7 mil milhões”, CIP, 20 de outubro de 2023, <https://cip.org.pt/empresas-privadas-do-setor-da-saude-com-valor-acrescentado-acima-de-67-mil-milhoes/>.

Como referido, até à criação do SNS, os cuidados de saúde estavam sobretudo a cargo das famílias, das instituições privadas ou da previdência. Ao ser criado um serviço nacional, universal e geral, e tendencialmente gratuito, esse paradigma foi alterado. De um cenário em que o Estado assumia apenas o cuidado dos mais pobres, passou-se para um em que o Estado procura assegurar o acesso a cuidados de saúde por parte de todos os cidadãos. Por isso, o SNS conta hoje com mais 10,5 milhões de utentes inscritos, dos quais 65,9% se encontram inscritos em unidades de saúde familiar⁹⁰⁸.

O número de médicos em Portugal sofreu também um grande aumento. Contrastando com os primeiros anos do SNS, o número de médicos por cada 100.000 habitantes triplicou. Em 1979, havia 186 médicos por cada 100.000 habitantes⁹⁰⁹. Em 2021, segundo dados do Eurostat, esse número atingiu os 562 médicos por cada 100.000 habitantes, sendo este rácio o segundo mais elevado da UE, atrás somente da Grécia (629 médicos por cada 100.000 habitantes)⁹¹⁰.

Há também mais hospitais. Em 1985, havia 94 hospitais públicos em Portugal⁹¹¹. Em 2021 havia 110. Tem também crescido o número de hospitais privados. Em 1999, por exemplo, existiam 97 hospitais privados⁹¹². Já em 2021, o número de hospitais privados supera o número de hospitais públicos, sendo que se contam 128 privados. Acrescem ainda 2 hospitais em regime de parceria público-privada (PPP). Ao todo, existem 240 hospitais em Portugal. Ressalta-se que, apesar de os hospitais públicos serem menos, estes têm maior capacidade de internamento instalada: de um total de 36,2 mil camas, em 2021, 23,9 mil estavam nos hospitais públicos, 11,6 mil nos hospitais privados e 705 nos hospitais em parceria público-privada⁹¹³.

O aumento do acesso aos cuidados de saúde, bem como o aumento do número de profissionais e de hospitais, reduziram grandemente a mortalidade infantil no país. Em 1979, a mortalidade infantil em crianças com menos de um ano era de 26 por mil⁹¹⁴ e, em 2022, de 2,6 por mil - 10 vezes menor⁹¹⁵.

Houve também aumentos consideráveis ao nível da esperança média de vida. Em 1979, a esperança média de vida em Portugal era de 71 anos⁹¹⁶. Em 2023, a esperança média de vida chegou aos 84,75 anos⁹¹⁷.

⁹⁰⁸ Conselho das Finanças Públicas, “Evolução do Desempenho do Serviço Nacional de Saúde em 2022 (Relatório n.º 7/2023)”, junho de 2023, 4, https://www.cfp.pt/uploads/publicacoes_ficheiros/cfp-rel-07-2023.pdf.

⁹⁰⁹ Cátia Mendonça e Rita Costa, “40 anos do SNS. O que mudou?”, *Público*, 14 de setembro de 2019, <https://www.publico.pt/2019/09/14/infografia/40-anos-sns-mudou-340>.

⁹¹⁰ “Physicians and physiotherapists in the EU: how many?”, *Eurostat*, 18 de agosto de 2023, <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230818-1>.

⁹¹¹ Mendonça e Costa, “40 anos do SNS. O que mudou?”, *Público*.

⁹¹² Mendonça e Costa, “40 anos do SNS. O que mudou?”, *Público*.

⁹¹³ INE, “Estatísticas da saúde 2021”, edição de 2023, 4-5, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=11677508&PUBLICACOESmodo=2

⁹¹⁴ Mendonça e Costa, “40 anos do SNS. O que mudou?”, *Público*.

⁹¹⁵ INE, “Estatísticas Demográficas 2022”, 16 de novembro de 2023, 1, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637367953&att_display=n&att_download=y#.

⁹¹⁶ Mendonça e Costa, “40 anos do SNS. O que mudou?”, *Público*.

⁹¹⁷ INE, “Estatísticas Demográficas 2022”, 6 e 7.

5.1.2. Especificidades tecnológicas

O setor da saúde lida, necessariamente, com um grande volume de dados que lhe permite operar, indo do registo de marcação de consultas e cirurgias, ao histórico de saúde dos diversos utentes e à vigilância epidemiológica. Tem, por isso, ao longo dos anos, avançado significativamente na integração da tecnologia na sua infraestrutura, nomeadamente através dos Serviços Partilhados do Ministério da Saúde (SPMS).

As melhorias na segurança da tecnologia utilizada no setor são de extrema importância, uma vez que os dados de saúde são de grande sensibilidade. A partilha de dados pessoais de saúde, mesmo com um empregador, um familiar ou um amigo, pode gerar estigmas, formas de discriminação, ou simplesmente ser motivo de embaraço para a pessoa a quem esses dados pertencem. Num estudo de 2005, uma em cada oito pessoas admitiu adotar comportamentos que poderiam comprometer a sua saúde por terem dúvidas em relação a como os seus dados de saúde poderiam ser utilizados uma vez partilhados, tais como mentir aos seus médicos sobre sintomas e comportamentos, recusar dar informação ou dar informação incorreta a profissionais de saúde, e até mesmo chegar ao ponto de evitar recorrer a quaisquer cuidados de saúde⁹¹⁸. Para melhor dar uma ideia de como a partilha de determinados dados de saúde pode gerar esses estigmas, apresentam-se, de seguida, alguns exemplos reais.

Em 2015, uma clínica de saúde em Londres, no Reino Unido, divulgou acidentalmente os dados de saúde de cerca de 780 pessoas com HIV positivo. Alguns indivíduos afetados pela divulgação destes dados reportaram terem sofrido discriminação nos seus locais de trabalho, terem tido as suas relações de amizade afetadas e terem sido socialmente ostracizados depois de a sua condição ter sido conhecida⁹¹⁹.

Também em 2015, um ataque ao Sistema de Saúde da UCLA (University of California, Los Angeles, EUA), afetou cerca de 4,5 milhões de pacientes. A exposição de dados de saúde, como os relativos à saúde mental de diversos pacientes, terão conduzido a discriminação no local de trabalho, micro-gestão junto dos trabalhadores cujos dados de saúde se tornaram conhecidos e até mesmo ao proferimento destes relativamente a promoções⁹²⁰. Casos como estes evidenciam a sensibilidade dos dados relativos à saúde.

⁹¹⁸ Institute of Medicine Committee on Health Research and the Privacy of Health Information, "The Value and Importance of Health Information Privacy" em *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, ed. Sharyl Nass, Laura Levit e Lawrence Gostin (Washington DC: National Academies Press, 2009), <https://www.ncbi.nlm.nih.gov/books/NBK9579/>.

⁹¹⁹ Cara McGoogan, "London HIV clinic accidentally leaks data of 780 patients", *Wired*, 2 de setembro de 2015, <https://www.wired.com/story/56-dean-street-hiv-leak/>.

⁹²⁰ Chad Turhune, "UCLA Health System data breach affects 4.5 million patients", *Los Angeles Times*, 17 de julho de 2015, <https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html>.

Os dados de saúde são também um alvo preferencial dos agentes de ameaça. E são um alvo preferencial porque podem ser utilizados por esses agentes de ameaça para cometer uma variedade de crimes: dados como o número do Cartão do Cidadão, de Segurança Social, morada fiscal, nome e data de nascimento podem ser utilizados para furtar a identidade de alguém e obter empréstimos ou cartões de alguém em seu nome. Os dados sobre o histórico de saúde de alguém podem também ser usados para cometer fraude de seguros ou obter medicamentos a que não conseguiriam normalmente aceder. Além disso, os dados de saúde podem ser usados indevidamente por longos períodos, ao contrário dos dados de cartões de crédito ou de débito cujo uso indevido pode ser rapidamente detetado e bloqueado⁹²¹.

Apresentam-se, de seguida, alguns dos sistemas utilizados no setor da saúde, bem como algumas das debilidades desses mesmos sistemas, apontadas por diversos profissionais do setor em análise.

SINAVE | Sistema Nacional de Vigilância Epidemiológica

O SINAVE (Sistema Nacional de Vigilância Epidemiológica) é um sistema integrado que tem como principais objetivos a vigilância, deteção precoce e resposta a surtos e epidemias de doenças transmissíveis de saúde pública. Este sistema pretende proteger a população contra riscos sanitários, melhorando assim a capacidade de resposta a emergências de saúde pública⁹²².

As principais características deste sistema são a notificação obrigatória de certas doenças por parte dos profissionais de saúde e dos laboratórios e o facto de utilizar uma plataforma de forma a facilitar a recolha e transmissão de dados em tempo real. Esta plataforma permite a monitorização contínua da incidência e prevalência de doenças transmissíveis fazendo assim análises epidemiológicas para identificar tendências e surtos.

O SINAVE tem vários componentes, tais como:

- **SINAVE Laboratorial:** Focado na notificação laboratorial de doenças transmissíveis;
- **SINAVE Clínico:** Baseado na notificação clínica feita por profissionais de saúde;
- **Plataforma de notificação:** permite a monitorização contínua da incidência e prevalência de doenças transmissíveis fazendo assim análises epidemiológicas para identificar tendências e surtos.

O SINAVE é crucial para a saúde pública em Portugal pois ajuda na deteção precoce de surtos, fornece dados para o planeamento de políticas de saúde e melhora a comunicação entre diferentes níveis do sistema de saúde⁹²³.

⁹²¹ Steve Alder, "Editorial: Why Do Criminals Target Medical Records", *The HIPAA Journal*, 2 de novembro de 2023, <https://www.hipaajournal.com/why-do-criminals-target-medical-records/>

⁹²² SPMS, "SINAVE | Sistema Nacional de Vigilância Epidemiológica", <https://www.spms.min-saude.pt/2020/07/sinave-2/>.

⁹²³ Daniela Oliveira, "Desenvolvimento de um Sistema Eletrónico de Vigilância Epidemiológica (eVDmed): recolha, análise e publicação de informação" (dissertação de mestrado, Universidade do Minho, 2017), 3-4. <https://repositorium.sdum.uminho.pt/bitstream/1822/49627/1/Daniela%20Pimentel%20de%20Oliveira.pdf>

BI CSP – Bilhete de Identidade dos Cuidados de Saúde Primários

O BI CSP é uma iniciativa do SNS e tem como objetivo melhorar a gestão, qualidade, eficiência e a transparência dos serviços de cuidados de saúde primários (CSP) e dados hospitalares. Este sistema permite ainda a monitorização e avaliação contínua das unidades de saúde, facilitando assim a tomada de decisões baseadas em dados concretos.

O sistema tem uma funcionalidade que permite avaliar o desempenho das unidades de saúde primários com base em diversos indicadores, ajudando assim a identificar áreas que precisam de melhorias e/ou implementar ações corretivas de forma eficiente. Com o BI CSP é ainda possível obter dados relevantes que podem ser úteis para profissionais de saúde, tais como: estatísticas sobre consultas, tempos de espera, cobertura vacinal e outros indicadores de desempenho⁹²⁴.

Existem três componentes agregados ao BI CSP: portal com acesso público e acesso autenticado, ferramenta para a exploração da informação, ferramenta para a criação e monitorização dos planos de ação em contexto dos CSP⁹²⁵.

PEM | Prescrição Eletrónica Médica

A PEM, Prescrição Eletrónica Médica tem como objetivo modernizar e agilizar todo o processo de prescrição de medicamentos, eliminando a necessidade de prescrições em papel, melhorando assim a eficiência do processo de prescrição e dispensa de medicamentos. Teve origem na Lei nº11/2012, de 8 de março, e na portaria n.º 137-A/2012, de 11 de maio e já funciona por DCI (Denominação Comum Internacional)⁹²⁶.

Esta ferramenta permite que os médicos façam prescrições eletronicamente e que sejam enviadas para uma base de dados centralizada. Os utentes podem aceder às prescrições através do portal do utente (versão *web* ou aplicação móvel), esta aplicação é responsável por mais de 90% do total de prescrições registadas diariamente e apresenta a possibilidade de prescrição diferenciada de medicamentos, cuidados respiratórios domiciliários e dispositivos médicos⁹²⁷. As farmácias também têm acesso às prescrições, permitindo assim a dispensa dos medicamentos de forma rápida, reduzindo o risco de erros de transcrição⁹²⁸.

A PEM também traz uma melhoria na segurança do processo de prescrição e reduz o risco de fraudes e falsificações, sendo que a plataforma está em conformidade com as normas e regulamentos de proteção de dados, garantindo assim a privacidade das informações de saúde dos utentes.

⁹²⁴ Mafalda Simão, "A Prestação de Cuidados de Saúde em Função do Território", publicado no Repositório Científico da Universidade de Coimbra, 2022, 7-9, <https://estudogeral.uc.pt/handle/10316/102463>.

⁹²⁵ SPMS, "BI CSP – Bilhete de Identidade dos Cuidados de Saúde Primários", <https://www.spms.min-saude.pt/2020/07/bi-csp-bilhete-de-identidade-dos-cuidados-de-saude-primarios/>.

⁹²⁶ SPMS, "PEM | Prescrição Eletrónica Médica", julho de 2020, <https://www.spms.min-saude.pt/2020/07/pem/>.

⁹²⁷ SPMS, "PEM | Prescrição Eletrónica Médica", julho de 2020.

⁹²⁸ SPMS, "Prescrição Eletrónica Médica: Especificação dos Serviços para integração com o Sistema Central de Prescrições", janeiro de 2018, [SPMS \(min-saude.pt\)](https://www.spms.min-saude.pt/).

Exames Sem Papel

Exames Sem Papel é uma iniciativa do Ministério da Saúde e tem como objetivo modernizar e agilizar o processo de gestão de exames médicos, desde a requisição até à consulta dos resultados, promovendo a digitalização utilizando múltiplas plataformas de serviços centrais. As principais finalidades desta iniciativa são: reduzir o tempo necessário para a realização dos exames e obtenção dos resultados, minimizar os erros associados à transcrição manual de dados, facilitar o acesso tanto a utentes como a médicos e a redução de desperdício⁹²⁹.

As requisições de exames são feitas eletronicamente pelos médicos e enviadas diretamente para os laboratórios e centros de diagnóstico através de uma API, sendo que a faturação dos prestadores para o SNS também é efetuada por via eletrónica. É importante referir que esta iniciativa também garante a segurança e privacidade dos dados de saúde dos utentes, pois a iniciativa está em conformidade com as normas de proteção de dados e as informações são armazenadas e transmitidas de forma segura⁹³⁰.

SClínico | Cuidados de Saúde Hospitalar

O SClínico Hospitalar é um sistema de informação evolutivo, este foi desenvolvido pela SPMS e está presente em 50 entidades do setor da saúde. Este sistema tem como principais objetivos melhorar a eficiência, a qualidade e a segurança dos cuidados de saúde prestados nos hospitais. Esta ferramenta permite a criação e gestão de registos clínicos eletrónicos, substituindo os registos em papel. Isto torna o acesso mais rápido e seguro às informações clínicas dos utentes, melhorando assim o funcionamento dos cuidados de saúde⁹³¹.

Nesta plataforma é possível gerir todos os processos clínicos, admitir pacientes, gerir consultas, prescrever medicamentos, requerer exames e elaborar relatórios clínicos, sendo este sistema interoperável com outros sistemas de saúde, permitindo assim a troca de informações entre diferentes unidades de saúde. Por fim, o SClínico conta com ferramentas de apoio à decisão clínica, fornecendo alertas e recomendações de forma a auxiliar os profissionais de saúde⁹³².

SClínico | Cuidados de Saúde Primários (CSP)

O SClínico Cuidados de Saúde Primários (CSP), tal como o SClínico Cuidados de Saúde Hospitalar, é um sistema de informação evolutivo onde a sua origem remonta duas aplicações: o SAM (Sistema de Apoio ao Médico) e o SAPE (Sistema de Apoio à Prática de Enfermagem). Este sistema tem crescido para ser uma aplicação única, comum a todos os prestadores de cuidados de saúde e centrada no doente. Os objetivos estabelecidos para este sistema são os mesmos do SClínico | Cuidados de Saúde Hospitalar, mas no âmbito dos cuidados de saúde primários⁹³³.

⁹²⁹ SPMS, "Exames Sem Papel", julho de 2020, <https://www.spms.min-saude.pt/2020/07/exames-sem-papel/>.

⁹³⁰ SPMS, "Exames Sem Papel".

⁹³¹ SPMS, "SClínico | Cuidados de Saúde Hospitalares (CSH)", julho de 2020, <https://www.spms.min-saude.pt/2020/07/sclinico-hospitalar/>.

⁹³² SPMS, "SClínico | Cuidados de Saúde Hospitalares (CSH)".

⁹³³ SPMS, "SClínico | Cuidados de Saúde Primários (CSP)", julho de 2020, <https://www.spms.min-saude.pt/2020/07/sclinico-cuidados-de-saude-primarios-csp/>.

Receita Sem Papel

A Receita Sem Papel tornou-se obrigatória para todas as entidades do SNS a 1 de abril de 2016, através do Despacho de 25 de fevereiro de 2016. O principal objetivo desta iniciativa é substituir as prescrições de medicamentos em papel por prescrições eletrónicas, de forma a simplificar o processo tanto para os profissionais de saúde como para os utentes⁹³⁴. Este novo modelo poderá incluir diferentes tipos de medicamentos, como medicamentos comparticipados e não comparticipados na mesma receita.

No ato da dispensa nas farmácias, o utente poderá optar por despachar todos os produtos prescritos, ou apenas parte deles, sendo possível levantar os restantes em diferentes estabelecimentos e em datas distintas⁹³⁵.

RNU | Registo Nacional de Utente

O Registo Nacional de Utente (RNU) figura-se como um dos pilares mais importantes do sistema de informação de saúde e visa proporcionar uma identificação única e centralizada de todos os utentes do SNS, melhorando assim a gestão dos serviços de saúde. Este sistema também facilita o acesso e a partilha de informações entre diferentes entidades do setor da saúde⁹³⁶.

O RNU tem por base três componentes: uma aplicação *Web*, onde é possível a gestão dos dados de identificação dos utentes, uma plataforma na qual são disponibilizados serviços que permitem a consulta de dados e uma base de dados nacional. Esta última é alimentada diretamente pelos administrativos dos CSP, pelos hospitais do SNS, pelos processos do Cartão de Cidadão e pela integração de dados com as Regiões Autónomas. A estrutura do utente tem três campos: "Identificação", onde consta toda a informação relativa à identificação do utente, "Entidades Responsáveis", referente à informação das entidades financeiras responsáveis pelo utente e "Benefícios", que contém a informação sobre os benefícios de saúde aplicáveis ao utente⁹³⁷.

O RNU também tem um *WebService* onde é possível efetuar uma chamada passando o número de SNS do utente ou a EFR (Entidade Financeira Responsável), de seguida, o *WebService* irá devolver o campo do Utente (caso os dados enviados sejam corretos) e uma mensagem com um código e uma descrição do mesmo. Este código funciona como uma garantia de correspondência entre a informação de referência no RNU e nos sistemas locais⁹³⁸.

Dispositivos médicos

Segundo o decreto-lei n.º 145/2009, de 17 de junho, um dispositivo médico é “qualquer instrumento, aparelho, equipamento, *software*, material ou artigo utilizado isoladamente ou em combinação, incluindo o *software* destinado pelo seu fabricante a ser utilizado especificamente para fins de diagnóstico ou terapêuticos e que seja necessário para o bom funcionamento do dispositivo médico, cujo principal efeito pretendido no corpo humano não seja alcançado por meios farmacológicos, imunológicos ou metabólicos, embora a sua função possa ser apoiada por esses meios, destinado

⁹³⁴ SPMS, “FAQs PEM - Receita sem papel”, novembro de 2015, <https://spms.min-saude.pt/wp-content/uploads/2015/11/FAQs1.pdf>.

⁹³⁵ SPMS, “Receita Sem Papel”, abril de 2019, <https://www.spms.min-saude.pt/2019/04/receita-sem-papel-2/>.

⁹³⁶ SPMS, “RNU: Registo Nacional de Utentes”, outubro de 2015, <https://www.spms.min-saude.pt/2015/10/rnu/>.

⁹³⁷ DSI, “RNU - Registo Nacional de Utentes: Especificação Técnica”, SPMS, 12 de novembro de 2015, [SC InfoSite 2015 \(min-saude.pt\)](https://www.min-saude.pt).

⁹³⁸ DSI, “RNU - Registo Nacional de Utentes: Especificação Técnica”, SPMS.

pelo fabricante a ser utilizado em seres humanos” para o diagnóstico, controlo e tratamento de doenças, compensações de lesões, substituição ou alteração da anatomia ou de processos fisiológicos e controlo da conceção⁹³⁹.

No caso dos dispositivos médicos que possuem componentes eletrónicos, *software*, e capacidade de ligação à Internet, tem-se-lhes chamado dispositivos da *Internet of Medical Things* - IoMT. Incluem-se, nesta categoria, tanto dispositivos mais pequenos e simples, que podem ser implantados no corpo humano, como *pacemakers*, bombas de insulina e estimuladores de bexiga, como dispositivos maiores de uso hospitalar, como ventiladores, monitores de sinais vitais, máquinas de suporte vida ou até mesmo sistemas de cirurgia robótica potenciados pelas velocidades 5G. A crescente utilização e interconectividade destes dispositivos tem aumentado a superfície de ataque para cibercriminosos, algo que será explorado em maior profundidade em **5.2. Ameaças**.

No final de 2020, o INFARMED, I.P. lançou o novo Sistema de Informação para Dispositivos Médicos (SIDM). Este sistema, que já existia desde 2015, foi revisto de forma a otimizar toda a gestão da informação relacionada com dispositivos médicos, simplificando assim o seu registo. O SIDM, para além da componente de registo, possui uma componente de pesquisa pública dos dispositivos médicos (infoDM)⁹⁴⁰ e uma área que permite a criação de notificações por parte de utilizadores com problemas em produtos de saúde. O principal objetivo do SIDM é gerir de forma eficiente os dispositivos médicos utilizados nos hospitais e outras unidades de saúde, ajudando assim a monitorizar o inventário, a manutenção, o uso e a rastreabilidade dos mesmos⁹⁴¹.

O SIDM permite o registo detalhado de todos os dispositivos médicos, como o tipo de dispositivo, número de série, fabricante, data de aquisição, localização atual, entre outros. A plataforma também monitoriza os cronogramas de manutenção e calibração dos dispositivos médicos, assim como mantém todo o histórico de uso do dispositivo, incluindo quem o utilizou e em que contexto⁹⁴².

⁹³⁹ Decreto-Lei n.º 145/2009, de 17 de junho, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/145-2009-494558>.

⁹⁴⁰ INFARMED, “Pesquisa de Dispositivos Médicos”, <https://www.infarmed.pt/web/infarmed/pesquisa-dispositivos#>.

⁹⁴¹ INFARMED, “Sistema de Informação para Dispositivos Médicos (SIDM)”, https://www.infarmed.pt/web/infarmed/infarmed?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content%2F101_assetEntryId=4088116&_101_type=content&_101_urlTitle=sistema-de-informacao-para-dispositivos-medicos-sidm-&inheritRedirect=false.

⁹⁴² INFARMED, “Dispositivos Médicos”, Perguntas Frequentes, <https://www.infarmed.pt/web/infarmed/perguntas-frequentes-area-transversal/novo-sistema-de-informacao-para-dispositivos-medicos-sidm>.

Sistemas *legacy*

Tal como muitos outros setores, também o setor da saúde utiliza sistemas *legacy*. Estes sistemas consistem em *hardware* ou *software* antigo que ainda cumprem as funções para as quais foram adquiridos, mas que são difíceis de tornar seguros por já não receberem atualizações, por não poderem ser integrados com outras tecnologias ou sistemas mais recentes, ou até por não possuírem capacidades criptográficas, deixando-os vulneráveis⁹⁴³. De acordo com o livro *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices*, de Robert Seacord, Daniel Plakosh e Grace Lewis, um sistema torna-se *legacy* quando começa a resistir à modificação e evolução. A mesma obra indica também que se um sistema ainda dá algum valor relevante ao negócio, este deverá ser modernizado ou substituído⁹⁴⁴. A modernização destes sistemas pode ser, no entanto, difícil e, por isso, devem ser tidos em conta diversos fatores para o conseguir fazer, tais como: complexidade, tecnologia e processos de engenharia, risco, componentes comerciais e objetivos de negócio⁹⁴⁵.

A utilização deste tipo de sistemas (*legacy*) é comum entre os setores que adquirem equipamentos com ciclos de vida relativamente longos, que podem durar, por exemplo, seis, 10, 20 ou ainda mais anos. Sublinha-se ainda que esta classificação de sistemas não se atribui apenas a grandes máquinas, como as utilizadas para realizar Tomografias Axiais Computadorizadas (TACs), mas também a dispositivos mais pequenos como os já referidos, como bombas de insulina e *pacemakers*.

Acresce ainda que a falta de modernização de alguns sistemas utilizados na saúde tem sido motivo de descontentamento entre os profissionais do setor. Segundo um estudo realizado pela Associação Nacional de Unidades de Saúde Familiar, onde foram inquiridos os coordenadores das 615 unidades, tendo sido reunidas 484 respostas, é notória a insatisfação dos profissionais de saúde com a qualidade dos sistemas utilizados na saúde em Portugal. Todas as unidades indicaram ter tido pelo menos uma falha informática nos 12 meses anteriores ao estudo e cerca de 96,5% dos inquiridos afirma que a falta de acesso às aplicações informáticas perturbou a qualidade dos cuidados prestados⁹⁴⁶.

⁹⁴³ Melissa Chase et al., "Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks", MITRE, 15 de novembro de 2023, <https://www.mitre.org/news-insights/publication/next-steps-toward-managing-legacy-medical-device-cybersecurity-risks>.

⁹⁴⁴ Robert Seacord, Daniel Plakosh e Grace Lewis, *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices* (Boston: Addison-Wesley, 2003), xiii.

⁹⁴⁵ Seacord, Plakosh e Lewis, *Modernizing Legacy Systems*, 1.

⁹⁴⁶ André Biscaia et al., "Síntese dos resultados do estudo 'O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023: Questionário aos coordenadores de USF'", Associação Nacional das Unidades de Saúde Familiar, <https://usf-an.pt/sintese-dos-resultados-do-estudo-o-momento-atual-da-reforma-dos-cuidados-de-saude-primarios-em-portugal-2022-2023-questionario-aos-coordenadores-de-usf/>.

Um dos pontos mais críticos é a falta de interoperabilidade entre os sistemas informáticos levando, por vezes, à introdução da mesma informação várias vezes. Em entrevista ao jornal Expresso, foi indicado por médicos membros da direção da Associação Nacional das Unidades de Saúde Familiar (USF-AN), da Faculdade de Medicina da Universidade do Porto (FMUP) e membros do grupo de trabalho para a gestão da informação em Saúde da Associação Portuguesa de Administradores Hospitalares (APAH) que um dos maiores problemas dos sistemas informáticos é que são desenvolvidos por pessoas sem conhecimento da prática clínica. É expectável que com o investimento que será realizado entre 2021 e 2026, de 300 milhões de euros no âmbito do Plano de Recuperação e Resiliência (PRR), onde este montante tem como objetivo ajudar à transição digital na área da Saúde, a maioria destes problemas sejam resolvidos⁹⁴⁷.

Estas falhas referidas acima ajudam a aumentar as ameaças no setor da Saúde. As ciberameaças inerentes aos dispositivos médicos e aos sistemas *legacy* utilizados na saúde serão exploradas em maior detalhe na subsecção seguinte.

⁹⁴⁷ Biscaia et al., “O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023”.

5.2. Ameaças

O setor da saúde é um dos setores mais apetecíveis para ciberataques por diversos motivos. Este setor contém uma grande riqueza de dados pessoais, desde números de identificação pessoal - como os números de identificação civil, fiscal, da segurança social e de utente, que podem ser utilizados para furto de identidade ou cometer fraudes de seguro -, aos problemas de saúde dos utentes, que podem ser utilizados contra os mesmos⁹⁴⁸. Existe, no setor da saúde, uma maior probabilidade de pagar um resgate quando afetado por *ransomware*⁹⁴⁹, uma vez que parar as atividades na saúde pode significar a perda de vidas humanas e, por isso, a prioridade do setor passa por retomar o seu normal funcionamento o mais rápido possível⁹⁵⁰.

Será por estes motivos que, no relatório *ENISA Threat Landscape: Health Sector*, publicado em julho de 2023, as duas ameaças mais prevalentes no setor da saúde a nível europeu são o *ransomware* (54% dos incidentes do setor entre 2021 e 2023) e as ameaças relativas a dados (46% dos incidentes também entre 2021 e 2023). Verifica-se uma grande discrepância entre a prevalência destas duas ameaças e quaisquer outras que possam afetar o setor da saúde. Tal demonstra-se pelo facto de a terceira ameaça que mais afetou este setor - a intrusão - ter sido 13% dos ataques, o que significa uma diferença de 33 pontos percentuais entre a segunda e a terceira ameaça mais prevalentes⁹⁵¹.

Os motivos por trás dos ataques de *ransomware* e de ameaças relativas a dados são normalmente os de ganho financeiro. Embora possa haver outros, tais como motivos ideológicos ou de espionagem, o mesmo relatório indica que na vasta maioria dos casos - 83% - os ciberataques realizados ao setor da saúde são motivados por ganho financeiro⁹⁵².

A realidade portuguesa não difere da apresentada pela ENISA no relatório referido. No Relatório Riscos e Conflitos de 2023, do Observatório de Cibersegurança do CNCS, evidenciou-se que o setor da saúde é um dos mais atacados em Portugal, e um dos que mais acaba por ter de notificar a CNPD por acessos indevidos a dados pessoais - cerca de 11% no setor privado e 13% no setor público das notificações recebidas pela CNPD vêm deste setor⁹⁵³. A par destes dados, é de notar que alguns dos ataques mais graves ocorridos no setor em Portugal foram ataques relativos a dados e de *ransomware*.

Um dos mais graves ciberataques no setor da saúde relativos a dados ocorreu em julho de 2020, em que milhares de credenciais de profissionais do SNS foram furtadas e divulgadas na Internet. No entanto, a lista de credenciais foi eliminada da hiperligação que permitia aceder à mesma algumas horas depois da sua divulgação⁹⁵⁴.

Um outro ataque, de *ransomware*, ocorreu em agosto de 2023, tendo bloqueado o sistema informático do Serviço Regional de Saúde da Madeira, que forçou o regresso ao papel e ao modo analógico de forma a não fechar os hospitais e os centros de saúde. Foi assegurado que os dados

⁹⁴⁸ Richard Pallardy, "The Unique Cyber Vulnerabilities of Medical Devices", *Information Week*, 14 de novembro de 2023, <https://www.informationweek.com/cyber-resilience/the-unique-cyber-vulnerabilities-of-medical-devices#close-modal>

⁹⁴⁹ Forma de ataque que afeta a disponibilidade da informação, bloqueando o acesso de utilizadores legítimos aos ativos de informação, exigindo um resgate - "*ransom*" - para devolver o acesso aos mesmos.

⁹⁵⁰ ENISA, "ENISA Threat Landscape: Health Sector", 13, <https://www.enisa.europa.eu/publications/health-threat-landscape>.

⁹⁵¹ ENISA, "ENISA Threat Landscape: Health Sector", 11.

⁹⁵² ENISA, "ENISA Threat Landscape: Health Sector", 19.

⁹⁵³ CNCS, "Relatório Riscos e Conflitos" (2023), 17, <https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obciber-cnccs.pdf>.

⁹⁵⁴ Hugo Séneca, "Hackers publicam passwords de milhares de médicos e enfermeiros do SNS na internet", *Expresso*, 20 de julho de 2020, <https://expresso.pt/sociedade/2020-07-20-Hackers-publicam-passwords-de-milhares-de-medicos-e-enfermeiros-do-SNS-na-internet>.

clínicos fossem preservados, mas é possível que dados pessoais como números de telefone e números de utente tenham sido expostos⁹⁵⁵.

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos⁹⁵⁶, de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal⁹⁵⁷.
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa⁹⁵⁸.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável⁹⁵⁹.
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso⁹⁶⁰. No caso, consideraram-se os colaboradores internos maliciosos.

⁹⁵⁵ Marta Caires, “Serviço de Saúde da Madeira: ataque informático deixa utentes sem consultas e sem exames”, *Expresso*, 7 de agosto de 2023, <https://expresso.pt/sociedade/2023-08-07-Servico-de-Saude-da-Madeira-ataque-informatico-deixa-utentes-sem-consultas-e-sem-exames-e0cee143>

⁹⁵⁶ CNCS, “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.

⁹⁵⁷ CNCS, “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”, maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf>.

⁹⁵⁸ CNCS, “Relatório Riscos & Conflitos 2021”, 75.

⁹⁵⁹ CNCS, “Relatório Riscos & Conflitos 2021”, 75-76.

⁹⁶⁰ CNCS, “Relatório Riscos & Conflitos 2021”, 76-77.

Tabela 46 - Agentes de ameaça mais prováveis (Saúde)

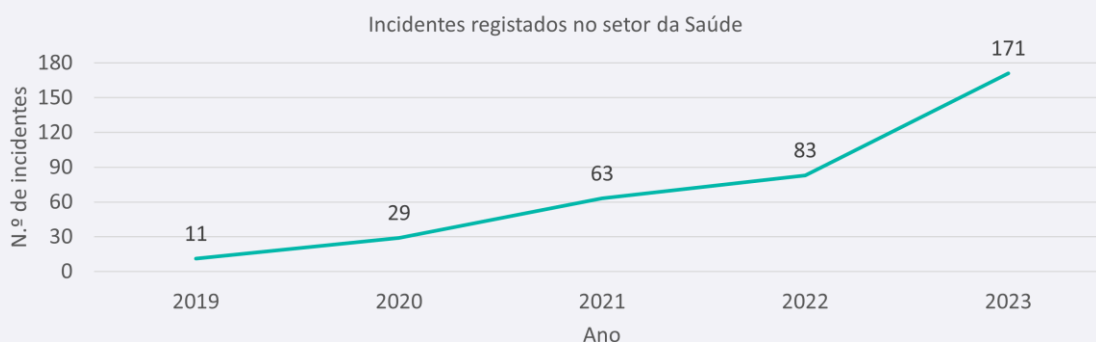
Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Ransomware	■	■	■	■
Malware	■	■	■	■
Vulnerabilidades	■	■	■	■
Phishing e Smishing	■	■	■	
Acesso indevido a dados pessoais	■	■	■	■
Manipulação de Sistemas (TO)	■	■		■
Manipulação de Sistemas (TI)	■	■		■

Legenda:

■ - Agente de ameaça provável

Segundo dados do CERT.PT, registaram-se, entre 2019 e 2023, 357 incidentes no setor da saúde⁹⁶¹. Deve-se, no entanto, sublinhar que entre 2019 e 2022, se tinham registado apenas 186 incidentes, ou seja, 171 incidentes foram registados só no ano de 2023. Tal significa que entre 2022, ano em que só se tinham registado 83 incidentes, e em 2023, houve um aumento na incidência de incidentes de 106%⁹⁶².

Figura 7 - Número de incidentes no setor da Saúde anualmente



(Fonte: CNCS, “Incidentes e Setores: 2019-2023”, Conhecimento Situacional: Estatísticas, última atualização em 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

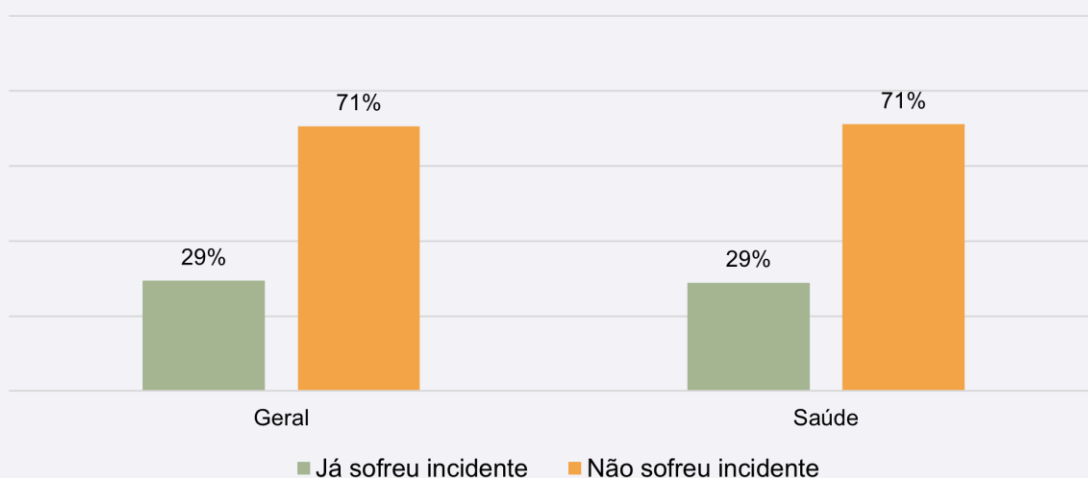
⁹⁶¹ CNCS, “Incidentes e Setores: 2019-2023”, Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>.

⁹⁶² CNCS, “Relatório Cibersegurança em Portugal: Riscos e Conflitos”, 5.ª edição, 2024, 25, <https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obciberncncs.pdf>.

Os resultados do questionário realizado aos OSE corroboram estas conclusões, uma vez que colocam o setor da saúde entre um dos mais afetados por ciberataques, juntamente com os operadores da banca e dos transportes (**Gráfico 68**), sendo as principais consequências a indisponibilidade dos serviços/sistemas devido a infeção por *malware* (possivelmente, *ransomware*) e a destruição de dados pelo *malware* instalado ou intruso. Os valores deste setor andam a par com os valores gerais de todos os setores.

A estas questões, acresce o facto de pelo menos 448 Unidades de Saúde Familiar terem registado pelo menos uma falha no sistema informático no ano de 2022. Mais de 20% reportaram ter tido problemas mais de 50 vezes. O próprio sistema informático da área da Saúde torna-se uma ameaça por si só, pois um sistema que falha mais de 50 vezes por ano não é fidedigno⁹⁶³.

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



Retomando o tema dos dispositivos médicos (IoMT e *legacy*) inicialmente abordado em **5.1.3. Especificidades tecnológicas**, importa sublinhar que segundo um relatório de dezembro de 2023 do Government Accountability Office do governo dos Estados Unidos da América (EUA), estes dispositivos têm, em média, 6 vulnerabilidades passíveis de serem exploradas por cibercriminosos⁹⁶⁴. Além disso, cerca de 40% dos dispositivos estarão no fim do seu ciclo de vida, sem *patches* ou atualizações disponíveis⁹⁶⁵. No pior cenário, ciberataques a dispositivos médicos podem afetar o bem-estar do paciente ou até mesmo causar perda de vida.

Nos casos dos dispositivos que são implantados no corpo humano, como *pacemakers*, bombas de insulina e estimuladores de bexiga, entre outros, essas vulnerabilidades devem-se, em parte, às próprias características desses dispositivos: o facto de terem de ser pequenos e leves para não impedirem outras funções fisiológicas e para que as baterias sejam duradouras, o espaço para *hardware* é muito limitado. Nalguns casos, não é necessário mais do que um sinal de rádio na frequência certa para interferir com estes dispositivos. Noutros casos como, por exemplo, com dispositivos que possam ser controlados através de um *smartphone* ou que transmitam dados para bases de dados, estes podem servir como ponto de entrada noutros sistemas para obter outras informações⁹⁶⁶.

⁹⁶³ Biscaia et al., "O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023".

⁹⁶⁴ United States Government Accountability Office, "Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination", Report to Congressional Committees, dezembro de 2023, 6, <https://www.gao.gov/assets/d24106683.pdf>.

⁹⁶⁵ "Hospitals' IoMT Device Security Risk Quantified in New Report", MedTech Dive, 23 de agosto de 2023, <https://www.medtechdive.com/press-release/20230823-hospitals-iomt-device-security-risk-quantified-in-new-report/>.

⁹⁶⁶ Pallardy, "Cyber Vulnerabilities of Medical Devices", *Information Week*.

Os dispositivos médicos, grandes e pequenos, são difíceis de substituir, no primeiro caso, porque a substituição de grandes máquinas é dispendiosa e pode obrigar a interromper o atendimento e a realização de exames urgentes aos utentes e, no segundo caso, porque substituir dispositivos implantáveis para os atualizar obrigaria a operar os pacientes que utilizam esses dispositivos e, em diversos casos, as operações acarretariam riscos que os pacientes não estão dispostos a aceitar, acabando assim por assumir um outro tipo de risco relativo à desatualização dos dispositivos implantados⁹⁶⁷.

Embora seja mais provável que as escolhas dos alvos dos agentes de ameaça recaiam sobre as bases de dados de instituições maiores em vez de sobre indivíduos, os ataques a pessoas singulares que utilizam os dispositivos referidos não deixam de ser uma possibilidade e uma ameaça preocupante.

⁹⁶⁷ Pallardy, "Cyber Vulnerabilities of Medical Devices", *Information Week*.

5.3. Capacitação

Em 2017, uma série de ciberataques, principalmente de *ransomware* (*WannaCry* e *Petya*), assolou vários países europeus, em particular a Ucrânia. O Banco Central Ucrainiano, o sistema de comboios metropolitanos e a empresa estatal de energia da Ucrânia foram os principais afetados⁹⁶⁸. Em Portugal, face a esta série de ataques, a SPMS desligou preventivamente o sistema de *e-mail* do SNS, tendo na altura evitado que o SNS português se juntasse ao grupo de entidades afetadas pelos ataques de *ransomware*⁹⁶⁹. Na sequência destes eventos, o ano de 2017 foi particularmente rico em iniciativas que visavam o reforço da cibersegurança no SNS.

Entre as iniciativas mais recentes, contam-se:

- Estruturar o circuito para o registo de incidentes de segurança;
- Elaborar iniciativas de auditoria à utilização da Política de Segurança com base na ISO 27799;
- Promover e sensibilizar a importância da segurança de informação nos Sistemas de Informação da Saúde;
- Adotar as boas práticas em alinhamento com a *Framework ITIL V3 - Foundation*;
- Promover nas entidades do SNS um processo de melhoria contínua do nível da Cibersegurança⁹⁷⁰.

A SPMS, responsável pela formação em matéria de cibersegurança no setor da saúde, tem criado campanhas de sensibilização para o tema, na qual se insere a criação de dicas mensais, manuais de cibersegurança, infografias⁹⁷¹ e de oportunidades de formação⁹⁷². A mesma disponibiliza ainda uma ligação para uma página denominada “Alertas e Segurança”, onde é possível consultar informação referente a boas práticas⁹⁷³.

⁹⁶⁸ Christian Borys, “The day a mysterious cyber-attack crippled Ukraine”, *BBC*, 4 de julho de 2017, <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine>.

⁹⁶⁹ SPMS, “Circular Normativa n.º 03/2017: medidas excecionais de segurança”, 19 de maio de 2017, 1, <https://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA3-Medidas-Excecionais-de-Ciberseguran%C3%A7a.pdf>.

⁹⁷⁰ Agência para a Modernização Administrativa (AMA), “Cibersegurança na Administração Pública: O Imperativo da Conformidade Global no SNS”, *Encontros SAMA 2020* (Lisboa), 26 de abril de 2020, <https://bo.tic.gov.pt/api/assets/etic/2e7a0cf7-68f5-4008-a95f-29594569d584/>.

⁹⁷¹ SPMS, “Cibersegurança”, abril de 2019, <https://www.spms.min-saude.pt/2019/04/ciberseguranca-2/>.

⁹⁷² SPMS, “Conteúdos de Sensibilização de Cibersegurança”, Academia SPMS, <https://academia.spms.min-saude.pt/atis-de-sensibilizacao-de-ciberseguranca/>.

⁹⁷³ SPMS, “Alertas e Segurança”, <https://www.spms.min-saude.pt/alertaseseguranca/>.

Adicionalmente, a 29 de janeiro de 2020, Portugal foi eleito como *Chair* do *Work Stream* criado para o setor da saúde, no âmbito do *NIS Cooperation Group*. Neste contexto o CNCS ficou responsável pela coordenação dos trabalhos, com o apoio da SPMS. Este evento decorreu em Bruxelas, na 14ª reunião do *NIS Cooperation Group*, que foi criado pela Diretiva NIS no ano de 2016, cujo objetivo passava por garantir a cooperação estratégica e a partilha de informações entre os Estados Membros da UE acerca das temáticas de segurança da informação e cibersegurança. A criação do grupo *Work Stream for Health* setor, surgiu na sequência de uma proposta do *European Cybersecurity Health Group* (ECHG), do qual faz parte a SPMS, e decorreu da necessidade de harmonização das práticas e requisitos mínimos de proteção da informação da saúde, cada vez mais fundamental num contexto de saúde heterogéneo e interconectado. No decorrer da reunião, vários foram os países que encorajaram este trabalho, e prontificaram-se a participar ativamente nestas discussões, considerando que a cibersegurança em saúde não pode ser descurada, uma vez que, em última instância, estará em causa o risco de vida dos utentes⁹⁷⁴.

Um outro momento marcante no setor foi o da pandemia de COVID-19, não só pelo enorme esforço exigido aos profissionais de saúde no combate à doença e à prestação de cuidados, mas também pelo grande aumento de ciberataques que houve nessa altura. Segundo um relatório da Check Point, a nível mundial, entre fevereiro de 2020 e abril de 2020, o número de ciberataques registados relacionados com a pandemia aumentou 40 vezes, de 5000 ataques por semana para 200 mil⁹⁷⁵. O confinamento e a rápida passagem ao teletrabalho de milhões de trabalhadores em todo o mundo sem que houvesse tempo para implementar medidas de segurança adequada nos seus dispositivos de trabalho foi uma oportunidade prontamente explorada pelos agentes de ameaças⁹⁷⁶. Este aumento exponencial dos ciberataques colocou a cibersegurança no centro das preocupações de pessoas individuais, empresas e governos. No entanto, o setor da saúde parece estar aquém do desejável em termos de capacitação em cibersegurança.

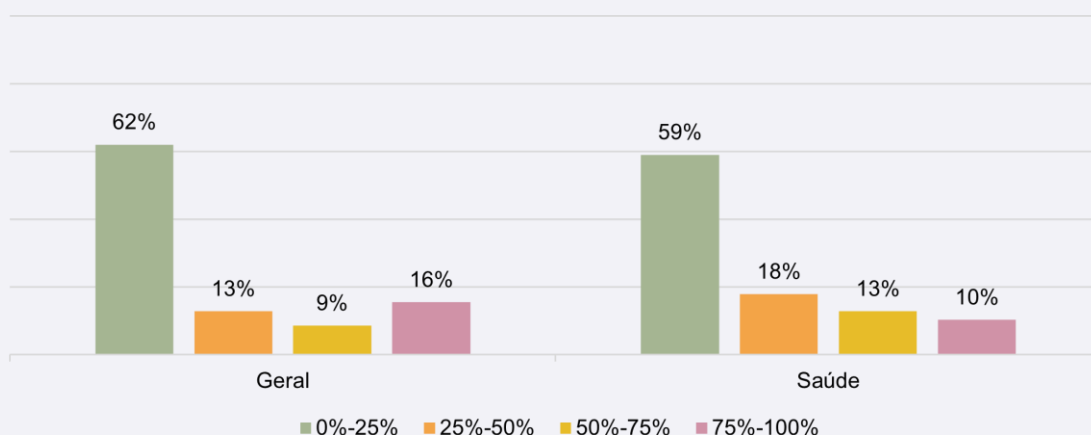
⁹⁷⁴ SNS, "Portugal lidera Grupo Europeu criado para o setor da saúde", 30 de janeiro de 2020, <https://www.sns.gov.pt/noticias/2020/01/31/saude-ciberseguranca/>.

⁹⁷⁵ "Cyber Attack Trends: 2020 Mid-Year Report", *Checkpoint*, 22 de julho de 2020, 4, <https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/>.

⁹⁷⁶ "Observatório de cibersegurança: nº 4/2021", CNCS, setembro de 2021, 1 <https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf>.

Embora seja possível verificar que o reforço da cibersegurança é uma preocupação e um objetivo estratégico do setor há vários anos, tanto através dos planos de atividades e orçamentos, como através das campanhas de sensibilização para o tema, as múltiplas notícias que reportam más práticas de cibersegurança no setor, bem como o questionário realizado no âmbito deste relatório revelam que o impacto destas medidas tem ficado aquém do desejado. De acordo com o questionário realizado, em quase 60% dos operadores do setor, apenas 0%-25% dos profissionais de saúde têm formação básica em cibersegurança. Já no âmbito geral, cerca de 62% dos operadores têm 0%-25% dos profissionais com formação básica em cibersegurança, o que demonstra que este setor, comparado com os outros setores, tem mais profissionais com formação em cibersegurança (**Gráfico 33**).

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Este é, no entanto, um cenário que pode vir a mudar. É importante relembrar que no seguimento dos impactos negativos causados pela pandemia surgiram também planos para os mitigar. Um dos mais importantes desses planos será o Plano de Recuperação e Resiliência (PRR), que gerou uma oportunidade sem precedentes para o investimento em cibersegurança, que será explorada em

5.4. Investimento em cibersegurança.

5.4. Investimento em cibersegurança

Tal como referido em

5.3. Capacitação, o PRR veio gerar uma oportunidade sem precedentes para o investimento em cibersegurança no setor da saúde. Ao todo, serão investidos, até ao final de 2024, cerca 300 milhões de euros para a transição digital da saúde, que se repartem por quatro pilares de investimento⁹⁷⁷. Os quatro pilares são:

Pilar I: Reforma e Modernização da Rede de Dados da Saúde;

Pilar II: Reforma dos Sistemas de Informação disponibilizados ao Cidadão;

Pilar III: Reforma dos Sistemas de Informação disponibilizados aos Profissionais de Saúde;

Pilar IV: Reforma do Sistema de Informação dos Registos Nacionais, Interoperabilidade e Circuito Digital do Medicamento, DM e MCDT⁹⁷⁸.

O pilar no qual se insere o investimento em cibersegurança é o Pilar I, da reforma e modernização da rede de dados da saúde. O principal objetivo deste pilar é a renovação da infraestrutura digital do SNS e essa renovação compreende:

- A substituição do parque informático ao serviço dos profissionais do SNS, por equipamentos e dispositivos mais recentes e atualizados;
- O desenvolvimento de dois polos de infraestrutura central, os dois com redundância em tempo real e com reforço das condições locais de redes e dados;
- Reforço do nível da segurança de informação e cibersegurança;
- Alavancar o desenvolvimento de um *Data Lake* (repositório massivo de dados nativos⁹⁷⁹) universal e transversal ao SNS⁹⁸⁰.

Espera-se, através da prossecução desses projetos, atingir os seguintes resultados:

- Assegurar a efetiva resiliência e redundância de serviços digitais no SNS;
- Melhoria do desempenho e segurança dos serviços e aplicações, comunicações e dados de saúde;
- Reforço muito substancial de robustez e fiabilidade ao nível da SI e cibersegurança;
- Neutralização da exposição a riscos, falhas e incidentes;
- Redução dos custos indiretos resultantes de falhas e incidentes⁹⁸¹.

Dos 300 milhões de euros do PRR destinados à saúde, 116 milhões ficam alocados a este primeiro pilar⁹⁸².

A execução orçamental dos fundos do PRR está, no entanto, atrasada. Na calendarização inicial, previa-se que o investimento no primeiro pilar ficaria completo até ao final de 2022. Contudo, em fevereiro de 2024, ainda só cerca 17% dos 300 milhões de euros (52,4 milhões) tinham sido pagos⁹⁸³.

Além disso, a larga maioria do investimento parece estar alocada à aquisição de equipamento⁹⁸⁴, sendo raras as referências à formação dos profissionais de saúde em matéria de cibersegurança. Embora a atualização de equipamento e de sistemas seja uma parte fundamental da

⁹⁷⁷ Recuperar Portugal, "Investimento RE-C01-i06: Transição Digital da Saúde (300 M€)", 8 de junho de 2021, <https://recuperarportugal.gov.pt/2021/06/08/investimento-re-c01-i06/>.

⁹⁷⁸ SPMS, "Plano de Atividades e Orçamento 2022", 76, setembro de 2021, https://www.spms.min-saude.pt/wp-content/uploads/2022/09/Plano-de-Atividades-e-Orçamento-2022_Assinado_09092022.pdf.

⁹⁷⁹ Dados próprios da aplicação ou aplicações do SNS e não de terceiros.

⁹⁸⁰ SPMS, "Plano de Atividades e Orçamento 2022", 107.

⁹⁸¹ SPMS, "Plano de Atividades e Orçamento 2022", 107.

⁹⁸² SPMS, "Plano de Atividades e Orçamento 2022", 111.

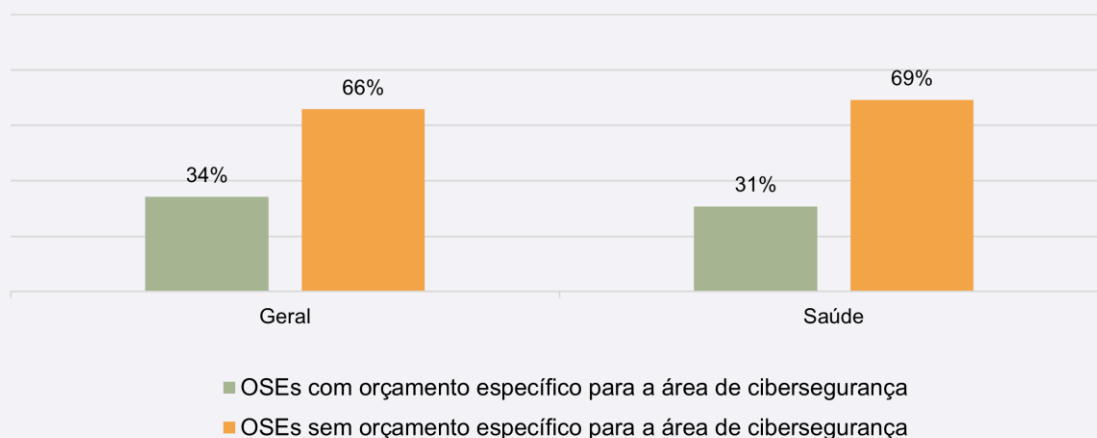
⁹⁸³ Recuperar Portugal, "Monitorização", <https://recuperarportugal.gov.pt/monitorizacao/>.

⁹⁸⁴ SPMS, "Plano de Atividades e Orçamento 2022", 76.

cibersegurança, é também importante que não seja esquecida a formação dos recursos humanos que vão utilizar esses equipamentos e sistemas. Como se sabe, a maioria dos incidentes de cibersegurança devem-se a erro humano e, tal como já foi evidenciado, a falta de formação dos profissionais de saúde em cibersegurança é uma fragilidade prevalente no setor.

Deste setor, cerca de 31% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Relativamente às áreas de aplicação do orçamento de cibersegurança, 92% aplica na segurança das redes, 75% na capacitação em tecnologia e aquisição de *hardware* e 67% em gestão de vulnerabilidades, análise de segurança e aquisição de *software*. Em relação à média geral, a maior diferença está na aquisição de *software* e formação, estando este setor abaixo da mesma (**Gráficos 110 e 110.4**).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

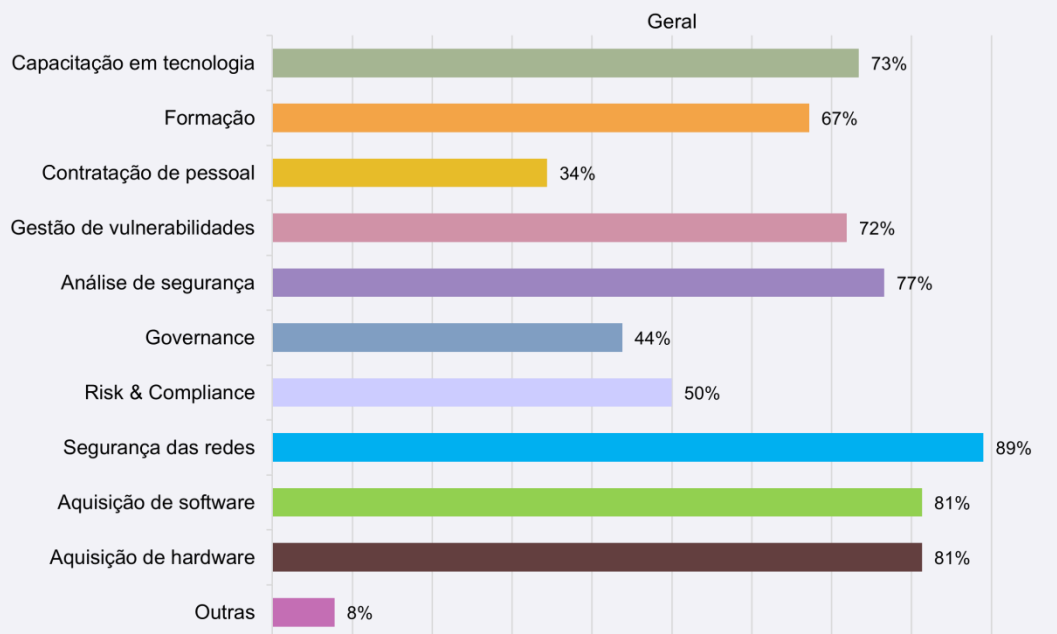
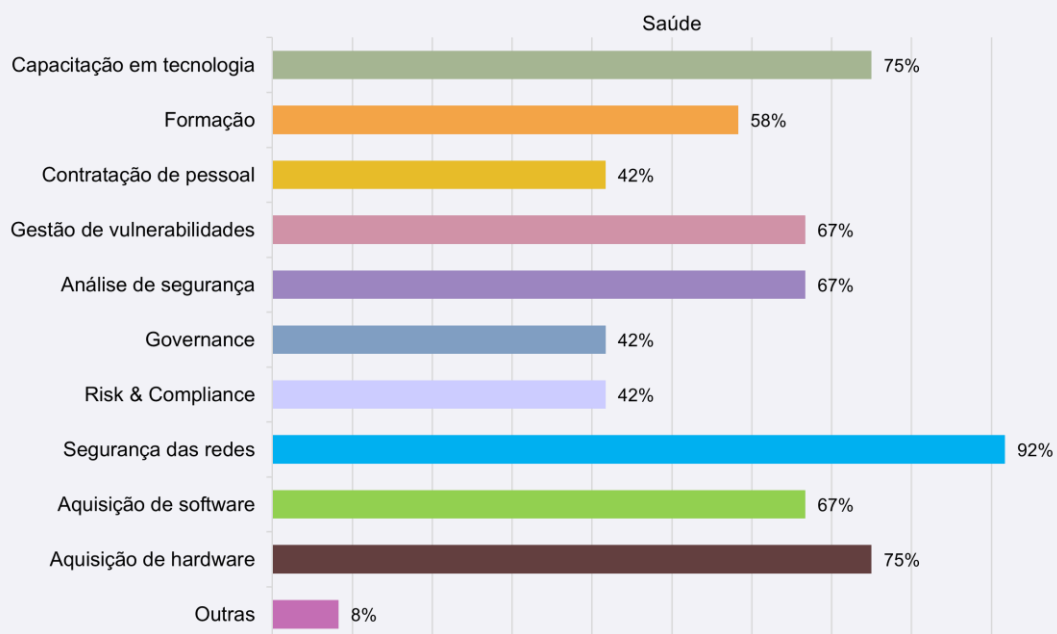
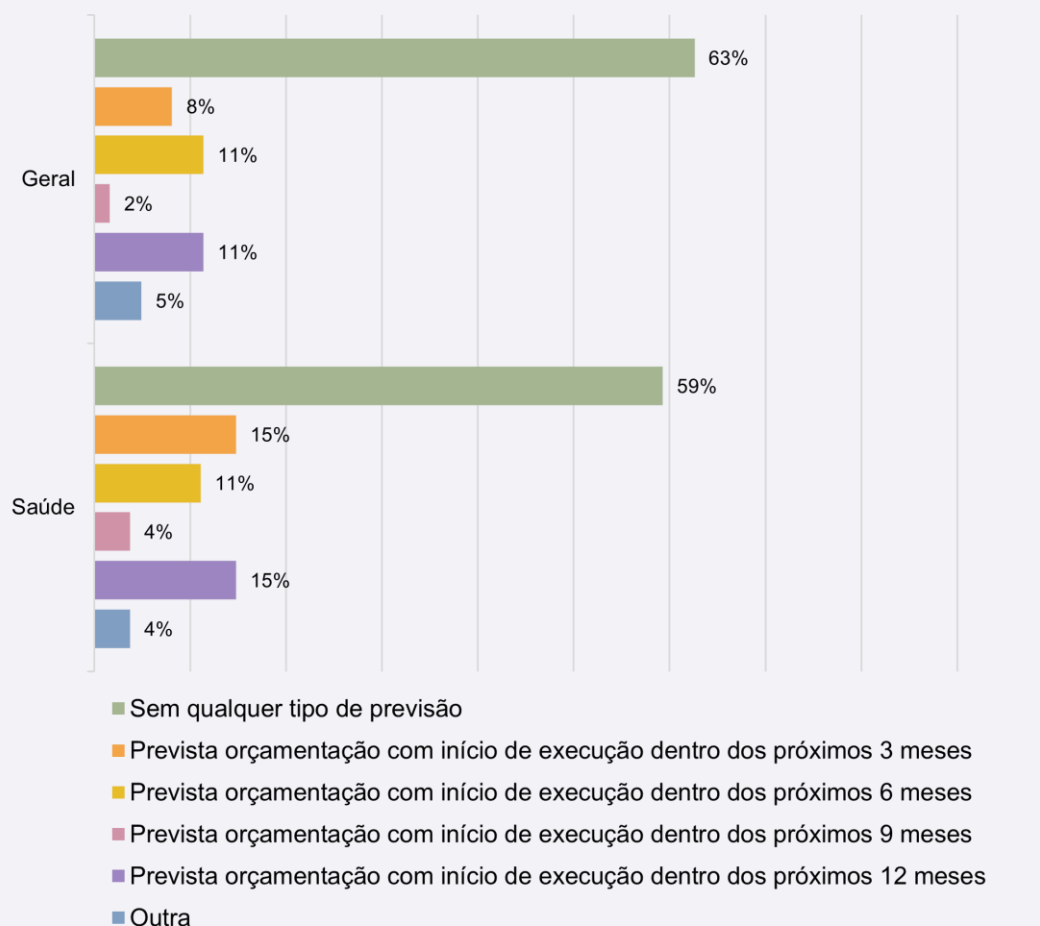


Gráfico 110.4 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 59% não tem qualquer previsão para a orçamentação, 15% tem previsto a orçamentação dentro dos próximos 3 meses ou 12 meses e 11% tem previsto a orçamentação para os próximos 6 meses. A maior diferença para o setor geral está na orçamentação a 3 e 12 meses com uma diferença de 7 pp e 4 pp, respetivamente (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



5.5. RJSC e legislação setorial

O setor da saúde não é, quer a nível nacional, quer a nível europeu, um setor amplamente legislado ao nível da cibersegurança. No entanto, legislação como o Despacho n.º 8877/2017 estabelece importantes bases sobre estas matérias, tais como o modelo de governação a seguir pela SPMS, em articulação com o Gabinete Nacional de Segurança e Centro Nacional de Cibersegurança (GNS/CNCS), as medidas e procedimentos de segurança a adotar pelas entidades prestadoras de cuidados de saúde, ao nível da gestão do risco, da nomeação de CISO e CSO, e elaboração de relatórios sobre o nível de implementação de políticas e controlos de segurança na entidade, de forma a permitir avaliar e comparar níveis de maturidade, orientações sobre a aquisição e gestão de tecnologias com vista à cibersegurança, a necessidade de realizar auditorias e avaliações de cibersegurança, versando ainda sobre a capacitação e recursos humanos e o investimento em cibersegurança⁹⁸⁵. O mesmo despacho exige que todas as entidades do SNS adotem uma política de cibersegurança, que tenham um plano de contingência em caso de incidentes de cibersegurança e impele à cooperação e partilha de informação entre as várias entidades do SNS⁹⁸⁶.

Há também legislação mais abrangente, destinada a múltiplas entidades, para além dos OSE, tal como a Lei da Proteção de Dados (Lei n.º 58/2019, de 8 de agosto), decorrente do Regulamento Geral sobre a Proteção de Dados, que impõe múltiplas obrigações ao nível do tratamento e proteção dos dados pessoais recolhidos, desde medidas de proteção, à obrigação de notificação aos titulares dos dados em caso de violação dos mesmos.

Aliás, na legislação existente sobre proteção de dados pessoais, os dados relativos à saúde constituem uma categoria especial de dados, tais como os dados pessoais que “revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como os dados genéticos, os dados biométricos destinados a identificar uma pessoa singular de forma inequívoca (...) ou dados relativos à vida sexual ou à orientação sexual”⁹⁸⁷ dos seus titulares. Tais dados podem ser apenas tratados com o consentimento explícito dos seus titulares, ou se o seu tratamento “for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos (...) em matéria de legislação laboral, de segurança social e de proteção social (...), necessário para proteger os interesses vitais do titular ou de outra pessoa (...) se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social” ou se este for necessário “por motivos de interesse público no domínio da saúde pública”⁹⁸⁸.

Surge, depois, legislação multissetorial, tal como o Regime Jurídico da Segurança do Ciberespaço (RJSC), que transpõe a Diretiva 2016/1148 (Diretiva NIS), acompanhado do decreto-lei n.º 65/2021, de 30 de julho, que regulamenta o RJSC, em diversas obrigações para os OSE a nível de cibersegurança, tais como a nomeação de um contacto permanente para articulação com o CNCS, a nomeação de um responsável de segurança, a elaboração de um inventário de ativos, de um plano de segurança, de um relatório anual, de análise, gestão e tratamento do risco, e de notificação de incidentes.

⁹⁸⁵ Despacho n.º 8877/2017, de 9 de outubro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/despacho/8877-2017-108269312>.

⁹⁸⁶ Despacho n.º 8877/2017.

⁹⁸⁷ Regulamento Geral sobre a Proteção de Dados, de 27 de abril de 2016 (artigo 9.º, n.º 1), https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis.

⁹⁸⁸ Regulamento Geral sobre a Proteção de Dados, de 27 de abril de 2016 (artigo 9.º, n.º 2, alíneas a) a i).

As diferentes obrigações legais que vão surgindo em matéria de cibersegurança tendem a conduzir as entidades a elas sujeitas a níveis mais elevados de maturidade, adotando práticas, processos e procedimentos cada vez mais seguros e robustos. Contudo, apesar da obrigatoriedade do cumprimento do RJSC, é notório que há um baixo cumprimento do exigido ao nível da análise do risco no setor da saúde, com apenas cerca de 50% das entidades a realizarem-na, segundo os dados do questionário.

O setor está ainda sujeito à Diretiva (UE) 2022/2555⁹⁸⁹, ou Diretiva NIS 2, que veio atualizar a Diretiva anterior passados seis anos sobre a sua publicação. A NIS 2 classifica dois tipos de setores: “setores de importância crítica”⁹⁹⁰ e “outros setores críticos”⁹⁹¹. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

O setor da saúde é um dos setores que passa abranger mais entidades. Enquanto a Diretiva NIS 1 incluía apenas instalações de prestação de cuidados de saúde (hospitais e clínicas privadas), a NIS 2 passa a incluir também no setor os laboratórios de referência da UE, entidades que fabricam produtos farmacêuticos de base e entidades que que fabricam dispositivos médicos considerados críticos durante uma emergência de saúde pública⁹⁹².

Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos⁹⁹³. Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto⁹⁹⁴.

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”⁹⁹⁵.

⁹⁸⁹ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

⁹⁹⁰ Diretiva (UE) 2022/2555, Anexo I.

⁹⁹¹ Diretiva (UE) 2022/2555, Anexo II.

⁹⁹² Diretiva (UE) 2022/2555, Anexo I.

⁹⁹³ Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

⁹⁹⁴ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

⁹⁹⁵ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

5.6. Standards e boas práticas aplicáveis

O setor da saúde dispõe de um conjunto alargado de *standards* internacionais que, diretamente ou indiretamente, se relacionam com o *procurement* de produtos e serviços no setor.

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor da saúde, segundo o relatório “*Mapping of OES Security Requirements to Specific sectors*” da ENISA.

Tabela 47 - Standards e Boas Práticas (Saúde)

Standards	Boas práticas
• ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002 • Health Insurance Portability and Accountability Act (HIPPA) • ISO 13485:2003 Medical devices -- Quality management systems – Requirements for regulatory purpOSE • ISO 80001-1:2010 Application of risk management for IT networks incorporating medical devices • ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth; • Digital Imaging and Communications in Medicine (DICOM) • EC Medical Devices Regulation (text agreed by EP and Council - in adoption process) • NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide • Manufacturer Disclosure Statement for Medical Device Security (MDS2)	• Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)

Na tabela anterior estão os *standards* referentes à área da saúde. De seguida, apresenta-se um breve sumário de cada um:

- **ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002:** Este *standard* estabelece diretrizes específicas para a gestão de segurança da informação em ambientes de saúde, baseando-se nos princípios e boas práticas da norma ISO/IEC 27002⁹⁹⁶;
- **Health Insurance Portability and Accountability Act (HIPPA):** A *HIPPA* é uma legislação dos Estados Unidos que foi promulgada em 1996 e tem como objetivo proteger a privacidade e a segurança das informações de saúde das pessoas⁹⁹⁷;

⁹⁹⁶ ISO, “Health informatics — Information security management in health using ISO/IEC 27002”, julho de 2008, <https://www.iso.org/standard/41298.html>.

⁹⁹⁷ Centers for Medicare & Medicaid Services, “HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules”, fevereiro de 2023, <https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf>.

- **ISO 13485:2003 Medical devices -- Quality management systems – Requirements for regulatory purpOSE:** Esta norma especifica os requisitos para um sistema de gestão da qualidade para a indústria de dispositivos médicos. Foi projetada para ser utilizada por organizações envolvidas no *design*, produção, instalação e manutenção de dispositivos médicos⁹⁹⁸;
- **ISO 80001-1:2010 Application of risk management for IT networks incorporating medical devices:** Esta norma especifica os requisitos para a aplicação de gestão de riscos em redes de *IT* que incorporam dispositivos médicos⁹⁹⁹;
- **ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth:** É um relatório técnico que foi publicado pela *ETSI* onde é abordada a arquitetura, modelos de serviços de utilizadores, tecnologias e aplicações de suporte ao *eHealth*¹⁰⁰⁰;
- **Digital Imaging and Communications in Medicine (DICOM):** Conjunto de normas desenvolvidas para a gestão, armazenamento, impressão e transmissão de informações em imagens médicas. Este conjunto de normas assegura a interoperabilidade entre diferentes sistemas e dispositivos utilizados em radiologia, cardiologia, entre outras áreas¹⁰⁰¹;
- **EC Medical Devices Regulation (text agreed by EP and Council - in adoption process):** Este regulamento, cujo texto foi acordado pelo Parlamento Europeu e pelo Conselho Europeu, está num processo de adoção e tem como objetivo substituir as diretivas anteriores sobre os dispositivos médicos (93/42/EEC e 90/385/EEC)¹⁰⁰²;
- **NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide:** É um guia elaborado pelo *NIST* e tem como objetivo fornecer orientações introdutórias para a implementação dos requisitos de segurança da *HIPAA*¹⁰⁰³;
- **Manufacturer Disclosure Statement for Medical Device Security (MDS2):** É um documento utilizado pelos fabricantes de dispositivos médicos onde é fornecido informações detalhadas sobre a segurança e a capacidade de gestão de riscos dos dispositivos¹⁰⁰⁴.

Um *standard* do setor muito relevante para a temática da cibersegurança e *procurement* é o *Manufacturer Disclosure Statement for Medical Device Security (MDS2)*. O formulário MDS2 dota os fornecedores de equipamentos médicos com os meios necessários para a divulgação das funcionalidades relacionadas com segurança dos seus equipamentos. O formulário contém um conjunto de questões relativas aos equipamentos médicos e permite a comparabilidade de funcionalidades de segurança entre diferentes equipamentos de diferentes fabricantes.

⁹⁹⁸ ISO, "Medical devices — Quality management systems — Requirements for regulatory purpOSE", julho de 2003, <https://www.iso.org/standard/36786.html>.

⁹⁹⁹ ISO, "Application of risk management for IT-networks incorporating medical devices", outubro de 2010, <https://www.iso.org/standard/44863.html>.

¹⁰⁰⁰ ETSI, "Analysis of user service models, technologies and applications supporting eHealth", fevereiro de 2009, https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf.

¹⁰⁰¹ DICOM, "Digital Imaging and Communications in Medicine (DICOM)", maio de 2017, https://www.researchgate.net/publication/355550688_Digital_Imaging_and_Communications_in_Medicine_DICOM.

¹⁰⁰² Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32017R0745>.

¹⁰⁰³ NIST, "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide", fevereiro de 2024, <https://csrc.nist.gov/pubs/sp/800/66/r2/final>.

¹⁰⁰⁴ Asimily, "What are MDS2s and Why Should You Care", <https://asimily.com/blog/what-are-mds2s-and-why-should-you-care>.

Adicionalmente, a ISO está a desenvolver mais de 25 novos *standards* focados em informática médica, dos quais se destacam:

- **ISO/DTR 21332 *Health informatics*:** Considerações sobre segurança e privacidade de informação em sistemas de computação em *cloud*¹⁰⁰⁵;
- **ISO/WD 13131 *Health informatics*:** Linhas orientadoras para planeamento de qualidade em prestação de serviços de saúde à distância (*telehealth*)¹⁰⁰⁶;
- **ISO/AWI 22697 *Health informatics*:** Aplicação de boas práticas de gestão de privacidade de dados a informação de saúde pessoal¹⁰⁰⁷.

¹⁰⁰⁵ ISO, "Health informatics — Cloud computing considerations for the security and privacy of health information systems", 2021, <https://www.iso.org/standard/70568.html>.

¹⁰⁰⁶ ISO, "Health informatics — Telehealth services — Quality planning guidelines", 2021, <https://www.iso.org/standard/75962.html>.

¹⁰⁰⁷ ISO, "Health informatics — Application of privacy management to personal health information", <https://www.iso.org/standard/73697.html>.

5.7. Desafios

O setor da saúde continuará a ser um alvo muito apetecível por parte dos cibercriminosos devido à riqueza dos dados que armazena. A par dessa atratividade para os atacantes devida ao tipo de dados armazenados, a utilização de equipamentos e sistemas menos seguros, como nos dispositivos médicos implantáveis, ou nos equipamentos e sistemas *legacy*, continua a ser uma vulnerabilidade do setor. Mesmo com a atualização prevista dos equipamentos através dos fundos do PRR, não há sistemas 100% seguros.

Um outro desafio enfrentado pelo setor são as práticas pouco seguras no âmbito da cibersegurança. Este é um desafio que possivelmente poderia ser solucionado com formação adequada, mas num setor em que muitos dos turnos de médicos e enfermeiros estão a ser assegurados pela realização de horas extraordinárias, o tempo para mais do que a prestação de cuidados de saúde, como formações em cibersegurança, é escasso.

A criação de um *data lake*¹⁰⁰⁸ neste setor, no qual podem existir práticas pouco seguras e há uma falta generalizada de formação no âmbito da cibersegurança, poderá constituir um elevado risco de segurança. Se dados pouco agregados já são um alvo apetecível, um repositório massivo de dados interoperáveis sê-lo-á ainda mais. Será necessária uma arquitetura de segurança robusta, bem como uma seleção criteriosa de quem poderá aceder ao *data lake* e formação adequada para a proteção do mesmo. Um facto importante é de que o ser humano tem um papel principal na maioria dos incidentes de cibersegurança (95%), tendo as falhas tecnológicas um papel menos importante¹⁰⁰⁹.

De acordo com um relatório da Check Point, os ataques por via tecnológica tiveram um aumento de 40% a nível global (entre 2021 e 2022), sendo a saúde um dos setores mais afetados¹⁰¹⁰. Acresce a este facto que o número de dispositivos médicos interligados em rede aumentou nos últimos anos, sendo que a maior parte dos sistemas utilizados por hospitais não tiveram um desenvolvimento focado na segurança informática, pelo que estão mais vulneráveis. Um exemplo desta falta de desenvolvimento focado na segurança informático é o facto de ainda serem utilizados em hospitais computadores cujo sistema operativo é o *Windows 95* que já não é suportado pela *Microsoft* desde 2006¹⁰¹¹.

Atualmente, a maior parte dos dispositivos médicos estão ligados à rede, alguns destes dispositivos são deveras importantes para o paciente, tais como: bombas de infusão, ventiladores, máquinas de hemodiálise, entre outros. É referido ainda que houve um ciberataque na Alemanha que levou à morte de uma paciente, tendo este ficado identificado como o primeiro homicídio causado por um ataque desta natureza¹⁰¹². De forma a ser possível prevenir este tipo de ataques é importante que todo o pessoal do setor da saúde coloque em prática os *standards* e as boas práticas de cibersegurança. Estas estarão descritas no próximo subcapítulo.

¹⁰⁰⁸ Repositório central com o propósito de guardar, processar e proteger grandes quantidades de dados (fonte: “What is a Data Lake?”, Google Cloud, Google, <https://cloud.google.com/learn/what-is-a-data-lake>).

¹⁰⁰⁹ Paul Mee e Rico Brandenburg, “After reading, writing and arithmetic, the 4th ‘r’ of literacy is cyber-risk”, *World Economic Forum*, 17 de dezembro de 2020, <https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/>.

¹⁰¹⁰ Check Point Research, 2023 Cyber Security Report, Check Point, 2023, 48.

¹⁰¹¹ “Cyberattacks on the Healthcare Sector”, *Checkpoint*, 2023, <https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/>.

¹⁰¹² “Cyberattacks on the Healthcare Sector”, *Checkpoint*.

5.8. Recomendações

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste setor. Tais cenários são indicados na seguinte tabela:

Tabela 48 - Cenários de risco (Saúde)

Cenários de risco

Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.

Campanha de PHISHING dirigida a colaboradores ou utentes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.

Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO WEB** (*SQL Injection* ou *Cross-site Scripting*).

Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.

FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.

VIOLAÇÃO DE DADOS da entidade (dados de utentes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.

RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em bitcoins, sob a ameaça da sua destruição ou exposição ao público.

Desenvolvimento de ações de CIBERESPIONAGEM, através de malware ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 23 de setembro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf>)

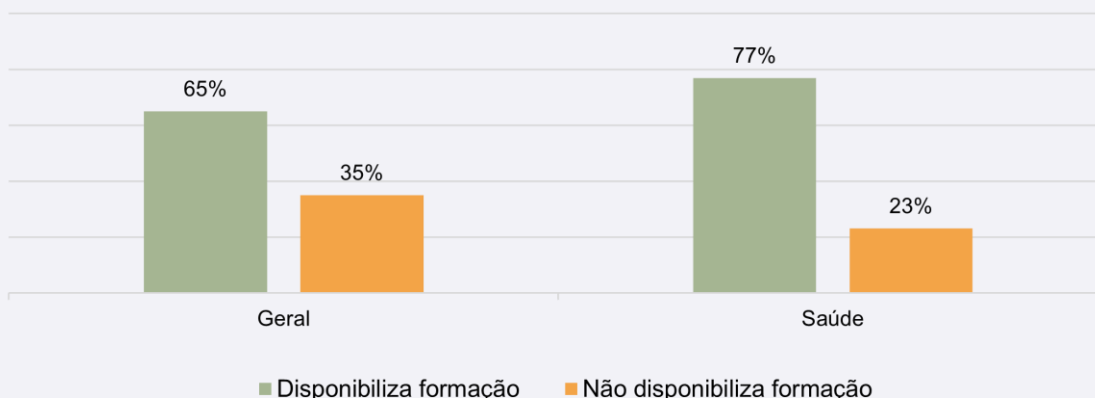
Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor da saúde, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

Como referido, as ameaças mais prevalentes no setor são o *ransomware* e ameaças relativas a dados, ameaças que geralmente só se concretizam quando tentativas de engenharia social são bem-sucedidas. A sensibilização para este tipo de riscos e a formação para identificar tais tentativas são essenciais para impedir que estas se concretizem, pois a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação nestas matérias é também importante para que se evitem divulgações de informação de forma indevida, ou que se utilizem, por exemplo, *pendrives* de origem desconhecida¹⁰¹³, entre outras ações de risco.

Os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor disponibilizarem formação em cibersegurança aos seus colaboradores (**Gráfico 38**), a maioria das formações (cerca de dois terços) são de carácter facultativo, e não obrigatório (**Gráfico 39**). Além disso, na maioria das entidades os momentos de formação têm frequência anual (**Gráfico 41**), o que no contexto do setor da saúde poderá ser insuficiente para assegurar a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



¹⁰¹³ “O maior banco do mundo sofreu ataque de ransomware e salvou-se graças a uma... pen USB”, *PpIWare*, 12 de novembro de 2023, <https://pplware.sapo.pt/internet/o-maior-banco-do-mundo-sofreu-ataque-de-ransomware-e-salvou-se-gracas-a-uma-pen-usb/>.

Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa

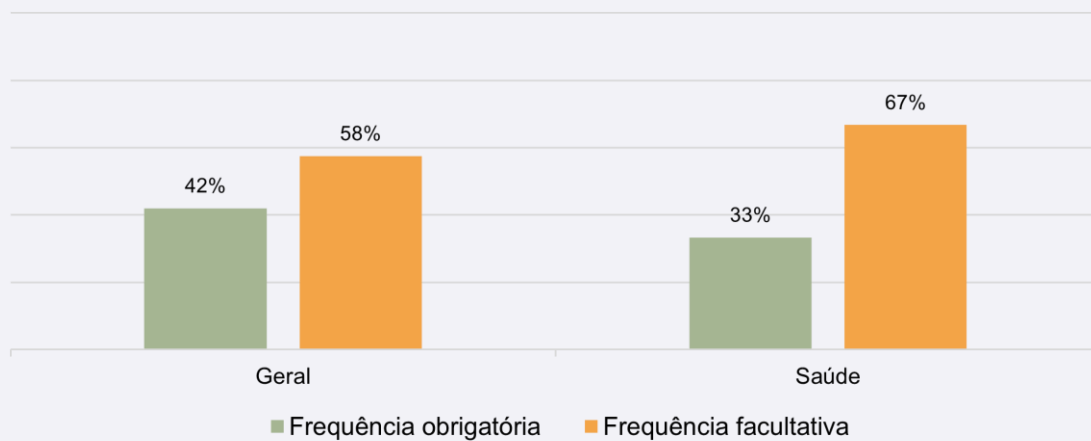
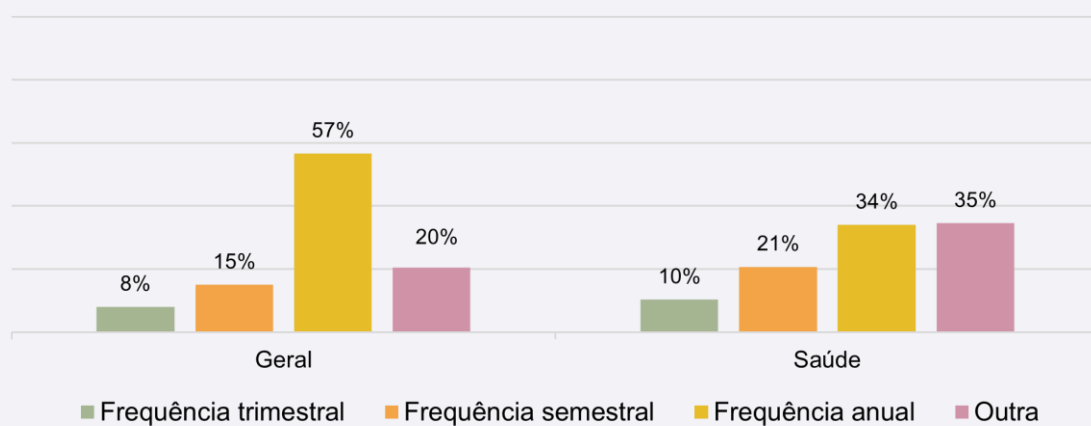


Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor da saúde, comparativamente com os restantes, é um dos setores onde menos se observa a realização de avaliações de segurança, de utilização de autenticação multifator, de cifragem, de sistemas de gestão de palavras-passe e de análises de risco periódicas.

Nesse sentido, recomenda-se aos OSE do setor da saúde que:

- Realizem avaliações de segurança pelo menos anualmente;
- Realizem análises de risco com periodicidade mínima anual;
- Implementem, onde possível, métodos de autenticação multifator;
- Utilizem, nos ficheiros relevantes e dados sensíveis, cifragem;
- Utilizem sistemas de gestão de palavras-passe, de modo a viabilizar a utilização de diversas palavras-passe complexas e seguras para cada sistema.

Medidas como estas auxiliam a impedir acessos iniciais por parte dos agentes de ameaça e a que os mesmos não sejam capazes de progredir na exploração dos dados, sistemas e ficheiros quando um primeiro acesso é obtido. Por exemplo, a autenticação multifator pode impedir a progressão caso uma palavra-passe seja descoberta e a cifragem pode evitar que os dados sejam utilizados mesmo tendo sido obtidos.

Políticas, procedimentos e planos de cibersegurança

De acordo com os dados obtidos no questionário, apenas 59% dos OSE do setor tinham documentado e implementado políticas e procedimentos de cibersegurança. Adicionalmente, apenas 46% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Face a esta realidade, recomenda-se aos OSE do setor que ainda não o tenham feito que elaborem e implementem uma política de cibersegurança que verse sobre:

- Os diversos papéis e responsabilidades dos colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, tais como os controlos de acesso (lógico e físico);
- A gestão de incidentes, devendo ser elaborados um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação dos mesmos, bem como um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização da política, de forma periódica (no mínimo, anual), de modo a manter atualizada face à evolução das ameaças de cibersegurança e da própria organização.

Face à baixa percentagem de OSE do setor que indicaram possuir uma política de continuidade de negócio (39%), recomenda-se também a elaboração de uma tal política alinhada com a política de cibersegurança.

A elaboração de políticas, procedimentos e planos de cibersegurança e a comunicação destes aos profissionais, quer de saúde, quer das áreas tecnológicas, é também uma forma de dar a conhecer a estes o que lhes é permitido ou não fazer em contexto de cibersegurança, como devem tratar ativos de informação, desde dados sensíveis a dispositivos, e como devem atuar perante uma situação suspeita ou de concretização de uma ameaça.

Modernização dos sistemas *legacy*

A existência de sistemas *legacy* acaba por constituir um risco ou ameaça no setor da saúde. Embora seja uma tarefa difícil, devem ser procuradas formas de evitar o aparecimento deste tipo de sistemas. Para tal, é necessário haver avaliações regulares por parte do departamento de TI e desenvolver planos de ação claros para a modernização de toda a infraestrutura, adotar arquiteturas baseada em microsserviços, de forma a ser possível atualizar cada componente de maneira individual, investir em tecnologias baseadas em nuvem, de modo a reduzir a dependência de infraestruturas físicas e haver um desenvolvimento contínuo para garantir que os sistemas estão sempre atualizados.

Realização de testes de intrusão (*pentesting*)

Embora não exista obrigação legal no setor da saúde de realizar testes de intrusão, importa voltar a frisar que este setor é um dos que mais sofre ciberataques no contexto dos OSE e que esses ciberataques são sobretudo ataques de *ransomware* e ataques relativos a dados. Tendo em conta estes factos, bem como a baixa realização de *pentesting* no setor (35%), considera-se pertinente a realização deste tipo de testes de forma a permitir a identificação de vulnerabilidades, a correção destas e a melhoria da resiliência em cibersegurança das organizações do setor a diversos ciberataques.

Por fim, o *CIS* (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o *CIS* considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches*, proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*¹⁰¹⁴.

No setor da saúde, os controlos fundacionais relacionados com a segurança de rede são particularmente críticos. Infraestruturas de saúde, como sistemas de gestão hospitalar, plataformas de telemedicina e redes que suportam a troca de dados de pacientes, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, a disponibilidade e a continuidade dos seus serviços. Falhas ou configurações incorretas nesses sistemas podem ser exploradas para interromper o acesso a dados vitais dos pacientes, comprometer a privacidade de informações sensíveis, ou até mesmo afetar a operação de dispositivos médicos conectados, colocando em risco a segurança dos pacientes e a eficácia do atendimento.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos¹⁰¹⁵:

¹⁰¹⁴ "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls-list>.

¹⁰¹⁵ "The 18 CIS Critical Security Controls".

Tabela 49 - Controlos de Segurança da CIS (Saúde)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: CIS, “The 18 CIS Critical Security Controls”, <https://www.cisecurity.org/controls/cis-controls-list>)

6. Fornecimento e distribuição de água potável

6.1. Contextualização setorial

O setor de águas e resíduos contribui significativamente para o desenvolvimento económico e social do país, tanto pela capacidade de gerar atividade económica e de criar emprego e riqueza, como pela crescente melhoria que tem conferido às condições de vida da população, gerando externalidades económicas positivas noutros setores. Os serviços deste setor são reconhecidos como serviços públicos essenciais pela legislação nacional, designadamente pela Lei dos Serviços Públicos Essenciais (Lei n.º 23/96, de 26 de julho, na redação atual)¹⁰¹⁶.

O acesso à água potável e ao saneamento básico foi, aliás, declarado um direito humano essencial pela Assembleia Geral da ONU em 2010. Tal significa que todos devem ter acesso adequado e seguro à água potável e ao saneamento, o que pode ser feito através de sistemas públicos tradicionais (redes de abastecimento ou de saneamento), sistemas públicos simplificados (por exemplo, fossas séticas coletivas) ou instalações individuais (por exemplo, fossas séticas individuais). Os serviços e as instalações devem estar fisicamente acessíveis, ter uma capacidade adequada e qualidade aceitável. É necessário que o acesso seja disponibilizado a todos de igual forma, colocar os cidadãos no processo de decisão e ocorrer uma monitorização e suporte. Devido ao elevado número de entidades com papel de gerir, a aplicação de um modelo único torna-se muito difícil. Nestes serviços existem monopólios naturais, pois, devido a razões tecnológicas, apenas uma entidade fornece os serviços em cada área geográfica¹⁰¹⁷.

A modernização deste setor foi, no entanto, tardia. Há cerca de 30 anos, em plena década de 1990, apenas 50% da água para consumo humano era controlada e de boa qualidade e apenas 30% da população portuguesa era servida com sistemas de tratamento de águas residuais. Também a deposição dos resíduos era feita, em larga medida, de forma não adequada, em lixeiras não controladas¹⁰¹⁸.

Em 1991, imperava no Grande Porto (e noutros pontos do país) uma situação de interrupção frequente e até mesmo de rutura do abastecimento de água às populações, já classificada de “pré-

¹⁰¹⁶ ERSAR, “Relatório Anual dos Serviços de Águas e Resíduos em Portugal: Volume 1 – Caracterização do setor de águas e resíduos”, 2022, 51, https://www.ersar.pt/_layouts/mpp/file-download.aspx?fileId=2169122.

¹⁰¹⁷ ERSAR, “Relatório Anual - Volume 1” (2022), 51.

¹⁰¹⁸ Águas de Portugal, “Águas de Portugal - Duas décadas que perspetivam o futuro”, publicado a 6 de outubro de 2016, vídeo, Youtube, <https://www.youtube.com/watch?v=2IPH9iW5wDg>.

calamidade pública”. Na origem desta, estava uma insuficiente capacidade de captação e produção de água para responder às necessidades da população e das atividades produtivas. Também no Algarve havia dificuldades semelhantes, sendo cada vez mais difícil satisfazer as necessidades de água da população residente e dos turistas, em particular durante a época balnear.

Para responder a estes e a outros problemas existentes no fornecimento e distribuição de água, o Estado iniciou, antes da reforma legislativa de 1993 que passou a permitir entrada de capitais privados neste setor, um conjunto de experiências piloto através de protocolos estabelecidos entre a Empresa Portuguesa das Águas Livres (EPAL) e grupos de municípios, tendo identificado como prioritária a intervenção nos municípios mais densamente povoados, localizados na faixa litoral, em especial o Algarve e o Grande Porto.

O racional por trás destas experiências assentava na adoção de soluções integradas, supramunicipais, que tivessem em conta a realidade física das bacias hidrográficas e que promovessem economias de escala substanciais e a fiabilidade dos serviços.

As parcerias então encetadas viriam a ser, em 1993, em boa parte convertidas nos primeiros sistemas multimunicipais de captação, tratamento e abastecimento de água para consumo dos municípios¹⁰¹⁹.

Encontrada uma parte da solução dos problemas do abastecimento de água em Portugal, veio a constituição da Águas de Portugal, nesse mesmo ano, dar resposta à inexistência de soluções empresariais, para além do caso da EPAL, que assegurassem a conciliação da realização dos avultados investimentos necessários com a boa utilização dos subsídios disponíveis nos fundos comunitários.

As primeiras empresas concessionárias dos sistemas multimunicipais de captação, tratamento e abastecimento de água foram criadas em 1995, tendo como acionistas a Águas de Portugal, com 51% do capital social, e os municípios servidos pelo respetivo sistema, com 49%.

Deu-se então início a um plano de infraestruturação sem precedentes no setor, complementado com a incorporação de infraestruturas municipais existentes, algumas das quais sofrendo obras de remodelação ou reconversão para dar respostas aos requisitos dos novos sistemas integrados.

Os investimentos realizados até 1999 (primeiro período de aplicação do Fundo de Coesão) ascenderam, na vertente do abastecimento de água, a 383 milhões de euros, dos quais 325 milhões de cofinanciamento, beneficiando cerca de 64 municípios e abrangendo cerca de 6,4 milhões de habitantes.

Estas soluções geraram economias de escala e permitiram uma utilização mais eficiente dos recursos, permitindo prosseguir os objetivos de melhorar a qualidade da água e os níveis de atendimento das populações, colocando Portugal entre os melhores desempenhos ambientais da Europa comunitária.

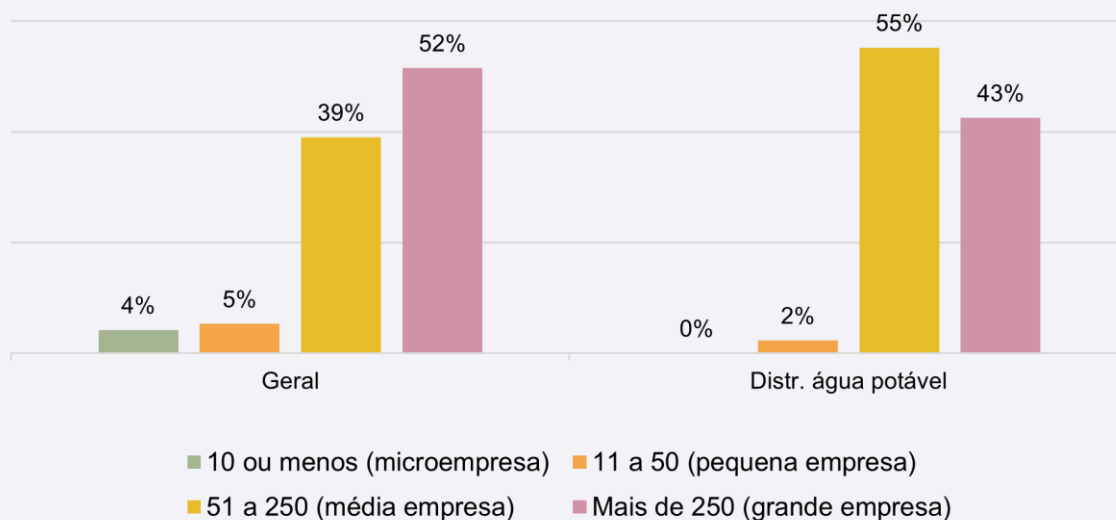
Desde então, o panorama nacional mudou. Atualmente, segundo dados de 2022, o setor abastece de água 9,8 milhões de habitantes e abrange 97% dos alojamentos do país. Por sua vez, o saneamento serve 8,7 milhões de habitantes, chegando a 86% dos alojamentos em Portugal. A qualidade da água fornecida melhorou também, com avaliações de qualidade na ordem dos 99,7%, a par dos Estados-membros da UE que obtenham melhores resultados nessas avaliações.

De acordo com o questionário realizado, o tecido empresarial dos operadores de serviços essenciais (OSE) do setor da distribuição de água potável é sobretudo composto por médias

¹⁰¹⁹ Águas de Portugal, *Livro Águas de Portugal* (Lisboa: By the Book, 2016), 32, https://www.adp.pt/pt/media/publicacoes/downloads/pub_pt17_pt.pdf.

empresas (55%), com entre 50 a 250 colaboradores, seguido por médias empresas (43%) e a restante minoria (2%) são pequenas empresas (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



O regulador do setor considera que a maturidade deste em cibersegurança é muito baixa (**Gráfico 9**), uma perceção que pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (cerca de 57% disponibiliza formação) (**Gráfico 38**) e pela falta de medidas cibersegurança adotadas.

Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores

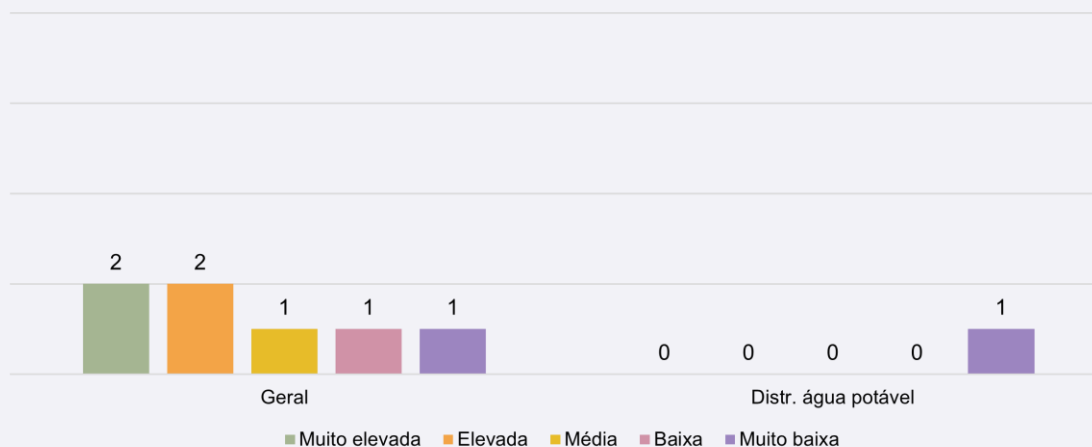
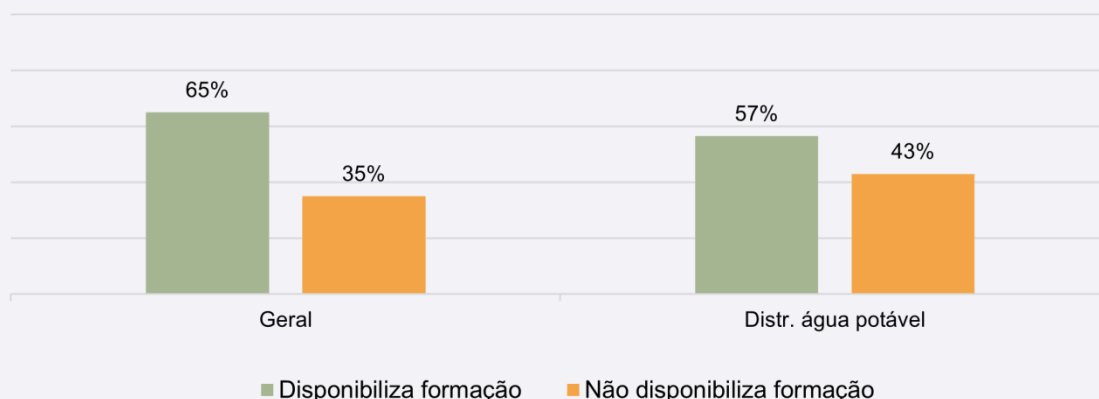
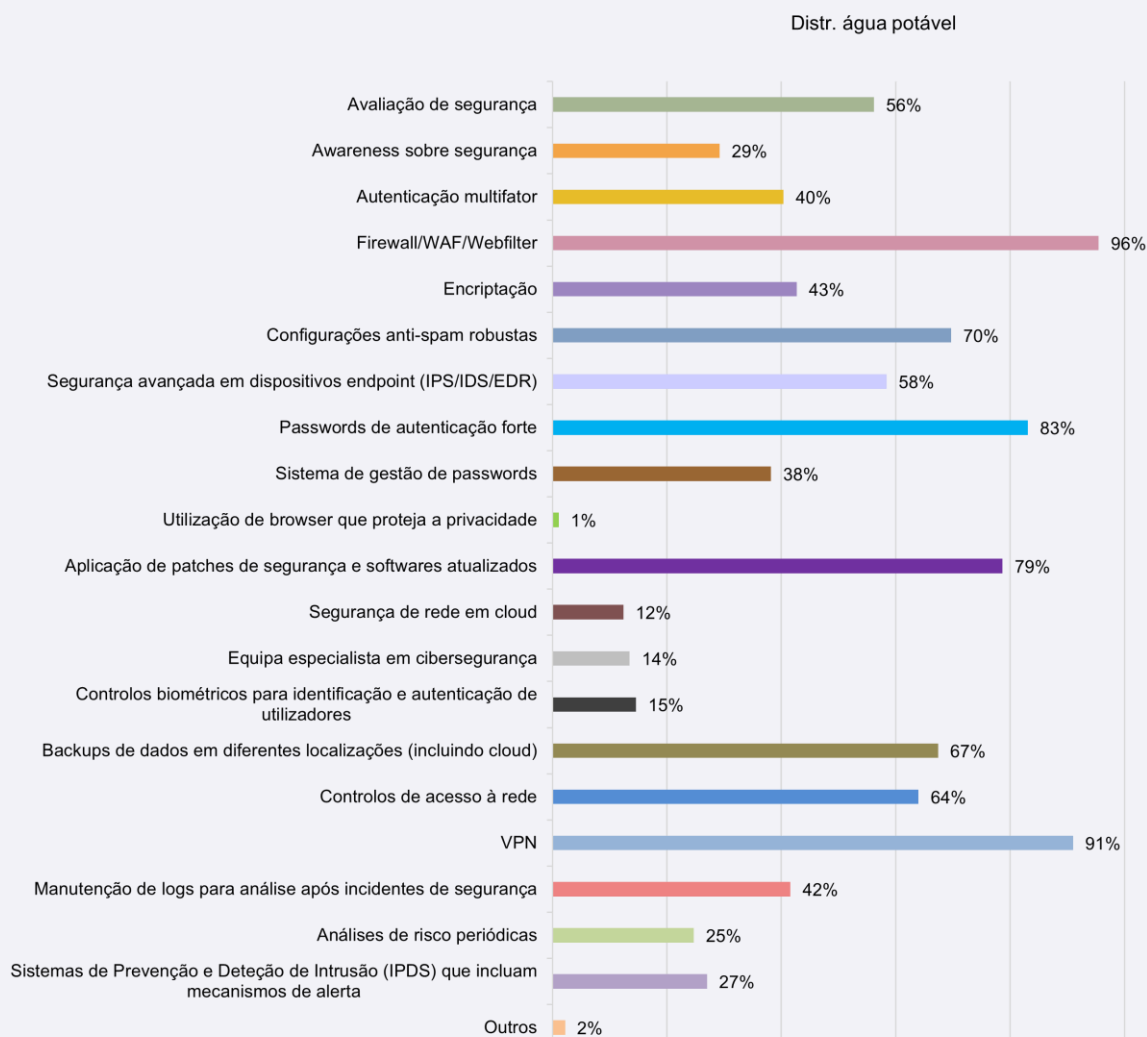


Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



As medidas menos adotadas foram: Segurança de rede em *cloud* com 12%, Equipa especialista em cibersegurança com 14%, a implementação de controlos biométricos para identificação e autenticação com 15%, Análise de risco periódicas com 25% e Sistemas de Prevenção e Detecção de Intrusão (IPDS) com 27% (**Gráfico 66.6**). A ressaltar também as políticas de cibersegurança e relacionadas implementadas, onde tanto a política de comunicação como a de continuidade de negócio estão abaixo dos 40% e pelo facto que apenas 25% dos operadores dedicarem orçamentos específicos à área de cibersegurança. É também um setor que tem, por enquanto, beneficiado de uma baixa incidência de ciberataques, onde 76% dos inquiridos nunca sofreu um incidente.

Gráfico 66.6 - Medidas de proteção contra ameaças de cibersegurança



6.1.1. Impacto socioeconómico

Tal como já foi referido, o setor do fornecimento e distribuição de água potável contribui significativamente para o desenvolvimento económico e social do país, gerando atividade económica, emprego e riqueza, bem como externalidades económicas positivas noutros setores de atividade.

De acordo com os dados mais recentes disponíveis (respeitantes a 2021) o volume de negócios anual do setor é superior a 2,5 mil milhões de euros, com um nível de rendimentos e ganhos totais reportado de 2,99 mil milhões de euros e com resultados líquidos agregados na ordem dos 106,7 milhões de euros¹⁰²⁰.

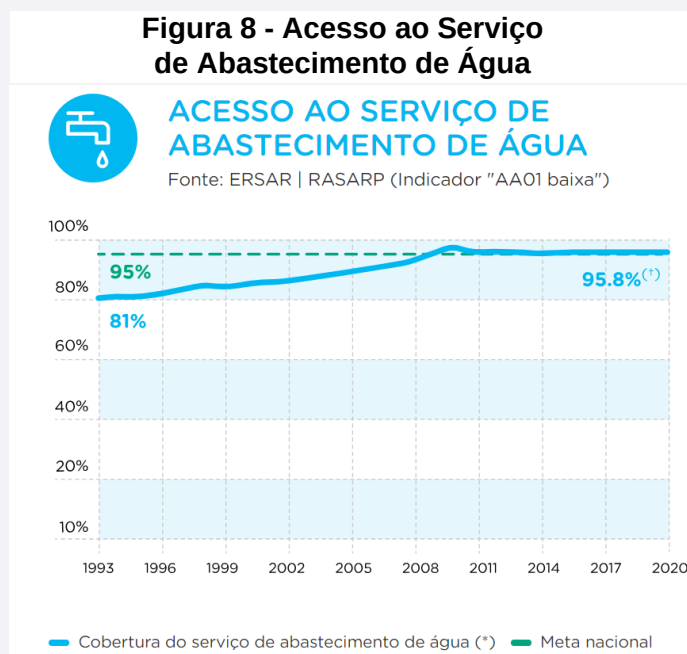
Ao nível do emprego, o setor empregava, no final de 2021, 9,8 mil trabalhadores (mais 1,2% do que em 2020), registando-se alguma estabilidade ao longo dos anos no número total de empregos. Ressalva-se, no entanto, que o número de trabalhadores em *outsourcing* tem vindo a aumentar na última década¹⁰²¹.

¹⁰²⁰ ERSAR, "Relatório Anual - Volume 1" (2022), Volume 1, 380-386.

¹⁰²¹ ERSAR, "Relatório Anual - Volume 1" (2022), 370.

Já no que diz respeito ao investimento realizado no setor, este foi, em 2021, na ordem dos 16,5 mil milhões de euros¹⁰²².

O acesso à água potável foi sempre uma questão da maior importância. Indispensável à sobrevivência humana, tornou-se também indispensável a diversas atividades do quotidiano humano. As reformas iniciadas em 1993 para resolver os problemas de acesso à água potável que até então subsistiam no país são prova disso, uma vez que trouxeram significativas melhorias à vida da população portuguesa. Os gráficos seguintes traçam essa evolução e melhoria:

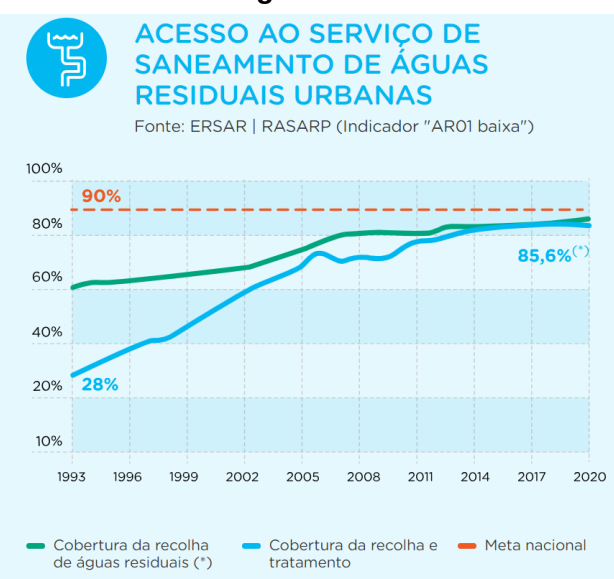


(Fonte: Waterhub - Plataforma Portuguesa da Água, “Evolução dos Serviços de Água em Portugal (1993-2017)”, <https://waterhub.pt/pt/portugal>)

Como se demonstra pela figura acima, as reformas iniciadas em 1993 permitiram aumentar a percentagem de população com acesso ao serviço de abastecimento de água de 81% em 1993 até à meta nacional de 95% em 2010, tendo esta percentagem estabilizado desde então, fixando-se em 95,8% em 2017.

¹⁰²² ERSAR, “Relatório Anual - Volume 1” (2022), 434.

Figura 9 - Acesso ao Serviço de Saneamento de Águas Residuais Urbanas

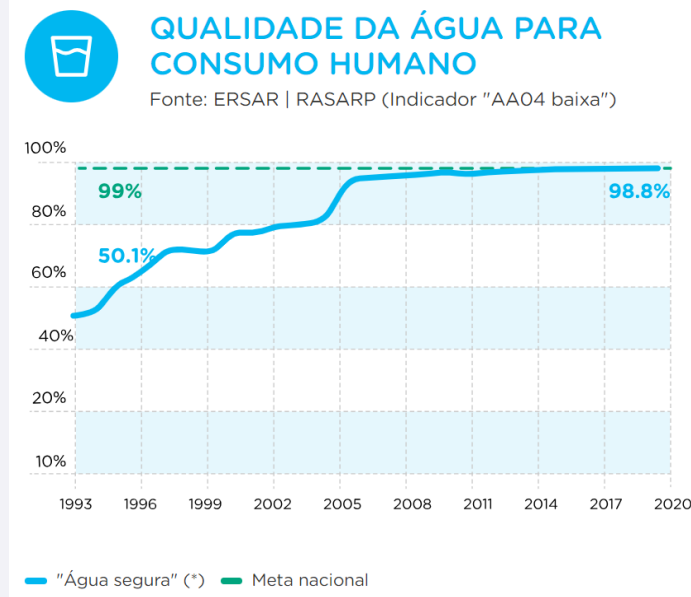


(Fonte: Waterhub - Plataforma Portuguesa da Água, “Evolução dos Serviços de Água em Portugal (1993-2017)”, <https://waterhub.pt/pt/portugal>)

Outra grande melhoria registada com as reformas iniciadas na década de 90 foi o aumento do acesso aos serviços de saneamento de águas residuais urbanas. Como se verifica pela Figura 12, em 1993 apenas 28% da população tinha acesso a estes serviços. Essa percentagem foi aumentando de ano para ano a bom ritmo, abrandando depois a partir de 2006, mas mantendo o crescimento. Em 2017, já 85,6% da população tinha acesso a estes serviços, mas ainda se estava aquém da meta de 90%. No entanto, dados mais recentes, como os do Relatório Anual dos Serviços de Água e Resíduos em Portugal (2022, Volume 1), revelam que a cobertura de recolha e tratamento se estende, pelo menos desde 2021, a 94% da população¹⁰²³, superando a meta estabelecida.

¹⁰²³ ERSAR, “Relatório Anual - Volume 1” (2022), 244.

Figura 10 - Qualidade da Água para Consumo Humano



(Fonte: Waterhub - Plataforma Portuguesa da Água, "Evolução dos Serviços de Água em Portugal (1993-2017)", <https://waterhub.pt/pt/portugal>)

Finalmente, a qualidade da água para consumo humano melhorou também drasticamente a partir de 1993. Ao passo que na década de 90 apenas 50,1% da água fornecida era considerada segura, em 2017 este valor atingia já os 98,8%. Dados mais recentes (2022) indicam que 99,59% da água fornecida é segura e de qualidade¹⁰²⁴.

6.1.2. Especificidades tecnológicas

As principais especificidades tecnológicas do abastecimento e fornecimento de água potável prendem-se com as tecnologias utilizadas na captação, tratamento e distribuição de água, bem como tecnologias de monitorização da qualidade, de medição de caudal e até mesmo dispositivos de deteção de fugas desta. Estas tecnologias inserem-se no campo da tecnologia operacional (TO).

¹⁰²⁴ ERSAR, "Relatório Anual - Volume 1" (2022), 199.

De acordo com o National Institute of Standards and Technology dos EUA (NIST), “a tecnologia operacional compreende um vasto conjunto de sistemas e dispositivos programáveis que interagem com o ambiente físico (ou gerem dispositivos que interagem com o ambiente físico). Estes sistemas e dispositivos detetam ou causam mudanças diretas através da monitorização e/ou controlo de dispositivos, processos e eventos. Exemplos [de tecnologia operacional] incluem sistemas de controlo industrial [*Industrial Control Systems* - ICS], sistemas de automação predial [*Building Automation Systems* - BAS]¹⁰²⁵, sistemas de controlo de acesso físico, sistemas de monitorização do ambiente físico e sistemas de medição do ambiente físico”¹⁰²⁶. A estes, acrescem ainda os sistemas de supervisão e aquisição de dados (*Supervisory Control and Data Acquisition* - SCADA), que são utilizados para recolher dados e controlar dispositivos dispersos, cuja centralização de dados é essencial para ter informação adequada sobre as operações realizadas. Estes sistemas são desenhados para recolher informação “no terreno”, transferindo-a para um centro de controlo, mostrando depois a informação de forma gráfica ou textual ao operador, permitindo a monitorização e o controlo centralizados em tempo real¹⁰²⁷.

Estes sistemas de TO estiveram, durante largos anos, separados dos sistemas de TI (Tecnologia da Informação), conferindo aos sistemas TO a segurança de não poderem ser acedidos ou atacados remotamente. No entanto, a evolução tecnológica dos últimos 20 anos tem conduzido à convergência dos dois tipos de sistemas, com a tecnologia operacional e a tecnologia da informação a estarem cada vez mais integradas uma com a outra¹⁰²⁸. Um exemplo disso é o *software* NAVIA, utilizado por alguns OSE no setor do fornecimento e distribuição de água potável.

De acordo com os próprios fornecedores do *software*, o NAVIA é um *software* que permite a gestão integral da infraestrutura de abastecimento de água e de recolha de águas residuais, de processos e de territórios, sendo “um agregador de dados e de conhecimento, que se integra com sistemas de telegestão (SCADA), de Laboratório (LIMS - Laboratory Information Management System), geográficos e de cadastros (SIG), financeiros (ERP) e comerciais (CRM)”¹⁰²⁹. A partir do mesmo, é ainda possível monitorizar, avaliar e corrigir operações através deste sistema, consoante o nível de integração deste *software* com outros sistemas¹⁰³⁰.

As Águas de Portugal desenvolveram também, internamente, uma ferramenta denominada Aquamod/Modelo Técnico. Esta ferramenta possibilita às entidades participadas e à própria administração central armazenar, analisar e calcular informação recolhida de todas as entidades para as atividades de abastecimento e de saneamento. Mais concretamente, o Aquamod é uma ferramenta de gestão que, através da recolha de dados, permite realizar análises preditivas da evolução dos caudais para longos períodos, cruza-os com outros dados relativos à região, tais como população residente e flutuante, cobertura, adesão, perdas, aflúências indevidas e captações, de modo a “estabelecer cenários de viabilidade técnico-financeira das operações e (...) definir projeções tarifárias capazes de, simultaneamente, garantir a progressiva recuperação de custos, necessária à sustentabilidade do sistema, e o ajustamento social dos preços”¹⁰³¹.

¹⁰²⁵ Sistemas de automação predial ou *Building Automation Systems* (BAS) são sistemas que controlam os três principais sistemas de um edifício: eletricidade, climatização (aquecimento e ar condicionado), e água e tratamento de resíduos.

¹⁰²⁶ Keith Stouffer et al., “NIST Special Publication NIST SP 800-82r3: Guide to Operational Technology (OT) Security”, *National Institute of Standards and Technology*, setembro de 2023, 8, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf>.

¹⁰²⁷ Keith Stouffer et al., “NIST SP 800-82r3: Guide to Operational Technology (OT) Security”, 12.

¹⁰²⁸ Keith Stouffer et al., “NIST SP 800-82r3: Guide to Operational Technology (OT) Security”, 8.

¹⁰²⁹ “Questões frequentes”, FAQs, NAVIA, <https://www.nviasolutions.com/faqs/>.

¹⁰³⁰ “Business & Operations Intelligence”, Porquê o NAVIA, NAVIA, <https://www.nviasolutions.com/porque-o-navia/>.

¹⁰³¹ Águas de Portugal, *Livro Águas de Portugal*, 55-56.

Adicionalmente, o facto de este sistema recolher dados de mais de 220 municípios, ou seja, cerca de 82% dos municípios portugueses, acaba por criar uma base de informação que oferece um quadro da realidade nacional e regional do país, cuja utilidade não se esgota nas operações das empresas do grupo Águas de Portugal, mas que constitui também um importante contributo para a definição de indicadores de base para políticas públicas nacionais e para análises comparativas com outros países¹⁰³².

Outro sistema utilizado pelas entidades participadas do grupo Águas de Portugal é o AQUASAFE. Este sistema tem uma vocação mais operacional do que os dois sistemas já referidos, e foi desenvolvido, como o nome indica, com o objetivo de manter a água “segura”. Objetivamente, o AQUASAFE recolhe e integra “informação de monitorização (...) em tempo real (sensores, telegestão, telemetria, etc.) com ferramentas de previsão e diagnóstico (modelos de previsão meteorológica, modelos técnicos dos sistemas, etc.), tornando possível antecipar problemas ou planear operações de forma mais eficiente”. O AQUASAFE permite assim manter a qualidade/salubridade da água, evitar problemas decorrentes de cheias, de excesso de fluxo para as estações de tratamento, e até mesmo planear intervenções de manutenção dos sistemas de abastecimento e tratamento de resíduos¹⁰³³.

A par destes, surge também o sistema WONE (*Water Optimization for Network Efficiency*), utilizado pela EPAL. Este é também um sistema de cariz mais operacional, destinado sobretudo à monitorização dos caudais e pressão e à deteção de fugas de água. Através de diversos elementos, tais como “o controlo de pressão e caudal, sistema de telemetria passivo, alarmes de pressão ativos, registos de 15 em 15 minutos e comunicações diárias”, o WONE vai realizando a devida monitorização desses parâmetros, servindo-se dos dados recolhidos para detetar as referidas fugas de água. Tal como o AQUASAFE, este sistema permite também planear intervenções no terreno, bem como quantificar os volumes de água a recuperar. A utilização deste sistema permitiu, entre 2005 e 2015, reduzir, na rede de distribuição de Lisboa, o nível de água não faturada de 23% para 8%¹⁰³⁴.

Existe ainda o Aquamatrix, o *software* de gestão comercial criado e utilizado pela EPAL. Este sistema é também comercializado para outras entidades fora do grupo Águas de Portugal há mais de uma década, em Portugal e Moçambique, e oferece diversas funcionalidades. Este *software* permite fazer a gestão da atividade e do desempenho através de indicadores variados, integrar interfaces como os de ERP, Sistemas de Informação Geográfica (GIS), os que apresentam as informações de telemetria, e outros, fazer o arquivo eletrónico de documentos, gerir processos relativos a projetos de redes prediais e urbanizações, fazer a gestão do ciclo de vida do parque de contadores e ainda realizar funções relacionadas com a leitura, faturação e cobrança dos serviços de fornecimento de água prestados. Segundo a EPAL, este *software* está atualmente presente em aproximadamente 30% do território, abrangendo cerca de 1,6 milhões de consumidores¹⁰³⁵.

¹⁰³² Águas de Portugal, *Livro Águas de Portugal*, 56.

¹⁰³³ Águas de Portugal, *Livro Águas de Portugal*, 105.

¹⁰³⁴ “WONE: Water Optimization Network Efficiency: A Global Solution to a Global Water Challenge”, WONE®, EPAL, <https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/wone>.

¹⁰³⁵ “Boosting business innovation”, Aquamatrix, EPAL, <https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/aquamatrix>.

Todos estes sistemas, para além de contribuírem para a segurança da água fornecida e para a boa gestão das empresas distribuidoras, são agentes de convergência entre os sistemas de TI e os sistemas de TO. Esta integração acarreta, no entanto, alguns riscos. Como se disse no início deste subcapítulo, os ambientes TI e os ambientes TO estiveram, durante muitos anos, separados, e têm vindo a convergir entre si ao longo dos últimos cerca de 20 anos. Essa convergência e integração entre os dois ambientes oferecem aos agentes de ameaça uma nova superfície de ataque, possibilitando o acesso ao ambiente TO depois de uma intrusão bem-sucedida no ambiente TI. Esta lógica de ataque poderá parecer estranha, uma vez que a tecnologia operacional, ou os equipamentos e dispositivos que a compõem, têm normalmente longos ciclos de vida, em muitos casos ultrapassando os 20 anos de longevidade, conduzindo à existência de sistemas *legacy*, ou seja, *hardware* ou *software* que já não recebe atualizações ou *patches* de segurança dos seus fabricantes, deixando estes sistemas desprotegidos contra novas vulnerabilidades¹⁰³⁶. No entanto, a maioria dos ataques concretizados nos ambientes TO começaram com acessos ganhos através do ambiente TI¹⁰³⁷, em casos onde os dois já estão integrados e interligados. Assim, a convergência entre os ambientes TI e os ambientes TO (por norma, menos seguros devido à falta de atualizações de segurança ou de capacidades de cifragem), acaba por se traduzir, na maioria dos casos, numa maior superfície de ataque para os agentes de ameaça, superfície essa onde os agentes de ameaça poderão interferir com a qualidade da água e respetivas redes de distribuição. Explorar-se-ão estas questões em maior detalhe no subcapítulo seguinte (

¹⁰³⁶ Keith Stouffer et al., “NIST SP 800-82r3: Guide to Operational Technology (OT) Security”, 37.

¹⁰³⁷ Amin Hassanzadeh et al., “A Review of Cybersecurity Incidents in the Water Sector”, *Journal of Environmental Engineering* 146 (25 de julho de 2020): 3, <https://arxiv.org/pdf/2001.11144>.

6.2. Ameaças).

6.2. Ameaças

Tal como indicado no subcapítulo anterior, um ciberataque à infraestrutura de um fornecedor de água potável pode traduzir-se em manipulações mal-intencionadas na qualidade da água ou no próprio fornecimento da mesma, o que pode ter diversos impactos negativos, diretos e indiretos. Segundo o relatório “*Cybersecurity Risk & Responsibility in the Water Sector*”, produzido pela *American Water Work Association*, em 2019, os efeitos de ciberataques nas infraestruturas de abastecimento de água potável podem resultar em contaminações, mau funcionamento operacional e comprometer serviços de emergência como bombeiros ou serviços médicos¹⁰³⁸. O mesmo relatório menciona, para além destes impactos, os relacionados com o acesso indevido a dados sensíveis de clientes e colaboradores detidos pelas entidades de fornecimento e distribuição de água potável, acabando por tornar este um setor atrativo para a realização de ciberataques¹⁰³⁹.

De acordo com um infográfico elaborado em outubro de 2021 pela Cybersecurity and Infrastructure Security Agency (CISA), dos Estados Unidos, as organizações de fornecimento e distribuição de água potável estão sujeitas a sofrer alguns ataques/ameaças. Entre os principais ataques estão os ataques de *Ransomware* e os de acesso indevido a dados. Estes ataques estão relacionados com os sistemas de TI e, de acordo com o mesmo infográfico, estes ataques podem ser evitados/reduzidos adotando boas práticas de cibersegurança dentro das redes de TI. Nos casos em que se verifica a convergência das redes de TI com as de TO, a não segmentação de rede pode ser uma ameaça, dado que as redes de TI, mais expostas, podem servir como meio para o acesso a redes de TO que foram integradas com a rede de TI. Uma forma de mitigar o risco associado a esta integração será segmentar adequadamente os sistemas de TI e TO e garantir que nenhum sistema de TO está ligado à Internet. Por último, são indicadas como principais ameaças aos sistemas de TO a falta de manutenção dos mesmos e a complexidade das redes. As medidas indicadas pela CISA passam pela aplicação dos *patches* de segurança nos sistemas e por mapeamentos de rede adequados¹⁰⁴⁰.

Entre os possíveis impactos de ataques concretizados ao setor do fornecimento e distribuição de água potável destacam-se impactos como:

- Envenenamento;
- Falsos alarmes;
- Furto de água;
- Furto de recursos;
- Impacto financeiro;
- Manipulação de controlos;
- Manipulação de dados;
- Perda de dados;
- Poluição ambiental;
- Violação de dados¹⁰⁴¹.

¹⁰³⁸ Judith H. Germano, “Cybersecurity Risk & Responsibility in the Water Sector”, *American Water Work Association*, 2019, 6, <https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf>.

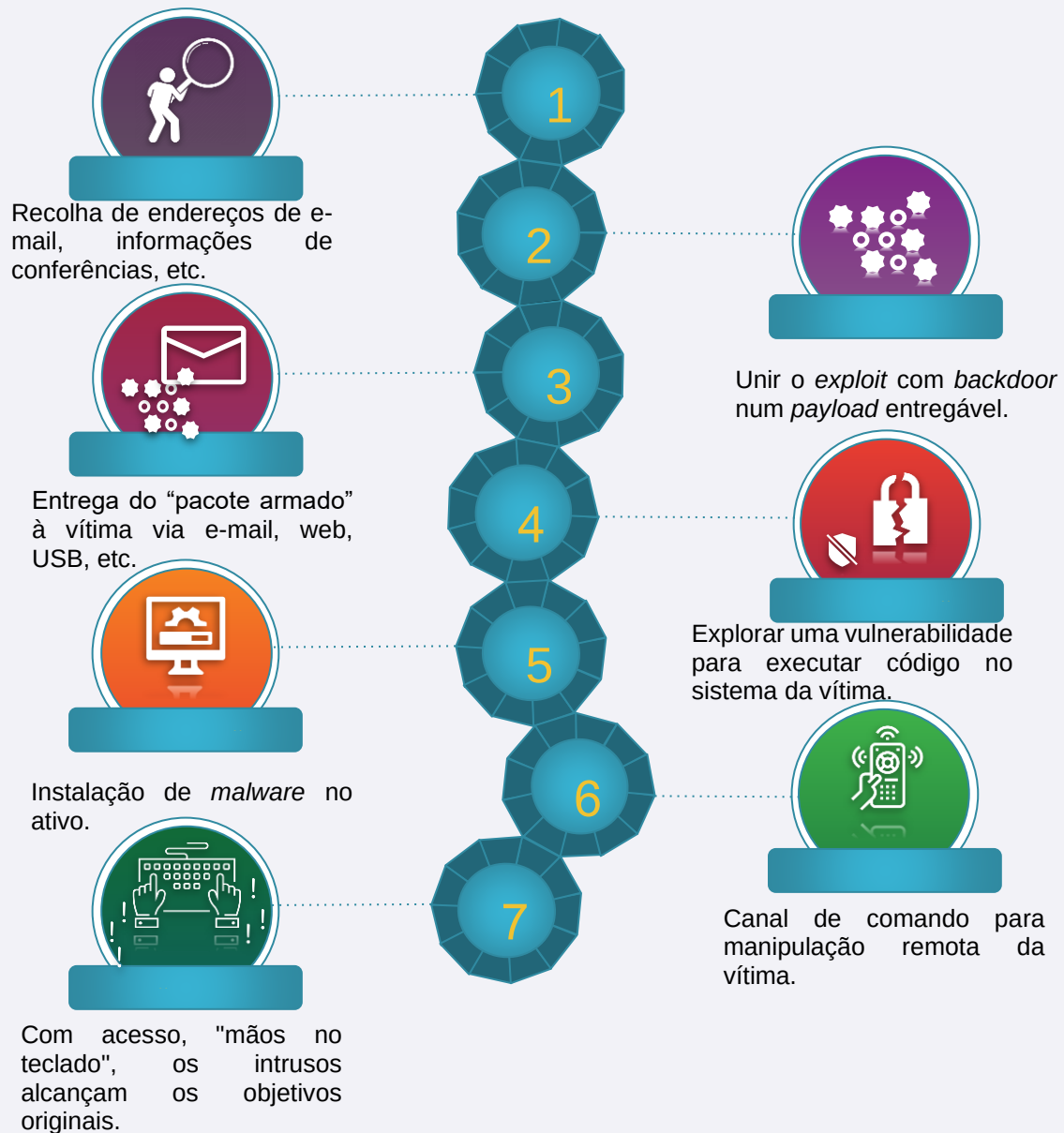
¹⁰³⁹ Germano, “Cybersecurity Risk & Responsibility in the Water Sector”, 6.

¹⁰⁴⁰ “Cyber Risks and Resources for the Water and Wastewater Systems Sector”, CISA, outubro de 2021, <https://www.cisa.gov/sites/default/files/publications/infographic-manage-wastewater-national-critical-function-102021-508.pdf>.

¹⁰⁴¹ Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 13.

Normalmente, um ciberataque tem um ciclo de vida que corresponde à *Cyber Kill Chain* (CKC) que inclui as etapas de Reconhecimento, Armamento (*weaponization*), entrega, exploração, instalação, comando e controlo (C2) e ação nos objetivos.

Figura 11 - Cyber Kill Chain (CKC)

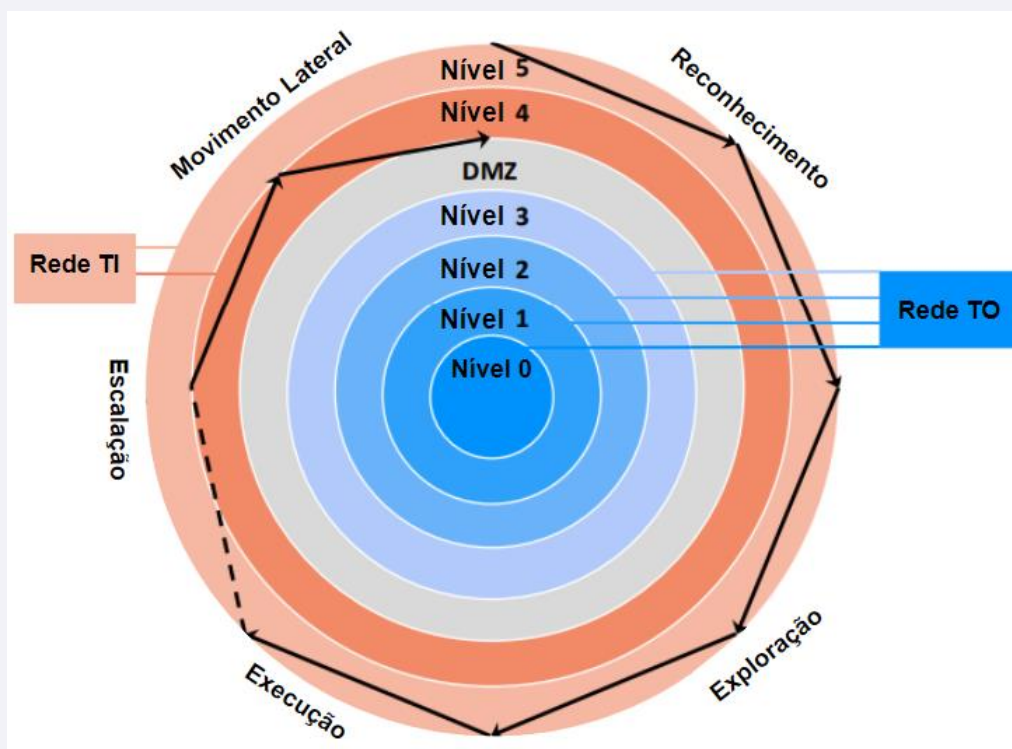


(Fonte: Cyber Kill Chain, *Lockheed Martin*,
<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>)

Nos ambientes industriais, o caminho de ataque é ligeiramente diferente devido à arquitetura destes ambientes. O alvo é, geralmente, um ativo de TO, ao qual o agente de ameaça ganha acesso depois de ter conseguido o acesso através de um dispositivo de TI, sendo o agente de ameaça depois obrigado a mover-se lateralmente ao longo da infraestrutura, e tendo de repetir passos da CKC até chegar ao ativo de TO. Isto é, à medida que o agente de ameaça chega a novos pontos da infraestrutura, poderá ter de voltar a fazer novo reconhecimento, explorar outras vulnerabilidades, voltar a instalar malware e repetir a remoção de restrições e voltar a escalar privilégios para poder prosseguir dentro da rede de uma organização.

Na **Figura 12**, está representado um modelo genérico de ataque em espiral, no qual o nível 5 representa ativos mais expostos publicamente, como servidores *web* ou de *e-mail* e aos quais táticas mais comuns como o *phishing* podem dar acesso inicial. Depois de conseguir o acesso a ativos como estes, o agente de ameaça está dentro da rede da organização e é a partir daqui que se pode mover lateralmente de ativo em ativo, até chegar ao objetivo pretendido. É uma vez chegado aos ativos de TO que o agente de ameaça conseguirá manipular processos críticos na gestão da água¹⁰⁴². Ressalva-se que este modelo é apenas um exemplo e que nem todos os ataques à TO partem necessariamente de ativos publicamente expostos, podendo começar de níveis inferiores, mais próximos do alvo pretendido, como nos casos em que a ameaça é interna à organização. Ver-se-ão exemplos desses na análise a alguns ataques ocorridos no setor.

Figura 12 - Modelo de ataque em espiral em redes onde convergem TI e TO



(Fonte: Amin Hassanzadeh et al, "A Review of Cybersecurity Incidents in the Water Sector", *Journal of Environmental Engineering* 146 (25 July 2020), <https://arxiv.org/pdf/2001.11144>)

¹⁰⁴² Hassanzadeh et al., "A Review of Cybersecurity Incidents", 3-4.

Torna-se assim necessário analisar os ciberataques ocorridos no setor. O estudo “A Review of Cybersecurity Incidents in the Water Sector”, publicado no *Journal of Environmental Engineering*, em 2020, faz uma análise de alguns dos principais ciberataques às redes de distribuição de água realizados até então, nomeadamente nos territórios da Austrália, dos Estados Unidos, do Reino Unido e da União Europeia. Os ataques em análise neste estudo são ataques que tanto visaram interferir com os ambientes TO das entidades distribuidoras de água potável, como com os seus ambientes TI. Abordam-se, de seguida, alguns dos mais relevantes, sobretudo aqueles nos quais foi possível interferir com os ambientes TO das organizações visadas, de modo a fazer-se uma ligação mais próxima com as especificidades tecnológicas deste setor.

O primeiro ataque analisado ocorreu na Austrália, no ano 2000. A entidade atacada - Maroochy Water Services -, processava cerca de 35 milhões de litros de água de esgoto, numa região com cerca de 120 mil habitantes. Entre 1997 e 2000, tinham sido instalados na entidade novos computadores, em todas as 142 estações elevatórias de águas de esgoto, que permitiam controlar remotamente e monitorizar essas estações através do sistema SCADA. No final do mês de janeiro de 2000, começaram a verificar-se falhas nesse mesmo sistema SCADA, tais como perdas de comunicação e de capacidade de controlo das estações, falsos alarmes e configurações alteradas. Estas falhas resultaram na descarga de cerca de um milhão de litros de águas residuais não tratadas no rio, nos parques e nas zonas residenciais. Em março do mesmo ano, a investigação realizada concluiu que a causa das falhas tinha sido interferência humana. Essa interferência vinha de um ex-funcionário da empresa que tinha fornecido os computadores que controlavam remotamente as estações. Esse ex-funcionário tinha-se demitido no mês anterior devido a desentendimentos dentro da sua empresa. Através de um computador do mesmo modelo daqueles que tinham sido instalados, um rádio, um computador portátil, um transformador e diversos cabos, o ex-supervisor foi capaz de causar todas as falhas referidas na tecnologia operacional da entidade visada. No final, as águas infetadas foram limpas, embora tenham sido necessários múltiplos recursos e vários dias para o fazer. O responsável acabou por ser condenado a dois anos de prisão e ao pagamento de pouco mais de 13 mil dólares à Câmara da cidade. Este caso em concreto é um bom exemplo da importância de desativar acessos imediatamente após a saída de funcionários ou colaboradores, assim como da importância de garantir uma boa gestão de ativos e a devolução dos mesmos quando se encerra uma relação laboral¹⁰⁴³.

O segundo incidente analisado refere-se a uma intrusão numa planta de filtragem de água em Harrisburg, Pensilvânia, nos Estados Unidos, em 2006. Segundo a investigação, os agentes de ameaça terão conseguido introduzir um vírus no computador portátil de um funcionário, utilizando este como um ponto de entrada para introduzir vírus nos restantes computadores da planta. Poder-se-á dizer que, por sorte, os responsáveis pela introdução do vírus queriam apenas disseminar e-mails e obter dados de colaboradores, mas, caso o desejassem, poderiam ter afetado as operações da planta de filtragem, por exemplo, alterando os níveis de concentração dos desinfetantes utilizados para tratar a água. Embora não se tenha materializado, este poderia ter sido um caso em que acesso ao ambiente TO teria sido obtido através do ambiente TI. Uma vez descoberto o sucedido, os acessos remotos foram desativados e todas as palavras-passe alteradas¹⁰⁴⁴.

¹⁰⁴³ Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 5.

¹⁰⁴⁴ Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 6.

Outro caso relevante foi o ocorrido com a Autoridade do Canal Tehama-Colusa em 2007 nos EUA. A Autoridade operava, nesse ano, dois canais - Canal Tehama Colusa e Canal Corning - que irrigam as plantações ao longo dos mesmos, ambos recebendo água do rio Sacramento. Neste caso, um eletricitista supervisor da Autoridade acedeu ao computador utilizado para desviar água do rio para o Canal Tehama-Colusa, tendo instalado *software* não autorizado no sistema SCADA e danificado o computador em questão, crê-se, numa tentativa de afetar o fornecimento de água às referidas plantações. As suas ações não surtiram o efeito desejado, uma vez que os canais podiam continuar a ser operados manualmente, evitando estragos. Este caso exemplifica a importância de ter implementados controlos que impeçam a instalação de *software* não autorizado nos sistemas de uma organização. Este foi também o segundo caso de um ataque perpetrado por alguém da organização afetada, embora aqui se tratasse ainda de alguém em funções, e não de alguém cujo vínculo laboral tivesse acabado¹⁰⁴⁵. A este propósito, a ENISA elaborou em 2020 um relatório sobre a questão das ameaças internas às organizações. Nesse relatório, categorizam-se diferentes tipos de ameaças internas, tais como colaboradores que tratam indevidamente os dados e informações, violando as políticas de uso, colaboradores que vendem informações confidenciais para ganho próprio, colaboradores que o fazem para beneficiar entidades externas, e colaboradores amargurados que desejam apenas prejudicar as suas organizações¹⁰⁴⁶. Pode-se também ler que, em 65% dos casos, as organizações que sofrem ataques internos são fortemente impactadas a nível reputacional e financeiro e que, em média, o custo anual de um ataque interno é de 11,450 milhões de euros¹⁰⁴⁷.

Outros ataques de relevo registaram-se também num passado mais próximo. Serão referidos ataques ocorridos em territórios como o de Israel e da Rússia. De seguida, descrevem-se esses ataques por ordem cronológica.

Israel sofreu um ataque em abril de 2020, mais concretamente um ataque de cloro nos abastecimentos de água do país. Este ataque teve como porta de entrada os PLCs (controlos lógicos programáveis) e, depois de os agentes de ameaça terem acesso aos mesmos, conseguiram tomar controlo da rede de abastecimento de água. Apesar disto, o governo israelita conseguiu evitar quaisquer consequências¹⁰⁴⁸. Em maio do mesmo ano, foi detetado outro ataque às estruturas de fornecimento de água de Israel. Este ataque foi, alegadamente, protagonizado por agentes de ameaça ligados ao governo do Irão. O ataque teve como alvo os computadores que controlam o fluxo de água e o tratamento da mesma em dois distritos rurais, sendo que as forças israelitas declararam que conseguiram detetar o ataque a tempo e, com isso, evitar quaisquer consequências danosas do mesmo¹⁰⁴⁹. O modo como o acesso aos PLCs foi obtido nunca foi oficialmente revelado, mas as hipóteses avançadas mais credíveis apontam para que o acesso inicial tenha sido obtido através de *routers* de rede móvel, comumente utilizados por fornecedores de água locais para fazer a comunicação entre sistemas ou através de ataques de *spear phishing* a prestadores terceiros com baixos níveis de segurança, mas com acesso legítimo aos sistemas dos fornecedores de água¹⁰⁵⁰.

¹⁰⁴⁵ Hassanzadeh et al., "A Review of Cybersecurity Incidents", 6-7.

¹⁰⁴⁶ "ENISA Threat Landscape: Insider Threat", ENISA, abril de 2020, 2, <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-insider-threat>.

¹⁰⁴⁷ "ENISA Threat Landscape: Insider Threat", ENISA, 3.

¹⁰⁴⁸ Joby Warrick e Ellen Nakashima, "Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran", *Washington Post*, 8 de maio de 2020, https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.

¹⁰⁴⁹ "Attack on Israeli water utilities", *Council on Foreign Relations*, maio de 2020, <https://www.cfr.org/cyber-operations/attack-israeli-water-utilities>

¹⁰⁵⁰ Eduard Kovacs, "Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources", *Security Week*, 30 de abril de 2020, <https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources/>.

Uma empresa de gestão de águas com base em Rosvodokanal na Rússia foi atacada, alegadamente, por um grupo ucraniano. Este ciberataque ocorreu em dezembro de 2023 e teve como objetivo destruir toda a infraestrutura de TI da empresa, tendo sido apagados mais de 50 TB de dados como documentos de gestão internos, *backups* e as proteções de cibersegurança. Alegadamente, este ataque foi uma resposta ao ataque russo contra as telecomunicações ucranianas que também ocorreu em dezembro do mesmo ano¹⁰⁵¹.

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos¹⁰⁵², de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal¹⁰⁵³.
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa¹⁰⁵⁴.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável¹⁰⁵⁵.
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso¹⁰⁵⁶. No caso, consideraram-se os colaboradores internos maliciosos.

¹⁰⁵¹ "Significant Cyber Incidents", Center for Strategic & International Studies, <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.

¹⁰⁵² CNCS, "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/observatorio/#relatorios>.

¹⁰⁵³ CNCS, "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021", maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>.

¹⁰⁵⁴ CNCS, "Relatório Riscos & Conflitos 2021", 75.

¹⁰⁵⁵ CNCS, "Relatório Riscos & Conflitos 2021", 75-76.

¹⁰⁵⁶ CNCS, "Relatório Riscos & Conflitos 2021", 76-77.

Tabela 50 - Agentes de ameaça mais prováveis (Fornecimento e distribuição de água potável)

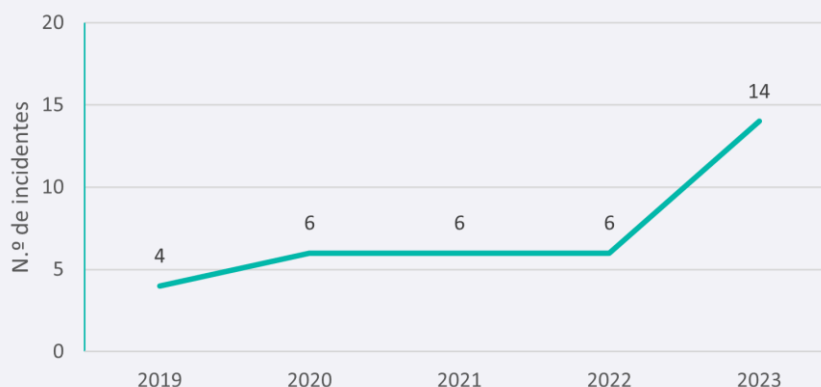
Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
<i>Ransomware</i>	■	■	■	■
<i>Malware</i>	■	■	■	■
Vulnerabilidades	■	■	■	■
<i>Phishing, Spear Phishing e Smishing</i>	■	■	■	
Manipulação de Sistemas (TO)	■	■		■
Manipulação de Sistemas (TI)	■	■		■
Contaminações	■	■		

Legenda:

■ - Agente de ameaça provável

No que diz respeito a ataques ao setor em Portugal, os dados obtidos pelo CNCS, tanto através do questionário dirigido aos Operadores de Serviços Essenciais, como dos registados pelo CERT.PT, indicam uma baixa incidência. A maioria dos operadores inquiridos no setor (76%) respondeu não ter sofrido qualquer incidente em contexto de segurança TIC. O próprio CERT.PT foi, entre 2019 e 2023, notificado de um máximo de 14 incidentes em cada ano (quatro incidentes em 2019, seis incidentes em cada um dos anos entre 2020 e 2022 e 14 incidentes em 2023)¹⁰⁵⁷.

Figura 13 - Número de incidentes no setor da Água anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, Obtido a 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

¹⁰⁵⁷ CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>.

Mesmo quando sofrem ciberataques, os operadores portugueses têm sido capazes de evitar males maiores. Em Portugal, as instituições afetadas foram divididas igualmente entre públicas e privadas, com destaque para o caso da Águas do Porto, por exemplo, quando a Águas do Porto foi atacada a 30 de janeiro de 2023, o ataque não afetou a operação de serviços públicos essenciais, tendo apenas conduzido à interrupção temporária de alguns serviços de atendimento aos cidadãos¹⁰⁵⁸.

¹⁰⁵⁸ “Comunicado: Águas e Energia do Porto alvo de ataque informático”, Águas e Energia do Porto, 8 de fevereiro de 2023, <https://aguasdoporto.pt/noticias/comunicado-aedp-ataqueinformatico>.

6.3. Capacitação

Embora haja ainda um longo caminho a percorrer em matéria de cibersegurança no setor, os operadores têm vindo a incluir o reforço da aposta no digital, na segurança dos sistemas de informação e na cibersegurança como prioridades estratégicas nos seus planos de atividades. Parte desse reforço passa pela formação dos colaboradores em cibersegurança. Em 2022, o Grupo Águas de Portugal deu início à concretização de um plano transversal de formação com temas basilares como ética, *corporate governance* e cibersegurança. A base para a formação em cibersegurança foi o curso “Cidadão/ã Ciberseguro”, disponibilizado gratuitamente em formato *e-learning* pelo CNCS na plataforma NAU, que permitiu sensibilizar os formandos para a temática no contexto familiar, profissional e público. Em 2022, 1500 colaboradores frequentaram a formação, e estava prevista a adição de mais conteúdos à formação para o ano de 2023¹⁰⁵⁹. Mais dados relativos à formação no ano de 2023 não estavam ainda publicamente disponíveis à data da elaboração deste relatório. O Estado português tem também procurado incentivar a capacitação das várias vertentes do setor, nas quais se inclui a cibersegurança.

Foi observada uma melhoria no setor nos últimos 30 anos, existindo, ainda assim, algumas falhas que precisam de ser colmatadas, nomeadamente a gestão das águas residuais. Para responder a essas falhas, o Estado português criou o Plano Estratégico para o Abastecimento de Água e Gestão de Águas Residuais e Pluviais 2030 (PENSAARP 2030). Este Plano estabelece as diretrizes principais para o setor na próxima década e apela ao alinhamento de todos os seus atores, promovendo uma convergência de esforços e ambição. O PENSAARP 2030 é constituído por dois volumes: o Plano Estratégico, com as grandes linhas de orientação, e o Plano de Ação, com o detalhe das medidas preconizadas e respetivas métricas e incentivos¹⁰⁶⁰.

O PENSAARP 2030 estabelece quatro objetivos estratégicos - o Objetivo A: Eficácia dos serviços; o Objetivo B: Eficiência dos serviços; o Objetivo C: Sustentabilidade dos serviços; Objetivo D: Valorização económica, ambiental e societal dos serviços¹⁰⁶¹. Estes objetivos subdividem-se depois em vários outros, que são operacionalizados por diversas medidas. Para os fins deste relatório, importam sobretudo o “Objetivo A4: Segurança, resiliência e ação climática” e o “Objetivo B2: Organização, modernização e digitalização”, operacionalizados pelas medidas M16 e M29, respetivamente.

¹⁰⁵⁹ Águas de Portugal, “Relatório e Contas 2022”, 26, https://www.adp.pt/pt/media/publicacoes/relatorios-e-contas/downloads/file597_pt.pdf.

¹⁰⁶⁰ Conselho de Ministros, “PENSAARP 2030”, versão de consulta pública, 1-2, https://apambiente.pt/sites/default/files/SNIAMB_Aqua/DRH/PlaneamentoOrdenamento/PlanosSetoriais/SetorUrbano/PENSAARP2030/PENSAARP_2030_Volume1.pdf.

¹⁰⁶¹ Conselho de Ministros, “PENSAARP 2030”, 19.

A medida “M16 - Reforço da segurança e da resiliência dos sistemas”, associada ao Objetivo A4, assenta na promoção de “intervenções construtivas e operacionais no reforço da segurança e da resiliência dos sistemas de abastecimento de água e de águas residuais e pluviais, quer para prevenir acessos não autorizados a equipamentos, instalações, materiais, documentos e sistemas de informação e de gestão, que colocam em risco a prestação dos serviços, quer para reduzir a vulnerabilidade dos mesmos a catástrofes naturais e provocadas, como cheias, secas, incêndios nos espaços rurais, sismos e ataques cibernéticos (cibersegurança), ataques terroristas, e de preparação das respetivas respostas e recuperação, por exemplo através da interligação de sistemas de distribuição ou da otimização da gestão de albufeiras”¹⁰⁶². Foram ainda identificados, como incentivos necessários para a prossecução desta medida, “a elaboração de guias técnicos sobre planos de segurança e resiliência dos sistemas, incluindo planos tipo; elaboração de cadernos de sensibilização para decisores sobre planos de segurança e resiliência; formação e capacitação em segurança e resiliência dos sistemas; ações de apoio à inovação sobre soluções tecnológicas de melhoria da segurança e resiliência dos sistemas”¹⁰⁶³.

Por sua vez, a medida “M29 - Modernização e digitalização dos serviços”, associada ao Objetivo B2, coloca o seu foco na eficiência de processos e procedimentos, enfatizando a necessidade de agilizar procedimentos internos e de fazer uma “maior utilização de equipamento e ferramentas automáticas de recolha de dados em tempo real, processamento de informação, *big data*, reporte, gestão do risco, apoio à decisão e sistemas de alerta, numa perspetiva mais preventiva e menos reativa”, enquanto simultaneamente se prepara a integração da rede 5G, “que permitirá ao setor beneficiar de mais velocidade, maior cobertura e mais recursos, mais equipamentos ligados e menor latência destes, com menos consumo de energia”. Como incentivo necessário, identificou-se apenas a necessidade de “alteração da legislação sobre digitalização de alguns procedimentos nos serviços”¹⁰⁶⁴.

Espera-se que a prossecução destes objetivos e a implementação destas medidas conduzam o setor a uma maior maturidade e resiliência em cibersegurança, capacitando o mesmo para lidar com as ciberameaças atuais e futuras

¹⁰⁶² Conselho de Ministros, “PENSAARP 2030”, 37.

¹⁰⁶³ Conselho de Ministros, “PENSAARP 2030”, 37-38.

¹⁰⁶⁴ Conselho de Ministros, “PENSAARP 2030”, 41.

6.4. Investimento em cibersegurança

Através da análise dos planos de atividades e orçamentos e dos relatórios de contas de diversas entidades, é possível verificar que apesar de o reforço do digital, incluindo a cibersegurança e a resiliência, fazer parte dos objetivos estratégicos a prosseguir, raros são os casos em que de facto se regista um investimento direto na área de cibersegurança.

Alguns desses raros casos são os da EPAL, da Águas e Energia do Porto, da Águas do Norte, da Águas do Algarve e da Águas do Alto Minho.

A EPAL realizou um investimento no valor de 3.249.870 euros para o desenvolvimento de ferramentas de analítica avançada de dados e diagnóstico e uma arquitetura de cibersegurança alinhada com a certificação ISO/IEC 27001, numa empreitada adjudicada à empresa Siemens¹⁰⁶⁵.

A Águas e Energia do Porto definiu, para o período compreendido entre 2022 e 2024, um investimento anual de cerca de 300 mil euros, que abrange diversas soluções integradoras e de suporte aos processos, tais como telemetria, infraestrutura de redes, redundância de informação, servidores, armazenamento, CCTV e controlo de acessos (físicos e a dados) e renovação dos equipamentos usados pelos colaboradores¹⁰⁶⁶.

Concomitantemente, a entidade candidatou-se também ao programa de financiamento comunitário “*Connecting Europe Facility – Telecom*”, para apoio ao desenvolvimento de capacidades operacionais na área da cibersegurança e implementação da Diretiva NIS, tendo sido aprovada a atribuição de um incentivo não reembolsável de 75% das despesas elegíveis, num projeto com um custo global de 292 230 euros, executado entre agosto de 2020 e agosto de 2022, que contou com a implementação de sistemas (*software*, *hardware* e soluções de gestão de informação) com o intuito de alcançar os níveis de segurança tecnológica necessários para proteger todas as redes e infraestruturas da Águas e Energia do Porto¹⁰⁶⁷.

Em 2021, a Águas do Norte foi outra candidata ao mesmo programa de financiamento que conseguiu também obter o apoio desejado ao seu plano de cibersegurança. O plano rondava também os 300 mil euros de investimento e os objetivos do mesmo passavam pela criação de um SOC com base nas plataformas SIEM (*Security Information and Event Management*) e em IA, de modo que a entidade conseguisse monitorizar todo o ecossistema, identificando e adaptando-se continuamente às ameaças de cibersegurança mais evoluídas, melhorando as suas capacidades técnicas e operacionais em matéria de cibersegurança. A Águas do Norte pretendia ainda que a solução tivesse a capacidade de fornecer informações relevantes para as partes interessadas em cibersegurança, nacionais e internacionais.¹⁰⁶⁸

¹⁰⁶⁵ Catarina Eusébio, Joaquim Baetas e Ana Conde, “Investimentos já em pleno desenvolvimento, com construção de infraestruturas ou contratualizados”, *Águas Livres* n.º 298, maio de 2022, <https://www.epal.pt/EPAL/docs/default-source/epal/newspaper-2014/2022/05-2022.pdf>.

¹⁰⁶⁶ Águas e Energia do Porto, “Instrumentos de Gestão Previsional 2022-2024”, 60, <https://aguasdoporto.pt/files/uploads/cms/adp/24/files/1647269981-EVymV2FxC3.pdf>.

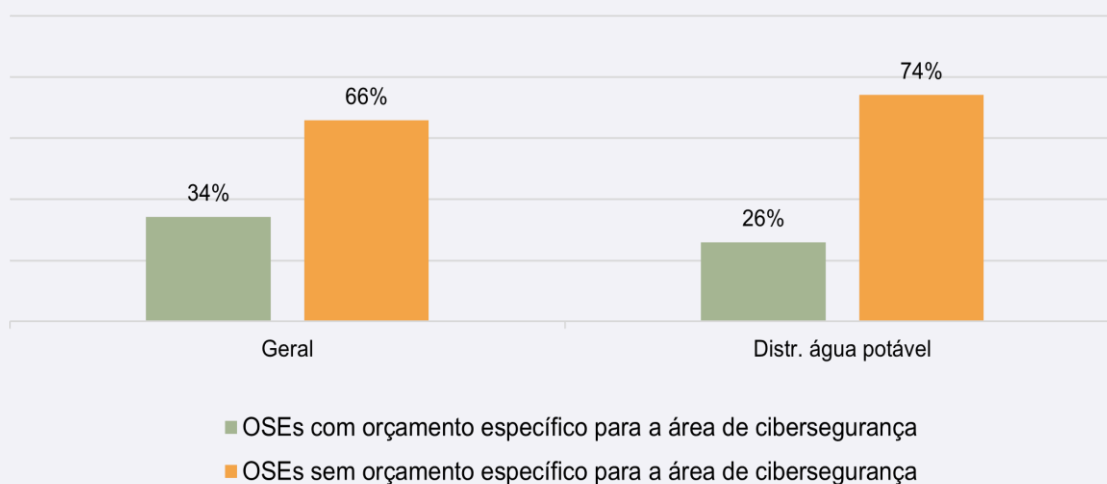
¹⁰⁶⁷ Águas e Energia do Porto, “Instrumentos de Gestão Previsional 2022-2024”, 60-61.

¹⁰⁶⁸ “Águas do Norte inicia implementação de um Security Operations Center”, *Computer World - Especial Cibersegurança*, 2021, 36.

Outras entidades, como a Águas do Algarve, não fazem menções específicas ao investimento em cibersegurança, mas indicam ter investido entre 95.000 e 98.000 euros em assessoria informática¹⁰⁶⁹. As Águas do Alto Minho, por sua vez, investiram na telegestão, tendo lançado o concurso para a contratação do *software* e *hardware* para a sala de comando de telegestão e respetiva instalação num valor aproximado de 800 mil euros. Nota-se ainda o investimento em *software* e serviços conexos para a solução de gestão documental no valor de cerca de 13 mil euros¹⁰⁷⁰.

Deste setor, cerca de 26% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança

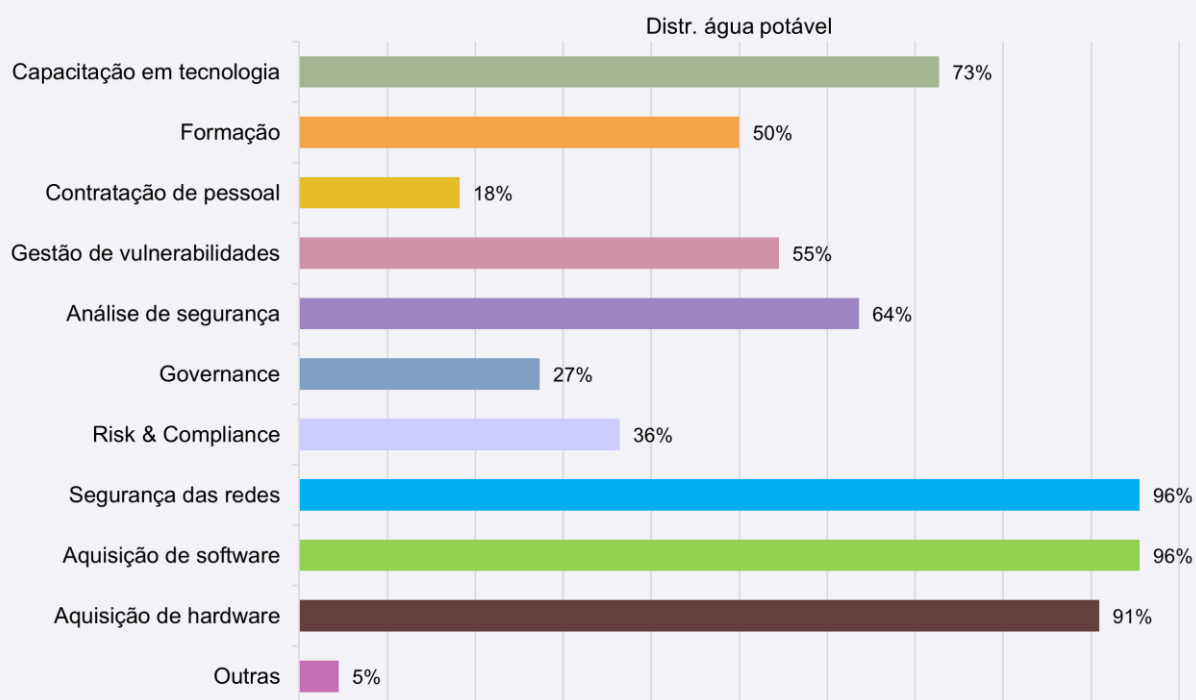


¹⁰⁶⁹ Águas do Algarve, “Plano de Atividades e Orçamento para o ano de 2022 (e projeções para 2023 e 2024)”, 106, https://www.aguasdoalgarve.pt/sites/aguasdoalgarve.pt/files/paginas_base/inf_financeira/pao-2022_28_10_2021_signedca_signed.pdf.

¹⁰⁷⁰ Águas do Alto Minho, “Relatório & Contas 2022”, 72 e 82, <https://adam.pt/component/phocadownload/category/23-relatorio-e-contas?download=262:2022-relatorio-e-contas>.

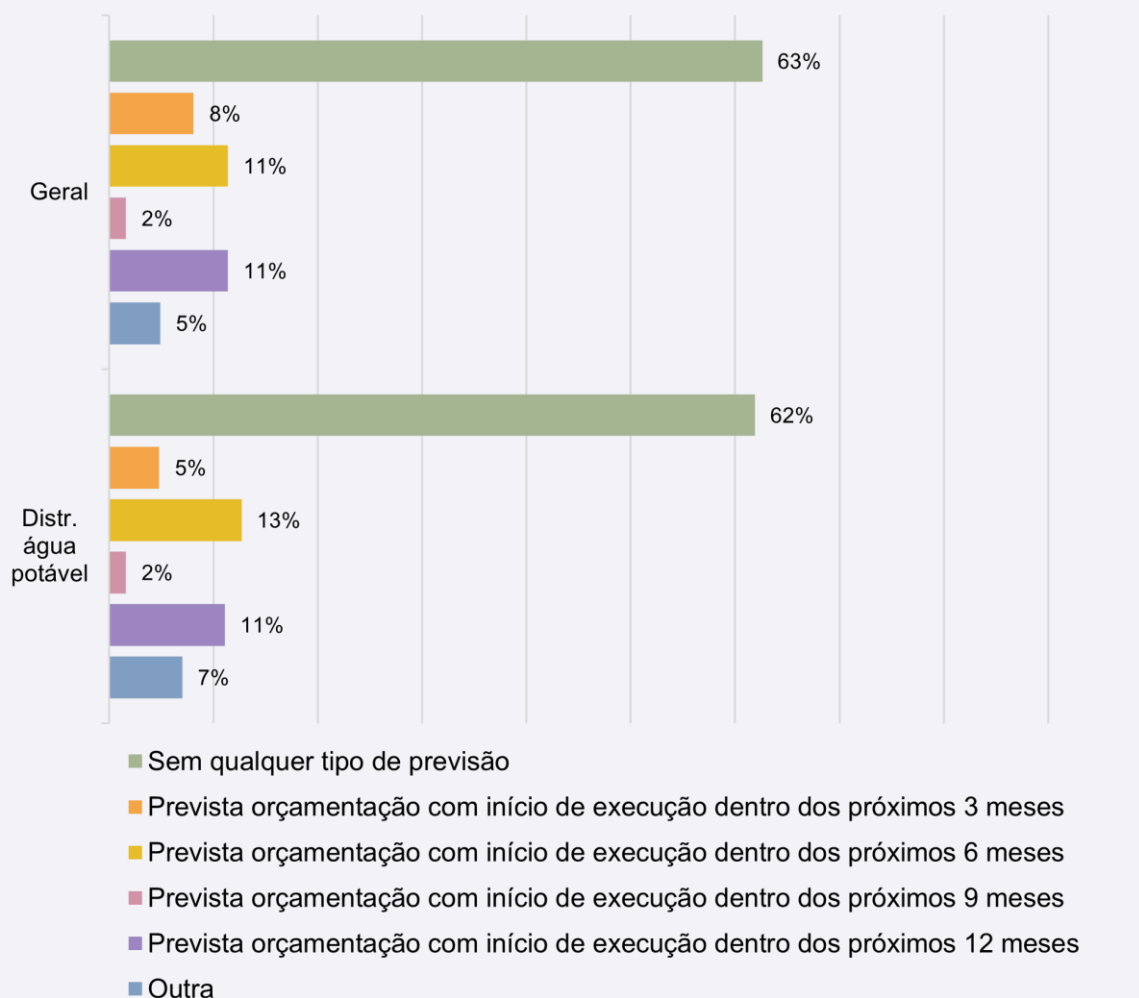
Relativamente às áreas de aplicação do orçamento de cibersegurança, 96% aplica na segurança das redes, 73% na capacitação em tecnologia e aquisição de *hardware* e 55% em gestão de vulnerabilidades, 64% em análise de segurança e cerca de 90% em aquisição de *software* e *hardware*. Em comparação com a média geral, este setor tem uma menor análise de segurança e gestão de vulnerabilidades. Por outro lado, tem está na média na capacitação em tecnologia e superior na aquisição de *software* e *hardware*. (Gráfico 110.5).

Gráfico 110.5 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 62% não tem qualquer previsão para a orçamentação, 5% tem previsto a orçamentação dentro dos próximos 3 meses, 13% tem previsto a orçamentação para os próximos 6 meses e 11% tem previsto a orçamentação para os próximos 12 meses. Este setor está dentro da média geral, a maior diferença, cerca de 3%, está na orçamentação com início de execução dentro dos próximos 6 meses (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Como se viu em **6.3. Capacitação**, o recurso a soluções formativas de carácter gratuito pode ser uma das causas que leva a que se verifique menos investimento expresso na área de cibersegurança.

6.5. RJSC e legislação setorial

O setor do fornecimento e distribuição de água potável não é um setor que possua uma vasta legislação setorial em matéria de cibersegurança. Alguma legislação setorial, tal como a Lei da Água (Lei n.º 58/2005), que transpõe a Diretiva n.º 2000/60/CE, do Parlamento Europeu e do Conselho, de 23 de outubro obriga os operadores deste setor a “proteger e melhorar o estado dos ecossistemas aquáticos”, a “promover uma utilização sustentável de água” e a “assegurar o fornecimento em quantidade suficiente de água de origem superficial e subterrânea de boa qualidade”¹⁰⁷¹, mas não faz qualquer menção específica à cibersegurança, segurança informática ou segurança da informação. Menciona, no entanto, a “proteção e valorização dos recursos hídricos”, bem como a “prevenção e a proteção contra riscos de cheias e inundações, de secas, de acidentes graves de poluição e de rotura de infra-estruturas hidráulicas”¹⁰⁷², de onde se pode subentender a necessidade fortalecer a componente de cibersegurança por parte dos operadores.

Existe também o Decreto-Lei n.º 306/2007, de 27 de agosto, que estabelece o regime da qualidade da água destinada ao consumo humano e impõe obrigações como a da implementação de um programa de controlo de qualidade da água ou de um Plano de Segurança da Água (PSA). Um PSA é suportado pela análise de perigos e avaliação do risco efetuada sistematicamente ao longo do sistema de abastecimento de água, desde a captação de água bruta, passando pelo processo de tratamento da água, pela rede de distribuição e rede predial até à torneira dos consumidores”¹⁰⁷³. É uma ferramenta que auxilia a mitigação, a redução e o controlo dos riscos associados às operações necessárias para distribuir de forma ininterrupta e segura água de qualidade aos consumidores, incluindo os riscos de cibersegurança.

Conta-se, ainda, com a Diretiva (UE) 2016/1148 (Diretiva NIS)¹⁰⁷⁴, publicada em 2016, e cuja transposição deu origem ao Regime Jurídico da Segurança do Ciberespaço, através da Lei n.º 46/2018, de 13 de agosto¹⁰⁷⁵, e do Decreto-Lei que a regulamenta, o Decreto-Lei n.º 65/2021, de 30 de julho¹⁰⁷⁶. O RJSC acaba assim por se qualificar como o primeiro diploma legal que de facto impõe obrigações ao nível da cibersegurança de forma direta neste setor, tais como a nomeação de um contacto permanente para articulação com o CNCS, a nomeação de um responsável de segurança, a elaboração de um inventário de ativos, de um plano de segurança, de um relatório anual, de análise, gestão e tratamento do risco, e de notificação de incidentes¹⁰⁷⁷. Apesar do elevado nível de cumprimento de algumas destas obrigações, verifica-se que 47% dos OSE inquiridos ainda não realizam anualmente avaliações de risco de cibersegurança e que 57% não possuem qualquer tipo de plano de resposta a incidentes de cibersegurança, segundo os dados obtidos através do questionário realizado.

¹⁰⁷¹ Lei n.º 58/2005 de 29 de dezembro (Lei da Água), *Diário da República*, 1.ª série - n.º 249, 29 de dezembro de 2005. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1191&tabela=leis&ficha=1&pagina=1.

¹⁰⁷² Lei n.º 58/2005 de 29 de dezembro (Lei da Água).

¹⁰⁷³ “Plano de Segurança da Água”, Avaliação do Risco, ERSAR, <https://www.ersar.pt/pt/o-que-fazemos/controlo-da-qualidade-da-agua/avaliacao-do-risco>.

¹⁰⁷⁴ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, *Jornal Oficial da União Europeia*, 1, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148>.

¹⁰⁷⁵ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

¹⁰⁷⁶ Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

¹⁰⁷⁷ Decreto-Lei n.º 65/2021, artigos 4.º a 15.º.

O setor está ainda obrigado ao cumprimento da Diretiva (UE) 2022/2555¹⁰⁷⁸, ou Diretiva NIS 2, que veio atualizar a Diretiva anterior, passados seis anos sobre a sua publicação. A Diretiva NIS 2 classifica dois tipos de setores: “setores de importância crítica”¹⁰⁷⁹ e “outros setores críticos”¹⁰⁸⁰. Os setores já visados pela Diretiva anterior inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsectores. São também introduzidas novas obrigações.

O setor do fornecimento e distribuição de água potável é um dos setores que recebe algumas modificações. Passa a ser denominado como setor da “água potável” passa-se também a incluir o setor das “águas residuais”, que não era considerado pela primeira Diretiva¹⁰⁸¹.

Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos¹⁰⁸². Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto¹⁰⁸³.

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”¹⁰⁸⁴.

Com a publicação de nova legislação, como a NIS 2, e com novas ações governativas, tal como o PENSAARP 2030, espera-se que a perceção da importância da cibersegurança seja melhorada, e que processos ainda em falta, como o da análise de risco anual, sejam implementados.

¹⁰⁷⁸ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

¹⁰⁷⁹ Diretiva (UE) 2022/2555, Anexo I.

¹⁰⁸⁰ Diretiva (UE) 2022/2555, Anexo II.

¹⁰⁸¹ Diretiva (UE) 2022/2555, Anexo I.

¹⁰⁸² Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

¹⁰⁸³ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

¹⁰⁸⁴ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

6.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor da Água, segundo o relatório “*Mapping of OES Security Requirements to Specific sectors*” da ENISA.

Tabela 51 - Standards e Boas Práticas (Água)

Standards	Boas práticas
• ISO 27001 Information technology - Security techniques - Information security management systems - Requirements • IEC 62443-2-1 • ISO 24512:2024 Activities relating to drinking water and wastewater services - Guidelines for the management of drinking water utilities and for the assessment of drinking water services	• ANSI/AWWA G430-09: Security Practices for Operations and Management • NIST Cybersecurity Framework (CSF) • NIST SP 800-82r3 • EN 15975-2

- **ISO 27001 Information technology - Security techniques - Information security management systems - Requirements:** Estabelece um quadro de políticas e processos para gerir a segurança da informação de forma sistemática, garantindo assim a confidencialidade, integridade e disponibilidade das informações¹⁰⁸⁵;
- **IEC 62443-2-1:** É um conjunto de normas internacionais focadas na segurança de sistemas de controlos e automação industrial. Fornece diretrizes para estabelecer e operar um programa de segurança para sistemas de controlo e automação industrial (IACS), ajuda a mitigar riscos específicos nos sistemas industriais e aborda todo o ciclo de vida de segurança dos mesmos¹⁰⁸⁶;
- **ISO 24512:2024 Activities relating to drinking water and wastewater services - Guidelines for the management of drinking water utilities and for the assessment of drinking water services:** *Standard* para a gestão de serviços de abastecimento de água potável para as populações e meio ambiente. Inclui métodos para avaliar a qualidade e eficiência dos serviços de água potável e promove práticas de gestão, a nível ambiental e de saúde pública¹⁰⁸⁷;

¹⁰⁸⁵ ISO, “ISO/IEC 27001:2022”, <https://www.iso.org/standard/27001>

¹⁰⁸⁶ International Electrotechnical Commission, “Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners”, 2024, <https://webstore.iec.ch/en/publication/62883>.

¹⁰⁸⁷ ISO, “Activities relating to drinking water and wastewater services — Guidelines for the management of drinking water utilities and for the assessment of drinking water services”, 2024, <https://www.iso.org/standard/82490.html>.

- **ANSI/AWWA G430-09: Security Practices for Operations and Management:** Define práticas recomendadas para garantir a segurança física e operacional das instalações e operações de abastecimento de água. Inclui métodos para identificar e mitigar riscos de segurança das operações de água¹⁰⁸⁸;
- **NIST Cybersecurity Framework (CSF):** Utilizado para ajudar as organizações a entender e gerir os riscos de cibersegurança. Está organizado em cinco funções principais: Identificar, Proteger, Detetar, Responder e Recuperar¹⁰⁸⁹;
- **NIST SP 800-82r3:** Guia para a segurança de tecnologia operacional. Fornece orientações detalhadas sobre como proteger sistemas de controlo industrial (ICS) contra ameaças de cibersegurança¹⁰⁹⁰;
- **EN 15975-2:** Guia para a segurança do abastecimento de água potável, gestão de riscos e crises. Inclui orientações para desenvolver e implementar planos de gestão de crises relacionadas ao abastecimento de água¹⁰⁹¹.

¹⁰⁸⁸ American Water Works Association, "Security Practices For Operation And Management", https://webstore.ansi.org/standards/awwa/awwaq43009?srltid=AfmBOopxVXFQqf7_VmKEeA34CyCKDf-czdhzHBps1dxXD8WktOp58Lc.

¹⁰⁸⁹ NIST, "NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral", fevereiro de 2024, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf>.

¹⁰⁹⁰ NIST, "Guide to Operational Technology (OT) Security", 26 de abril de 2022, <https://csrc.nist.gov/pubs/sp/800/82/r3/ipd>.

¹⁰⁹¹ European Standards, "General Information", 14 de agosto de 2023, <https://standards.iteh.ai/catalog/standards/cen/39c119d3-607d-4a49-9ab7-74f51574ab42/en-15975-2-2013?srltid=AfmBOoqHieQKOaJiD8Wnu57c-zFcHTCY1zv392baYX23wWb5a98ws5er>.

6.7. Desafios

Analisando o relatório “*Cybersecurity Risk and Responsibility in the Water sector*”, da *American Water Work Association*, de 2019, é possível verificar que os principais desafios do setor estão relacionados com as infraestruturas que o compõem. Como se viu em 6.1.3. Especificidades tecnológicas, a TO, que muitas vezes inclui sistemas *legacy* que não podem ser integrados com tecnologias mais avançadas e mais seguras, constituem uma fragilidade no setor¹⁰⁹².

Além disso, a gestão das infraestruturas de abastecimento de água é muitas vezes partilhada com entidades municipais que, em Portugal, têm sido alvos preferenciais para a realização de ciberataques¹⁰⁹³.

Acresce ainda que embora se verifique, nos últimos 30 anos, uma elevada evolução dos serviços do setor da água (abastecimento de água e gestão de águas residuais), os desafios que este setor encara baseiam-se na dificuldade que entidades maiores e menores têm em evoluir ao mesmo ritmo, provocando um acentuado desequilíbrio entre entidades mais modernizadas e entidades mais tradicionais.

Tratando-se de um setor que depende diretamente das condições climáticas, todos os impactos, positivos e negativos, que estão associados aos respetivos fenómenos (escassez hídrica, degradação das massas de água, risco de ocorrência de inundações, necessidade de controlo de poluentes emergentes, entre outros) constituem desafios acrescidos à atividade do setor. Além dos desafios ambientais, acrescentam-se a este contexto desafios económicos (oportunidades a explorar e a necessidade de maior circularidade e valorização ambiental e territorial dos serviços) e desafios sociais (adaptabilidade do mercado de trabalho).

Para responder a estes desafios os Estados Unidos da América, por parte do NCCoE (*National Cybersecurity Center of Excellence*, pertencente ao NIST), lançaram um projeto, em junho de 2023, com o objetivo de melhorar a cibersegurança nos sistemas de água e de esgoto. Esta iniciativa concentra-se, em grande parte, em melhorar as soluções práticas utilizando as tecnologias disponíveis. Tais soluções para mitigar riscos de cibersegurança nos sistemas de água e esgoto vão resultar num guia de práticas de cibersegurança da *NIST* que irá ser disponibilizado de forma gratuita a todas as organizações do setor¹⁰⁹⁴.

¹⁰⁹² Germano, “Cybersecurity Risk & Responsibility in the Water Sector”, 14.

¹⁰⁹³ Lusa, “Ciberataques a autarquias aumentam com a transição digital”, *SIC Notícias*, 18 de outubro de 2023, <https://sicnoticias.pt/pais/2023-10-18-Ciberataques-a-autarquias-aumentam-com-a-transicao-digital-e984cece>.

¹⁰⁹⁴ “Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems”, National Cybersecurity Center of Excellence (NCCoE), junho de 2023, 4, <https://www.nccoe.nist.gov/sites/default/files/2023-06/securing-water-and-wastewater-utilities-project-description-final.pdf>.

Neste projeto, os principais desafios de cibersegurança no setor da água e dos esgotos dos Estados Unidos da América foram:

- **Gestão de ativos:** Identificar e categorizar todos os dispositivos na rede de forma a ser possível detetar potenciais riscos de equipamentos vulneráveis;
- **Integridade dos dados:** Proteger a integridade dos dados tanto em trânsito como em repouso. É esperado a criação de métodos para manter essa integridade e, também, fornecer soluções para testes;
- **Acesso remoto:** Detetar possíveis falhas na rede analisando o comportamento da mesma, implementar o controlo e autenticação de acessos externos à rede e garantir a segurança de todos os dispositivos e sistemas;
- **Segmentação da rede:** Isolar a rede para garantir uma maior segurança utilizando produtos com código aberto. Serão também incluídos controlos de segurança na segmentação da rede¹⁰⁹⁵.

As normas e orientações mais relevantes utilizadas neste projeto foram:

- **NIST Cybersecurity Framework (CSF):** Utilizado para ajudar as organizações a entender e gerir os riscos de cibersegurança;
- **NIST SP 800-82r3:** Guia para a segurança de tecnologia operacional;
- **NIST SP 800-53r5:** Catálogo de controlos de segurança e privacidade para sistemas de informação¹⁰⁹⁶.

¹⁰⁹⁵ “Cybersecurity for the Water and Wastewater Sector”, *National Cybersecurity Center of Excellence (NCCoE)*, 6-8.

¹⁰⁹⁶ “Cybersecurity for the Water and Wastewater Sector”, *National Cybersecurity Center of Excellence (NCCoE)*, 11.

6.8. Recomendações

A reconhecida importância do setor do fornecimento e distribuição de água potável, bem como os potenciais efeitos de ciberataques no mesmo, levaram a que a Comissão Europeia elaborasse, em 2022, um plano de segurança da água, cujo principal objetivo é sensibilizar e garantir, junto das autoridades locais, dos proprietários e dos operadores dos sistemas de água, que a sua principal prioridade deve ser o fornecimento ininterrupto de água com qualidade para o consumo humano. Nesse sentido, estes deverão também ter preparado um plano para qualquer tipo de emergência (desastres naturais, ciberataques, pandemias, entre outros) e os planos deverão ter uma série de instruções a indicar como proceder e como é que a emergência em questão pode afetar os sistemas de água¹⁰⁹⁷.

Este plano recomenda a utilização de uma ferramenta para a identificação de possíveis cenários de risco e criar sugestões de forma a reduzir esse mesmo risco. Essa ferramenta denominada *RIDB* (*Risk Identification Database*) ajuda a identificar o tipo de ameaças, a origem dos riscos, a descrição dos eventos e o tipo de consequências que estes podem produzir. O propósito desta ferramenta não é substituir a identificação de riscos por parte das aplicações, mas sim funcionar de forma complementar às mesmas¹⁰⁹⁸.

Relativamente a sistemas de monitorização de incidentes de cibersegurança, o plano indica algumas soluções tais como:

- Sensores de tráfego de rede e sistemas de análise que utilizam algoritmos não supervisionados que, com isto, conseguem criar um modelo de comportamento normal do sistema de água. Caso ocorra uma variação, este sistema consegue detetar um comportamento anómalo e lançar um alerta;
- Um sistema de deteção de dados em tempo real que pode ser usado para garantir a integridade dos dados gerados;
- Implementar um SIEM (*Security Information and Event Management*) que seja capaz de lançar alertas de uma perspetiva de negócio levando em conta todos os eventos gerados¹⁰⁹⁹.

¹⁰⁹⁷ Rui Teixeira et al., "JRC Technical Report: Water Security Plan Implementation Manual for Drinking Water Systems", Comissão Europeia, 3, <https://ec.europa.eu/newsroom/cipr/items/738662/en>.

¹⁰⁹⁸ Teixeira et al., "Water Security Plan Implementation Manual", Comissão Europeia, 11.

¹⁰⁹⁹ Teixeira et al., "Water Security Plan Implementation Manual", Comissão Europeia, 21.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste setor. Tais cenários são indicados na seguinte tabela:

Tabela 52 - Cenários de risco (Água)

Cenários de risco

Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.

Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.

Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO WEB** (SQL Injection ou Cross-site Scripting).

VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.

Um agente de ameaças consegue o acesso às INSTALAÇÕES FÍSICAS da entidade, acedendo indevidamente a dispositivos, furtando material informático e modificando dados sensíveis armazenados.

RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em bitcoins, sob a ameaça da sua destruição ou exposição ao público.

Desenvolvimento de ações de CIBERESPIONAGEM, através de malware ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 23 de setembro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>)

Com base nos resultados obtidos no questionário dirigido aos Operadores de Serviços Essenciais, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor da distribuição de água potável, surgem diversas recomendações que se consideram pertinentes para as entidades do setor, que se apresentam de seguida.

Formação

Os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor disponibilizarem formação em cibersegurança aos seus colaboradores (**Gráfico 38**), as formações são, na maioria dos OSE inquiridos (cerca de 65%) são de caráter facultativo, e não obrigatório (**Gráfico 39**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

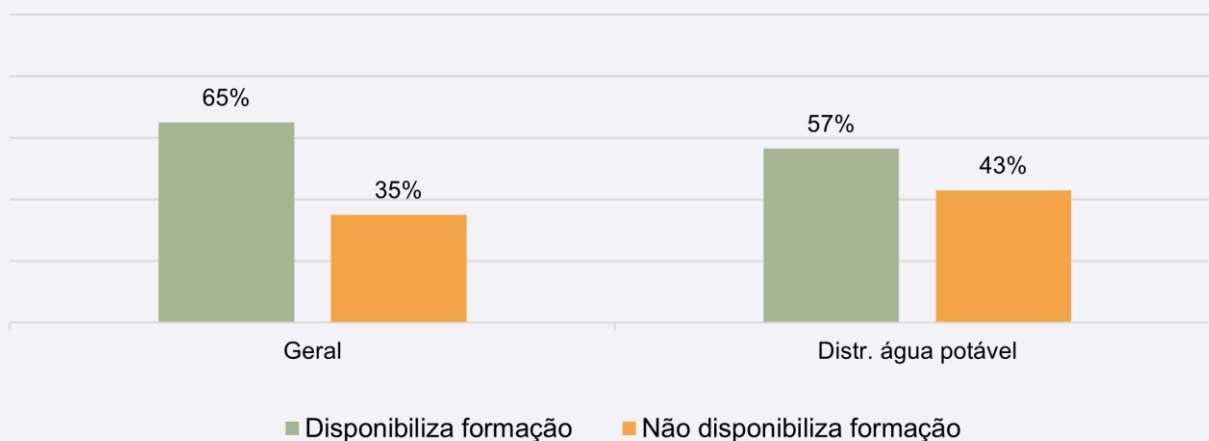
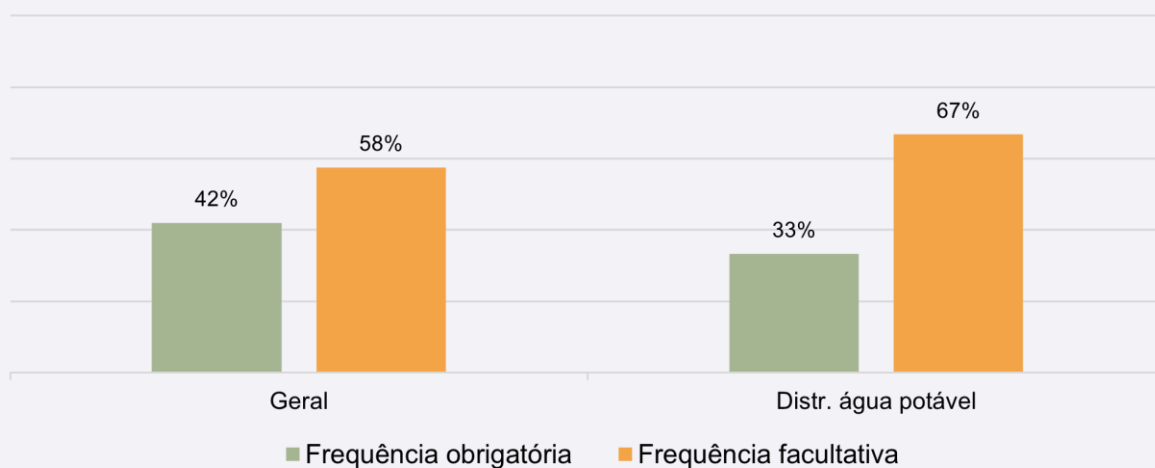
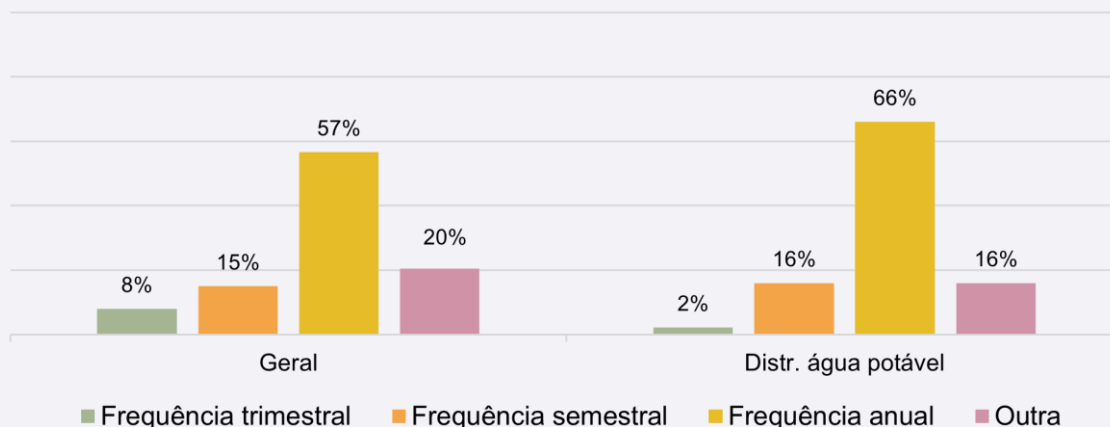


Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



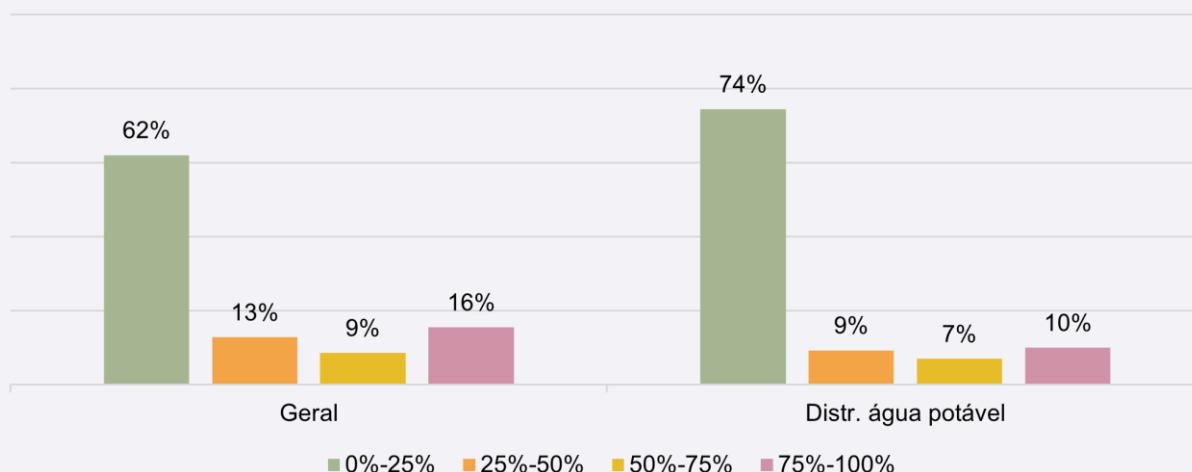
O facto de os momentos de formação serem, na sua maioria, anuais (**Gráfico 41**), sem obrigatoriedade de participação poderá conduzir a que passe demasiado tempo sem que os colaboradores tomem conhecimento sobre boas práticas ou riscos de cibersegurança.

Gráfico 41 - Frequência média dos momentos de formação



O facto de cerca de três quartos dos OSE indicarem que apenas entre 0%-25% dos colaboradores têm formação básica em cibersegurança (**Gráfico 33**) poderá corroborar esta hipótese. Concomitantemente, a maturidade do setor nesta área é considerada, pelo regulador, muito baixa. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória. É importante referir que a existência de cursos de atualização no setor é muito baixa (verifica-se em apenas cerca de um quarto dos inquiridos), sendo que estes tipos de cursos são importantes para manter os colaboradores atualizados para novas ameaças.

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor da distribuição de água potável, comparativamente com os restantes, é um dos setores onde menos se observa a autenticação multifator, a existência de sensibilização sobre segurança, a utilização de sistemas de gestão de palavras-passe, a existência de controlos biométricos para a identificação e autenticação de utilizadores, a implementação de um *SIEM* e a manutenção de *logs* para futura análise após incidentes de cibersegurança.

Nesse sentido, recomenda-se aos OSE do setor da distribuição de água potável que:

- Implementem, onde possível, métodos de autenticação multifator;
- Desenvolvam programas de sensibilização sobre segurança e disponibilizam aos seus colaboradores;
- Utilizem sistemas de gestão de palavras-passe, de modo a viabilizar a utilização de diversas palavras-passe complexas e seguras para cada sistema;
- Implementem, onde possível, controlos biométricos para a identificação e autenticação de utilizadores;
- Mantenham os *logs* durante um período mínimo de 90 dias para ser possível a análise dos mesmos caso ocorra um incidente de cibersegurança.

Políticas, procedimentos e planos de cibersegurança

Com base nos dados reunidos no questionário, apenas 60% dos OSE do setor possuíam políticas e procedimentos de cibersegurança documentados e implementados. Além disso, apenas 43% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Diante desta situação, recomenda-se aos OSE do setor que ainda não o tenham feito que elaborem e implementem uma política de cibersegurança que verse sobre:

- Os diversos papéis e responsabilidades dos vários colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, como os controlos de acesso (lógico e físico);
- A gestão de incidentes, incluindo a elaboração de um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação, além de um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir, que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização periódica da política (pelo menos anualmente), para manter a mesma atualizada conforme a evolução das ameaças de cibersegurança e as mudanças na organização.

Considerando a baixa percentagem de OSE do setor que indicaram possuir uma política de continuidade de negócio (35%), recomenda-se também a elaboração de uma política de continuidade de negócios alinhada com a política de cibersegurança.

Análise de vulnerabilidades e realização de testes de intrusão (*pentesting*)

Apenas cerca de metade (51%) dos OSE do setor da distribuição de água potável realizam procedimentos de deteção e gestão de vulnerabilidades, sendo importante implementar estes procedimentos tendo em vista a diminuição e antecipação de possíveis ataques. A deteção e análise, e correção de vulnerabilidades é uma prática importante para a proteção proativa e preventiva dos sistemas e aplicações em utilização em qualquer setor de atividade.

Quanto à realização de testes de intrusão, embora não exista uma obrigação legal no setor da distribuição de água potável de os realizar, o setor do fornecimento e distribuição de água potável surge como o segundo que menos realiza estes testes (40% dos OSE), somente atrás do setor da saúde. Apesar da baixa incidência de ataques registada, a realização de testes de intrusão é mais uma maneira de identificar vulnerabilidades, corrigi-las e tornar os OSE mais resilientes em matéria de cibersegurança.

Reforço da segurança da Tecnologia Operacional (TO)

Sendo o setor de fornecimento e distribuição de água potável um setor essencial, a segurança da TO é crucial, isto porque envolve sistemas críticos que controlam a distribuição e o tratamento da água para consumo. De forma a reforçar a segurança da Tecnologia Operacional podem ser seguidas algumas recomendações, tais como:

- **Controlar acessos:** Implementar controlos rigorosos de acesso físico aos locais onde se encontram os sistemas de TO, tais como centrais de controlo e instalações de tratamento de água;
- **Monitorizar:** Instalar câmaras de vigilância e sensores de movimento de forma a detetar atividades suspeitas;
- **Segmentação da rede:** Separar as redes de TO das redes de TI de forma a minimizar o risco de algum possível ataque se propagar da rede de TI para a rede de TO;
- **VLANS:** Utilizar VLANS na segmentação do tráfego da rede dentro da infraestrutura TO para isolar as diferentes partes do sistema e assim conter possíveis invasões;
- **IDS/IPS:** Implementar sistemas de deteção e prevenção específicos para TO, de forma a supervisionar e bloquear possível tráfego malicioso;
- **Normas:** Assegurar a conformidade com as normas e regulamentações relevantes, como a ISO/IEC 62443 para a segurança de sistemas de controlo industrial e a ISO/IEC 27001 que fornece diretrizes para implementar melhores práticas na gestão e redução de riscos de cibersegurança.

Implementar, pelo menos, algumas destas recomendações pode ajudar a proteger melhor todas as infraestruturas críticas de TO do setor de fornecimento e distribuição de água potável contra possíveis ameaças de cibersegurança.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*¹¹⁰⁰.

No setor da distribuição de água potável, os controlos fundacionais, relacionados com segurança de rede, desempenham um papel especialmente crítico. Infraestruturas essenciais, como estações de tratamento de água, sistemas de monitorização e controlo de distribuição, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, a disponibilidade e a continuidade dos serviços de abastecimento. Falhas ou configurações inadequadas nesses sistemas podem ser exploradas para interromper o fornecimento de água, adulterar os processos de tratamento, ou comprometer a segurança e a qualidade da água distribuída, colocando em risco a saúde pública e o bem-estar das comunidades.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos¹¹⁰¹:

¹¹⁰⁰ "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls-list>.

¹¹⁰¹ "The 18 CIS Critical Security Controls".

Tabela 53 - Controlos de Segurança da CIS (Distr. Água Potável)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls>)

7. Infraestruturas digitais

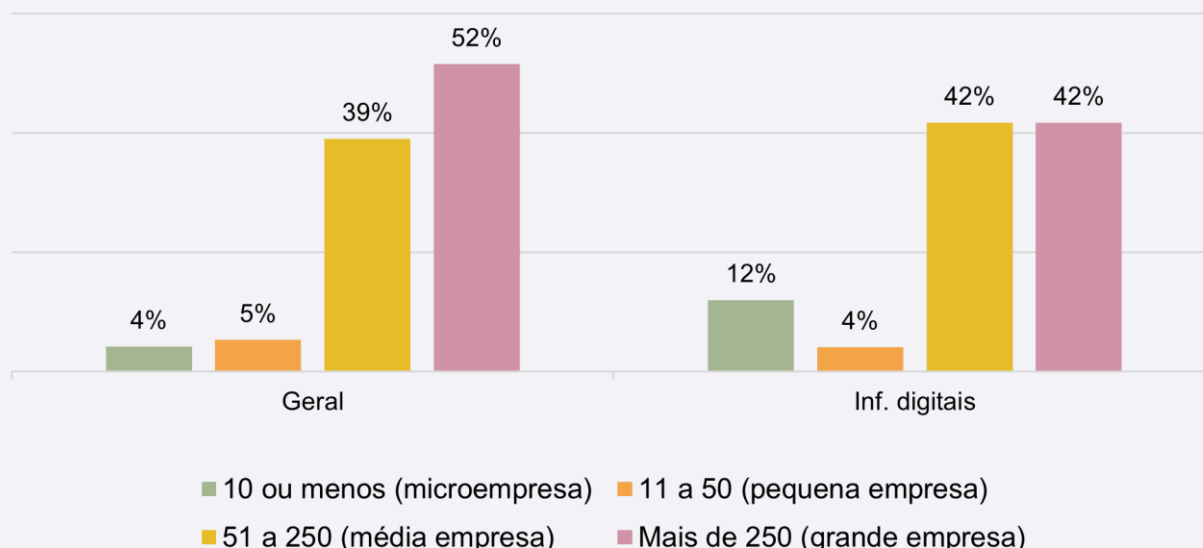
7.1. Contextualização setorial

O setor das infraestruturas digitais refere-se às entidades e aos serviços que são essenciais para o funcionamento das redes e sistemas de informação na União Europeia. No âmbito do Regime Jurídico de Segurança do Ciberespaço (RJSC) e da Diretiva 2016/1148 (NIS), este setor compreende três tipos de entidades: pontos de troca de tráfego (Internet Exchange Points: IXP), fornecedores de serviços de DNS e registos de nomes de domínio de topo¹¹⁰². O desenvolvimento deste setor em Portugal tem-se devido sobretudo à ação de duas entidades: a Fundação para a Computação Científica Nacional (FCCN) e a associação DNS.PT.

¹¹⁰² Diretiva (UE) 2016/1148, Anexo II: Tipos de entidades para efeitos do artigo 4.º, ponto 4, *Jornal Oficial da União Europeia*, 19 de julho de 2016, 29, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L1148>

Segundo o questionário realizado, foi possível aferir que este setor é sobretudo composto por grandes e médias empresas, representando estas 84% dos operadores do setor, com as pequenas e microempresas a constituírem a restante minoria (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



Também segundo os dados obtidos através do questionário, foi possível verificar que o regulador do setor considera que a maturidade deste em cibersegurança é média, uma perceção que pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores. Este é o setor que menos operadores tem a disponibilizar formação (42%), abaixo da média dos setores (65%). As medidas menos adotadas pelo setor foram: Ter uma equipa especialista em cibersegurança (16% dos inquiridos), utilização de controlos biométricos para a identificação e autenticação dos utilizadores (também 16%), operadores que apostam nas formações de sensibilização em cibersegurança (28%). Apenas uma pequena minoria dos operadores dedicam orçamentos específicos à área de cibersegurança (17% contra 34% no geral dos setores). É também um setor que, por enquanto, se mantém com uma taxa de incidentes cibersegurança abaixo dos 50%, com 33% dos inquiridos a já terem sofrido um incidente.

Pontos de Troca de Tráfego

De acordo com o disposto na Diretiva NIS, “a função de um ponto de troca de tráfego consiste em interligar redes. Os pontos de troca de tráfego não proporcionam o acesso às redes nem atuam como prestadores ou operadores de tráfego. Os pontos de troca de tráfego também não prestam outros serviços não relacionados com interligação, embora isso não impeça o operador de um ponto de troca de tráfego de prestar também serviços não conexos. Os pontos de troca de tráfego existem para interligar redes que estejam separadas em termos técnicos e organizativos”¹¹⁰³. Por outras palavras, pontos de troca de tráfego são “terrenos comuns” de rede Internet Protocol (IP), onde ocorre troca de tráfego entre diferentes organizações, permitindo que os fornecedores de serviços de Internet neles incluídos troquem dados destinados às suas respetivas redes e que essas redes se possam interligar da forma mais eficiente¹¹⁰⁴.

¹¹⁰³ Diretiva (UE) 2016/1148, 4.

¹¹⁰⁴ “QUE FAZ O GIGAPIX?”, GigaPIX, <https://gigapix.pt/pt/home/>.

O primeiro operador destes pontos de troca de tráfego em Portugal foi a GigaPIX, estabelecida em outubro de 1995 pela FCCN. A GigaPIX nasceu com a implementação de portas Gigabit no Portuguese Internet eXchange (PIX). Atualmente, a GigaPIX conecta dezenas de redes nas suas instalações em Lisboa e no Porto, oferecendo velocidades que variam de 10Gbps a 100Mbps¹¹⁰⁵. Outras duas entidades que se dedicam principalmente à gestão de pontos de troca de tráfego são a LIS-IX e a Equinix. A LIS-IX foi criada em 2023 e tem como grande objetivo agitar as trocas de tráfego em Portugal. Para isso, a LIS-IX reduz a distância que os dados necessitam de efetuar e oferece uma rede estratégica devido às parcerias com entidades chave da internet e telecomunicações¹¹⁰⁶. A Equinix é outra entidade que também está localizada em Lisboa e é uma empresa global de *datacenters* e serviços de troca de tráfego¹¹⁰⁷.

Os principais objetivos de entidades como estas são melhorar e aumentar a qualidade da rede IP em Portugal, o que é feito evitando o uso de ligações internacionais para comunicações locais, o que também ajuda a reduzir os custos dessas operações. Estas entidades visam também diminuir a latência dos serviços e proporcionar uma melhor experiência aos utilizadores. Os principais pontos de troca de tráfego em Portugal estão distribuídos pelas cidades de Lisboa e do Porto. As organizações comumente conhecidas como “operadoras”, que fornecem os tradicionais serviços de telefone, internet e televisão, também costumam operar pontos de troca de tráfego. Por exemplo, através da rede MEO, o serviço de interligação “Trânsito Nacional PT” permite fazer a ligação para troca de tráfego entre dois outros operadores, sem que estes se tenham de interligar diretamente. Este tipo de serviço de pontos de troca de tráfego permite que a rede transporte uma chamada que tenha origem na rede de um operador cujo destino é o ponto terminal da rede ou o serviço de um terceiro operador, através de um acordo entre os operadores de origem/destino. As vantagens deste serviço são o valor económico, por não ser necessário estabelecer ligações entre operadores, a eficiência, a transparência, a flexibilidade de acesso, segurança e elevado grau de disponibilidade e a supervisão¹¹⁰⁸.

Prestadores de serviços de DNS

Os DNS (*Domain Name Systems*) são responsáveis pela tradução dos nomes de domínio normalmente usados para referir *websites* nos seus endereços IP, de modo a serem compreendidos pelos computadores. A título ilustrativo, DNS é o que traduz o que é conhecido normalmente como “exemplo.com” no seu endereço IP real, como “192.0.2.1”.

A FCCN foi a primeira entidade responsável pela gestão dos DNS em Portugal, tendo sido nomeada pela Internet Assigned Numbers Authority (IANA) para tal em 1988¹¹⁰⁹.

Atualmente, existem em Portugal diversos prestadores deste tipo de serviços, abrangendo tanto opções locais como internacionais, com diferentes características e níveis de serviço. Os principais fornecedores locais incluem grandes operadoras de telecomunicações como a MEO, NOS, Vodafone Portugal e NOWO. Todas estas operadoras fornecem um serviço de *DNS* integrado com os seus serviços de Internet¹¹¹⁰.

¹¹⁰⁵ “Sobre nós”, GigaPIX, <https://gigapix.pt/pt/sobre-nos/>.

¹¹⁰⁶ “What is LIS-IX?”, LIS-IX, <https://lis-ix.pt/#what-is>.

¹¹⁰⁷ “LS1”, Equinix, <https://www.equinix.com/data-centers/europe-colocation/portugal-colocation/lisbon-data-centers/ls1>.

¹¹⁰⁸ “Interligação e Serviço Universal”, ANACOM, 23 de fevereiro de 2006, <https://www.anacom.pt/render.jsp?categoryId=183071&languageId=0>

¹¹⁰⁹ Pedro Fonseca, Paul McCarthy e Marian-Andrei Rizo, *Registentes: Os primeiros domínios .pt* (Loures: Conclusão das Letras, julho de 2021), 13, https://tictank.pt/wp-content/uploads/2021/08/2107-registentes_livro.pdf.

¹¹¹⁰ “DNS servers in Portugal”, Public DNS, <https://public-dns.info/nameserver/pt.html>.

Além dos fornecedores locais, existem vários fornecedores internacionais que também têm uma presença significativa em Portugal. Por exemplo, a Google Public DNS¹¹¹¹ utiliza os endereços 8.8.8.8 e 8.8.4.4. Já o OpenDNS¹¹¹² oferece filtros de conteúdo e proteção contra *phishing* e opera com os endereços 208.67.222.222 e 208.67.220.220. Estes fornecedores oferecem diferentes opções para as diferentes necessidades e preferências, desde serviços básicos até soluções mais avançadas com foco na segurança e privacidade.

Registo de nomes de domínio de topo

Os nomes de domínio de topo (*top-level domains* - TLD) são a parte de um endereço *web* depois do seu nome de domínio. Ou seja, em “exemplo.com”, “.com” é o TLD em questão. Existem diversos TLDs, sendo alguns dos mais comuns o “.com” e “.org”, havendo também os TLDs relativos a diferentes países, como “.us”, dos EUA, “.es”, de Espanha, “.fr”, de França e, no caso de Portugal, “.pt”. Em 1988, a par da sua nomeação para gestão dos DNS, a FCCN foi designada como a responsável pelos registos de domínios “.pt”¹¹¹³. Seria depois constituída, em 2013, a Associação DNS.PT, associação sem fins lucrativos que é composta por membros como a Fundação para a Ciência e Tecnologia, IP (FCT), a Associação de Economia Digital (ACEPI) e a Associação Portuguesa para a Defesa do Consumidor (DECO), sucedendo à FCCN nos direitos e obrigações na gestão, registo e manutenção dos domínios “.pt”. A missão da DNS.PT é a de fortalecer o ecossistema digital em Portugal, em conformidade com a Europa e o Mundo, respondendo às necessidades do público consumidor, parceiro e colaborador. O principal objetivo é o de oferecer elevados níveis de qualidade, fiabilidade e segurança no registo de nomes de domínio “.pt”, assim como assegurar o correto funcionamento e manutenção do mesmo¹¹¹⁴.

7.1.1. Impacto socioeconómico

Segundo o documento final de “Avaliação do Potencial Económico da Transição Digital em Portugal” de 2023, conclui-se que o impacto das infraestruturas digitais se verifica em três vertentes:

- Impacto das infraestruturas e conectividade:
 - **Acesso:** A disponibilidade de infraestruturas digitais de qualidade amplia o acesso a tecnologias avançadas, permitindo que empresas e indivíduos aproveitem os benefícios da economia digital;
 - **Cobertura:** A ampla cobertura de redes digitais assegura que uma maior parte da população e das empresas tenha acesso a serviços de alta velocidade, facilitando a inclusão digital;
 - **Funcionalidades de Rede:** A capacidade das redes de suportar diferentes funcionalidades é crucial para impulsionar a inovação, a eficiência e a produtividade em diversos setores económicos¹¹¹⁵.

Estas variáveis - acesso, cobertura e funcionalidades de rede - são fundamentais para explicar o aumento do valor acrescentado bruto (VAB) e a melhoria da produtividade, que são indicadores importantes do impacto positivo das infraestruturas digitais na economia nacional.

¹¹¹¹ “Google Public DNS”, Google, <https://dns.google/>.

¹¹¹² “About Us”, OpenDNS, <https://www.opendns.com/about/>.

¹¹¹³ “História”, .PT, <https://www.pt.pt/pt/historia/>.

¹¹¹⁴ “Quem somos”, .PT, <https://www.pt.pt/pt/quem-somos/>.

¹¹¹⁵ Deloitte e Universidade de Coimbra, “Avaliação do Potencial Económico da Transição Digital em Portugal”, 2023, 89, https://portugaldigital.gov.pt/wp-content/uploads/2023/05/Portugal-Digital_Avaliacao-Transicao-Digital_Documento-Final_v20230330_VF.pdf.

Segundo o Índice de Digitalidade da Economia e da Sociedade (IDES), publicado no último trimestre de 2023, Portugal melhorou o seu desempenho nas redes fixas de alta capacidade (VHCN) e na cobertura de fibra (91% de cobertura de instalações) e na oferta de banda larga fixa com, no mínimo, 100 Mbps (77%)¹¹¹⁶. Embora na dimensão do 5G, o contexto nacional esteja mais atrasado, a melhoria destas infraestruturas faz com que as empresas estejam mais capazes de adotar meios digitais mais avançados como computação *cloud*, *big data* ou IA. Uma condição essencial às empresas para que possam ter acesso a tecnologias mais complexas que impulsionem os seus serviços, como as referidas anteriormente, é o acesso à internet de alta velocidade. A análise da amostra do Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas (IUTICE) e do Sistema de Contas Integrado das Empresas (SCIE) revela um crescimento significativo no acesso rápido à internet entre as empresas em Portugal. Esse crescimento é refletido no gráfico e no relatório correspondente.

- **Crescimento do Acesso Rápido à Internet:**

1. **Evolução do Acesso:**

- Em 2020, 29% do valor acrescentado bruto (VAB) era gerado por empresas com acesso rápido à internet¹¹¹⁷.
- Em 2022, o número de empresas com acesso a velocidades de internet iguais ou superiores a 1 Gb/s aumentou para cerca de 23%, representando um crescimento de 3% em relação a 2021¹¹¹⁸.

2. **Significado do Crescimento:**

- **Produtividade e Competitividade:** O aumento da velocidade de internet nas empresas contribui diretamente para a produtividade e competitividade. Acesso a internet de alta velocidade permite operações mais eficientes, maior capacidade de processamento de dados e melhor comunicação interna e externa¹¹¹⁹.
- **Inovação e Transformação Digital:** Empresas com acesso rápido à internet estão mais bem posicionadas para adotar novas tecnologias, como inteligência artificial, *big data* e internet das coisas (IoT), impulsionando a inovação e a transformação digital.
- **Inclusão Digital:** A expansão do acesso rápido à internet ajuda a reduzir a desigualdade digital, permitindo que mais empresas, independentemente do seu tamanho ou localização, acessem as mesmas oportunidades e ferramentas digitais¹¹²⁰.

¹¹¹⁶ Manuel Dias, "Estará no plano do próximo Governo colocar Portugal na vanguarda da Europa digital?", *Observador*, 3 de janeiro de 2024, <https://observador.pt/opiniao/estara-no-plano-do-proximo-governo-colocar-portugal-na-vanguarda-da-europa-digital/>.

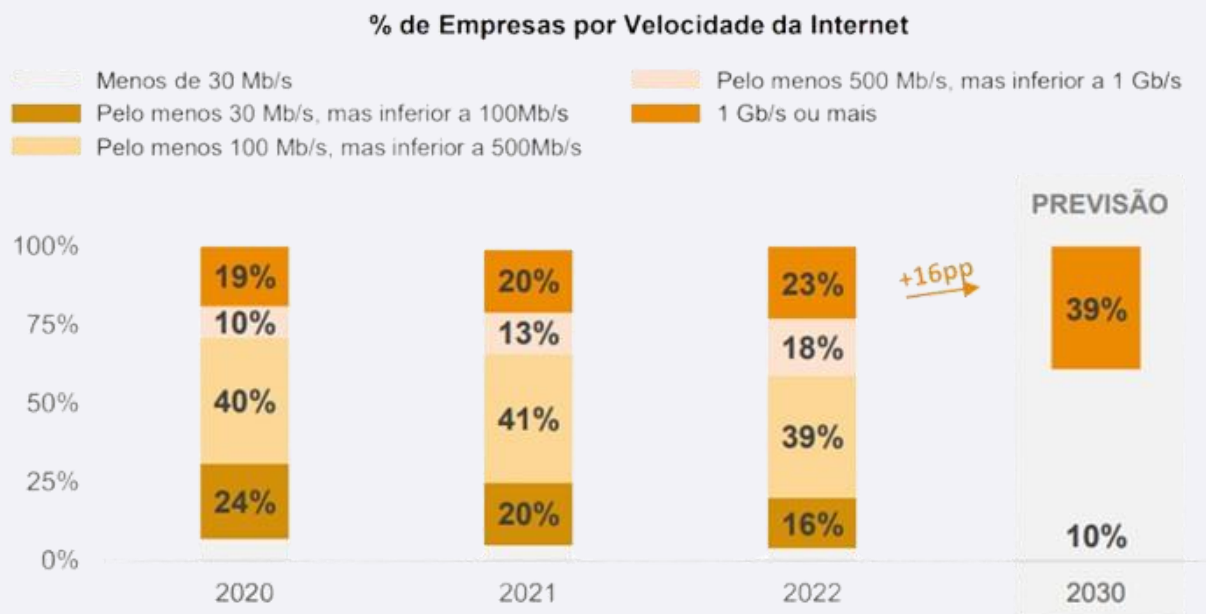
¹¹¹⁷ Deloitte e Universidade de Coimbra, "Avaliação do Potencial Económico", 89.

¹¹¹⁸ Deloitte e Universidade de Coimbra, "Avaliação do Potencial Económico", 89.

¹¹¹⁹ Deloitte e Universidade de Coimbra, "Avaliação do Potencial Económico", 91.

¹¹²⁰ "Inquérito à utilização de tecnologias da informação e da comunicação nas empresas", *INE*, 21 de novembro de 2023, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637881953&att_display=n&att_download=y.

Figura 14 - Velocidade de Internet



(Fonte: Deloitte e Universidade de Coimbra, “Avaliação do Potencial Económico da Transição Digital em Portugal”, 2023, 89)

- Cobertura de internet de alta velocidade:
 - Um estudo comparativo entre os preços dos pacotes de acesso a banda larga, voz e dados móveis, concluiu que os preços nacionais aparentam estar acima da média europeia. Através da análise aos preços dos cabazes das 3 vertentes - internet fixa, dados móveis e convergente - verificou-se que Portugal se insere nos *clusters* de países com os preços mais elevados da UE;
 - Para o ano de 2021, Portugal apresentou o indicador relativo à cobertura 5G com valores nulos nas estatísticas do Eurostat de 2021 - o que representava um atraso significativo em comparação com os valores da UE nesse mesmo ano (65,8% de cobertura 5G).
 - Portugal encontra-se na sétima posição no que diz respeito à cobertura de internet de alta velocidade, segundo a Eurostat, com Malta, Luxemburgo e Dinamarca a liderar. Países como a Grécia, Chipre e Itália são os Estados-Membros que ocupam as posições finais da tabela, com valores mínimos de 44% de cobertura¹¹²¹.
 - No entanto, a ANACOM revelou que no ano de 2022, 98% dos concelhos e 49% das freguesias estavam já cobertos por 5G. Este aumento é justificado pela estratégia para a quinta geração de comunicações móveis (5G) e pelo Leilão 5G¹¹²².

¹¹²¹ “Broadband Coverage in Europe 2021”, Comissão Europeia, agosto de 2022, <https://ec.europa.eu/newsroom/dae/redirection/document/88314>.

¹¹²² Deloitte e Universidade de Coimbra, “Avaliação do Potencial Económico da Transição Digital”, 85.

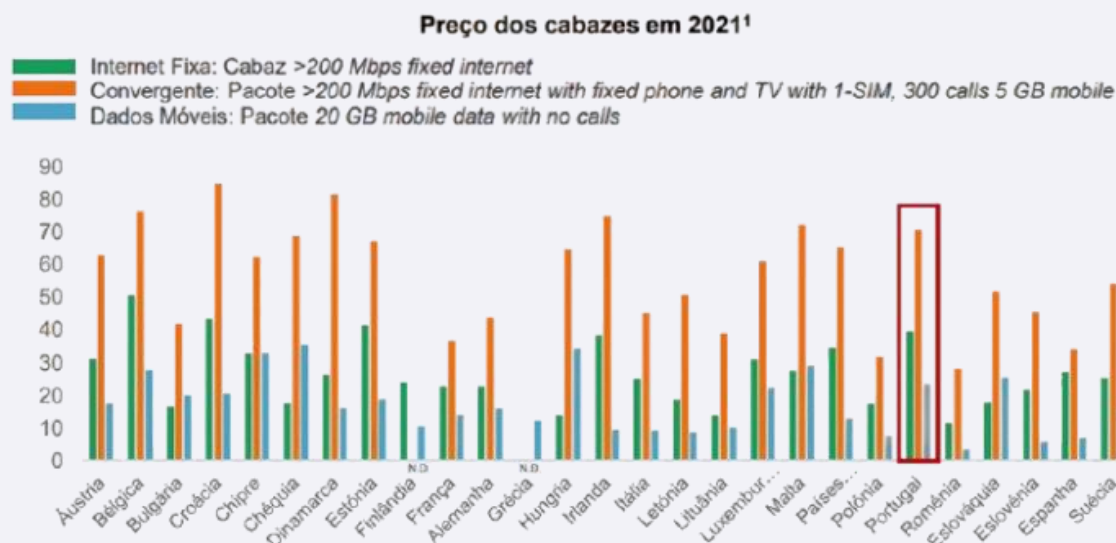
Tabela 54 - Velocidade de Internet

	Cobertura por rede gigabit (%)	Cobertura 5G (%)
<i>Target</i>	100	100
EU 2021	70,2	65,8
PT 2021	90,5	0
PT 2022	-	Concelhos - 98
		Freguesias - 49

(Fonte: Deloitte e Universidade de Coimbra, “Avaliação do Potencial Económico da Transição Digital em Portugal”, 2023, 85)

Uma nota importante relativamente a estes dados é a forma como a recolha dos valores dos indicadores é feita pela ANACOM em Portugal e pela UE. Até à data deste relatório, não há forma de identificar e validar que a recolha é feita da mesma forma por ambas as entidades. Neste sentido, não se pode concluir se o atraso significativo verificado em 2021 foi ou não recuperado em 2022. Esta validação só se poderá confirmar na próxima atualização anual dos dados por parte do Eurostat, através de comparação direta.

Figura 15 - Preço dos Cabazes



(Fonte: Deloitte e Universidade de Coimbra”, Avaliação do Potencial Económico da Transição Digital em Portugal”, 2023, 87)

Ainda no contexto da cobertura 5G em Portugal, em 2019 a Ericsson conduziu a um estudo relativo ao Impacto da quinta geração (5G) em Portugal - Relatório de Mobilidade da Ericsson¹¹²³. As conclusões da Ericsson avançam que, até ao fim de 2025, o 5G deverá cobrir 65% da população mundial e será responsável por 45% do tráfego global de dados móveis. No contexto nacional, o

¹¹²³ Juliana Guerra, “Impacto do 5G em Portugal pode chegar aos 3,6 mil milhões de euros”, *Ericsson*, 11 de junho de 2019, <https://www.ericsson.com/pt/press-releases/2019/6/ericsson-mobility-report-a-adocao-da-tecnologia-5g-e-ainda-mais-rapida-do-que-esperada>.

Relatório de Mobilidade da Ericsson relata que o lançamento de cobertura de 5G terá um impacto de cerca de 3,6 mil milhões de euros na economia portuguesa até 2030.

Segundo as estimativas da empresa, haverá um consumo global de 24 Gigabyte (GB) por mês, em média, por parte dos utilizadores de *smartphones*. Até 2019, a utilização era de 7,2 GB.

O impacto e papel que as infraestruturas digitais trazem para o contexto económico nacional, o investimento feito na área, a adaptação de ações a contextos europeus e a crescente colaboração entre países europeus atuam também, consequentemente, como forte impulsionador a empresas, indivíduos, serviços e contextos que dependem, direta ou indiretamente, de infraestruturas digitais.

No seguimento do papel da GigaPIX na qualidade de rede IP em Portugal, é de notar o forte impacto que é promovido através da redução de latência de serviço (e, consequente, melhoria das ligações de rede IP), aumento da velocidade e diminuição dos custos de serviço - aumentando o acesso a mais entidades coletivas e individuais.

Dados divulgados pela Associação .PT - DNS.PT, mostram que o aumento do domínio .pt cresceu 11% no ano de 2021, em relação ao ano de 2019, batendo recorde e tornando-se o .pt um dos domínios de topo que mais cresceu no espaço europeu¹¹²⁴.

Foi também criado o projeto Empresa na Hora, enquadrado na iniciativa 3em1¹¹²⁵ que permite atribuir, a alguém que crie uma empresa, um pacote de serviços gratuitos com domínio registado em .pt, ferramenta de desenvolvimento de site, alojamento técnico e caixas de correio eletrónico. Esta é uma ação que permite às “empresas, em particular, perceberem que têm de continuar a fazer esta transformação e a investir numa presença *online* para impulsionar os seus negócios”¹¹²⁶.

A pandemia de covid-19 veio trazer uma mudança significativa no setor das infraestruturas digitais, sendo a mais importante a adoção do teletrabalho. Inicialmente, as infraestruturas de TI da maior parte das empresas não estavam preparadas para suportar um volume tão alto de acessos remotos e, de forma a mitigar estes problemas, as empresas tiveram de investir na segurança, melhorar as capacidades de rede e implementar soluções como VPNs e ferramentas de monitorização e gestão de forma remota. A medida “TD-C16-i05” surgiu como uma das iniciativas do Plano de Recuperação e Resiliência de Portugal, conhecida como Plano Renova Portugal. Este plano foi desenvolvido em resposta à crise económica e social provocada pela pandemia COVID-19, com o objetivo de promover a recuperação e fortalecer a resiliência da economia portuguesa¹¹²⁷.

De forma a suportar todo este acréscimo de utilização, o setor das infraestruturas digitais teve avanços significativos, houve um aumento da capacidade de processamento dos centros de dados, assim como de armazenamento. Portugal está no sexto lugar de melhor país para trabalho remoto, segundo a *NordLayer* (empresa que criou o Índice Global de Trabalho Remoto¹¹²⁸). Este índice leva em conta 4 dimensões: cibersegurança, economia, infraestrutura física e digital e a segurança no país.

¹¹²⁴ “Domínio .pt cresceu 11% em 2021”, Comunicados, República Portuguesa, 25 de janeiro de 2022, <https://www.portugal.gov.pt/pt/gc22/comunicacao/comunicado?i=dominio-pt-cresceu-11-em-2021>.

¹¹²⁵ “Sobre”, Três Em Um, <https://3em1.pt/>.

¹¹²⁶ Fátima Caçador, “Registo de domínios .pt com novo recorde em 2022. Foram registados mais de 150 mil”, *Sapo TEK*.

¹¹²⁷ “TD-C16-i05 CAPACITAÇÃO E TRANSFORMAÇÃO DIGITAL DAS EMPRESAS DOS AÇORES”, Recuperar Portugal, <https://recuperarportugal.gov.pt/transicao-digital/empresas-4-0/td-c16-i05-capacitacao-e-transformacao-digital-das-empresas-dos-acores/>.

¹¹²⁸ “Which countries score the highest?”, *Nordlayer*, última atualização em 22 de agosto de 2024, <https://nordlayer.com/global-remote-work-index/#countries-score-table>.

Atualmente, segundo as estatísticas do emprego realizadas pelo INE, no primeiro trimestre do ano de 2024, mais de 19% da população empregada trabalhou a partir de casa. O regime misto é o mais adotado pelas empresas, sendo que mais de 73% das pessoas que indicaram trabalhar regularmente a partir de casa referiu que está neste regime¹¹²⁹.

7.1.2. Especificidades tecnológicas

A fibra ótica e a tecnologia 5G são componentes essenciais para o avanço do setor das infraestruturas digitais. A fibra ótica tem a capacidade de transmitir grandes volumes de dados a uma velocidade extremamente alta com uma perda de sinal mínima, e permite suportar os crescentes pedidos pela largura de banda devido ao aumento de consumo de conteúdos digitais, como serviços de *streaming*. Já a tecnologia 5G trouxe a disponibilização de conectividade sem fios, com velocidades de *download* e *upload* significativamente mais altas do que a tecnologia 4G (geração anterior). O aumento da capacidade de dispositivos ligados e a redução da latência são outras duas características importantes da tecnologia. A primeira permite o desenvolvimento da Internet das Coisas (IoT) e a segunda permite várias aplicações como cirurgias remotas, carros autónomos e até a realidade aumentada.

Em 2023, foi aberto um concurso público internacional com o objetivo de dar cobertura de fibra a zonas sem acesso. A data prevista de finalização é entre 2026 e 2027 e, caso seja implementado com sucesso, Portugal poderá ser um dos primeiros países da União Europeia a ter uma cobertura com redes fixas de capacidade muito elevada em todo o seu território. É importante realçar que, com este projeto, também haverá um reforço significativo na cobertura de rede móvel, nomeadamente, a rede 5G¹¹³⁰. O investimento em causa será de 425 milhões de euros, sendo cerca de 150 milhões comparticipados pelos Programas Regionais do Portugal 2030¹¹³¹. De forma a perceber que zonas não têm cobertura de redes fixas de capacidade muito elevada, a ANACOM procedeu a um levantamento geográfico onde foram identificados cerca de 417 mil edifícios residenciais e não residenciais sem cobertura¹¹³².

De acordo com o relatório de tecnologias emergentes, elaborado pelo CNCS em maio de 2023, a tecnologia 5G já tem um fim previsto. A próxima tecnologia (6G) já está a ser preparada, estando previsto para 2027 as discussões finais sobre a alocação do espectro a ser utilizado e a especificação final deverá sair em 2030¹¹³³.

¹¹²⁹ “Estatísticas do emprego”, INE, 8 de maio de 2024,

https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=665513779&att_display=n&att_download=y.

¹¹³⁰ “Telecomunicações e acesso à Internet de qualidade finalmente uma realidade em todo o País”, Anacom, 6 de dezembro de 2023, <https://www.anacom.pt/render.jsp?contentId=1769445>.

¹¹³¹ “Fibra ótica vai chegar a todo o país até 2027”, Portugal.gov.pt, 12 de dezembro de 2023,

<https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=esta-aberto-o-concurso-para-levar-a-fibra-otica-a-todo-o-pais>.

¹¹³² “Telecomunicações e acesso à Internet de qualidade finalmente uma realidade em todo o País”, Anacom, 6 de dezembro de 2023.

¹¹³³ “Tecnologias Emergentes”, Centro Nacional de Cibersegurança, maio de 2023, 73, <https://www.cncs.gov.pt/docs/rel-tecemer2023-observ-cnccs.pdf>.

Portugal tem uma localização estratégica pois liga três continentes (Europeu, Americano e Africano), tendo sido este um fator importante para atrair investimentos nesta área. Devido ao crescente número de pedidos pelos serviços digitais, necessidade de armazenamento e processamento de dados, espera-se um crescimento ainda maior de centros de dados em Portugal¹¹³⁴.

A maioria das tecnologias digitais têm sistemas de segurança, nomeadamente do tipo criptográfico. Por exemplo, os dados enviados e recebidos por um ponto de troca de tráfego são sempre cifrados. Atualmente, a forma de cifragem mais utilizada é a cifragem de chave pública, onde existe uma chave pública que, como o nome indica, é do conhecimento público e tem como propósito cifrar os dados. Existe, também, uma chave privada de acesso restrito que pode descriptar os mesmos. Como este processo de cifragem é baseado no poder computacional disponível e não em provas matemáticas, não é possível garantir a segurança e/ou privacidade dos dados num período razoável. Uma das soluções atuais é cifrar os dados com chaves cada vez mais longas. No futuro, com o surgimento da computação quântica, será possível decifrar estes dados numa questão de minutos. Ainda de acordo com o relatório do CNCS: "É previsível o aparecimento na próxima década de um computador quântico plenamente funcional" e deverá ser criada uma tecnologia criptográfica¹¹³⁵.

Devido ao grande volume de dados processados nos pontos de troca de tráfego (por exemplo, o GigaPix, de setembro de 2023 a agosto de 2024 processou, em média, cerca de 193.49GB por segundo¹¹³⁶), estes têm recorrido aos serviços *cloud* para aumentar a sua capacidade de armazenamento e processamento de dados. A IA (Inteligência Artificial) também está a ser amplamente difundida via *cloud* pois as utilizações de ferramentas de IA necessitam de um elevado poder computacional, assim como de recursos humanos especializados e, utilizando as soluções de *cloud*, este problema consegue ser evitado¹¹³⁷.

Segundo a IDC, a área de *cloud computing* vai atingir um investimento de mil milhões de euros em 2026 onde o destaque vai para a área de *Software as a Service (SaaS)* que representa 70% do mercado e tem uma previsão de subir 685 milhões de euros até 2026. Prevê-se um crescimento de 30% até 2026 para o modelo *Platform as a service (PaaS)*, atingindo 223,4 milhões de euros. Já o modelo *Infrastructure as a service (IaaS)* deverá ter um crescimento de 25% e 264 milhões de euros de investimento até ao mesmo ano¹¹³⁸.

¹¹³⁴ "A economia dos Data Centers em Portugal: o que esperar para os próximos anos?", *DatacenterDynamics*, 26 de abril de 2023, <https://www.datacenterdynamics.com/br/an%C3%A1lises/a-economia-dos-data-centers-em-portugal-o-que-esperar-para-os-proximos-anos/>.

¹¹³⁵ "Tecnologias Emergentes", Centro Nacional de Cibersegurança, 87,88 e 89.

¹¹³⁶ <https://gigapix.pt/en/technical/traffic-stats/> (dados de tráfego são apresentados em contínuo e não é possível definir um período para a consulta do tráfego)

¹¹³⁷ "Tecnologias Emergentes", Centro Nacional de Cibersegurança, 21 e 22.

¹¹³⁸ Dave McCarthy et al, "IDC FutureScape: Worldwide Cloud 2023 Predictions", *IDC*, outubro de 2022, <https://www.idc.com/getdoc.jsp?containerId=US48602322>.

7.2. Ameaças

As principais ameaças de cibersegurança neste setor prendem-se com os serviços por este prestados, ou seja, são sobretudo as ameaças e os ataques relativos aos DNS, como *DNS amplification*, *spoofing/cache poisoning*, *tunneling*, ataques aos pontos de troca de tráfego, tais como ataques de interseção (*Man-in-the-Middle*) ou de *rerouting*, e ataques aos registos de domínios de topo, tais como ataques de *domain hijacking*.

Segundo o relatório da Enisa "*DNS Identity*", elaborado em 2023, as credenciais são uma parte essencial do registo dos domínios e, como tal, os ataques a estas credenciais resultam em alguns problemas, tais como interceção de tráfego, ataques de engenharia social, ataques ao domínio, entre outros. O relatório refere alguns exemplos, como o ataque ao domínio de cripto *Coin Check* e ao domínio da Lenovo¹¹³⁹.

O primeiro ataque ocorreu em junho de 2020 e, como resultado, a *Coin Check* sofreu uma violação de dados após um terceiro, não autorizado, aceder à conta de registo de domínio da empresa. O atacante utilizou o domínio ".jp" para enviar e-mails fraudulentos, resultando na exposição de dados de cerca de 200 clientes¹¹⁴⁰. No segundo ataque, ocorrido em fevereiro de 2015, os domínios da Lenovo e da Google no Vietname foram sequestrados pelo grupo Lizard Squad, que explorou uma vulnerabilidade na Webnic (empresa de registo de domínios). Através do controlo do *DNS*, os atacantes redirecionaram o tráfego para servidores controlados pelo grupo ficando assim com acesso a toda a informação¹¹⁴¹.

De acordo com a *OWASP (Open Web Application Security Project)*, existem três ataques típicos que podem afetar tanto os registos como os sistemas de gestão de identidade que os mesmos utilizam:

1. Utilizar listas de palavras-passe conhecidas e utilizar essa informação numa aplicação que não contenha qualquer tipo de proteção contra ataques de *credential stuffing*;
2. Elaborar ataques de autenticação contra aplicações sem requisitos de complexidade ou rotação de palavras-passe, ou até mesmo sem *MFA* (autenticação multifator) implementada;
3. A aplicação não tem os tempos das sessões implementadas corretamente ou o utilizador usa um computador público para aceder a uma aplicação e, quando sai, não termina a sessão. Com isto, um atacante consegue aceder à sua conta no mesmo *browser*, passado uma ou duas horas¹¹⁴².

Existem outros tipos de ataques, todos com o mesmo objetivo: obter de forma ilegítima as credenciais do registo de domínios. Estes ataques podem ser de engenharia social levando a que um utilizador coloque as credenciais num *website* falso (*Phishing*). Também existem ataques de *brute-force* que consistem no uso de ferramentas automatizadas que geram milhares de milhões de possíveis palavras-passe e ocorrem outras tantas tentativas até ser descoberto a combinação correta. Este tipo de ataque é facilmente evitado limitando o número de tentativas falhadas na aplicação¹¹⁴³.

¹¹³⁹ "DNS IDENTITY Verification and Authentication of Domain Name Owners", ENISA, maio de 2023, 18, <https://www.enisa.europa.eu/publications/dns-identity>.

¹¹⁴⁰ Paddy Baker, "Coincheck Customers Fall Victim to Data Breach After Domain Account Error", Coincheck, 3 de junho de 2020, <https://www.coindesk.com/markets/2020/06/03/coincheck-customers-fall-victim-to-data-breach-after-domain-account-error/>.

¹¹⁴¹ "Webnic Registrar Blamed for Hijack of Lenovo, Google Domains", KrebsonSecurity, 26 de fevereiro de 2015, <https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/>.

¹¹⁴² ENISA, "DNS IDENTITY Verification and Authentication of Domain Name Owners", 19.

¹¹⁴³ ENISA, "DNS IDENTITY Verification and Authentication of Domain Name Owners", 19 e 20.

Conforme já referido anteriormente, o sistema de nomes de domínio é uma parte crucial da infraestrutura da Internet e é essencial para a tradução de nomes de domínio legíveis para endereços de *IP* e vice-versa. Devido a esta importância, o *DNS* é um alvo sistemático de ataques de cibersegurança. Um dos ataques mais frequentes é o ataque de negação de serviço onde é enviado um grande número de requisições *DNS* para sobrecarregar o servidor em questão, tornando assim o servidor lento e sem capacidade de resposta. Outro ataque passa pela modificação dos dados, mais conhecido por ataque *man-in-the-middle*, onde existe um atacante entre o recetor e o emissor dos dados, conseguindo assim romper a cadeia de confiança e modificar os dados enviados. Ainda dentro dos ataques de *DNS*, temos o ataque *DNS ID hacking* onde um atacante faz-se passar por um servidor de *DNS* fidedigno e, por fim, temos o ataque por envenenamento de cache que consiste num atacante a injetar dados maliciosos de *DNS* nos servidores de *DNS* utilizados pelos *ISPs*¹¹⁴⁴.

Existem outros tipos de ataques denominados por ataques de amplificação. Estes ataques aumentam o volume do tráfego enviado a um alvo, utilizando respostas de *DNS* amplificadas. Estas são caracterizadas por enviar uma consulta a um servidor de *DNS* que replica com uma resposta muito maior, aumentando assim o tráfego. Fora deste tipo de ataques, temos o *DNS Hijacking* que tem como objetivo subverter a resolução de consultas *DNS*. Pode ser realizado por um *malware* que modifica as configurações *TCP/IP* de um computador de forma a colocar o mesmo a apontar para um servidor *DNS* controlado por um atacante ou pela modificação de um servidor *DNS* confiável. Este tipo de ataque pode servir como porta de entrada para ataques de *Phishing*, pois o atacante pode redirecionar as vítimas para um site falso, pedindo às mesmas para introduzirem as credenciais de *login* ou até mesmo informações bancárias confidenciais¹¹⁴⁵.

Dados apresentados no Relatório de Atividades e Contas de 2022¹¹⁴⁶ da .PT, sugerem que se manteve, em 2022, um crescimento da deteção e/ou reporte de eventos e incidentes nos canais internos e externos da .PT. Este crescimento deveu-se, não só ao crescimento de atividade maliciosa no contexto de atuação do .PT como também à capacidade interna na identificação e reporte de qualquer atividade maliciosa. O relatório espelha ainda que, comparativamente com o mesmo período do ano de 2021, foram registados mais de 600 eventos de cibersegurança - representando um aumento de 69,4%. Destes eventos de cibersegurança, 2 foram classificados como incidentes de segurança, embora mitigados de forma que não causassem um impacto significativo nas operações do .PT. Foi criada uma maior segurança e confiança no domínio .pt, através da monitorização e gestão de atividades de *DNS Abuse* e através da identificação proativa de domínios registados sob .PT usados para desenvolver atividade maliciosa, como a disseminação de *malware* ou de *phishing* e na colaboração para a sua rápida mitigação, através da cooperação com parceiros e autoridades competentes, quando necessário. Em 2022, foram identificados 130 casos de *DNS Abuse*. Do total, 96 dos casos tinham o objetivo de desenvolver atividade de *phishing*, 28 distribuíam *malware* e 6 estavam a ser utilizados para *spam*. Estes valores representam um aumento de 36% desta atividade quando comparado com 2021.

¹¹⁴⁴ "DNS Advanced Attacks and Analysis", Adam Ali.Zare Hudaib e Esra'a Ali Zare Hudaib, 2014, 65, https://www.academia.edu/download/35520765/DNS_Advanced_Attacks_and_Analysis.pdf.

¹¹⁴⁵ Adam Ali.Zare Hudaib e Esra'a Ali Zare Hudaib, "DNS Advanced Attacks and Analysis", 67 e 68.

¹¹⁴⁶ .pt, "Relatório de Atividades e Contas 2022", 33, https://www.pt.pt/fotos/editor2/relatorios/relatorio_atividades_contas_2022.pdf.

De acordo com o relatório anual de 2023 elaborado pelo SOCPT, existiram 164 eventos reportados, cerca de 330 mil e-mails maliciosos recebidos, 647 casos identificados de abuso de DNS e 130 reportados, 89% destes casos tratava-se de *phishing* e 82% foram resolvidos em menos de 8 dias. Em relação a *standards* de segurança implementados nos registadores, cerca de 94% têm *HTTPS* e um certificado digital válido, 22% têm *DNSSEC* e 35% têm *HSTS*¹¹⁴⁷. Relativamente à formação e sensibilização, em 2023, houve 5 cursos de cibersegurança onde participaram mais de 3 mil pessoas, houve sete publicações da PTSOC {Digest} e 4 edições da {News} e ocorreram 16 *workshops* onde participaram mais de 650 pessoas¹¹⁴⁸.

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos¹¹⁴⁹, de 2021 a 2024. Para melhor se compreender a mesma, deixa-se também uma breve descrição de cada agente de ameaça.

- **Cibercriminosos:** agentes de ameaça que se organizam, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal¹¹⁵⁰.
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuítos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa¹¹⁵¹.
- **Hacktivistas:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável¹¹⁵².
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso¹¹⁵³. No caso, consideraram-se os colaboradores internos maliciosos.

¹¹⁴⁷ “Annual Report PTSOC 2023”, PTSoc, 12-13, <https://ptsoc.pt.pt/en/relatorio-anual-ptsoc-2023/>.

¹¹⁴⁸ “Annual Report PTSOC 2023”, PTSoc, 16.

¹¹⁴⁹ CNCS, “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança, <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.

¹¹⁵⁰ CNCS, “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”, maio de 2021, 74, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>.

¹¹⁵¹ CNCS, “Relatório Riscos & Conflitos 2021”, 75.

¹¹⁵² CNCS, “Relatório Riscos & Conflitos 2021”, 75-76.

¹¹⁵³ CNCS, “Relatório Riscos & Conflitos 2021”, 76-77.

Tabela 55 - Agentes de ameaça mais prováveis (Infraestruturas Digitais)

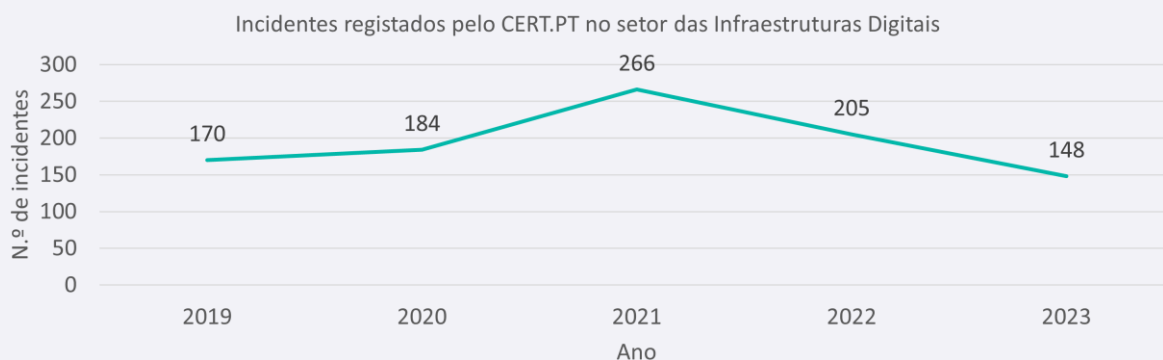
Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Ransomware	■	■	■	■
DDoS	■	■	■	
Ataques DNS	■	■	■	
Vulnerabilidades	■	■	■	■
Phishing, Spear Phishing e Smishing	■	■	■	
Manipulação de Sistemas (TI)	■	■		■

Legenda:

■ - Agente de ameaça provável

A atratividade do setor das infraestruturas digitais para ciberataques é comprovada pelo número de ataques que o setor tem sofrido em Portugal. Segundo dados do CERT.PT, registaram-se 825 ataques entre 2019 e 2022, tornando este setor o setor que sofreu mais ataques. Este registo ficou apenas atrás do setor bancário¹¹⁵⁴.

Figura 16 - Número de incidentes no setor das Infraestruturas Digitais anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>)

¹¹⁵⁴ CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, <https://www.cncs.gov.pt/pt/estatistica/>.

7.3. Capacitação

Capacitação Digital em Portugal

O Relatório de atividades e contas de 2022 da .PT permite fazer um resumo geral da estratégia presente (2022) e futura¹¹⁵⁵:

- 1. Desenvolvimento de competências**
 - 1.1. Programas de Formação e Workshops
 - 1.1.1. Organização de *workshops* com o objetivo de fortalecer as competências técnicas dos *registrars* em *DNSSEC*;
 - 1.1.2. Adoção do programa *Cisco Networking Academy® (NetAcad)* pelo .PT no âmbito das atividades do seu Centro de Formação.
 - 1.2. Sensibilização e Educação
 - 1.2.1. Disponibilização de materiais educativos sobre segurança, como campanhas sobre o *Registry Lock Service*;
 - 1.2.2. Realização de exercícios internos de *phishing* para aumentar a sensibilização sobre cibersegurança da organização e entre os *registrars*.
 - 1.3. Formação Especializada
 - 1.3.1. Desenvolvimento de formações específicas para a equipa do PTSOC, com o objetivo de melhorar as competências na monitorização e resposta a incidentes de segurança.
- 2. Cibersegurança**
 - 2.1. Monitorização
 - 2.1.1. Implementação da monitorização contínua das ameaças e manutenção da plataforma *SIEM*;
 - 2.1.2. Revisão dos procedimentos e destacamento da importância da proteção dos domínios contra acessos não autorizados.
 - 2.2. Auditorias e Certificações
 - 2.2.1. Realização periódica de auditorias para garantir a conformidade com os padrões de segurança;
 - 2.2.2. Alcançar novos níveis de certificação, de forma a reforçar a credibilidade e segurança dos serviços prestados.
- 3. Parcerias estratégicas**
 - 3.1. Colaboração com entidades de segurança
 - 3.1.1. Participação ativa nas iniciativas da rede nacional *CSIRT*;
 - 3.1.2. Desenvolvimento de uma plataforma em colaboração com o CNCS, com capacidade de deteção e mitigação de vulnerabilidades em *websites*.
- 4. Promoção da segurança digital**
 - 4.1. Conscientização e adesão
 - 4.1.1. Elaborar iniciativas colaborativas com os *registrars* para promover a adoção de medidas de segurança;
 - 4.1.2. Publicação de um relatório sobre os padrões de segurança nos *registrars* por parte da equipa PTSOC, com o objetivo de melhorar a transparência.

¹¹⁵⁵ .pt, “Relatório de Atividades e Contas 2022”, 18-19 e 30-36.

Portugal tem feito uma aposta significativa em tecnologias e infraestruturas digitais, como o Plano de Ação para a Transição Digital. O desafio reside, em grande parte, na adoção e integração destas tecnologias pelas empresas e na formação dos seus trabalhadores para utilizar eficazmente as novas ferramentas digitais. A resistência à mudança e a falta de competências digitais entre os trabalhadores são barreiras que precisam de ser superadas para que o país possa aproveitar plenamente os benefícios da economia digital¹¹⁵⁶.

A iniciativa Plano de Ação para a Transição Digital tem como grande objetivo acelerar a transformação digital de Portugal (estado, empresas e pessoas), tornando o país mais competitivo a nível internacional, conforme é definido pela Diretiva NIS. Os três principais pilares de atuação deste plano são: “Capacitação e inclusão digital”, “Transformação digital empresarial” e “Digitalização do Estado”¹¹⁵⁷.

O primeiro pilar, “Capacitação e inclusão digital”, tem como foco três subpilares: “Educação digital”, “Requalificação e formação digital”, e “Literacia digital”¹¹⁵⁸. O primeiro subpilar propõe-se a ser cumprido com a implementação de um programa para transformar digitalmente as escolas, colocar a disciplina de TIC no ensino básico, fazer uma promoção da programação e robótica na escola e criar uma iniciativa denominada por “Engenheiras por 1 Dia”, onde incentiva a participação de pessoas do género feminino nas áreas de tecnologias¹¹⁵⁹. No subpilar “Requalificação e formação digital” propõe-se a ser criado um programa “UpSkill” que irá formar intensivamente cerca de 3000 profissionais na área digital, haverá formações nas áreas digitais para desempregados, professores e formadores, e irão ser aplicadas metodologias inovadoras em cursos profissionais. Por fim, no subpilar “Literacia digital”, propõe-se a ser criado um programa de inclusão digital com o objetivo de oferecer competências digitais básicas a cerca de um milhão de adultos, irá também ser criada uma tarifa social para garantir o acesso a serviços de Internet a preços mais reduzidos e irão ser desenvolvidas comunidades criativas para promover a inclusão digital¹¹⁶⁰. O principal objetivo deste pilar é melhorar a qualidade do ensino, dotar os alunos de competências digitais, promover a igualdade de oportunidades, alargar a oferta formativa das instituições de ensino superior, aproximando-as das necessidades do mercado laboral e requalificar trabalhadores para minimizar o impacto da automatização que já está a decorrer no mercado de trabalho¹¹⁶¹. A Diretiva NIS exige que as infraestruturas essenciais, como saúde, energia, telecomunicações e transportes, estejam protegidas contra incidentes de cibersegurança. Devido a isto, é vital assegurar que as pessoas que operam ou interagem com estas infraestruturas tenham o conhecimento necessário e estejam aptas para manter a segurança e a integridade dos sistemas¹¹⁶².

¹¹⁵⁶ Miguel Abecasis et al., “O impacto do digital na economia portuguesa”, https://web-assets.bcg.com/img-src/O-impacto-do-Digital-na-economia-portuguesa_tcm9-214461.pdf.

¹¹⁵⁷ “Sobre nós”, Portugal Digital, <https://portugaldigital.gov.pt/sobre-nos/>.

¹¹⁵⁸ “Plano de Ação para a Transição Digital de Portugal”, Portugal Digital, 5 de março de 2020, 16, https://portugaldigital.gov.pt/wp-content/uploads/2022/01/Plano_Acao_Transicao_Digital.pdf.

¹¹⁵⁹ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 17.

¹¹⁶⁰ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 18.

¹¹⁶¹ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 22,23 e 25.

¹¹⁶² Diretiva 2016/1148, <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148>.

O segundo pilar denominado por “Transformação digital empresarial” é constituído por três subpilares: “Empreendedorismo e atração de investimento”, “Tecido empresarial, com foco nas PME” e “Transferência de conhecimento científico e tecnológico para a economia”¹¹⁶³. No primeiro subpilar está planeada a criação do programa “e-Residency”, e tem como objetivo criar um sistema de identidade digital de forma a facilitar a relação das empresas estrangeiras com Portugal. Este subpilar conta com mais iniciativas, nomeadamente: A criação de um programa de capacitação digital de Pequenas e Médias empresas (PMEs) localizadas no interior do país, financiamento e apoio a investimento feito em iniciativas digitais e a criação do programa *Experience i4.0* que tem como objetivo fornecer ferramentas para medir a maturidade digital das empresas. O objetivo do segundo subpilar é conectar as PME com grandes empresas, desenvolver ferramentas para apoiar as PME no registo de patentes e financiar o aumento da presença digital das PME. Por fim, no último subpilar a principal medida é a promoção das zonas livres tecnológicas (ZLT), estas ZLT têm como grande objetivo incentivar a inovação e a criação de parcerias com universidades. Este pilar tem como grande objetivo tornar o tecido empresarial das PME mais digital¹¹⁶⁴. De acordo com a Diretiva NIS, a adoção de novas tecnologias e a digitalização dos processos empresariais aumentam a exposição a riscos de cibersegurança, devido a isto, é importante garantir que esta inovação tecnológica não compromete a segurança e a continuidade operacional nos setores essenciais para a economia e segurança nacional¹¹⁶⁵.

Por fim, o terceiro pilar “Digitalização do Estado” tem, também, três subpilares e o principal objetivo deste pilar é digitalizar os serviços do estado. O primeiro subpilar “Serviços Públicos Digitais” apresenta medidas como a digitalização dos serviços públicos mais utilizados pelos cidadãos e empresas, e aumentar a oferta de serviços digitais no portal ePortugal. O segundo subpilar “Administração central ágil e aberta” tem como principais medidas: tramitação eletrónica de processos de contraordenação, desenvolvimento de uma estratégia *cloud* para a administração pública e uma promoção ativa do teletrabalho. Por fim, o subpilar “Administração regional e local conectada e aberta” tem como medidas a implementação da estratégia nacional de Cidades Inteligentes e a coordenação do território através do Balcão Único do Prédio¹¹⁶⁶.

Esta iniciativa é considerada um documento “vivo”, pois está sujeito à inclusão de novas medidas ou atualização das já existentes. A iniciativa deverá refletir o dinamismo das prioridades e preocupações da economia e da sociedade e, também, deve respeitar a estrutura estabelecida¹¹⁶⁷. Conforme o contexto da Diretiva NIS, a transição digital das infraestruturas digitais é fundamental no setor. É importante assegurar que esta transformação ocorre de maneira segura, protegendo sempre as infraestruturas críticas de forma a garantir a segurança nacional num cenário digital global.

¹¹⁶³ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 27.

¹¹⁶⁴ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 27-37.

¹¹⁶⁵ Diretiva 2016/1148.

¹¹⁶⁶ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 39-46.

¹¹⁶⁷ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 65 e 66.

7.4. Investimento em cibersegurança

Segundo o documento final “Avaliação do potencial económico da transição digital em Portugal” de 2023, existem dois principais “Apoios públicos no âmbito de Infraestruturas e Conectividade”¹¹⁶⁸:

- Apoios públicos no âmbito de intervenções em infraestruturas digitais e conectividade a nível nacional:
 - intervenções enquadradas no objetivo específico “RSO1.5. Reforçar a conectividade digital” integrado no **Portugal 2030**.
- Apoios públicos, iniciativas, planos e programas europeus no âmbito da promoção das infraestruturas digitais e conectividade na **UE**:
 - UE dispõe de um conjunto de instrumentos, iniciativas, planos e programas destinados a promover as infraestruturas digitais e a conectividade a nível europeu, em alinhamento com os objetivos definidos no programa Década Digital¹¹⁶⁹;
 - No caso da produção de semicondutores, existe a Aliança para Tecnologias de Processadores e Semicondutores¹¹⁷⁰.
 - No caso do aumento da implantação de nós periféricos, destacam-se a Aliança Europeia para os Dados Industriais, *Edge* e Nuvem¹¹⁷¹, que resultará potencialmente em sinergias de investimento, e o Programa Europa Digital¹¹⁷², que tem como objetivo financiar, entre outros temas, a criação de nós periféricos.
 - Sobre a criação do primeiro computador com aceleração quântica, destaca-se a iniciativa *Quantum Technologies Flagship*¹¹⁷³.

¹¹⁶⁸ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 95.

¹¹⁶⁹ Comissão Europeia, “Década Digital da Europa: metas digitais para 2030”, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt.

¹¹⁷⁰ Comissão Europeia, “Aliança sobre processadores e tecnologias de semicondutores”, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/pt/policies/alliance-processors-and-semiconductor-technologies>.

¹¹⁷¹ Comissão Europeia, “Aliança Europeia para os Dados Industriais, a Edge e a Nuvem”, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/pt/policies/cloud-alliance>.

¹¹⁷² Comissão Europeia, “Programa Europa Digital”, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/pt/activities/digital-programme>.

¹¹⁷³ Comissão Europeia, “Quantum Technologies Flagship”, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>.

No contexto dos apoios públicos no âmbito de intervenções em infraestruturas digitais e conectividade a nível nacional, estão definidas ações enquadradas no objetivo específico “RSO1.5. Reforçar a conectividade digital” integrado no **Portugal 2030**, a aplicar a diferentes regiões:

Tabela 56 - Intervenções em Infraestruturas Digitais

Região	Prioridade	Ações
PT - Programa Regional de Lisboa ¹¹⁷⁴	Não estão definidas ações no contexto de reforço de conectividade digital na região de Lisboa.	
PT - Programa Regional do Centro 2021-2027 ¹¹⁷⁵	Conectividade Digital	Instalação de redes de banda larga
PT - Programa Regional do Norte 2021-2027 ¹¹⁷⁶	Norte mais Competitivo e Conectividade Digital	Instalação, gestão, exploração e manutenção de redes de comunicações eletrónicas de capacidade muito elevada (Gigabit)
PT - Programa Regional do Alentejo 2021-2027 ¹¹⁷⁷	Alentejo mais digital	Instalação, gestão, exploração e manutenção de redes de comunicações eletrónicas de capacidade muito elevada (banda larga) - Instalação, gestão, exploração e manutenção de redes de comunicações eletrónicas de capacidade muito elevada: Infraestruturas digitais de banda larga (fixa e móvel) seguras, eficientes e sustentáveis prioritariamente em espaços de baixa densidade populacional ou do interior, instalando redes de comunicações eletrónicas de elevada capacidade nos territórios não cobertos pelo mercado de telecomunicações (e.g. zonas brancas), onde estas operações comerciais não são rentáveis, procurando, assim, suprir através de investimento público, nas componentes grossista e (parte) retalhista, a oferta de serviços não coberta pelas obrigações decorrentes do leilão 5G.
PT - Programa Regional do Algarve 2021-2027 ¹¹⁷⁸	Conectividade Digital	Instalação e gestão de redes de comunicações eletrónicas de capacidade muito elevada (banda larga)

¹¹⁷⁴ “PT - Programa Regional de Lisboa 2021-2027”, *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_lisboa.pdf.

¹¹⁷⁵ “PT - Programa Regional do Centro 2021-2027”, *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_centro.pdf.

¹¹⁷⁶ Alina Silva et al., “Estratégia de Desenvolvimento do Norte para Período de Programação 2021-27 das Políticas da União Europeia”, PT - Programa Regional do Norte 2021-2027, *Portugal 2030*, <https://www.ccdr-n.pt/storage/app/media/2021/CCDRN%202030-compactado.pdf>.

¹¹⁷⁷ “PT - Programa Regional do Alentejo 2021-2027”, *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_alentejo.pdf.

¹¹⁷⁸ “PT - Programa Regional do Algarve 2021-2027”, *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_algarve.pdf.

Lançada em julho de 2021 pela Comissão Europeia, a **Aliança sobre processadores e tecnologias de semicondutores** tem como objetivo reunir *stakeholders* essenciais que contribuam para a projeção e produção de *microchips*. O objetivo final destes *stakeholders* é o de dotar a UE das capacidades necessárias em tecnologias de semicondutores para alimentar as suas infraestruturas digitais críticas e redes de comunicação. As principais ações são as seguintes¹¹⁷⁹:

1. O reforço do ecossistema europeu de conceção eletrónica, incluindo nós finais e soluções de *hardware* de código aberto.
2. O estabelecimento da capacidade de fabrico necessária, incluindo testes de montagem para produção de processadores fiáveis, componentes eletrónicos e tecnologias. Semicondutores mais avançados permitirão o aumento de desempenho e a redução da energia utilizada por *data centers* ou *endpoints*.

Da mesma maneira, a **Aliança Europeia para os Dados Industriais, a Edge e a Nuvem** pretendem reunir representantes que tenham um papel determinante no reforço da posição da UE no que diz respeito a tecnologias de computação em nuvem e periféricas (IA, IoT e tecnologia 5G). As suas ações são as seguintes¹¹⁸⁰:

- reunir os intervenientes relevantes para preparar e atualizar roteiros de investimento horizontais e tecnológicos específicos em matéria de computação em nuvem e de vanguarda;
- formular recomendações para assegurar a integração coerente dos investimentos para a instalação de espaços comuns europeus de dados em domínios relevantes;
- aconselhar a Comissão sobre os requisitos e normas aplicáveis aos serviços de computação em nuvem, incluindo os contratos públicos.

O **Programa Europa Digital** consiste num programa de financiamento da UE centrado na integração da tecnologia digital nas empresas, cidadãos e administrações públicas. Neste sentido, e com foco nas PME, o orçamento previsto de 7,5 mil milhões de euros pretende apoiar projetos em cinco principais domínios de capacidade: supercomputação, IA, cibersegurança, competências digitais avançadas e garantia de uma ampla utilização das tecnologias digitais em toda a economia e na sociedade, nomeadamente através de polos de inovação digital¹¹⁸¹.

Com um orçamento previsto de mil milhões de euros da UE, a iniciativa **Quantum Technologies Flagship** pretende apoiar o trabalho de centenas de investigadores quânticos num período de 10 anos. O principal objetivo deste projeto é o de apoiar diferentes ramos da investigação em domínio europeu, tais como: computação quântica, simulação quântica, comunicação quântica e deteção quântica¹¹⁸².

¹¹⁷⁹ Comissão Europeia, “Aliança sobre processadores e tecnologias de semicondutores”, *Shaping Europe’s digital future*.

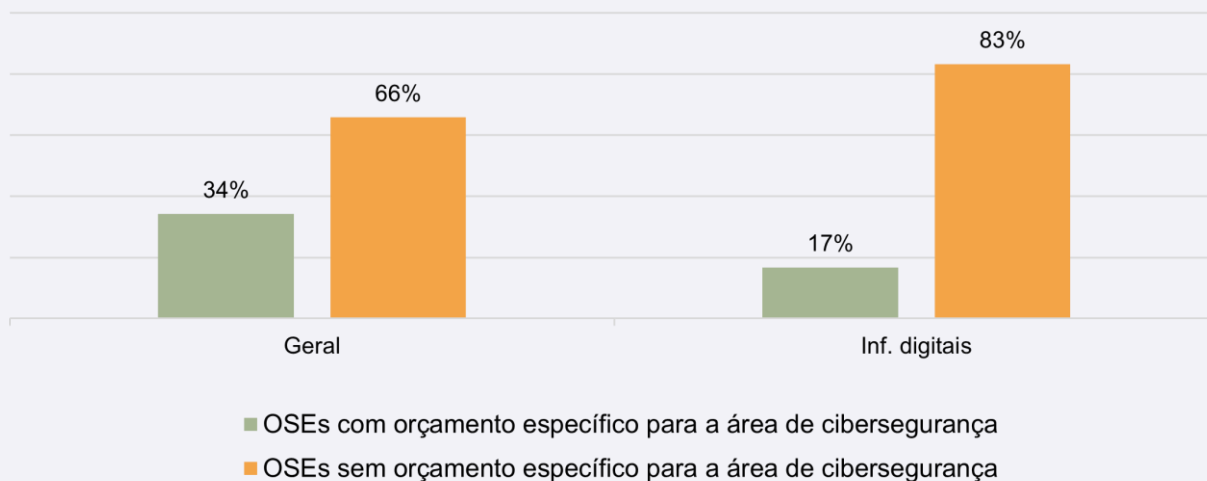
¹¹⁸⁰ Comissão Europeia, “Aliança Europeia para os Dados Industriais, a Edge e a Nuvem apresenta os seus primeiros resultados”, *Shaping Europe’s digital future*.

¹¹⁸¹ Comissão Europeia, “Programa Europa Digital”, *Shaping Europe’s digital future*.

¹¹⁸² Comissão Europeia, “Quantum Technologies Flagship”, *Shaping Europe’s digital future*.

Deste setor, cerca de 17% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Relativamente às áreas de aplicação do orçamento de cibersegurança, a maior parte das áreas de aplicação têm um valor de 50%, exceção para a gestão de vulnerabilidades, análise de segurança, segurança das redes e aquisição de *software* com 75%. Relativamente ao contexto geral, este setor tem uma percentagem maior na contratação de pessoal, gestão de vulnerabilidades e *governance* (**Gráfico 110 e 110.6**).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

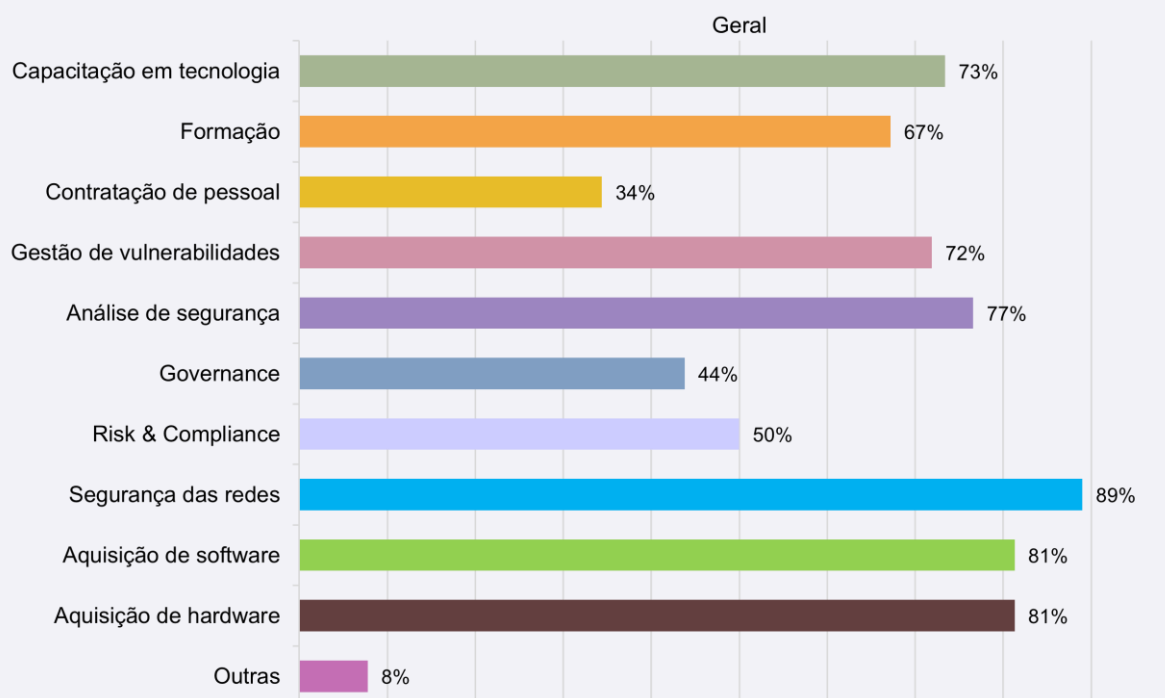
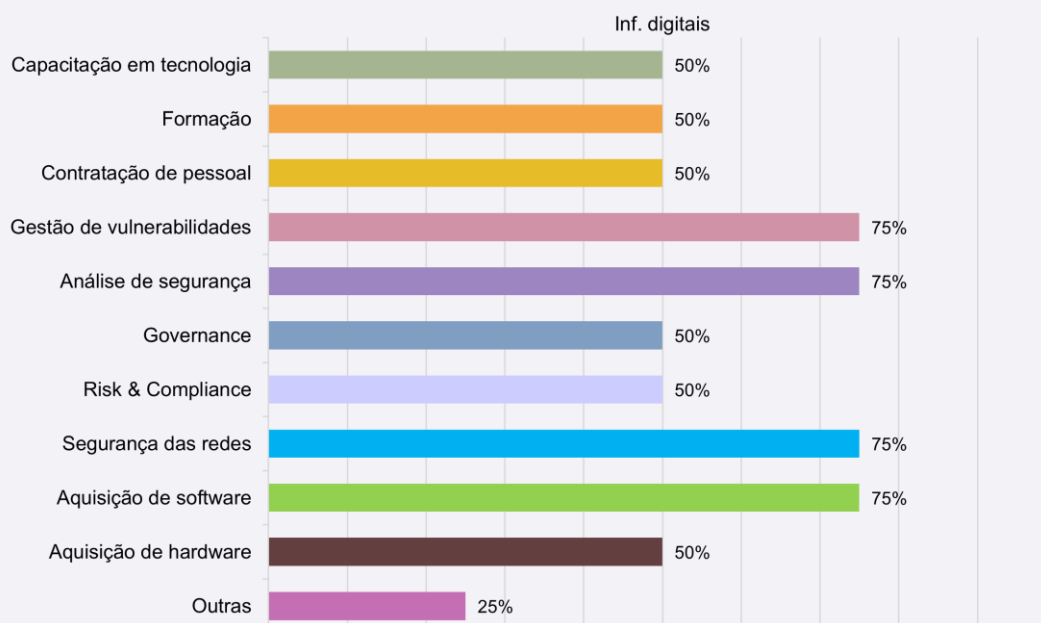
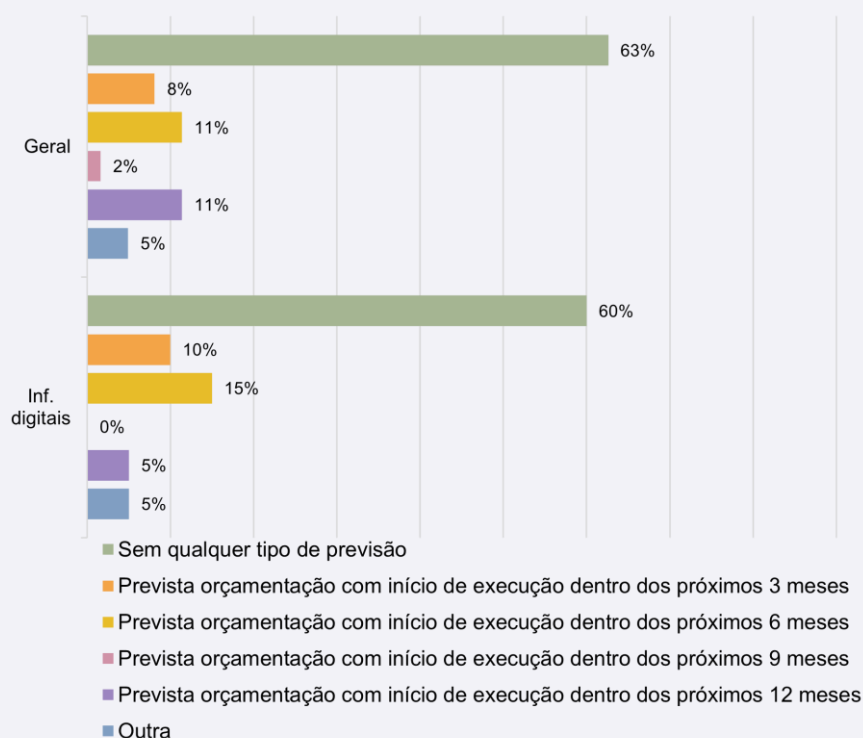


Gráfico 110.6 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 60% não tem qualquer previsão para a orçamentação, 10% tem previsto a orçamentação dentro dos próximos 3 meses, 15% tem previsto a orçamentação para os próximos 6 meses e 5% para os próximos 12 meses. A maior diferença em relação à média geral está na orçamentação com início de execução dentro dos próximos 6 meses, onde este setor tem 15% e a média geral é de 11% (**Gráfico 111**).

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



Atualmente, os centros de dados são peças fundamentais para o funcionamento das empresas. Há cada vez mais centros de dados em Portugal, o que leva a um crescimento da economia e à formação de novos empregos. Ainda relativamente à transição digital, existem outros conjuntos de iniciativas e medidas:

- **Indústria 4.0:** É uma iniciativa que está integrada na Estratégia Nacional para a Digitalização da Economia, com o objetivo de criar condições favoráveis para o desenvolvimento da indústria nacional;
- **Open Days i4.0:** Integra a iniciativa da Indústria 4.0 e tem como grande objetivo demonstrar e partilhar as boas práticas das empresas nacionais;
- **Capacitar i4.0:** Também integra a iniciativa da Indústria 4.0 e tem como objetivo preparar e qualificar pessoas e organizações com competências técnicas para a Indústria 4.0;
- **SHIFT2Future:** O principal objetivo deste projeto é o de acelerar e apoiar a transição para a economia 4.0 e tem como publica alvo as PMEs dos setores de moldes e plásticos, pedra, cerâmica, automóvel, TI, *IoT*, entre outros, nas regiões Norte, Centro e Alentejo;
- **SHIFT to 4.0:** É uma ferramenta de diagnóstico para avaliar a maturidade digital de uma empresa, elaborando um relatório com linhas orientadoras de forma a ser possível melhorar a mesma com base na economia 4.0¹¹⁸³.

¹¹⁸³ "Transição Digital", *IAPMEI*, 23 de novembro de 2023, <https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Industria-e-Sustentabilidade/Transformacao-digital.aspx>.

7.5. RJSC e legislação setorial

A União Europeia tem sido o principal legislador do setor das infraestruturas digitais ao nível da cibersegurança, através da publicação de regulamentos e diretivas. A nível nacional, a legislação existente decorre principalmente da transposição dos diplomas europeus para o ordenamento jurídico português e da regulamentação feita pela entidade reguladora do setor - a Autoridade Nacional de Comunicações (ANACOM).

Apesar da atual preponderância do direito europeu no setor, é importante referir que este foi primeiro legislado a nível nacional no ano de 2004. A Lei n.º 5/2004, de 10 de fevereiro, também conhecida como Lei das Comunicações Eletrónicas, impunha “às empresas que oferecem redes e serviços de comunicações eletrónicas [condições de] segurança das redes públicas contra o acesso não autorizado (...) [e de] proteção dos dados pessoais e da privacidade no domínio específico das comunicações eletrónicas, em conformidade com a legislação aplicável à proteção de dados pessoais e da privacidade”¹¹⁸⁴. Com o tempo, esta lei foi sendo alterada por outras, de modo a acomodar novos requisitos legais face à evolução tecnológica e à legislação europeia que foi sendo produzida. A lei n.º 5/2004 acabaria por ser integralmente revogada com a Lei n.º 16/2022, de 16 de agosto, que transpõe o Código Europeu das Comunicações Eletrónicas (Diretiva (UE) 2018/1972).

Veja-se então que legislação, nacional e europeia, foi surgindo para o setor das infraestruturas digitais até à revogação da Lei n.º 5/2004.

Diretiva n.º 2002/58/CE e Lei n.º 41/2004, de 18 de agosto (transposição): Esta diretiva e lei estabeleciam o regime aplicável ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, colocando obrigações “às empresas que oferecem redes e as empresas que oferecem serviços de comunicações eletrónicas”¹¹⁸⁵ ao nível da segurança, tal como o dever de “colaborar entre si no sentido da adoção de medidas técnicas e organizacionais eficazes para garantir a segurança dos seus serviços e, se necessário, a segurança da própria rede”¹¹⁸⁶, bem como de “garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público”¹¹⁸⁷.

¹¹⁸⁴ Lei n.º 5/2004, de 10 de fevereiro, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/5-2004-581061>.

¹¹⁸⁵ Lei n.º 41/2004, de 18 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/41-2004-480710>.

¹¹⁸⁶ Lei n.º 41/2004.

¹¹⁸⁷ Lei n.º 41/2004.

Diretivas n.ºs 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/CE, 2009/140/CE e Lei n.º 51/2011, de 13 de setembro (transposição):

Respetivamente, a primeira diretiva era relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos¹¹⁸⁸, a segunda relativa à autorização de redes e serviços de comunicações eletrónicas¹¹⁸⁹, a terceira relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas¹¹⁹⁰, a quarta relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas¹¹⁹¹. A quinta diretiva (2009/140/CE) introduziu alterações às primeiras quatro referidas. A Lei n.º 51/2011, de 13 de setembro, transpõe estas diretivas para o ordenamento jurídico português. Estas diretivas e lei impuseram obrigações de “avaliar a segurança e integridade das redes e serviços no âmbito das políticas de segurança adotadas”¹¹⁹², de adotar “medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços visando, em especial, impedir ou minimizar o impacto dos incidentes de segurança”¹¹⁹³, bem como de informar as autoridades reguladoras competentes (ENISA) e o público sobre graves violações de segurança¹¹⁹⁴.

Regulamento (UE) 2015/2120: Este regulamento não introduziu novas obrigações ao nível da cibersegurança, mas alterou a Lei das Comunicações Eletrónicas de modo a fortalecer os direitos dos cidadãos europeus no acesso à Internet aberta e ao tratamento equitativo do tráfego de dados por dos prestadores de serviços de acesso à Internet¹¹⁹⁵.

¹¹⁸⁸ Diretiva 2002/19/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos (diretiva acesso), *Jornal Oficial das Comunidades Europeias*, 7, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0019>.

¹¹⁸⁹ Diretiva 2002/20/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa à autorização de redes e serviços de comunicações eletrónicas (diretiva autorização), *Jornal Oficial das Comunidades Europeias*, 21, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:PT:PDF>.

¹¹⁹⁰ Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), *Jornal Oficial das Comunidades Europeias*, 33, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:pt:PDF>.

¹¹⁹¹ Diretiva 2002/22/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas (diretiva serviço universal), *Jornal Oficial das Comunidades Europeias*, 51, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0022>.

¹¹⁹² Lei n.º 51/2011, de 13 de setembro, *Procuradoria-Geral Distrital de Lisboa*, https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=1515&pagina=1&ficha=1#.

¹¹⁹³ Lei n.º 51/2011.

¹¹⁹⁴ Lei n.º 51/2011.

¹¹⁹⁵ Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta, *Jornal Oficial da União Europeia*, 8, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015R2120>.

Diretiva (UE) 2016/1148 (NIS), Lei n.º 46/2018, de 13 de agosto (transposição que estabelece o Regime Jurídico da Segurança do Ciberespaço - RJSC) e Decreto-Lei n.º 65/2021, de 30 de julho (que regulamenta o RJSC): A Diretiva (UE) 2016/1148¹¹⁹⁶, bem como a Lei n.º 46/2018, de 13 de agosto¹¹⁹⁷, foram os diplomas que identificaram os operadores deste setor como operadores de serviços essenciais. Embora legislação anterior impusesse já obrigações ao nível da cibersegurança, estes foram os atos legislativos de maior importância dedicados exclusivamente à segurança das redes e sistemas. Foram também estes atos legislativos que impuseram obrigações de reporte de incidentes relevantes ao Centro Nacional de Cibersegurança. Depois, com a publicação do Decreto-Lei n.º 65/2021, de 30 de julho, que veio regulamentar o RJSC, foram impostas obrigações como a designação de um ponto de contacto permanente, um responsável de segurança, a elaboração e manutenção de um inventário de ativos, a elaboração e implementação de um plano de segurança, a elaboração de um relatório anual que inclua as principais atividades desenvolvidas em matéria de cibersegurança e estatísticas análises agregadas dos incidentes relevantes ocorridos, bem como a realização de uma análise de risco anual¹¹⁹⁸.

Lei n.º 16/2022, de 16 de agosto: Face às diversas alterações que foram sendo introduzidas à primeira Lei das Comunicações Eletrónicas, foi criada em 2022 uma nova Lei das Comunicações Eletrónicas, alinhada com a evolução tecnológica ocorrida desde 2004 e com as exigências legais europeias, revogando a Lei n.º 5/2004. Ao nível da cibersegurança, foram introduzidos novos requisitos, tais como o dever de cooperar com a Autoridade Reguladora Nacional (a ANACOM) no âmbito da segurança do ciberespaço; a utilização de cifragem, quando adequada, para maior proteção das redes e dos serviços, bem como para minimização dos impactos dos incidentes de segurança¹¹⁹⁹. A nova lei refere também que, ao adotar medidas técnicas e organizacionais de segurança, devem ser tidos em conta diversos aspetos, como a segurança física e ambiental, a capacidade de deteção e os procedimentos de gestão de incidentes de segurança, a continuidade operacional e de prestação do serviço, bem como auditorias testes exercícios aos planos de contingência, à segurança das redes e à capacidade de prestação de serviços¹²⁰⁰. Ao nível dos incidentes de segurança, esta lei reproduz a necessidade já inscrita no RJSC (Lei n.º 46/2018, de 13 de agosto) de notificar o Centro Nacional de Cibersegurança de qualquer incidente de segurança com impacto significativo no funcionamento das redes ou serviços, mas acrescentando também a necessidade de o comunicar à ANACOM¹²⁰¹.

¹¹⁹⁶ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, *Jornal Oficial da União Europeia*, 14 e 29, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148>.

¹¹⁹⁷ Lei n.º 46/2018, de 13 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.

¹¹⁹⁸ Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.

¹¹⁹⁹ Lei n.º 16/2022, de 16 de agosto, *Diário da República*, <https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298>.

¹²⁰⁰ Lei n.º 16/2022.

¹²⁰¹ Lei n.º 16/2022.

Diretiva (UE) 2022/2555¹²⁰² (NIS 2): Seis anos depois da publicação da Diretiva NIS, as instituições europeias publicaram uma nova Diretiva que veio atualizar a anterior. A Diretiva NIS 2 classifica dois tipos de setores: “setores de importância crítica”¹²⁰³ e “outros setores críticos”¹²⁰⁴. Os setores já visados pela Diretiva NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

O setor das infraestruturas digitais é um dos setores que passa por uma maior transformação. Enquanto na Diretiva NIS 1 o setor era composto por apenas três tipos de entidades (IXPs, prestadores de serviços de DNS, e registos de domínios de topo), na Diretiva NIS 2 o setor passa abranger seis novos tipos de entidades. São eles: prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados (*data centres*), fornecedores de redes de distribuição de conteúdos, prestadores de serviços de confiança, fornecedores de redes públicas de comunicações eletrónicas e prestadores de serviços de comunicações eletrónicas acessíveis ao público¹²⁰⁵.

Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos¹²⁰⁶. Adicionalmente, as medidas de gestão de risco adotadas devem ter em consideração diversos aspetos, tais como as políticas de análise dos riscos e de segurança dos sistemas de informação, o tratamento dos incidentes, a continuidade das atividades, a segurança da cadeia de abastecimento, segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, práticas básicas de ciber-higiene e formação em cibersegurança, políticas e procedimentos sobre a utilização de criptografia, segurança dos recursos humanos (com ênfase no controlo de acessos e na gestão de ativos) e ainda a utilização de soluções de autenticação multifator ou contínua, bem como comunicações seguras de voz, vídeo e texto¹²⁰⁷.

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como “ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques”¹²⁰⁸.

¹²⁰² Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

¹²⁰³ Diretiva (UE) 2022/2555, Anexo I.

¹²⁰⁴ Diretiva (UE) 2022/2555, Anexo II.

¹²⁰⁵ Diretiva (UE) 2022/2555, Anexo I.

¹²⁰⁶ Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

¹²⁰⁷ Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

¹²⁰⁸ Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

7.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor de Infraestruturas Digitais, segundo o relatório “*Mapping of OES Security Requirements to Specific sectors*” da ENISA.

Tabela 57 - Standards e Boas Práticas (Infraestruturas Digitais)

Standards	Boas práticas
- ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 - NIST Cybersecurity Framework - TIA-942 - ISO/IEC 20000 - ISO/IEC 17788	- Technical guidance on the security measures for Telcos in Article 13a, ENISA - Best Practices – IX-F - ITIL - Information Technology Infrastructure Library

De seguida, apresenta-se um breve sumário de cada um dos *standards* e boas práticas:

- **ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:** Estabelece um quadro de políticas e processos para gerir a segurança da informação de forma sistemática para organizações de telecomunicações, garantindo assim a confidencialidade e a integridade de informações sensíveis¹²⁰⁹;
- **NIST Cybersecurity Framework:** Utilizado para ajudar as organizações a entender e gerir os riscos de cibersegurança. Está organizado em cinco funções principais: Identificar, Proteger, Detetar, Responder e Recuperar¹²¹⁰;
- **TIA-942:** Estabelece requisitos para a infraestrutura de centro de dados, incluindo para a arquitetura, energia e segurança¹²¹¹;
- **ISO/IEC 20000:** Norma para a gestão de serviços de TI, baseada em *ITIL*¹²¹²;
- **ISO/IEC 17788:** Define os conceitos e terminologia a utilizar nos serviços de *cloud*¹²¹³;
- **Technical guidance on the security measures for Telcos in Article 13a, ENISA:** O artigo 13 da ENISA detalha os requisitos de proteção contra ameaças de cibersegurança. Fornece também diretrizes específicas para garantir a resiliência e segurança dos serviços de telecomunicações¹²¹⁴;
- **Best Practices – IX-F:** Fornece diretrizes para uma operação eficiente e com segurança de *IXPs* (*Internet Exchange Points*). É abordado, também, a gestão de tráfego, segurança e infraestrutura¹²¹⁵;
- **ITIL - Information Technology Infrastructure Library:** Conjunto de práticas para a gestão de serviços de TI¹²¹⁶.

¹²⁰⁹ ISO, “Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002”, 2008, <https://www.iso.org/standard/43751.html>.

¹²¹⁰ NIST, “NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral”, fevereiro de 2024, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf>.

¹²¹¹ Telecommunications Industry Association, “ANSI/TIA-942 Standard”, <https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/>.

¹²¹² ISO, “Part 1: Service management system requirements”, 2018, <https://www.iso.org/standard/70636.html>.

¹²¹³ ISO, “Information technology — Cloud computing — Overview and vocabulary”, 2014, <https://www.iso.org/standard/60544.html>.

¹²¹⁴ ENISA, “Technical Guideline on Security Measures”, <https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures>.

¹²¹⁵ Euro-IX, “IX-F – Best Practices”, agosto de 2015, <https://www.af-ix.net/sites/default/files/08%20-%20Bijal%20Sanghani%20-%20IX-F%20Best%20Practices.pdf>.

¹²¹⁶ CIO, “What is ITIL? Your guide to the IT Infrastructure Library”, 16 de maio de 2022, <https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-til-definition-and-solutions.html>.

7.7. Desafios

No contexto da área de Infraestruturas e Conectividade analisado no documento “Avaliação do Potencial Económico da Transição Digital em Portugal” de 2023, encontram-se identificados alguns desafios e obstáculos resultado de exercícios de auscultação aos principais *stakeholders* (entre empresas e entidades institucionais/ públicas) no âmbito da transição digital. Cerca de 3% destes *stakeholders* (13% PME) dizem haver uma inadequada/reduzida infraestrutura digital em Portugal. As limitações levantadas são as seguintes¹²¹⁷:

- desequilíbrio da presença de infraestruturas de suporte digital (3G, 4G e 5G) no território nacional (urbano vs rural), que provoca uma escassa presença de infraestruturas que suportem a Transição Digital no setor agrícola na totalidade do território, revelando-se fundamental a participação das câmaras municipais na mitigação desta situação;
- a escassez de redes de suporte desenvolvidas a nível nacional;
- falta de disponibilidade e qualidade da infraestrutura digital disponível, limitando a rentabilidade de certas zonas do país por escassez de infraestruturas;
- a escassez de infraestruturas de conectividade e computação a preços competitivos;
- elevado valor dos equipamentos/manutenção para as empresas mais pequenas, resultando em *outsourcing*;
- equipamentos obsoletos que não suportam a Transição Digital;
- dificuldades de licenciamento para *setup* e expansão da atividade.

De acordo com o artigo “O desafio digital” elaborado em junho de 2022, existem vários desafios neste setor, nomeadamente o aumento das desigualdades sociais e tensões sociais se não forem tomadas medidas adequadas na educação e formação, pois existe uma divisão crescente entre as pessoas que têm acesso às competências digitais e os que não têm e, esta desigualdade pode resultar em disparidades de bem-estar e possíveis exclusões no mercado de trabalho. A criação de nova tecnologia também traz alguns dilemas éticos com a crescente facilidade de vigilância personalizada e maciça, assim como o uso de dados pessoais sem autorização dos proprietários dos mesmos¹²¹⁸.

Este setor tem como principais tecnologias, para a conectividade, a fibra ótica e a rede 5G. Estas tecnologias oferecem diversas vantagens, já referidas anteriormente, mas encerram também algumas desvantagens, passíveis de colocar desafios ao setor, sobretudo a nível de custos. A fibra ótica tem um grande custo de instalação, e as interfaces e os conectores apresentam também custos elevados. O processo de reparar e manter os sistemas de fibra é, também este, elevado¹²¹⁹. Relativamente à tecnologia 5G, o grande desafio estará sempre na sua infraestrutura e no custo da mesma. Esta tecnologia requer a instalação de mais torres e antenas do que a tecnologia 4G, o que irá aumentar exponencialmente os seus custos, tanto de instalação como de manutenção e reparação¹²²⁰.

¹²¹⁷ “Avaliação do Potencial Económico da Transição Digital em Portugal”, Deloitte Business Consulting S.A e Universidade de Coimbra, 2023.

¹²¹⁸ Pedro Duarte, “O DESAFIO DIGITAL”, *Janus*, junho de 2022, <https://repositorio.ual.pt/server/api/core/bitstreams/350ce9d5-f3e3-45e2-aa85-8c76378eb077/content>.

¹²¹⁹ Kareem et al., “A Survey of Optical Fiber Communications: Challenges and Processing Time Influences”, abril de 2021, https://www.researchgate.net/profile/Subhi-Zeebaree/publication/351005349_A_Survey_of_Optical_Fiber_Communications_Challenges_and_Processing_Time_Influences/links/607ed8d48ea909241e10b11a/A-Survey-of-Optical-Fiber-Communications-Challenges-and-Processing-Time-Influences.pdf.

¹²²⁰ Ahmed A. Thabit, Bassam H. Abd e Ahmed Alkhayyat, “Challenges and Solutions of 5G Technology”, 2021, 55, <https://ieeexplore.ieee.org/abstract/document/9717458>.

Outro futuro desafio neste setor será a implementação da criptografia quântica. A criptografia quântica é mais complexa de implementar, uma vez que é baseada em algoritmos matemáticos altamente complexos. O maior desafio será implementar esta criptografia em certos dispositivos como por exemplo os de *IoT*. Estes dispositivos têm recursos muito limitados para correr algoritmos complexos o que torna a implementação difícil e pouco prática¹²²¹.

Por fim, o setor enfrenta um desafio crescente no âmbito do processamento de dados. Todos os dias existem novos dispositivos ligados à Internet, gerando assim um aumento da circulação de novos dados. Tal implica um aumento nos custos de armazenamento, bem como um grande aumento no esforço de gestão dos dados guardados e espaço de armazenamento disponível.

¹²²¹ David Ott et al., “Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility”, setembro de 2019, 7, <https://arxiv.org/pdf/1909.07353>.

7.8. Recomendações

Segundo o documento de “Avaliação do Potencial Económico de Transição Digital em Portugal”, e fruto dos exercícios de auscultação aos *stakeholders* identificados no âmbito da transição digital, foram levantadas várias recomendações a aplicar a esta área no futuro, como consequência da necessidade em assegurar uma adequada Infraestrutura Digital¹²²²:

- Fomento de lógicas de *public computing*;
- Dinamização e apoio às infraestruturas tecnológicas (e.g.: 5G), nomeadamente, para a criação de *test beds*;
- Desenvolvimento de *clusters* de computação de fácil acesso;
- Reforço da conectividade;
- Desenvolvimento/ implementação de infraestruturas de conectividade e computação avançada, com modelos de disponibilização, preferencialmente abertas ou a preços competitivos;
- Implementação de incentivos à renovação da infraestrutura existente.

No mesmo documento, são levantadas 3 grandes áreas de oportunidade de trabalho para o futuro do digital¹²²³:

- **Acesso a Internet de Alta Velocidade e Desempenho** através da promoção do desenvolvimento da cobertura e utilização de internet fixa e móvel de alta velocidade e desempenho, com foco na cobertura da rede de internet fixa de alta velocidade e aumento dos níveis de utilização deste tipo de serviço e na maximização da cobertura da rede 5G e participação ativa no desenvolvimento da rede 6G. As iniciativas levantadas e responsáveis por promover a melhoria desta área são as seguintes:
 - Criação de incentivos e/ou mecanismos regulatórios e contratuais que garantam a cobertura da rede de internet fixa de alta velocidade nos pontos onde não exista;
 - Desenvolvimento de mecanismos de suporte e estímulo à adoção de serviços de internet fixa de alta velocidade;
 - Normalização dos preços das comunicações tendo em consideração as práticas da UE, nomeadamente nos pacotes mais usados pelas empresas;
 - Investimento na cobertura total do território com rede de internet móvel 5G;
 - Diagnóstico e reflexão às melhores práticas e áreas de melhoria na implementação do 5G, como forma de participar no desenvolvimento ativo e apostar na posterior rápida instalação do 6G;
 - Desenho de regulamentação e legislação que favoreça e facilite a adoção e o desenvolvimento da tecnologia 6G;
 - Promoção da alocação e participação de especialistas em fóruns internacionais relativamente à rede 6G.
- Aposta na instalação de **Data Centres**;
- **Cooperação Internacional** para o Desenvolvimento das Infraestruturas Digitais: Dinamização da participação de Portugal nos instrumentos/ planos da UE, para promoção do desenvolvimento de ações em conjunto e criação de parcerias.

¹²²² Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 95.

¹²²³ Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 95.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste setor. Tais cenários são indicados na seguinte tabela:

Tabela 58 - Cenários de risco (Infraestruturas Digitais)

Cenários de risco

Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.

Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.

Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO WEB** (*SQL Injection* ou *Cross-site Scripting*).

FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.

VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.

RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

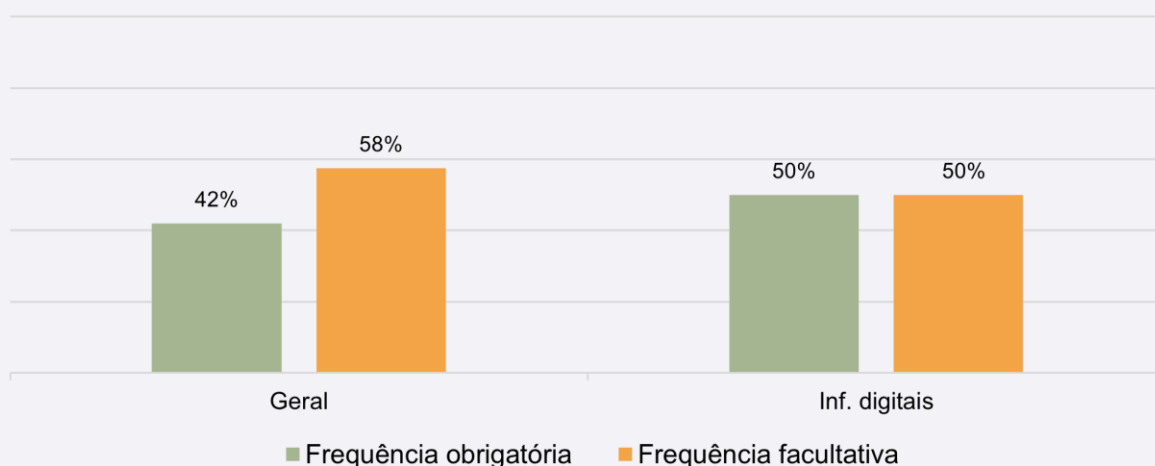
(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 23 de setembro de 2024, <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf>)

Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor, de seguida sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

Os resultados do questionário evidenciam que os OSE do setor se encontram divididos em partes iguais, onde 50% das formações em cibersegurança são de caráter facultativo e a restante percentagem não é, ressalvando que menos de metade do setor oferece formação. Relativamente ao contexto geral, este setor tem uma percentagem superior de frequência obrigatória com 42% no contexto geral contra 50% neste setor (**Gráfico 39**). Salientando que na maioria das entidades os momentos de formação têm frequência anual, o que, no contexto em questão, poderá ser insuficiente para assegurar a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores. Verifica-se ainda que a existência de cursos de atualização é escassa no setor. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória.

Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor das infraestruturas digitais, comparativamente com o geral, está abaixo em quase todas as medidas de proteção, com exceção das seguintes: *Firewall/WAF/Webfilter*, controlos de acesso à rede, manutenção de *logs* para análise após incidentes de segurança e análises de risco periódicas. Das medidas de proteção abaixo da média destacam-se as medidas de *awareness* sobre segurança, encriptação, autenticação multifator, equipa especialista em cibersegurança e *backups* de dados em diferentes localizações onde existe uma diferença entre 10 a 12%. Recomenda-se que estas medidas sejam aplicadas para se manterem com a média geral dos setores (Gráfico 66.7).

Gráfico 66.7 - Medidas de proteção contra ameaças de cibersegurança



É recomendado aos OSE do setor das infraestruturas digitais que:

- Realizem **avaliações de segurança** regularmente, conduzindo, no mínimo, uma avaliação anual, que inclua testes de penetração e auditorias de segurança para identificar e corrigir vulnerabilidades;
- Implementem **programas de sensibilização** em cibersegurança com a realização de sessões de formação semestrais obrigatórias para todos os colaboradores, com foco em boas práticas de cibersegurança, identificação de ameaças e resposta a incidentes;
- Adotem **métodos de cifragem**, utilizando a cifragem para proteger dados sensíveis tanto em trânsito quanto armazenados, assegurando que mesmo em caso de acesso não autorizado, os dados não possam ser lidos ou utilizados indevidamente;
- Implementem **autenticação multifator** (MFA) para todos os sistemas críticos, garantindo uma camada adicional de segurança;
- Realizar uma **monitorização da conformidade legal**, assegurando que a organização está em conformidade com todas as leis e regulamentos aplicáveis em matéria de cibersegurança, realizando auditorias regulares para verificar e manter essa conformidade;
- Façam uma **revisão e atualização de políticas de cibersegurança** de forma periódica (no mínimo, anualmente) para mantê-las alinhadas com a evolução das ameaças e as mudanças organizacionais.

Políticas, procedimentos e planos de cibersegurança

De acordo com os dados obtidos no questionário, mais de dois terços dos OSE do setor tinham documentado e implementado políticas e procedimentos de cibersegurança, uma percentagem superior à média dos setores. Além disso, apenas 46% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança, o que coloca este setor 4% abaixo da média geral dos outros setores (**Gráficos 77 e 78**).

Gráfico 77 - Documentação/Implementação de políticas e procedimentos de cibersegurança

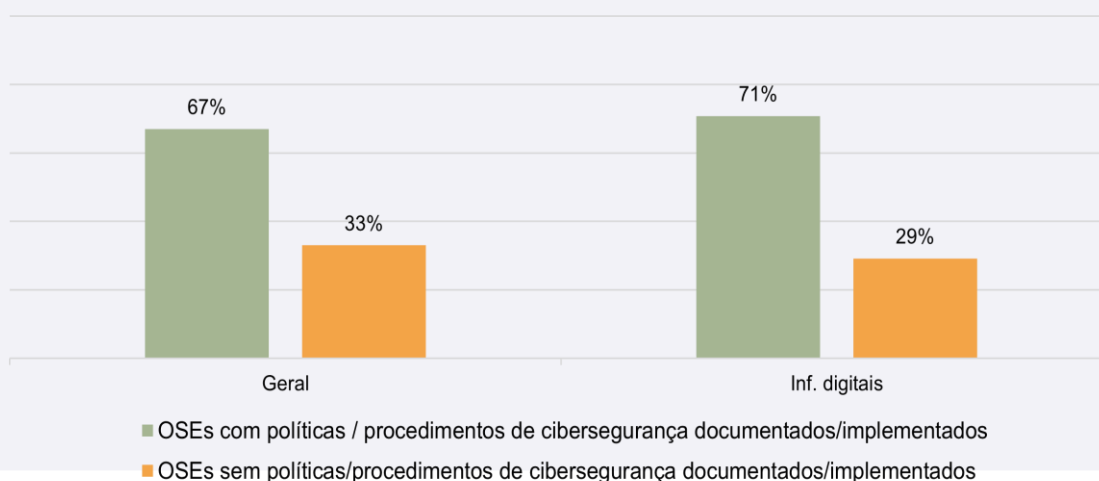
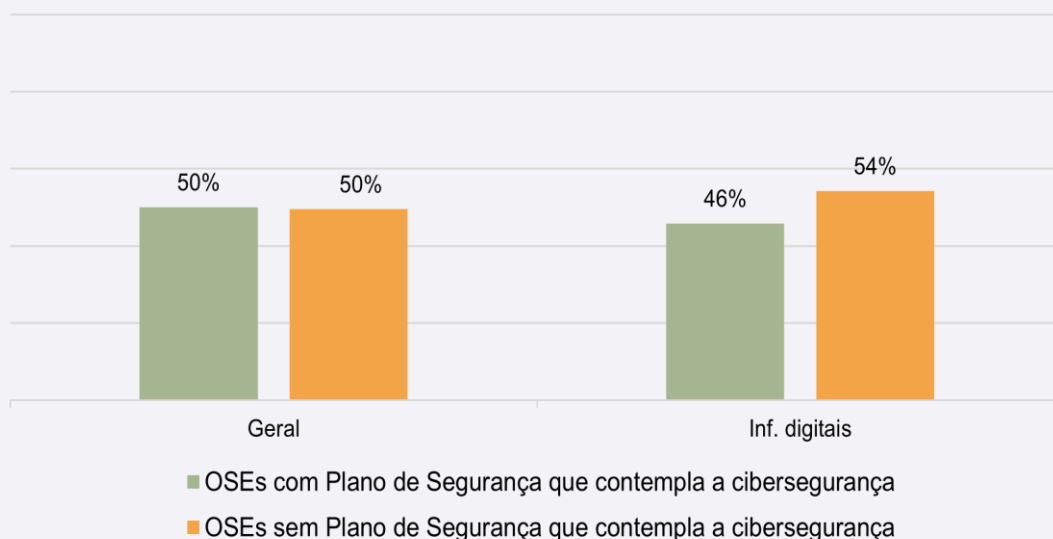


Gráfico 78 - Existência de Plano de Segurança que contemple a cibersegurança



Face a esta realidade, recomenda-se aos OSE do setor que ainda não o tenham feito que elaborem e implementem uma política de cibersegurança que verse sobre:

- **Papéis e responsabilidades:** definindo claramente os papéis e responsabilidades dos colaboradores em matéria de cibersegurança, assegurando que todos entendem as suas funções e o impacto das suas ações na segurança geral;
- **Gestão de riscos:** implementando processos para a identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança, incluindo a realização de análises de risco periódicas;
- **Controlos de segurança:** através do estabelecimento de controlos de segurança rigorosos, como controlos de acesso lógicos e físicos, para proteger infraestruturas críticas e dados sensíveis;
- **Gestão de Incidentes:** com o desenvolvimento de um plano de resposta a incidentes, que inclua procedimentos para a deteção, identificação, resposta e recuperação de incidentes de cibersegurança. Também deve ser estabelecido um plano de comunicação de incidentes para notificar as partes interessadas;
- **Conformidade Legal:** garantindo que a organização cumpre todas as leis e regulamentos aplicáveis em matéria de cibersegurança, realizando auditorias regulares para verificar a conformidade;
- **Revisão e atualização da política de cibersegurança:** periodicamente (no mínimo, anualmente), para mantê-la alinhada com a evolução das ameaças de cibersegurança e as mudanças na organização;
- **Continuidade de Negócio:** através de uma política de continuidade de negócio que esteja alinhada com a política de cibersegurança, incluindo planos detalhados para assegurar a continuidade das operações em caso de incidentes significativos.

Estas medidas ajudarão a fortalecer a resiliência das infraestruturas digitais contra ciberataques, garantindo a continuidade e a integridade dos serviços essenciais prestados.

Face à baixa percentagem de OSE do setor que indicaram possuir uma política de continuidade de negócio (27%), recomenda-se também a elaboração de uma política de continuidade de negócio alinhada com a política de cibersegurança. Deve incluir-se também a elaboração de uma política de comunicação, visto que se encontra abaixo dos 50%, tal como verificado na política de continuidade de negócio. Comparativamente com a média geral dos setores, apenas a política de gestão de risco se encontra acima da média. Recomenda-se a elaboração da política de gestão de acessos devido a encontrar-se com uma percentagem muito inferior em relação à média geral, assim como as políticas de comunicação e *backups* (**Gráfico 79 e gráfico 79.7**).

Gráfico 79 - Políticas incluídas no Plano de Segurança

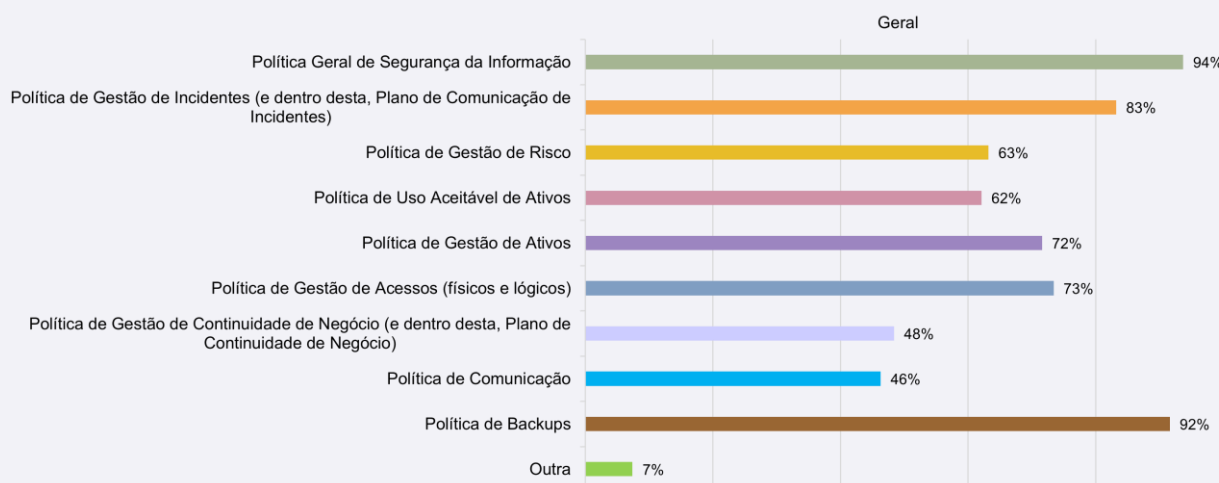
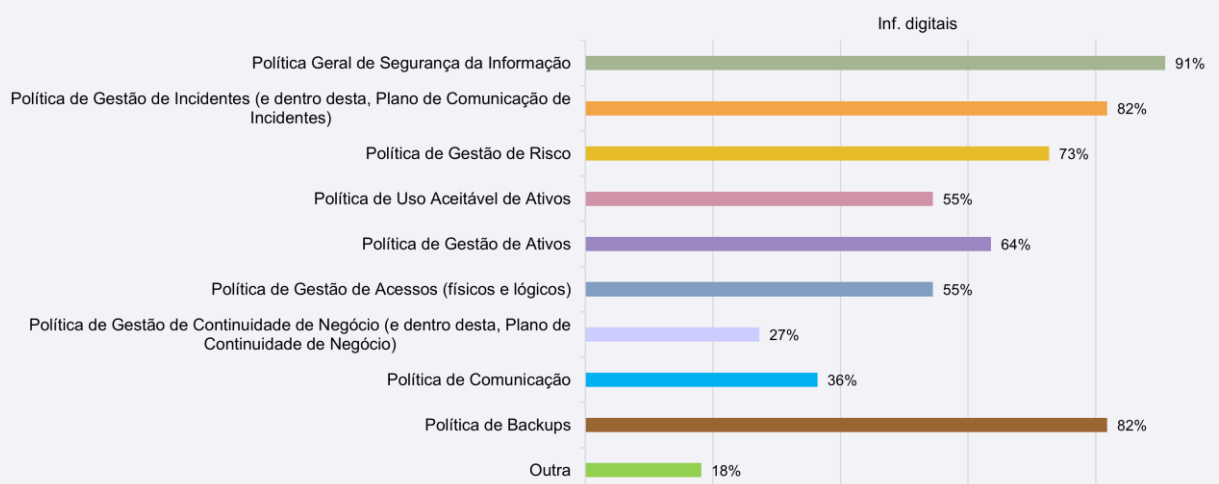


Gráfico 79.7 - Políticas incluídas no Plano de Segurança



Embora não exista obrigação legal no setor das infraestruturas digitais de realizar testes de intrusão (*pentesting*), é importante enfatizar que este setor também é alvo frequente de ciberataques, particularmente ataques de negação de serviço (DDoS), ataques de *ransomware* e violações de dados e, devido a isto, recomenda-se a realização de testes de intrusão.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos:** controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais:** controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais:** controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*¹²²⁴.

No setor das infraestruturas digitais, os controlos fundacionais, relacionados com a segurança de rede, são particularmente críticos. Infraestruturas digitais, como *data centers*, serviços *cloud*, e redes de comunicação, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, a disponibilidade e a continuidade dos seus serviços. Qualquer falha ou configuração inadequada pode ser explorada para interromper serviços digitais essenciais, comprometer a segurança dos dados, desviar tráfego, ou provocar quedas na rede, afetando significativamente a atividade das organizações que dependem dessas infraestruturas.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos¹²²⁵:

¹²²⁴ "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls-list>.

¹²²⁵ "The 18 CIS Critical Security Controls".

Tabela 59 - Controlos de Segurança da CIS (Inf. Digitais)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de <i>Software</i>
	Proteção de Dados
	Configuração Segura de Ativos e <i>Software</i>
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de <i>e-mail</i> e de Navegadores
	Defesas Contra <i>Malware</i>
	Recuperação de Dados
	Gestão da Infraestrutura de Rede
	Monitorização e Defesa da Rede
Controlos organizacionais	Formação e Consciencialização em Segurança
	Gestão de Fornecedores de Serviços
	Segurança de Aplicações de <i>Software</i>
	Gestão e Resposta a Incidentes
	Testes de Penetração

(Fonte: "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, <https://www.cisecurity.org/controls/cis-controls-list>.)

Notas metodológicas

O presente relatório teve como propósito fazer uma extensa análise dos vários setores de operadores de serviços essenciais no âmbito do RJSC.

Com este propósito, foram realizados os questionários cujos resultados se apresentam no relatório, bem como uma aprofundada pesquisa sobre o contexto setorial, impacto socioeconómico, ameaças, capacitação e investimento em cibersegurança, legislação relevante, *standards* e boas práticas e desafios para cada setor em análise, procurando ter por base as mais confiáveis fontes académicas e científicas.

A análise das informações recolhidas e consequente produção e elaboração do relatório foram realizadas pela PwC, entidade parceira do CNCS na elaboração do presente documento.

Bibliografia

- .PT, “Relatório de Atividades e Contas 2022”. https://www.pt.pt/fotos/editor2/relatorios/relatorio_atividades_contas_2022.pdf.
- .PT. “História”. <https://www.pt.pt/pt/historia/>.
- .PT. “Quem somos”. <https://www.pt.pt/pt/quem-somos/>.
- 9/11 Memorial and Museum. “The Memorial”. <https://www.911memorial.org/visit/memorial>.
- Abecasis, Miguel, Pedro Pereira, Dominic Field e Eduardo Bicacro. “O impacto do digital na economia portuguesa”, dezembro de 2018. https://web-assets.bcg.com/img-src/O-impacto-do-Digital-na-economia-portuguesa_tcm9-214461.pdf.
- Abreu, Laurinda. “Pensar historicamente os cuidados de saúde em Portugal”. *O Referencial: Revista da Associação* 25 de Abril. https://dspace.uevora.pt/rdpc/bitstream/10174/24717/1/REFERENCIAL%20130_bx_12_17.pdf.
- Accenture. “Fast forward: accelerating the journey to reinvention”. <https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-157/accenture-fast-forward-accelerating-the-journey-to-reinvention.pdf>.
- Agência para a Modernização Administrativa (AMA). “Cibersegurança na Administração Pública: O Imperativo da Conformidade Global no SNS”, *Encontros SAMA 2020* (Lisboa), 26 de abril de 2020. <https://bo.tic.gov.pt/api/assets/etic/2e7a0cf7-68f5-4008-a95f-29594569d584/>.
- Águas de Portugal. “Águas de Portugal - Duas décadas que perspetivam o futuro”, vídeo publicado a 6 de outubro de 2016, Youtube. <https://www.youtube.com/watch?v=2IPH9iW5wDg>.
- Águas de Portugal. “Relatório e Contas 2022”. https://www.adp.pt/pt/media/publicacoes/relatorios-e-contas/downloads/file597_pt.pdf.
- Águas de Portugal. *Livro Águas de Portugal*. Lisboa: By the Book, 2016. https://www.adp.pt/pt/media/publicacoes/downloads/pub_pdf17_pt.pdf.
- Águas do Algarve. “Plano de Atividades e Orçamento para o ano de 2022 (e projeções para 2023 e 2024)”. https://www.aguasdoalgarve.pt/sites/aguasdoalgarve.pt/files/paginas_base/inf_financeira/pao-2022_28_10_2021_signedca_signed.pdf.
- Águas do Alto Minho. “Relatório & Contas 2022”. <https://adam.pt/component/phocadownload/category/23-relatorio-e-contas?download=262:2022-relatorio-e-contas>.
- Águas e Energia do Porto. “Comunicado: Águas e Energia do Porto alvo de ataque informático”, 8 de fevereiro de 2023. <https://aguasdoporto.pt/noticias/comunicado-aedp-ataqueinformatico>.

- Águas e Energia do Porto. “Instrumentos de Gestão Previsional 2022-2024”. <https://aguasdoporto.pt/files/uploads/cms/adp/24/files/1647269981-EVymV2FxC3.pdf>.
- Ahmed A. Thabit, Bassam H. Abd e Ahmed Alkhayyat. “Challenges and Solutions of 5G Technology”. 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 2021, pp. 54-59. <https://ieeexplore.ieee.org/abstract/document/9717458>.
- Air Transport Action Group (ATAG). “Aviation: Benefits Beyond Borders”, setembro de 2020. <https://atag.org/industry-topics/supporting-economic-social-development>.
- Airport Technology. “New Technologies for Smarter Airports: Beacon Technology”. <https://www.airport-technology.com/contractors/data/pressreleases/smarter-airports-beacon-technology>.
- Alder, Steve “Editorial: Why Do Criminals Target Medical Records”. *The HIPAA Journal*, 2 de novembro de 2023. <https://www.hipaajournal.com/why-do-criminals-target-medical-records/>
- Alexandre, Lília. “Mobilizar Rumo à Poluição Zero – Ruído”. *Associação Zero*, janeiro de 2022. <https://zero.org/wp-content/uploads/2023/06/Mobilizar-Ruido .pdf>.
- Allsopp, Peter, Bruce Summers e John Veale. “The Evolution of Real-Time Gross Settlement: Access, Liquidity and Credit, and Pricing”. *World Bank*, fevereiro de 2009. <https://documents1.worldbank.org/curated/en/736521468331852042/pdf/490020WP0TheEv10Box338937B01PUBLIC1.pdf>.
- Almeida, Gonçalo. “Preço da eletricidade dispara para novo máximo. Já subiu 115% com a guerra”. *CNN Portugal*, 6 de março de 2022. <https://cnnportugal.iol.pt/geral/eletricidade-em-portugal-atinge-novo-maximo-historico-segunda-feira-preco-subiu-115-com-a-guerra/20220306/6224b6bc0cf2cc58e7e70a67>.
- Alphonsus, Ryan e Mohammad Abdullah. “A review on the applications of programmable logic controllers (PLCs)”, julho de 2016. <https://www.sciencedirect.com/science/article/abs/pii/S1364032116000551>.
- Alves, Maria. “Bancos privados com 3,3 mil milhões de lucros em 2023 a subirem 74,2% face ao ano anterior”. *Jornal Económico*, 5 de março de 2024. <https://leitor.jornaleconomico.pt/noticia/bancos-privados-com-3-3-mil-milhoes-de-lucros-em-2023-a-subirem-74-2-face-ao-ano-anterior>.
- American Gas Association. “Natural Gas Cybersecurity Guidelines & Standards Portfolio”, março de 2017. https://www.aga.org/wp-content/uploads/2022/11/ong_cybersecurity_guidelines_and_standards_002.pdf.
- American Institute of Aeronautics and Astronautics (AIAA). “A Framework for Aviation Cybersecurity”, agosto de 2013. https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/aiaa-cyber-framework-final.pdf?sfvrsn=7bd09ec9_0.
- American National Standards Institute. “X9: Accredited Standards Committee X9, Inc.”. ANSI Webstore. https://webstore.ansi.org/sdo/x9?source=blog& gl=1*v6wen5* gcl au*NzI0ODc2NzI1LjE3MjU1NTU5ODc.
- American Water Works Association, “Security Practices For Operation And Management”, <https://webstore.ansi.org/standards/awwa/awwag43009?srsId=AfmBOopxVXFQqfg7 VmKEeA34CyCkDf-czdhzHBps1dxXD8WktOp58Lc>.
- AMT. “AMT assina protocolo com Centro Nacional de Cibersegurança”, 1 de junho de 2017. <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-assina-protocolo-com-centro-nacional-de-ciberseguran%C3%A7a/>.
- AMT. “AMT promoveu ação de formação interna sobre cibersegurança”, 12 de dezembro de 2023. <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-promoveu-a%C3%A7%C3%A3o-de-forma%C3%A7%C3%A3o-interna-sobre-ciberseguran%C3%A7a/>.
- AMT. “AMT promoveu debate sobre ‘Transição digital, ambiental e energética - impacto na gestão dos modelos de concessão’”, 22 de novembro de 2022. <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-promoveu-debate-sobre->

transi%C3%A7%C3%A3o-digital-ambiental-e-energ%C3%A9tica-impacto-na-gest%C3%A3o-dos-modelos-de-concess%C3%A3o/.

- AMT. “Inovação na Era Digital: Zonas Livres Tecnológicas (ZLT) e Digital Innovation Hubs (DIH)”, 25 de janeiro de 2022. <https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/inova%C3%A7%C3%A3o-na-era-digital-zonas-livres-tecnol%C3%B3gicas-zlt-e-digital-innovation-hubs-dih/>.
- AMT. “Relatório de Atividades, Gestão e Contas de 2023”, 16 de abril de 2024. https://www.amt-autoridade.pt/media/4423/relatorio_de-atividades_2023_16042024.pdf.
- AMT. “Transporte Ferroviário em Portugal – 2022”, dezembro de 2023. <https://observatorio.amt-autoridade.pt/storage/100/8jtMIB1Gfmvaf20hBO1DofNpYO1DxF-metaRmVycm92aWFmMjAyMl9Ob3RhX2VzdGF0aXN0aWNhLnBkZg==-.pdf>.
- ANAC. “Plano Nacional de Segurança Operacional da Aviação 2022-2024: Revisão 1”, março de 2024. https://www.anac.pt/SiteCollectionDocuments/PNSO/PNSOA_2022_2024_rev_1.pdf.
- ANACOM. “Interligação e Serviço Universal”, 23 de fevereiro de 2006. <https://www.anacom.pt/render.jsp?categoryId=183071&languageId=0>
- ANACOM. “Telecomunicações e acesso à Internet de qualidade finalmente uma realidade em todo o País”, 6 de dezembro de 2023. <https://www.anacom.pt/render.jsp?contentId=1769445>.
- ANACOM. “Utilização da Internet das Coisas (IoT - Internet of Things)”, 2022. https://www.anacom.pt/streaming/relatorioInternet_dasCoisas_IoT2022.pdf?contentId=173794_0&field=ATTACHED_FILE.
- ANSR. “O Impacto Económico e Social da Sinistralidade Rodoviária em Portugal”, outubro de 2021. http://www.ansr.pt/Documents/Impacto_Economico_Social_Sinistralidade_Rodoviaria.pdf.
- API. “API Standard 1164, 3rd Edition”. <https://www.api.org/products-and-services/standards/important-standards-announcements/1164>.
- APS. “Porto de Sines integra exercício de cibersegurança enquadrado na Singapore Maritime Week”, abril de 2024. <https://www.apsinesalgarve.pt/noticias/2024/porto-de-sines-integra-exerc%C3%ADcio-de-ciberseguran%C3%A7a-enquadrado-na-singapore-maritime-week/>.
- ARC Advisory Group. “Oil & Gas Operations Technology and Supplier Selection”. <https://www.arcweb.com/technology-evaluation-and-selection/oil-gas-operations-technology-supplier-selection>.
- Arner, Douglas. “FinTech: Evolution and Regulation”, Asian Institute of International Financial Law, University of Hong Kong, junho de 2016. https://law.unimelb.edu.au/data/assets/pdf_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf.
- Asimily. “What are MDS2s and Why Should You Care”. <https://asimily.com/blog/what-are-mds2s-and-why-should-you-care>.
- Associação Portuguesa de Empresas de Gás, “Utilização Doméstica”. <https://www.apeg.pt/gas-natural/utilizacao-domestica/>.
- Associação Portuguesa de Empresas de Gás, “Utilização na Indústria”. <https://www.apeg.pt/gas-natural/industria/>.
- Associação Portuguesa de Empresas de Gás, “Utilização no setor da mobilidade”. <https://www.apeg.pt/gas-natural/utilizacao-no-setor-da-mobilidade/>.
- Associação Portuguesa de Empresas de Gás, “Utilização no Terciário”. <https://www.apeg.pt/gas-natural/setor-terciario/>.
- Associação Portuguesa de Empresas de Gás, “Utilizações e Vantagens”. <https://www.apeg.pt/gas-natural/utilizacoes-vantagens/>.
- Autoridade Nacional da Aviação Civil (ANAC). “A nossa história”. <https://www.anac.pt/vPT/Generico/ANAC/QuemSomos/Historia/Paginas/Historia.aspx>.
- AVEVA. “AVEVA Predictive Analytics”, 2023. https://www.aveva.com/content/dam/aveva/documents/brochures/Brochure_AVEVA_PredictiveAnalytics_23-02.pdf

- Bação, Pedro, Carlos Carreira, João Cerejeira, Gilberto Loureiro, António Martins e Miguel Portela. “Investimento Empresarial e o Crescimento da Economia Portuguesa”. Coordenação de Fernando Alexandre. *Fundação Calouste Gulbenkian*, 2017. https://gulbenkian.pt/wp-content/uploads/2017/11/Estudo_relatorio_Investimento_Empresarial_final_dez2017.pdf.
- Baker, Paddy. “Coincheck Customers Fall Victim to Data Breach After Domain Account Error”. Coincheck, 3 de junho de 2020. <https://www.coindesk.com/markets/2020/06/03/coincheck-customers-fall-victim-to-data-breach-after-domain-account-error/>.
- Banco Central Europeu. “Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures”, maio de 2023. <https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html>
- Banco Central Europeu. “Central Counterparty Clearing Houses and Financial Stability”. *Financial Stability Review*, 2005. https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart200512_06.en.pdf.
- Banco Central Europeu. “Cyber resilience and financial market infrastructures”. <https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html>.
- Banco Central Europeu. “ECB and EBA publish joint report on payment fraud”, agosto de 2024, <https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html>
- Banco Central Europeu. “TIBER-EU Guidance for Target Threat Intelligence Report”, julho de 2020. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.
- Banco de Portugal. “Análise das empresas do setor dos transportes”, BPStat, 2022. <https://bpstat.bportugal.pt/conteudos/publicacoes/1343>.
- Banco de Portugal. “Banco de Portugal atualiza séries longas do setor bancário português”. BPStat, 26 de julho de 2023. <https://bpstat.bportugal.pt/conteudos/noticias/1955>.
- Banco de Portugal. “Banco de Portugal avança na cooperação para a cibersegurança”, maio de 2024. <https://www.bportugal.pt/comunicado/banco-de-portugal-avanca-na-cooperacao-para-ciberseguranca>.
- Banco de Portugal. “Campanha #ficaadica. Banco de Portugal divulga brochura com conselhos sobre o acesso a produtos e serviços bancários digitais”, 7 de fevereiro de 2023. <https://www.bportugal.pt/comunicado/campanha-ficaadica-banco-de-portugal-divulga-brochura-com-conselhos-sobre-o-acesso>.
- Banco de Portugal. “Economia numa imagem”, março de 2022. <https://www.bportugal.pt/page/economia-numa-imagem-148-0>.
- Banco de Portugal. “História do Banco de Portugal”. Sobre o Banco. <https://www.bportugal.pt/page/historia-do-banco-de-portugal>
- Banco de Portugal. “Instituições autorizadas”, última atualização em 23 de setembro de 2024. <https://www.bportugal.pt/page/listagem-entidades-autorizadas>
- Banco de Portugal. “Lista de agências”, agosto de 2024. <https://www.bportugal.pt/sites/default/files/listaagencias.xls>
- Banco de Portugal. “Outros sistemas de liquidação”. Infraestruturas de mercado. <https://www.bportugal.pt/page/outros-sistemas-de-liquidacao>.
- Banco de Portugal. “Recomendações sobre Gestão da Continuidade de Negócio”, Carta Circular n.º CC/2021/00000047, 2021. https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares//463107899_6.docx.pdf.
- Banco de Portugal. “Relatório de Estabilidade Financeira”, novembro de 2023. https://www.bportugal.pt/sites/default/files/documents/2024-02/ref_11_2023_pt.pdf.
- Banco Montepio. “Relatório e Contas 2023”, 15 de abril de 2024. <https://www.bancomontepio.pt/content/dam/montepio/pdf/institucional/investor-relations/relatorios-comunicados-e-informacao-financeira/2023/informacao-anual/relatorio-contas-anual-banco-montepio-2023.pdf>.
- Banco Português de Investimento. “Relatório e Contas 2023”. https://www.bancobpi.pt/contentservice/getContent?documentName=PR_UCMS02106736.

- Banco Santander Totta. “Annual Report 2023: Proposal”, 17 de maio de 2024. <https://www.santander.pt/pdfs/investor-relations/santander-totta-sa/relatorio-e-contas/2023/BST Annual Report 2023 non official non audited.pdf>.
- Bank for International Settlements e International Organization of Securities Commissions. “Guidance on cyber resilience for financial market infrastructures”, junho de 2016. <https://www.bis.org/cpmi/publ/d146.pdf>.
- Bank for International Settlements. “Basel II: Revised international capital framework”, Basel Committee on Banking Supervision. <https://www.bis.org/publ/bcbsca.htm>.
- Bank of England. “CHAPS”. <https://www.bankofengland.co.uk/payment-and-settlement/chaps>.
- Banking Act of the Federal Republic of Germany, “Gesetz iiber das Kreditwesen”, setembro de 1998. <https://www.cftc.gov/sites/default/files/idc/groups/public/@otherif/documents/ifdocs/eurexmcobankingact.pdf>
- Barata, André. “O Regime Europeu de Resolução de Contrapartes Centrais: a peça que faltava ao mercado dos derivados de balcão?”. *Revista de Direito Financeiro e dos Mercados de Capitais*, dezembro de 2023. <https://rdfm.com/wp-content/uploads/2024/01/Revista-de-Direito-Financeiro-e-do-Mercado-de-Capitais-2-20231.pdf>.
- BBVA. “História da Segurança Social (parte I)”, 20 de novembro de 2013. <https://www.aminhapensao.pt/blog/historia-da-seguranca-social-parte-i/>.
- BIMCO. “The Guidelines on Cyber Security Onboard Ships”. <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>.
- BIP. “INESC TEC e EDP assinam contrato-programa na área de energia”, junho de 2019. <https://bip.inesctec.pt/noticias/inesc-tec-e-edp-assinam-contrato-programa-na-area-de-energia/>.
- Biscaia, André, António Pereira, Ana Alves, Rui Carneira, Leonor Xavier da Rocha e Gonçalo Melo. “Síntese dos resultados do estudo ‘O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023: Questionário aos coordenadores de USF’”. *Associação Nacional das Unidades de Saúde Familiar*. <https://usf-an.pt/sintese-dos-resultados-do-estudo-o-momento-atual-da-reforma-dos-cuidados-de-saude-primarios-em-portugal-2022-2023-questionario-aos-coordenadores-de-usf/>.
- Björnberg, Arne e Ann Phang. “Euro Health Consumer Index 2018”. *Health Consumer Powerhouse*, 2019. <https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf>
- Boaz, Lawrence Shubi Kaijage e Ramadhani Sinde. “An overview of pipeline leak detection and location systems”, julho de 2014. <https://ieeexplore.ieee.org/abstract/document/7055147>.
- Borys, Christian. “The day a mysterious cyber-attack crippled Ukraine”, *BBC*, 4 de julho de 2017. <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine>.
- Bouveret, Antoine. “Cyber Risk for the Financial sector: A framework for Quantitative Assessment”. *Working Paper* do Fundo Monetário Internacional, junho de 2018. <https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924>.
- Boyanov, Luben. “Financial Data Processing in Big Data Platforms”. *Economic Alternatives* 4, 2021. <https://www.unwe.bg/doi/eajournal/2021.4/EA.2021.4.03.pdf>.
- Braidotti, Luca, Marco Mazzarino, Maurizio Cociancich e Vittorio Bucci. “On the Automation of Ports and Logistics Chains in the Adriatic Region”, setembro de 2020. https://link.springer.com/chapter/10.1007/978-3-030-58820-5_8.
- Business IT. “A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor”, 21 de outubro de 2022. <https://business-it.pt/2022/10/21/a-tecnologia-e-a-banca-as-inovacoes-que-estao-a-permitir-digitalizar-o-setor/>.
- Caires, Marta. “Serviço de Saúde da Madeira: ataque informático deixa utentes sem consultas e sem exames”. *Expresso*, 7 de agosto de 2023. <https://expresso.pt/sociedade/2023-08-07-Servico-de-Saude-da-Madeira-ataque-informatico-deixa-utentes-sem-consultas-e-sem-exames-e0cee143>

- Caixa Geral de Depósitos. “Fintech: o que são e o que fazem”. Saldo Positivo, 4 de abril de 2023. <https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/o-que-sao-fintech.aspx>
- Caixa Geral de Depósitos. “Relatório de Gestão e Contas 2023”. <https://www.cgd.pt/Investor-Relations/Informacao-Financeira/CGD/Relatorios-Contas/Pages/Relatorios-Contas-CGD.aspx>.
- Calzolari, Giacomo. “Artificial Intelligence market and capital flows: Artificial Intelligence and the financial sector at crossroads”. Estudo para o Parlamento Europeu, maio de 2021. [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU\(2021\)662912_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf).
- Carris. “História”, A Carris. <https://www.carris.pt/a-carris/historia/>.
- Carris. “Plano de Atividades e Orçamento 2024”. https://www.carris.pt/media/4duh1ymp/carris_pao-2024-2027.pdf.
- Carris. “Plano de Prevenção de Riscos de Corrupção e Infrações Conexas 2022”, 2023. <https://www.carris.pt/media/22uhz5qn/plano-de-preven%C3%A7%C3%A3o-de-riscos-de-corrup%C3%A7%C3%A3o-e-infra%C3%A7%C3%B5es-conexas-2022.pdf>.
- Carris. “Relatório e Contas 2023”. <https://www.carris.pt/media/lwsixqty/relatorio-e-contas-2023.pdf>.
- Carris. “Relatório Governo Societário 2023”. <https://www.carris.pt/media/3g1lrm01/relatorio-governo-societario-2023.pdf>.
- Cassauwers, Tom. “Winds of change – the new tech steering commercial shipping towards a more sustainable future”. *Horizon*. <https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine/winds-change-new-tech-steering-commercial-shipping-towards-more-sustainable-future>.
- Castaño, David, Daniel Marcos, Ana Fonseca e Pedro Lains. *Os Petróleos em Portugal: Do Estado à Privatização 1937-2012*. Lisboa: Imprensa de Ciências Sociais, 2017.
- Castro, José. “Tendências de Evolução dos Transportes Marítimos Internacionais e Implicações nas Infraestruturas Portuárias”, junho de 2018. <https://repositorio-aberto.up.pt/bitstream/10216/113509/2/275756.pdf>.
- CatimProjetos, “Green Pipeline Project”. <https://www.projetoscatim.com/projects-green-pipeline>.
- Center for Internet Security. “The 18 CIS Critical Security Controls”, CIS Critical Security Controls. <https://www.cisecurity.org/controls/cis-controls-list>.
- Center for Strategic & International Studies. “Significant Cyber Incidents”. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- Centers for Medicare & Medicaid Services. “HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules”, fevereiro de 2023. <https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf>.
- CGI. “Endesa aposta na transformação digital e reinventa o seu modelo de negócio”. <https://www.cgi.com/portugal/pt-pt/case-study/business-consulting/endesa-aposta-na-transformacao-digital-e-reinventa-o-seu-modelo-de>.
- Checkpoint. “Cyberattacks on the Healthcare Sector”, 2023. <https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/>.
- Checkpoint. “Cyber Attack Trends: 2020 Mid-Year Report”, 22 de julho de 2020. <https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/>.
- Chen, Bo, Nishant Pattanaik, Ana Goulart, Karen L. Butler-Purry, Deepa Kundur. “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed”, 25 de junho de 2015. <https://ieeexplore.ieee.org/abstract/document/7129084>.
- Cheney, Julia. “Heartland Payment Systems: Lessons Learned from a Data Breach”, janeiro de 2010. <https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/d-2010-january-heartland-payment-systems.pdf?la=en&hash=EFAF5C96513D6E176D6C5312E4007061>.

- CIO. “What is ITIL? Your guide to the IT Infrastructure Library”. 16 de maio de 2022, <https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-til-definition-and-solutions.html>.
- CIP. “Empresas privadas do setor da saúde com valor acrescentado acima de 6,7 mil milhões”, 20 de outubro de 2023. <https://cip.org.pt/empresas-privadas-do-setor-da-saude-com-valor-acrescentado-acima-de-67-mil-milhoes/>.
- CISA. “Cyber Risks and Resources for the Water and Wastewater Systems Sector”, outubro de 2021. <https://www.cisa.gov/sites/default/files/publications/infographic-manage-wastewater-national-critical-function-102021-508.pdf>.
- CISA. “Cyber-Attack Against Ukrainian Critical Infrastructure”, 20 de julho de 2021. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.
- CISA. “Safeguarding and Securing Cyberspace”. Press Release, News, 20 de julho de 2020. <https://www.cisa.gov/news-events/news/safeguarding-and-securing-cyberspace>.
- CISA. “Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector”, novembro de 2022. <https://www.cisa.gov/sites/default/files/2022-11/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf>.
- CISA. “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years”, 7 de maio de 2023. <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>.
- Civil Aviation Cybersecurity Subcommittee. “Civil Aviation Supply Chain Cybersecurity Recommendations Report”, Aerospace Industries Association, outubro de 2023. <https://www.aia-aerospace.org/wp-content/uploads/Supply-Chain-Cybersecurity-Recommendations-Report.pdf>.
- Clarksons. “What is the International Safety Management Code?”. <https://www.clarksons.com/glossary/international-safety-management-code>.
- CLC. “Relatório de Gestão & Contas 2023”. https://www.clc.pt/DocsCLC/2024/CLC_RC_2023.pdf.
- CMVM. “Circular 003/2024 - Gestão de Ativos – Circular anual de gestão de ativos 2024”. <https://www.cmvm.pt/PIInstitucional/Content?Input=C1B8E11C9FC436AFE660445BDC7E1867050C25D72FD472228ABA2E3FEA4A338B#>.
- CMVM. “Circular 005/2023 - Gestão de Ativos e Empresas de Investimento | Tecnologias da Informação e Comunicação: Cibersegurança”. <https://www.cmvm.pt/PIInstitucional/Content?Input=C6DE3F376C5004D8E490034ED0FAA70C0A71D3AE04178CDC0170C5EC472B7D19#>.
- CNCS. “Boletim do Observatório de cibersegurança n.º 4/2021”, setembro de 2021. <https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf>.
- CNCS. “C-Academy: Sensibilização e Formação”. <https://www.cncs.gov.pt/pt/c-academy/>.
- CNCS. “Compromisso C-Academy”. <https://www.cncs.gov.pt/pt/c-academy-compromisso/>.
- CNCS. “Estratégia Nacional de Segurança do Ciberespaço 2019-2023”. <https://www.cncs.gov.pt/docs/cnsc-2019-2023.pdf>.
- CNCS. “Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança”, dezembro de 2022. <https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf>.
- CNCS. “Incidentes e Setores: 2019-2023”. Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024. <https://www.cncs.gov.pt/pt/estatistica/>.
- CNCS. “Incidentes e Setores”. Conhecimento Situacional: Estatísticas. <https://www.cncs.gov.pt/pt/estatistica/#cert.pt>.
- CNCS. “ISAC Portos”, Comunidades de Cibersegurança, última atualização em abril de 2024. <https://www.cncs.gov.pt/pt/comunidades-ciberseguranca/isacs/portos/>.

- CNCS. “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”. <https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cnccs.pdf>.
- CNCS. “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2023”. <https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obciber-cnccs.pdf>.
- CNCS. “Relatório Cibersegurança em Portugal: Riscos e Conflitos 2024”. <https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obciber-cnccs.pdf>.
- CNCS. “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança. <https://www.cncs.gov.pt/pt/observatorio/#relatorios>.
- CNCS. “Tecnologias Emergentes”, maio de 2023. <https://www.cncs.gov.pt/docs/rel-tecemer2023-observ-cnccs.pdf>.
- CNCS. ISAC. <https://www.cncs.gov.pt/pt/isac/>.
- Colégio Nacional de Energia e Minas. “O petróleo nas nossas vidas. Com exceção da água, o petróleo é o líquido mais presente nas nossas vidas”. *Ingenium*, II Série, n.º 158 (março/abril de 2017).
- Comboios de Portugal. “Cronologia da história dos caminhos de ferro em Portugal”. <https://www.cp.pt/institucional/pt/cultura-ferroviaria/historia-cp/cronologia>.
- Comboios de Portugal. “Relatório do Governo Societário 2023”, 16 de maio de 2024. [https://www.cp.pt/StaticFiles/Institucional/1 a empresa/3 Relatório Contas/2023/relatorio-governo-societario-2023.pdf](https://www.cp.pt/StaticFiles/Institucional/1%20a%20empresa/3%20Relatorio%20Contas/2023/relatorio-governo-societario-2023.pdf).
- Comboios de Portugal. “Relatório do Governo Societário 2023”, maio de 2024. [https://www.cp.pt/StaticFiles/Institucional/1 a empresa/3 Relatório Contas/2023/relatorio-governo-societario-2023.pdf](https://www.cp.pt/StaticFiles/Institucional/1%20a%20empresa/3%20Relatorio%20Contas/2023/relatorio-governo-societario-2023.pdf).
- Comissão Europeia, “Broadband Coverage in Europe 2021”, agosto de 2022. <https://ec.europa.eu/newsroom/dae/redirection/document/88314>.
- Comissão Europeia. “€1.3 billion from the Digital Europe Programme for Europe’s digital transition and cybersecurity”. <https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity>.
- Comissão Europeia. “Aliança Europeia para os Dados Industriais, a Edge e a Nuvem”. *Shaping Europe’s digital future*. <https://digital-strategy.ec.europa.eu/pt/policies/cloud-alliance>.
- Comissão Europeia. “Aliança sobre processadores e tecnologias de semicondutores”. *Shaping Europe’s digital future*. <https://digital-strategy.ec.europa.eu/pt/policies/alliance-processors-and-semiconductor-technologies>.
- Comissão Europeia. “Década Digital da Europa: metas digitais para 2030”. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt.
- Comissão Europeia. “ETCS Levels and Modes”. https://transport.ec.europa.eu/transport-modes/rail/ertms/what-ertms-and-how-does-it-work/etcs-levels-and-modes_en.
- Comissão Europeia. “European Digital Innovation Hubs”. <https://digital-strategy.ec.europa.eu/en/activities/edihs>.
- Comissão Europeia. “Ficha temática sobre o semestre europeu: Setor Bancário e estabilidade financeira”, 16 de outubro de 2017. https://commission.europa.eu/system/files/2021-01/european-semester-thematic-factsheet-banking-sector-financial-stability_pt.pdf.
- Comissão Europeia. “Programa Europa Digital”, *Shaping Europe’s digital future*. <https://digital-strategy.ec.europa.eu/pt/activities/digital-programme>.
- Comissão Europeia. “Quantum Technologies Flagship”, *Shaping Europe’s digital future*. <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>.
- Comissão Europeia. “Risk assessment report on cyber resilience on EU’s telecommunications and electricity sectors”, 24 de julho de 2024. <https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors>.
- Comissão Europeia. “Smart Mobility”. https://transport.ec.europa.eu/transport-themes/smart-mobility_en.

- Comissão Europeia. “Tecnologias-chave para impulsionar a digitalização dos transportes”. <https://digital-strategy.ec.europa.eu/pt/policies/technologies-digitalisation-transport>.
- Compete 2030, “Europa lidera combate à emergência climática”, 8 de julho de 2024. <https://www.compete2030.gov.pt/comunicacao/europa-lidera-combate-a-emergencia-climatica/>.
- Conselho da União Europeia. “Conclusões do Conselho sobre ‘Impulsionar o transporte ferroviário para a vanguarda da mobilidade sustentável e inteligente’”, maio de 2021. <https://data.consilium.europa.eu/doc/document/ST-8790-2021-INIT/pt/pdf>.
- Conselho das Finanças Públicas, “Evolução do Desempenho do Serviço Nacional de Saúde em 2022 (Relatório n.º 7/2023)”, junho de 2023. https://www.cfp.pt/uploads/publicacoes_ficheiros/cfp-rel-07-2023.pdf.
- Conselho de Ministros. “PENSAARP 2030”, versão de consulta pública. [https://apambiente.pt/sites/default/files/SNIAMB_Aqua/DRH/PlaneamentoOrdenamento/PlanosSetoriais/SetorUrbano/PENSAARP2030/PENSAARP_2030_Volume1.pdf](https://apambiente.pt/sites/default/files/SNIAMB_Agua/DRH/PlaneamentoOrdenamento/PlanosSetoriais/SetorUrbano/PENSAARP2030/PENSAARP_2030_Volume1.pdf).
- Conselho Europeu. “Cibersegurança: Como combate a UE as ciberameaças”. <https://www.consilium.europa.eu/pt/policies/cybersecurity/>
- Conselho Europeu. “Construção da União dos Mercados de Capitais da UE”, última revisão a 12 junho de 2024. <https://www.consilium.europa.eu/pt/policies/what-the-eu-is-doing-to-deepen-its-capital-markets/>.
- Conselho Europeu. “Horizonte Europa”. <https://www.consilium.europa.eu/pt/policies/horizon-europe/>.
- Constituição da República Portuguesa. <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>
- Correia, Rafael. “Acordo de Paris pode criar oito milhões de empregos na energia até 2050”. *Revista Sustentável*, 30 julho de 2021. <https://www.revistasustentavel.pt/destaques/acordo-de-paris-pode-criar-oito-milhoes-de-empregos-na-energia-ate-2050/>.
- Council on Foreign Relations. “Attack on Israeli water utilities”, maio de 2020. <https://www.cfr.org/cyber-operations/attack-israeli-water-utilities>
- *DatacenterDynamics*, “A economia dos Data Centers em Portugal: o que esperar para os próximos anos?”, 26 de abril de 2023. <https://www.datacenterdynamics.com/br/an%C3%A1lises/a-economia-dos-data-centers-em-portugal-o-que-esperar-para-os-proximos-anos/>.
- DCO. “Cyber Risk Management in the Maritime Transportation System”. <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Commercial-Regulations-standards-CG-5PS/Design-Engineering-Standards/Systems-Engineering-Division/Cyber-Risk-Management/>.
- Decreto-Lei n.º 13:969, de 20 de julho de 1927. *Diário do Governo*. <https://files.diariodarepublica.pt/1s/1927/07/15300/13921396.pdf>.
- Decreto-Lei n.º 142/2019, de 19 de setembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/142-2019-124831327>.
- Decreto-Lei n.º 143, de 26 de junho de 1860. *Diário da República*. <https://legislacaoregia.parlamento.pt/V/1/35/9/p232>.
- Decreto-Lei n.º 145/2009, de 17 de junho. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/145-2009-494558>.
- Decreto-Lei n.º 150/2015, de 5 de agosto, *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/150-2015-69951097>.
- Decreto-lei n.º 16:424 de 26 de janeiro de 1929, *Diário do Govêrno*. <https://files.diariodarepublica.pt/1s/1929/01/02200/02890290.pdf>.
- Decreto-Lei n.º 20/2022, de 28 de janeiro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/20-2022-178264070>.
- Decreto-Lei n.º 205-B/75, de 26 de junho. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/205-b-1975-497832>.

- Decreto-Lei n.º 226/2006, de 15 de novembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/226-2006-544783>.
- Decreto-Lei n.º 23/2009, de 20 de janeiro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/23-2009-602570>.
- Decreto-Lei n.º 257/2002, de 22 de novembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/257-2002-448755>.
- Decreto-Lei n.º 270/2003, de 28 de outubro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/270-2003-466832>.
- Decreto-Lei n.º 298/92, de 31 de dezembro, “Regime Geral das Instituições de Crédito e Sociedades Financeiras - RGICSF”, *Diário da República*. <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1992-70072322>.
- Decreto-Lei n.º 299-B/98, de 29 de setembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/299-b-349923>.
- Decreto-Lei n.º 317/89, de 22 de setembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/317-547635>.
- Decreto-Lei n.º 319/93, de 21 de setembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/319-1993-655527>.
- Decreto-lei n.º 33:967, *Diário do Governo*, 22 de setembro de 1944. <https://files.diariodarepublica.pt/1s/1944/09/20800/09290931.pdf>.
- Decreto-lei n.º 34:593: Plano Rodoviário, de 11 de maio de 1945. *Diário do Governo*. <https://files.dre.pt/1s/1945/05/10201/03730394.pdf>.
- Decreto-Lei n.º 380/85, de 26 de setembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/380-176998>.
- Decreto-Lei n.º 49-A/2012, de 29 de fevereiro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/49-a-2012-551446>.
- Decreto-Lei n.º 49-A/2012, de 29 de fevereiro. *Diário da República*. <https://dre.pt/application/file/a/551481>.
- Decreto-Lei n.º 65/2021, de 30 de julho. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988>.
- Decreto-Lei n.º 93/2020, de 3 de novembro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/decreto-lei/93-2020-147432950>.
- Dehlawi, Zakariya e Norah Abokhodair. “Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident”. *Paper apresentado na 2013 IEEE International Conference on Intelligence and Security Informatics*, junho de 2013. https://www.researchgate.net/publication/261456882_Saudi_Arabia's_response_to_cyber_conflict_A_case_study_of_the_Shmoon_malware_incident.
- Dellinger, AJ. “Understanding the First American Financial Data Leak: How Did It Happen And What Does It Mean?”. *Forbes*, maio de 2019. <https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/>
- Deloitte e Universidade de Coimbra. “Avaliação do Potencial Económico da Transição Digital em Portugal”, 2023. https://portugaldigital.gov.pt/wp-content/uploads/2023/05/Portugal-Digital_Avaliacao-Transicao-Digital_Documento-Final_v20230330_VF.pdf.
- Department for Science, Innovation & Technology. “Cyber security breaches survey 2023”, 19 de abril de 2023. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>
- Department of Homeland Security. “Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)”, fevereiro de 2014. <https://www.energy.gov/oe/articles/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014>.
- Department of Transport. “Rail Cyber Security Guidance to Industry”, fevereiro 2016. <https://assets.publishing.service.gov.uk/media/5efcace9e90e075c52d05a94/rail-cyber-security-guidance-to-industry-document.pdf>.

- Department of Transportation FAA. “Aviation Rulemaking Advisory Committee-New Task”, fevereiro de 2015. https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf.
- Despacho n.º 8877/2017, de 9 de outubro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/despacho/8877-2017-108269312>.
- DGRM. “Breve História”. <https://www.dgrm.pt/breve-historia>.
- DGRM. “Plano de Atividades 2023”. <https://www.dgrm.pt/documents/20143/714947/Plano+de+Atividades+da+DGRM+2023.pdf/53fb147c-46be-7094-77f5-af80a530dcad>.
- DGRM. “Plano de Formação 2024”, janeiro de 2024. <https://www.dgrm.pt/documents/20143/714947/PlanoForma%C3%A7%C3%A3o2024.pdf/5a6f158d-257e-4aeb-68a7-9d5f8c46c329>.
- DGRM. “Sistema VTS”. <https://www.dgrm.pt/sistema-vts>.
- Dias, Manuel. “Estará no plano do próximo Governo colocar Portugal na vanguarda da Europa digital?”. *Observador*, 3 de janeiro de 2024. <https://observador.pt/opiniao/estara-no-plano-do-proximo-governo-colocar-portugal-na-vanguarda-da-europa-digital/>.
- Dias, Manuel. “Segurança dos Transportes Marítimos e Portos – Visão Prospetiva”, abril de 2022. https://pianc.pt/wp-content/uploads/2022/05/6-Seguranc%CC%A7a_dos_Transportes_Mari%CC%81timos_e_Portos_Visa%CC%83o_Prospetiva_Dinis-Dias-PIANC-2022.pdf.
- Dias, Mariana. “Cinco maiores bancos pagaram 17% do IRC total arrecadado em 2023”. *Diário de Notícias*, 25 de março de 2023. <https://www.dn.pt/3384889811/cinco-maiores-bancos-pagaram-17-do-irc-total-arrecadado-em-2023/>.
- Dias, Mariana. “Euronext Lisboa cresce em 2022. Foram negociados 137 milhões de euros por dia”, *Dinheiro Vivo*, 28 de fevereiro de 2023. <https://www.dinheirovivo.pt/bolsa/euronext-lisboa-cresce-em-2022-foram-negociados-137-milhoes-de-euros-por-dia-15918612.html>.
- DICOM. “Digital Imaging and Communications in Medicine (DICOM)”, maio de 2017. https://www.researchgate.net/publication/355550688_Digital_Imaging_and_Communications_in_Medicine_DICOM.
- Direção-Geral de Energia e Geologia. “Estratégia Nacional de Longo Prazo para o Combate à Pobreza Energética 2023-2050”. <https://www.dgeg.gov.pt/pt/areas-transversais/relacoes-internacionais/politica-energetica/estrategia-nacional-de-longo-prazo-para-o-combate-a-pobreza-energetica/>.
- Direção-Geral de Energia e Geologia. “História da Prospeção e Pesquisa”. <https://www.dgeg.gov.pt/pt/areas-setoriais/geologia/petroleo-armazenamento-de-co2/geologia-do-petroleo/historia-da-prospecao-e-pesquisa/>.
- Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366>.
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148>.
- Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3AOJ.L.2016.138.01.0044.01.POR>.
- Diretiva (UE) 2016/798 do Parlamento Europeu e do Conselho. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/AUTO/?uri=celex:32016L0798>.
- Diretiva (UE) 2020/700 do Parlamento Europeu e do Conselho. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32020L0700>.
- Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União

que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1792 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285>

- Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2557>.
- Diretiva (UE) 2023/1791 do Parlamento Europeu e do Conselho, de 13 de setembro de 2023, relativa à eficiência energética e que altera o Regulamento (UE) 2023/955. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32023L1791>.
- Diretiva 2001/14/CE do Parlamento Europeu e do Conselho de 26 de fevereiro de 2001 relativa à repartição de capacidade da infraestrutura ferroviária, à aplicação de taxas de utilização da infraestrutura ferroviária e à certificação da segurança. *Jornal Oficial das Comunidades Europeias*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001L0014>.
- Diretiva 2002/19/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos (diretiva acesso). *Jornal Oficial das Comunidades Europeias*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0019>
- Diretiva 2002/20/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa à autorização de redes e serviços de comunicações eletrónicas (diretiva autorização). *Jornal Oficial das Comunidades Europeias*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:PT:PDF>
- Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro). *Jornal Oficial das Comunidades Europeias*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:pt:PDF>.
- Diretiva 2002/22/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas (diretiva serviço universal). *Jornal Oficial das Comunidades Europeias*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0022>.
- Diretiva 2005/65/CE do Parlamento Europeu e do Conselho de 26 de outubro de 2005 relativa ao reforço da segurança nos portos. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:PT:PDF>.
- Diretiva 2005/89/CE do Parlamento Europeu e do Conselho de 18 de janeiro de 2006 relativa a medidas destinadas a garantir a segurança do fornecimento de eletricidade e o investimento em infraestruturas. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32005L0089>.
- Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007 relativa aos serviços de pagamento no mercado interno. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32007L0064>.
- Diretiva 2008/114/CE do Conselho de 8 de dezembro de 2008 relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114>.
- Diretiva 2010/40/UE do Parlamento Europeu e do Conselho de 7 de Julho de 2010 que estabelece um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010L0040>.
- Diretiva 2012/18/UE do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas, que altera e subsequentemente revoga a Diretiva 96/82/CE do Conselho. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012L0018>.

- Diretiva 2014/65/UE do Parlamento Europeu e do Conselho de 15 de maio de 2014 relativa aos mercados de instrumentos financeiros, *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014L0065>.
- DNV GL, “Cyber security resilience management for ships and mobile offshore units in operation”, setembro de 2016. <https://www.dnv.com/siteassets/images/pdf-documents/dnv-gl-rp-0496.pdf>.
- DSI. “RNU - Registo Nacional de Utentes: Especificação Técnica”, SPMS, 12 de novembro de 2015. [SC InfoSite 2015 \(min-saude.pt\)](https://sc.infoSite.2015(min-saude.pt)).
- Duarte, Pedro. “O Desafio Digital”. *Janus*, junho de 2022. <https://repositorio.ual.pt/server/api/core/bitstreams/350ce9d5-f3e3-45e2-aa85-8c76378eb077/content>.
- EASA. “Artificial Intelligence and Aviation”. <https://www.easa.europa.eu/en/light/topics/artificial-intelligence-and-aviation-0>.
- EASA. “Aviação sustentável: rumo a uma aviação com emissões zero”. <https://www.easa.europa.eu/pt/light/topics/sustainable-aviation-towards-zero-emission-aviation>.
- EASA. “EASA Artificial Intelligence Roadmap 2.0”, maio de 2023. <https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20>.
- EBA. “Orientações definitivas sobre a segurança dos pagamentos efetuados através da internet”. https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/558993c7-c253-472c-bae3-f897f6c6038a/EBA-GL-2014-12_PT_rev1%20GL%20on%20Internet%20Payments.pdf.
- EBA. “Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)”, 12 de janeiro de 2018. [https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20\(EBA-GL-2017-17\)_PT.pdf](https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf).
- ECS. “Energy Networks and Smart Grids”, novembro de 2018. <https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf>.
- EDP. “A nossa transformação digital”. *Inovação na EDP*. <https://www.edp.com/pt-pt/inovacao/transformacao-digital>.
- EDP. “AI4PV”. <https://www.edp.com/pt-pt/inovacao/new/ai4pv>.
- EDP. “ARIA 2”. <https://www.edp.com/pt-pt/inovacao/aria-2>.
- EDP. “BEHYOND: sinergias entre o hidrogénio e a eólica offshore”. <https://www.edp.com/pt-pt/inovacao/behyond-sinergias-entre-o-hidrogenio-e-a-eolica-offshore>.
- EDP. “BladeBug: Inspeção e Manutenção de Turbinas Eólicas”. <https://www.edp.com/pt-pt/edp-group/bladebug-inspecao-e-manutencao-de-turbinas-eolicas>.
- EDP. “Cyber Range: Promover a sensibilização da cibersegurança”, julho de 2020. https://www.edp.com/sites/default/files/2021-03/10_cyber_range_novo_PT.pdf.
- EDP. “FIRMe: Flexibilidade Integrada em Regime de Mercado”. <https://www.edp.com/pt-pt/edp-group/firme-flexibilidade-integrada-em-regime-de-mercado>.
- EDP. “Inovação na EDP”. <https://www.edp.com/pt-pt/inovacao>.
- EDP. “IONATE”. <https://www.edp.com/pt-pt/inovacao/ionate>.
- EDP. “O que é a transição energética e qual o impacto na forma como vivemos?”. <https://www.edp.com/pt-pt/o-que-e-a-transicao-energetica-e-qual-o-impacto-na-forma-como-vivemos>.
- EDP. “Parte I – Relatório de Gestão 2023”, setembro de 2024. <https://www.edp.com/sites/default/files/2024-09/Parte%20I%20-%20Relat%C3%B3rio%20de%20Gest%C3%A3o%202023.pdf>.
- EDP. “Pobreza Energética em Portugal”. *Histórias EDP*, 16 de março de 2021. <https://www.edp.com/pt-pt/historias-edp/pobreza-energetica-em-portugal>.

- EDP. “PRR Be Neutral – Ubiquitous Charging”. <https://www.edp.com/pt-pt/innovation/prr-be-neutral-ubiquitous-charging>.
- EDP. “Uma história de dois séculos: Portugal acende a primeira lâmpada”, *Histórias EDP*, 14 de agosto de 2019. <https://www.edp.com/pt-pt/historias-edp/uma-historia-de-dois-seculos-portugal-acende-a-primeira-lampada>.
- Empowering EU ISACs. “European ISACs”. <https://www.isacs.eu/european-isacs>.
- ENISA. “Appropriate security measures for smart grids”, dezembro de 2012. <https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids>.
- ENISA. “Cyber Europe Programme”, 2024. <https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme>
- ENISA. “Cyber Security and Resilience of smart cars”. <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>.
- ENISA. “Cybersecurity Skills Conference: Strengthening human capital in the EU”. <https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu>.
- ENISA. “DNS Identity Verification and Authentication of Domain Name Owners”, maio de 2023. <https://www.enisa.europa.eu/publications/dns-identity>.
- ENISA. “ENISA Threat Landscape 2023”, 19 de outubro de 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@download/fullReport>.
- ENISA. “ENISA Threat Landscape: Health Sector”, 5 de julho de 2023. <https://www.enisa.europa.eu/publications/health-threat-landscape>.
- ENISA. “ENISA Threat Landscape: Insider Threat”, abril de 2020. <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-insider-threat>.
- ENISA. “ENISA Threat Landscape: Transport Sector”, março de 2023. <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>.
- ENISA. “EU Cybersecurity Initiatives in the Finance Sector”, março de 2021. [https://www.enisa.europa.eu/publications/EU Cybersecurity Initiatives in the Finance Sector/@download/fullReport](https://www.enisa.europa.eu/publications/EU%20Cybersecurity%20Initiatives%20in%20the%20Finance%20Sector/@download/fullReport).
- ENISA. “Guidelines - Cyber Risk Management for Ports”, dezembro de 2020. <https://safety4sea.com/wp-content/uploads/2021/12/ENISA-Guidelines-Cyber-Risk-Management-for-Ports.pdf>.
- ENISA. “Mapping of OES Security Requirements to Specific Sectors”, 18 de janeiro de 2018. <https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors>.
- ENISA. “NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist”, 11 de dezembro de 2020. <https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist>.
- ENISA. “NIS Investments”, 2021. <https://www.enisa.europa.eu/publications/nis-investments-2021>.
- ENISA. “NIS Investments”, 2022. <https://www.enisa.europa.eu/publications/nis-investments-2022>.
- ENISA. “NIS Investments”, 2023. <https://www.enisa.europa.eu/publications/nis-investments-2023>.
- ENISA. “Railway Cybersecurity”, novembro de 2021. <https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management>.
- ENISA. “Technical Guideline on Security Measures”. <https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures>.
- EPAL, “WONE: Water Optimization Network Efficiency: A Global Solution to a Global Water Challenge”. <https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/wone>.

- EPAL. “Aquamatrix: EPAL, Boosting business innovation”. <https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/aquamatrix>.
- Epcol. “Repsol contrata novo grupo de colaboradores e lança curso com o IEFP para os formar”, 17 de março de 2022. <https://www.epcol.pt/noticias-das-associadas/repsol-contrata-novo-grupo-de-colaboradores-e-lanca-curso-com-o-iefp-para-os-formar/1236>.
- Equinix. “LS1”. <https://www.equinix.com/data-centers/europe-colocation/portugal-colocation/lisbon-data-centers/ls1>.
- E-Redes. “Cybersecurity: New challenges, the same priority”. <https://www.e-redes.pt/en/networks-of-future/cybersecurity/cybersecurity>.
- E-Redes. “Plano de Desenvolvimento e Investimento da Rede de Distribuição: Período 2021-2025”. https://www.erse.pt/media/0wji5213/anexo-i_j-proposta-ren-portq%C3%A1s-distribui%C3%A7%C3%A3o.pdf.
- ERSAR. “Plano de Segurança da Água”. Avaliação do Risco. <https://www.ersar.pt/pt/o-que-fazemos/controlo-da-qualidade-da-agua/avaliacao-do-risco>.
- ERSAR. “Relatório Anual dos Serviços de Águas e Resíduos em Portugal: Volume 1 – Caracterização do setor de águas e resíduos”, 2022. https://www.ersar.pt/_layouts/mpp/file-download.aspx?fileId=2169122.
- ESMA. “Financial Reporting”. Issuer Disclosure. <https://www.esma.europa.eu/issuer-disclosure/financial-reporting>.
- Esteves, Raul. “O Problema Nacional dos Caminhos de Ferro”. *Gazeta dos Caminhos de Ferro* n.º 1208, 16 de abril de 1938. https://hemerotecadigital.cm-lisboa.pt/obras/gazetacf/1938/N1208/N1208_master/GazetaCFN1208.pdf.
- Établissement Public de Sécurité Ferroviaire, “Taking cybersecurity challenges into account in railway safety”, 2021. <https://www.era.europa.eu/system/files/2022-11/enr135-taking-cybersecurity-challenges-into-account-in-railway-safety-en.pdf>.
- ETSI. “Analysis of user service models, technologies and applications supporting eHealth”, fevereiro de 2009. https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf.
- ETSI. “ETSI TR 103000 103099/10306106/01.01.01_60/tr_10306106v010101p.pdf”. https://www.etsi.org/deliver/etsi_tr/103000_103099/10306106/01.01.01_60/tr_10306106v010101p.pdf.
- ETSI. “ETSI TS 103000 103099/10309603/01.04.01_60/ts_10309603v010401p.pdf”. https://www.etsi.org/deliver/etsi_ts/103000_103099/10309603/01.04.01_60/ts_10309603v010401p.pdf.
- ETSI. “Intelligent Transport Systems (ITS)”. <https://cdn.standards.iteh.ai/samples/59261/357d2dcaa38c4977b9b395c643b2114c/ETSI-TS-102-940-V2-1-1-2021-07-.pdf>.
- EUROCAE, “ED-201A - Aeronautical Information System Security (AISS) Framework Guidance”, dezembro de 2021. <https://www.eurocae.net/news/posts/2021/december/ed-201a-aeronautical-information-system-security-aiiss-framework-guidance/>.
- EuroControl. “Automatic dependent surveillance – broadcast”. <https://www.eurocontrol.int/service/automatic-dependent-surveillance-broadcast>.
- Euro-IX. “IX-F – Best Practices”, agosto de 2015. <https://www.af-ix.net/sites/default/files/08%20-%20Bijal%20Sanghani%20-%20IX-F%20Best%20Practices.pdf>.
- Euronext, “Financial Statements as of 31 December 2022”. https://www.euronext.com/sites/default/files/2023-06/cassa_di_compensazione_e_garanzia_spa_financial_statement_31.12.2022_eng.pdf.
- European Energy Information Sharing & Analysis Centre (EE-ISAC). “Impact”. <https://www.ee-isac.eu/impact/#>.
- European Marchant Bank. “Target2 Explained: What is Target2?”, 12 de junho de 2023. <https://em.bank/blog/target2-explained-what-is-target2/>.

- European Standards. “CLC/TS 50701:2023”. <https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/?srsltid=AfmBOorDKQDhbsSznl-J4WKrvDMc6xbxHRStGpKIGvUiP344XdenbQwR>.
- European Standards. “General Information”, 14 de agosto de 2023. <https://standards.iteh.ai/catalog/standards/cen/39c119d3-607d-4a49-9ab7-74f51574ab42/en-15975-2-2013?srsltid=AfmBOoqHieQKOaJiD8Wnu57c-zFcHTCY1zv392baYX23wWb5a98ws5er>.
- European Union Agency for Railways. “European Rail Traffic Management System (ERTMS)”. https://www.era.europa.eu/domains/infrastructure/european-rail-traffic-management-system-ertms_en.
- European Union Agency for Railways. “TSI Revision Package 2023: Key Changes Part I – Rolling stock and CCS”, junho de 2023. <https://www.era.europa.eu/system/files/2023-06/15%2006%2023%20Webinar%20Slides.pdf>.
- Eurostat. “Electricity price statistics”. Dados extraídos em outubro de 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_price_statistics#Electricity_prices_for_household_consumers.
- Eurostat. “New indicator on annual average salaries in the EU”, 19 de dezembro de 2022. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/DDN-20221219-3>.
- Eurostat. “Physicians and physiotherapists in the EU: how many?”, 18 de agosto de 2023. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230818-1>.
- Eurostat. “Renewable energy statistics”. dados relativos a 2022, extraídos em dezembro de 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.
- Eusébio, Catarina, Joaquim Baetas e Ana Conde, “Investimentos já em pleno desenvolvimento, com construção de infraestruturas ou contratualizados”, *Águas Livres* n.º 298, maio de 2022. <https://www.epal.pt/EPAL/docs/default-source/epal/newspaper-2014/2022/05-2022.pdf>.
- Executive Digest. “Quais são as empresas com maior volume de negócios em Lisboa?”, Executive Digest, 25 de agosto de 2023. https://executivedigest.sapo.pt/noticias/quais-sao-as-empresas-com-maior-volume-de-negocios-em-lisboa/?doing_wp_cron=1709902761.2706060409545898437500.
- Fátima Caçador. “Registo de domínios .pt com novo recorde em 2022. Foram registados mais de 150 mil”, *Sapo TEK*, 4 de janeiro de 2023. <https://tek.sapo.pt/noticias/internet/artigos/registo-de-dominios-pt-com-novo-recorde-em-2022-foram-registados-mais-de-150-mil>.
- Federal Financial Supervisory Authority. “Risk management”, dezembro de 2017. https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Risikomanagement/risikomanagement_node_en.html
- Federal Trade Commission. “Equifax Data Breach Settlement”, fevereiro de 2024. <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>.
- Fedwire, “Fedwire Funds Service”. <https://www.frb services.org/binaries/content/assets/crsocms/financial-services/wires/funds.pdf>.
- Felner, Ricardo. “Maior choque de sempre”. *Público*, fevereiro de 2000. <https://www.publico.pt/2000/02/22/jornal/maior-choque-de-sempre-140333>.
- Ferreira, Ana, William Melo, Rita Costa, Sabrina Pereira e Nuno Duarte. “Os Profissionais do SNS: Retrato e Evolução”. *PLANAAP: Coleção Profissionais da Saúde* - n.º 2, março de 2024. https://www.planapp.gov.pt/wp-content/uploads/2024/03/PlanAPP_ProfissionaisSNS-2.pdf.
- FIN-FSA. “Management of operational risk in supervised entities of the financial sector”, agosto de 2014. https://www.finanssivalvonta.fi/globalassets/en/regulation/fin-fsa-regulations-and-guidelines/2014/08_2014/08_2014.m4_en.pdf.
- FIX Trading Community. “FIX 5.0 Specifications”. <https://www.fixtrading.org/standards/unsupported/fix-5-0/>.
- Flightradar24. “How flight tracking works”. <https://www.flightradar24.com/how-it-works>.

- Fonseca, Pedro, Paul McCarthy e Marian-Andrei Rizoiu. *Registentes: Os primeiros domínios .pt*. Loures: Conclusão das Letras, julho de 2021. https://tictank.pt/wp-content/uploads/2021/08/2107-registentes_livro.pdf.
- ForeNova. “Cyber Threat Analysis Done the Right Way”. <https://www.forenova.com/threat-detection/how-to-conduct-a-cyber-threat-analysis>.
- Fortinet. “What is OT Security?”. <https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security>.
- Fundação Galp Energia. “Gás A História Natural”. <https://www.fundacaogalp.com/Portals/1/Documentos/livro-gas-a-historia-natural.pdf>.
- Galp. “As nossas raízes: cronologia ilustrada”. <https://www.galp.com/corp/pt/sobre-nos/a-galp/as-nossas-raizes>.
- Galp. “Galp e empresas de energia unidas contra ciber-ataques no Fórum Económico Mundial”, 25 de maio de 2022. <https://www.galp.com/media/comunicados-de-imprensa/comunicado/id/1351/galp-e-empresas-de-energia-unidas-contr-a-ciber-ataques-no-forum-economico-mundial>.
- Galp. “Parte 1: Relatório Integrado de Gestão 2023”, 30. <https://www.galp.com/corp/Portals/0/Recursos/Investidores/IMR2023/PT/RelatorioIntegradoAnual2023HQ.pdf>.
- Garmin. “Funcionalidades úteis que distinguem os pilotos automáticos Garmin”. <https://www.garmin.com/pt-PT/garmin-technology/marine-technology/autopilot/advanced-autopilot-features/>.
- Gas Infrastructure Europe. “Security Risk Assessment Methodology”, maio de 2015. https://www.gie.eu/wp-content/uploads/filr/2751/GIE_Security_Risk_Assessment_Methodology_May2015.pdf.
- Gas-Cybersecurity. “Cybersecurity in the Energy Sector, Gas Subsector”. <https://www.gas-cybersecurity.com/>.
- Germano, Judith. “Cybersecurity Risk & Responsibility in the Water Sector”. *American Water Work Association*, 2019. <https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf>.
- GigaPIX. “QUE FAZ O GIGAPIX?”. <https://gigapix.pt/pt/home/>.
- GigaPIX. “Sobre nós”. <https://gigapix.pt/pt/sobre-nos/>.
- Google. “Google Public DNS”. <https://dns.google/>.
- Google. “What is a Data Lake?”, Google Cloud. <https://cloud.google.com/learn/what-is-a-data-lake>.
- Gotev, Georgi. “Belgium suffers major cyberattack”. *Euractiv*, 5 de maio de 2021. https://www.euractiv.com/section/politics/short_news/belgium-suffers-major-cyber-attack/.
- Grupo Brisa. “História”. Sobre nós. <https://grupobrisa.pt/sobre-nos/historia/>.
- Guerra, Ana. “IBM e Galp juntas em projeto de Inteligência Artificial”. *Ntech.news*, 12 de julho de 2018. <https://www.ntech.news/ibm-e-galp-juntas-em-projeto-de-inteligencia-artificial/>.
- Guerra, Juliana. “Impacto do 5G em Portugal pode chegar aos 3,6 mil milhões de euros”. *Ericsson*, 11 de junho de 2019. <https://www.ericsson.com/pt/press-releases/2019/6/ericsson-mobility-report-a-adocao-da-tecnologia-5g-e-ainda-mais-rapida-do-que-esperada>.
- Gulyas, Oliver e Gabor Kiss. “Cybersecurity threats in the banking sector”. 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT), junho de 2022. <https://ieeexplore.ieee.org/abstract/document/9804140>.
- Gulyas, Oliver e Gabor Kiss. “Impact of cyber-attacks on the financial institutions”, *Procedia Computer Science* 219, 2023. <https://doi.org/10.1016/j.procs.2023.01.267>.
- Gupta, Nidhi. “Analysing Transit Time Delays Along Key Global Trade Routes”. *SupplyChain Digital*, Agosto de 2024. <https://supplychaindigital.com/logistics/analysing-transit-time-delays-along-key-global-trade-routes>.
- Han, Mingyu e Peter Crossle. “Vulnerability of IEEE 1588 under Time Synchronization Attacks”, 4 de Agosto de 2019. <https://ieeexplore.ieee.org/abstract/document/8973494>.

- Hassanzadeh, Amin, Amin Rasekhab, Stefano Gallelli, Mohsen Aghashahid, Riccardo Taorminae, Avi Ostfeld e Katherine Banks. “A Review of Cybersecurity Incidents in the Water Sector”. *Journal of Environmental Engineering* 146: 25 de julho de 2020. <https://arxiv.org/pdf/2001.11144>.
- Health Cluster Portugal. “Saúde fecha o ano de 2023 a ultrapassar a meta dos 3 mil milhões”, 27 de fevereiro de 2024. <https://www.healthclusterportugal.pt/pt/noticias/exportacoes-em-saude-2023/>.
- Heider, Florian. “Collateral, central clearing counterparties and regulation”, *European Central Bank Research Bulletin* 41, 6 de dezembro de 2017. <https://www.ecb.europa.eu/press/research-publications/resbull/2017/html/ecb.rb171206.en.html>.
- Hewlett-Packard Enterprise. “HPE AI and data transformation services”. <https://www.hpe.com/pt/en/services/consulting/big-data.html>.
- Holroyd, Matthew. “Gridlock as hackers order hundreds of taxis to same place in Moscow”. *Euronews*, 2 de setembro de 2022. <https://www.euronews.com/my-europe/2022/09/02/gridlock-as-hackers-order-hundreds-of-taxis-to-same-place-in-moscow>.
- HPCC Systems. “Home”. <https://hpccsystems.com/>.
- Hudaib, Adam e Esra'a Hudaib. “DNS Advanced Attacks and Analysis”, 2014. https://www.academia.edu/download/35520765/DNS_Advanced_Attacks_and_Analysis.pdf.
- Hulewicz, Arkadiusz, Zbigniew Krawiecki e Krzysztof Dziarski, “Distributed control system DCS using a PLC controller”, 15 de julho de 2019. https://www.itm-conferences.org/articles/itmconf/pdf/2019/05/itmconf_zkwe2019_01041.pdf.
- Hussain, Shatha, Amer Alaya e Thana Azizi. “The impact of financial accounting disclosures on investors’ reactions towards bad news: The moderating role of investors’ sentiments”. *Cogent Economics and Finance*, 16 de julho de 2023. <https://www.tandfonline.com/doi/pdf/10.1080/23322039.2023.2228087?download=true>.
- Hydro. “Cyber-attack on Hydro”, março de 2019. <https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/>.
- HYFUELUP. “Shaping a better tomorrow with renewable natural gas”. <https://hyfuelup.eu/>.
- I Am the Cavalry, “Five Star Automotive Cyber Safety Framework”. <https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf>.
- IAPMEI. “Horizonte 2020”, última atualização a 10 de maio de 2024. <https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Empreendedorismo-Inovacao-Inovacao-e-Competitividade/Incentivos-e-financiamento/Horizonte-2020.aspx>.
- IAPMEI. “Transição Digital”, 23 de novembro de 2023. <https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Industria-e-Sustentabilidade/Transformacao-digital.aspx>.
- ICAO. “Aviation Cybersecurity: Emerging Challenges and Solutions”, novembro de 2023. <https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/8.4%20MedAire%20-%20Cybersecurity%20Symp%20PPT%20-%20November%202023.pdf>.
- ICAO. “Aviation Security Manual (Doc 8973 – Restricted)”. <https://www.icao.int/security/sfp/pages/securitymanual.aspx>.
- IEC. “Find out more about IEC 61850”. <https://iec61850.dvl.iec.ch/>.
- IEC. “IEC 61162-1:2024”. <https://webstore.iec.ch/en/publication/72729>.
- IEC. “IEC 62351-7”. <https://webstore.iec.ch/en/publication/30593>.
- IEEE. “IEEE Guide for Physical Security of Electric Power Substations”. <https://standards.ieee.org/ieee/1402/6050/>.
- IEEE. “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”, 24 de julho de 2008. <https://standards.ieee.org/ieee/1588/4355/>.
- IEFP. “Cheque-Formação + Digital”. <https://www.iefp.pt/cheque-formacao-digital>.
- IMO. “Maritime cyber risk”. <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>.

- IMT. “Anuário Estatístico da Mobilidade e dos Transportes - 2022”, maio de 2024. <https://www.imt-ip.pt/sites/IMTT/Portugues/Noticias/Paginas/Anuario-Estatistico-Mob-Transp2022.aspx>.
- INE. “Em 2022, a despesa corrente em saúde aumentou a um ritmo inferior ao do PIB”. Informação à Comunicação Social, 4 de julho de 2023. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=594883237&DESTAQUESmodo=2.
- INE. “Estatística dos Transportes e Comunicações 2022”, novembro de 2023. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=141725&PUBLICACOESmodo=2.
- INE. “Estatísticas da Saúde - 2022”, edição de 2024. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=660521049&att_display=n&att_download=y.
- INE. “Estatísticas da saúde 2021”, edição de 2023. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=11677508&PUBLICACOESmodo=2.
- INE. “Estatísticas Demográficas 2022”, 16 de novembro de 2023. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637367953&att_display=n&att_download=y#.
- INE. “Estatísticas do emprego”, 8 de maio de 2024. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=665513779&att_display=n&att_download=y.
- INE. “Inquérito à Utilização das TIC nas Empresas”, 2022. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=585250024&att_display=n&att_download=y.
- INE. “Inquérito à utilização de tecnologias da informação e da comunicação nas empresas”, 21 de novembro de 2023. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637881953&att_display=n&att_download=y.
- INE. “Metainformação”, janeiro de 2007, atualizado em junho de 2024. https://www.ine.pt/bddXplorer/htdocs/minfo.jsp?var_cd=0002613&lingua=PT.
- INE. “TRANSPORTE DE PASSAGEIROS CONTINUOU A AUMENTAR NO 1º TRIMESTRE DE 2024”, junho de 2024. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=670913041&att_display=n&att_download=y.
- INE. “Transportes e Comunicações 2022”, novembro de 2023. https://www.ine.pt/xportal/xmain?xpgid=ine_inst_infografia&INST=637341691&xpid=INE.
- INFARMED. “Dispositivos Médicos”, Perguntas Frequentes. <https://www.infarmed.pt/web/infarmed/perguntas-frequentes-area-transversal/novo-sistema-de-informacao-para-dispositivos-medicos-sidm>.
- INFARMED. “Pesquisa de Dispositivos Médicos”. <https://www.infarmed.pt/web/infarmed/pesquisa-dispositivos#>.
- INFARMED. “Sistema de Informação para Dispositivos Médicos (SIDM)”. https://www.infarmed.pt/web/infarmed/infarmed?p_p id=101&p_p lifecycle=0&p_p state=maximized&p_p mode=view& 101 struts action=%2Fasset_publisher%2Fview_content& 101 as setEntryId=4088116& 101 type=content& 101 urlTitle=sistema-de-informacao-para-dispositivos-medicos-sidm-&inheritRedirect=false.
- Infracontrol. “Sistemas de Transporte Inteligentes”. <https://www.infracontrol.com/pt-pt/sistemas-de-transporte-inteligentes-its/>.
- Infraestruturas de Portugal. “A IP promove ações sobre Cibersegurança”, outubro de 2019. <https://www.infraestruturasdeportugal.pt/pt-pt/ip-promove-acoes-sobre-ciberseguranca>.
- Infraestruturas de Portugal. “A Rede em Números”, Infraestruturas. <https://www.infraestruturasdeportugal.pt/pt-pt/rede-rodoviaria-ip>.

- Infraestruturas de Portugal. “Apresentação da instalação de Piloto ETCS L2”, novembro de 2021. <http://www.infraestruturasdeportugal.pt/pt-pt/apresentacao-da-instalacao-de-piloto-etcs-l2>.
- Infraestruturas de Portugal. “Linha de Alta Velocidade Porto – Lisboa”. <https://www.infraestruturasdeportugal.pt/pt-pt/principais-investimentos/linha-de-alta-velocidade-porto-lisboa>.
- Infraestruturas de Portugal. “O Futuro é Coletivo: Use os Transportes Públicos”, 19 de setembro de 2022. <https://www.infraestruturasdeportugal.pt/pt-pt/o-futuro-e-coletivo-use-os-transportes-publicos>
- Infraestruturas de Portugal. “Primeiro comboio a Hidrogénio realiza testes na rede ferroviária portuguesa”, Infraestruturas de Portugal, abril de 2024. <https://www.infraestruturasdeportugal.pt/pt-pt/primeiro-comboio-hidrogenio-realiza-testes-na-rede-ferroviaria-portuguesa>.
- Ingrams Time Systems. “Master & Slave Systems”. <https://www.ingrams.com.au/master-and-slave-systems>.
- Institute of Medicine Committee on Health Research and the Privacy of Health Information. “The Value and Importance of Health Information Privacy”, em *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, editado por Sharyl Nass, Laura Levit e Lawrence Gostin. Washington DC: National Academies Press, 2009. <https://www.ncbi.nlm.nih.gov/books/NBK9579/>.
- Intel. “Estradas Inteligentes Começam com Infraestrutura Inteligente”. <https://www.intel.com.br/content/www/br/pt/transportation/smart-road-infrastructure.html>.
- International Air Transport Association (IATA). “IATA Annual Safety Report Executive Summary and Safety Overview - 2023”, 2024. <https://www.iata.org/contentassets/a8e49941e8824a058fee3f5ae0c005d9/safety-report-executive-and-safety-overview-2023.pdf>.
- International Citizens Insurance. “The Best Healthcare in the World: Country Rankings”, 2024. <https://www.internationalinsurance.com/health/systems/>.
- International Electrotechnical Commission. “Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners”, 2024. <https://webstore.iec.ch/en/publication/62883>.
- International Energy Agency. “World Energy Outlook 2023”. <https://iea.blob.core.windows.net/assets/ed1e4c42-5726-4269-b801-97b3d32e117c/WorldEnergyOutlook2023.pdf>.
- International Monetary Fund. “Cyber Risk: A Growing Concern for Macroeconomic Stability”, abril de 2024, 7. <https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3onlineannex.ashx>
- International Monetary Fund. “World Economic Outlook: Challenges to Steady Growth”, outubro de 2018. <https://www.imf.org/-/media/Files/Publications/WEO/2018/October/English/main-report/Text.ashx>.
- International Transport Forum. “Road Safety: Annual Report 2023”. <https://www.itf-oecd.org/sites/default/files/docs/irtad-road-safety-annual-report-2023.pdf>.
- IP Património. “O passado, presente e futuro da Ferrovia que celebra 167 anos”, outubro de 2023. <https://www.ippatrimonio.pt/pt-pt/167-anos-do-caminho-de-ferro-em-portugal>.
- IPCC. “Framing and Context”. <https://www.ipcc.ch/sr15/chapter/chapter-1/>.
- Irani, Zahir, Raul Abril, Vishanth Weerakkody, Amizan Omar e Uthayasankar Sivarajah. “The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis”. *Government Information Quarterly* vol. 40, n.º 1, janeiro de 2023. <https://www.sciencedirect.com/science/article/pii/S0740624X22001204>.
- ISA. “ISA/IEC 62443 Series of Standards”. <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.
- ISAC. “Best Practices”. <https://automotiveisac.com/best-practices>.

- Islam, Mohammed, Sami Azam, Bharanidharan Shanmugam, Asif Karim, Jamal El-Den e Friso DeBoer. "Smart Parking Management System to Reduce Congestion In Urban Area", novembro de 2020. <https://ieeexplore.ieee.org/abstract/document/9309546>.
- ISO, "Information technology — Cloud computing — Overview and vocabulary", 2014, <https://www.iso.org/standard/60544.html>.
- ISO. "Activities relating to drinking water and wastewater services — Guidelines for the management of drinking water utilities and for the assessment of drinking water services", 2024. <https://www.iso.org/standard/82490.html>.
- ISO. "Application of risk management for IT-networks incorporating medical devices", outubro de 2010. <https://www.iso.org/standard/44863.html>.
- ISO. "Health informatics — Application of privacy management to personal health information". <https://www.iso.org/standard/73697.html>.
- ISO. "Health informatics — Cloud computing considerations for the security and privacy of health information systems", 2021. <https://www.iso.org/standard/70568.html>.
- ISO. "Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)", 2020. <https://www.iso.org/standard/73696.html>.
- ISO. "Health informatics — Information security management in health using ISO/IEC 27002", julho de 2008. <https://www.iso.org/standard/41298.html>.
- ISO. "Health informatics — Telehealth services — Quality planning guidelines", 2021. <https://www.iso.org/standard/75962.html>.
- ISO. "Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002", 2008. <https://www.iso.org/standard/43751.html>.
- ISO. "ISO 13613:2011". <https://www.iso.org/standard/54090.html>.
- ISO. "ISO 14885:2014". <https://www.iso.org/standard/55259.html>.
- ISO. "ISO 15031-7:2013". <https://www.iso.org/standard/62489.html>.
- ISO. "ISO 15764:2004". <https://www.iso.org/standard/28775.html>.
- ISO. "ISO 20138-2:2019". <https://www.iso.org/standard/68443.html>.
- ISO. "ISO 22163:2023". <https://www.iso.org/standard/79427.html>.
- ISO. "ISO 22888:2020". <https://www.iso.org/standard/74080.html>.
- ISO. "ISO 24113:2023". <https://www.iso.org/standard/83494.html>.
- ISO. "ISO 26262-1:2011". <https://www.iso.org/standard/43464.html>.
- ISO. "ISO 4170:1995". <https://www.iso.org/standard/20263.html>.
- ISO. "ISO 6772:2012". <https://www.iso.org/standard/54516.html>.
- ISO. "ISO/IEC 27001:2022". <https://www.iso.org/standard/27001>.
- ISO. "ISO/IEC 27019:2017". <https://www.iso.org/standard/68091.html>.
- ISO. "ISO/SAE 21434:2021". <https://www.iso.org/standard/70918.html>.
- ISO. "ISO/TR 13569:2005", novembro de 2005. <https://www.iso.org/standard/37245.html>.
- ISO. "ISO/TR 27015:2012", dezembro de 2012. <https://www.iso.org/standard/43755.html>.
- ISO. "Medical devices — Quality management systems — Requirements for regulatory purpose", julho de 2003. <https://www.iso.org/standard/36786.html>.
- ISO. "Part 1: Service management system requirements", 2018. <https://www.iso.org/standard/70636.html>.
- IT Channel. "Euronext adota solução da Cymulate para melhorar resposta a ameaças", 28 de novembro de 2019. <https://www.itchannel.pt/news/negocios/euronext-adota-solucao-da-cymulate-para-melhorar-resposta-a-ameacas>.
- Jia, Hao, Yuxiang Huan, Chen Ding, Yulong Yan, Jianjun Cui e Jiachen Wang. "A Domain-Specific Accelerator for Ultralow Latency Market Data Distribution System," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, abril de 2023. <https://ieeexplore.ieee.org/abstract/document/9801674>.

- Jornal de Negócios. “Setor do transporte marítimo é barómetro da economia mundial”, 29 de março de 2023. <https://www.jornaldenegocios.pt/negocios-em-rede/detalhe/setor-do-transporte-maritimo-e-barometro-da-economia-mundial>.
- Jumaa, Bassim, Anwaar Abdulhassan e Ammar Abdulhassan. “Advanced Driver Assistance System (ADAS): A Review of Systems and Technologies”. *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 8, n.º 6, junho 2019. https://www.academia.edu/42907359/Advanced_Driver_Assistance_System_ADAS_A_Review_of_Systems_and_Technologies.
- Kansas Adjutant General’s Department. “Chemical Facility Antiterrorism Standards (CFATS)”. <https://www.kansastag.gov/310/Chemical-Facility-Antiterrorism-Standard>.
- Kareem, Fairoz, Subhi Zeebaree, Hivi Dino, Mohammed Sadeeq, Zryan Rashid, Dathar Hasan e Karzan Sharif. “A Survey of Optical Fiber Communications: Challenges and Processing Time Influences”, abril de 2021. https://www.researchgate.net/profile/Subhi-Zeebaree/publication/351005349_A_Survey_of_Optical_Fiber_Communications_Challenges_and_Processing_Time_Influences/links/607ed8d48ea909241e10b11a/A-Survey-of-Optical-Fiber-Communications-Challenges-and-Processing-Time-Influences.pdf.
- Kelly, Stephanie e Jessica Resnick-ault. “One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators”. *Reuters*, 9 de junho de 2021. <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/>.
- Khan, Shaharyar, Ilya Kabanov, Yunke Hua e Stuart Madnick. “A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned”, novembro de 2022. <https://dl.acm.org/doi/10.1145/3546068>
- Kontas, Vasilis. “What is the Automatic Identification System (AIS)?”, MarineTraffic. <https://support.marinetraffic.com/en/articles/9552859-what-is-the-automatic-identification-system-ais>.
- Kovacs, Eduard. “Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources”. *Security Week*, 30 de abril de 2020. <https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources/>.
- Krebson Security. “Webnic Registrar Blamed for Hijack of Lenovo, Google Domains”, 26 de fevereiro de 2015. <https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/>.
- Kwan, Campbell. “Air India discLOSE data of 4.5m passengers were stolen in SITA cyber attack”, *ZdNet*, maio de 2021. <https://www.zdnet.com/article/air-india-discLOSE-data-of-4-5m-passengers-were-stolen-in-sita-cyber-attack/>.
- Laura, Ana. “Os primeiros automóveis em Portugal”. *RTP Ensina*, 1990. <https://ensina.rtp.pt/artigo/os-primeiros-automoveis-em-portugal/>.
- Lei n.º 10/90, de 17 de março, *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/lei/10-1990-333167>.
- Lei n.º 16/2022, de 16 de agosto, *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298>.
- Lei n.º 35/2018, de 20 de julho, *Procuradoria-Geral Distrital de Lisboa*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2920&tabela=leis&so_miolo=.
- Lei n.º 41/2004, de 18 de agosto, *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/lei/41-2004-480710>.
- Lei n.º 46/2018, de 13 de agosto, *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384>.
- Lei n.º 5/2004, de 10 de fevereiro, *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/lei/5-2004-581061>.
- Lei n.º 51/2011, de 13 de setembro, *Procuradoria-Geral Distrital de Lisboa*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=1515&pagina=1&ficha=1#.

- Lei n.º 58/2005 de 29 de dezembro (Lei da Água), *Diário da República*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1191&tabela=leis&ficha=1&pagina=1.
- Li, Meixuan, Jianying Zhou, Sudipta Chattopadhyay e Mark Goh. "Maritime Cybersecurity: A Comprehensive Review", *Journal of the ACM*, vol. 1, n.º 1, janeiro de 2024. <https://arxiv.org/pdf/2409.11417v1>.
- Lisboa para Pessoas (LPP), "Semáforos em Lisboa começam a ser ligados ao novo sistema inteligente", novembro de 2021. <https://lisboaparapessoas.pt/2021/11/02/semaforos-lisboa-sistema-inteligente/>.
- LIS-IX. "What is LIS-IX?". <https://lis-ix.pt/#what-is>.
- Llorach, Carles. "Cyber-attacks received in the railway sector", *Phoeniix*, 2024. <https://phoeniix.eu/2024/02/29/cyber-attacks-received-in-the-railway-sector/>.
- Lourenço, Luciano. "Alcáface: 30 anos depois". Riscos, maio de 2017. https://www.riscos.pt/wp-content/uploads/2018/SRC_V/Ebook_Alcáface_30_anos_depois.pdf.
- LR. "ISPS Code". <https://www.lr.org/en/services/statutory-compliance/isps-code>.
- LR. "Out of the box – Implementing autonomy and assuring AI". <https://www.lr.org/en/knowledge/research-reports/2023/ai-and-autonomy/?creative=708188340864>.
- LR. "Revised update of LR's Cyber-enabled ships ShipRight procedure", dezembro de 2017. <https://www.lr.org/en/knowledge/press-room/press-listing/press-release/2017/early-adopters-and-innovators-in-connected-assets-on-ships/>.
- Lusa. "Portugal desperdiça todos os anos várias barragens do Alqueva' em fugas de água". *Público*, 6 de maio de 2023. <https://www.publico.pt/2023/05/06/azul/noticia/portugal-desperdica-anos-varias-barragens-alqueva-fugas-agua-2048583>.
- Lusa. "Ciberataques a autarquias aumentam com a transição digital". *SIC Notícias*, 18 de outubro de 2023. <https://sicnoticias.pt/pais/2023-10-18-Ciberataques-a-autarquias-aumentam-com-a-transicao-digital-e984cece>.
- Magalhães, Flávia. "IA e o setor financeiro: A revolução da tecnologia". *Consumidor Moderno*, 29 de fevereiro de 2024. <https://consumidormoderno.com.br/ia-e-o-setor-financeiro-a-revolucao-da-tecnologia/>.
- Maré, Florbela. "História das Infraestruturas Rodoviárias". Dissertação de mestrado, Universidade do Porto, 2011. <https://repositorio-aberto.up.pt/bitstream/10216/61562/1/000148960.pdf>.
- MarineTraffic. <https://www.marinetraffic.com/>.
- Maritime Cybersecurity. "Mediterranean Shipping Company (MSC) hit by a malware attack in Geneva, Switzerland", abril de 2020. <https://maritimecybersecurity.nl/incident/KPgmlrZz5r>.
- Marktest. "Gás canalizado: penetração aumenta mas não chega à maioria da população", Marktest, 11 de dezembro de 2018. <https://www.marktest.com/wap/a/n/id~2470.aspx>.
- Martani, Claudio, Natalia Papathanasiou e Bryan Adey. "A Review of the State-of-the-Art in Railway Risk Management", outubro de 2016. https://www.researchgate.net/publication/309609809_A_Review_of_the_State-of-the-Art_in_Railway_Risk_Management.
- Martínez-Díaz, Margarita e Francesc Soriguera. "Autonomous Vehicles: theoretical and practical challenges". *Transportation Research Procedia*, 2018. <https://www.sciencedirect.com/science/article/pii/S2352146518302606>.
- Martins, Rui. "Aumentar o uso dos transportes públicos". *Observador*, 2 de outubro de 2023. <https://observador.pt/opiniao/aumentar-o-uso-dos-transportes-publicos/>.
- Maurer, Tim e Arthur Nelson. "The Global Cyber Threat to Financial Systems", *FINANCE & DEVELOPMENT*, março de 2021. <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>.
- McCarthy, Dave, Lara Greden, Jason Bremner, Brad Casemore, Jennifer Cooke, Stephen Elliot, Al Gillen, Phil Goodwin, Ashish Nadkarni, Adelaide O'Brien, Peter Rutten, Bjoern Stengel, Rick

Villars, Natalya Yezhkova, Jevin Jensen, Mary Johnston Turner. "IDC FutureScape: Worldwide Cloud 2023 Predictions", IDC, outubro de 2022. <https://www.idc.com/getdoc.jsp?containerId=US48602322>.

- McGoogan, Cara. "London HIV clinic accidentally leaks data of 780 patients". *Wired*, 2 de setembro de 2015. <https://www.wired.com/story/56-dean-street-hiv-leak/>.
- MedTech Dive. "Hospitals' IoMT Device Security Risk Quantified in New Report", 23 de agosto de 2023. <https://www.medtechdive.com/press-release/20230823-hospitals-iomt-device-security-risk-quantified-in-new-report/>.
- Mee, Paul e Rico Brandenburg. "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk". *World Economic Forum*, 17 de dezembro de 2020. <https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/>.
- Mendonça, Cátia e Rita Costa, "40 anos do SNS. O que mudou?", *Público*, 14 de setembro de 2019. <https://www.publico.pt/2019/09/14/infografia/40-anos-sns-mudou-340>.
- Menzies, James. "Under Attack: Trucking industry increasingly at risk of cyberattacks". *Trucknews*, 10 de novembro de 2023. <https://www.trucknews.com/features/under-attack-trucking-industry-increasingly-at-risk-of-cyberattacks/>.
- Metropolitano de Lisboa. "Novo sistema de sinalização do Metropolitano de Lisboa entra em fase final de testes", maio de 2024. <https://www.metrolisboa.pt/institucional/2024/05/10/novo-sistema-de-sinalizacao-do-metropolitano-de-lisboa-entra-em-fase-final-de-testes/>.
- Metropolitano de Lisboa. "Relatório Consolidado 2023", junho de 2024. https://www.metrolisboa.pt/institucional/wp-content/uploads/sites/2/2024/08/Relatorio_Consolidado_2023.pdf.
- Microsoft. "Estado da Cibersegurança em Portugal", 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- Ministério das Finanças. "Orçamento do Estado 2024: Relatório - versão consolidada de 16 de outubro de 2023". https://www.dgo.gov.pt/politicaorcamental/OrcamentodeEstado/2024/Proposta%20do%20Or%C3%A7amento/Documentos%20do%20OE/OE2024_doc16_Relatorio.pdf.
- Mitchell, Alex. "Hackers are taking over planes' GPS — experts are lost on how to fix it". *New York Post*, 20 de novembro de 2023. <https://nypost.com/2023/11/20/lifestyle/hackers-are-taking-over-planes-gps-experts-are-lost-on-how-to-fix-it/>.
- MITRE. "Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks", 15 de novembro de 2023. <https://www.mitre.org/news-insights/publication/next-steps-toward-managing-legacy-medical-device-cybersecurity-risks>.
- Mohammed, Abubakar e et al., "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective", setembro de 2022. <https://dl.acm.org/doi/10.1145/3548691>.
- Museu do Ar. "Blériot XI". <https://museudoar.pt/pagina-001.003.002.005-bl-riot-xi>.
- Nakashima, Ellen e Paul Sonne. "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare". *The Washington Post*, 8 de junho de 2018. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.
- National Cybersecurity Center of Excellence (NCCoE). "Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems", junho de 2023. <https://www.nccoe.nist.gov/sites/default/files/2023-06/securing-water-and-wastewater-utilities-project-description-final.pdf>.
- NAVIA. "Business & Operations Intelligence", Porquê o NAVIA. <https://www.naviasolutions.com/porque-o-navia/>.
- NAVIA. "Questões frequentes", FAQs. <https://www.naviasolutions.com/faqs/>.
- NERC, "Standards". <https://www.nerc.com/pa/Stand/Pages/Default.aspx>.

- Neto, Rita. “Gás natural dispara 55% e bate recorde com guerra na Ucrânia”, *Eco*, 2 de março de 2022. <https://eco.sapo.pt/2022/03/02/gas-natural-dispara-55-para-recorde-de-194-euros-por-mwh/>.
- Nicolau, Teresa. “Da democracia nasceu o Serviço Nacional de Saúde”. *RTP Ensina*, 2014. <https://ensina.rtp.pt/artigo/da-democracia-nasceu-o-servico-nacional-de-saude/>.
- NIS Cooperation Group. “Sectorial implementation of the NIS Directive in the Energy sector”, outubro de 2019. <https://smart-lighting.es/wp-content/uploads/2019/11/SectorialimplementationoftheNISDirectiveintheEnergysectorpdf.pdf>.
- NIST. “Guide to Operational Technology (OT) Security”, 26 de abril de 2022. <https://csrc.nist.gov/pubs/sp/800/82/r3/ipd>.
- NIST. “Guidelines for Smart Grid Cybersecurity”. <https://csrc.nist.gov/pubs/ir/7628/r1/final>.
- NIST. “Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide”, fevereiro de 2024. <https://csrc.nist.gov/pubs/sp/800/66/r2/final>.
- NIST. “NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral”, fevereiro de 2024. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf>.
- NIST. “NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral”, fevereiro de 2024. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf>.
- NIST. “Threat Intelligence”. Glossary. https://csrc.nist.gov/glossary/term/threat_intelligence.
- Nogueira, Miguel. “Centro tecnológico da Euronext no Porto vai contratar para continuar ‘história de sucesso’”. *Porto.*, 12 de novembro de 2021. <https://www.porto.pt/pt/noticia/centro-tecnologico-da-euronext-no-porto-vai-contratar-para-continuar-historia-de-sucesso>.
- Nokia. “Best Master Clock Algorithm”. <https://infocenter.nokia.com/public/7705SAR234R1A/index.jsp?topic=%2Fcom.nokia.basic-system-guide%2Fbest-master-clock-algorithm.html>.
- Nordlayer, “Which countries score the highest?”. Última atualização a 22 de agosto de 2024. <https://nordlayer.com/global-remote-work-index/#countries-score-table>.
- Novais, Vera. “Estónia alvo de maior ciberataque desde 2007. Grupo russo reivindica ataque”. *Observador*, 18 de agosto de 2022. <https://observador.pt/2022/08/18/estonia-alvo-de-maior-ciberataque-desde-2007-grupo-russo-reinvindica-ataque/>.
- Novo Banco. “Relatório e Contas 2023”, 28 de fevereiro de 2024. <https://www.novobanco.pt/content/dam/novobancopublicsites/docs/pdfs/divulga%C3%A7%C3%B5es-financeiras/2023/relat%C3%B3rio-e-contas/RC%20novobanco%202023.pdf.coredownload.inline.pdf>.
- NTSB. “Pipeline Rupture and Subsequent Fire in Bellingham, Washington”. <https://www.nts.gov/investigations/AccidentReports/Reports/PAR0202.pdf>.
- Nunes, Flávio. “Ciberataque à TAP: o que disse a empresa (e o que aconteceu depois)”. *Eco*, 22 de setembro de 2022. <https://eco.sapo.pt/2022/09/22/ciberataque-a-tap-o-que-disse-a-empresa-e-o-que-aconteceu-depois/>.
- Observador. “Inovação e setor financeiro: simplificar é a regra”, 29 de novembro de 2023. <https://observador.pt/2023/11/29/inovacao-e-setor-financeiro-simplificar-e-a-regra/>.
- OCIMF. “Tanker Management and Self Assessment 3 - A Best Practice Guide”. <https://www.ocimf.org/pt/publications-advocacy-5/publica%C3%A7%C3%B5es/livros/tanker-management-and-self-assessment-3>.
- Oliveira, Ana. “Dependência europeia de combustíveis fósseis subiu em 2022. Portugal fica ligeiramente abaixo dos 70%”. *ECO*, 30 de janeiro de 2024. <https://eco.sapo.pt/2024/01/30/dependencia-europeia-de-combustiveis-fosseis-subiu-em-2022-portugal-fica-ligeiramente-abaixo-dos-70/>.
- Oliveira, Ana. “Emprego nas renováveis cresce a pique com solar a brilhar. E os “fósseis”?”. *CNN Portugal*, 22 de julho de 2023. <https://cnnportugal.iol.pt/energia/energias-renovaveis/emprego-nas-renovaveis-cresce-a-pique-com-solar-a-brilhar-e-os-fosseis/20230722/64b902ccd34e72171a0b5971>.

- Oliveira, Daniela. “Desenvolvimento de um Sistema Eletrónico de Vigilância Epidemiológica (eVDmed): recolha, análise e publicação de informação”. Dissertação de mestrado, Universidade do Minho, 2017. <https://repositorium.sdum.uminho.pt/bitstream/1822/49627/1/Daniela%20Pimentel%20de%20Oliveira.pdf>.
- OMI, “Relatório Integrado OMI 2022”, maio de 2023. https://www.omie.es/sites/default/files/2023-05/omi_reporting_integrado_2022_PT_4.pdf.
- OMIClear. “Quem somos”. <https://www.omiclear.pt/pt>.
- Onkst, David. “The First U.S. Airshows – the Air Meets of 1910”, U.S. Centennial of Flight Commission https://www.centennialofflight.net/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.
- ONU. “Transporte marítimo perfaz mais de 80% do comércio global”, 24 de setembro de 2020. <https://news.un.org/pt/story/2020/09/1727312>.
- Open DNS. “About Us”. <https://www.opendns.com/about/>.
- OPT, “Empresa”. <https://www.opt.pt/empresa/>.
- Ott, David, Christopher Peikert, Mark Hill, Ann Drobnis e Chris Ramming. “Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility”. *Computing Community Consortium*, setembro de 2019. <https://arxiv.org/pdf/1909.07353>.
- Pacheco, Elsa. “Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte: expectativas, intervenções e resultantes”. Tese de doutoramento, Universidade do Porto, 2001. https://www.academia.edu/10413987/Altera%C3%A7%C3%A3o_das_acessibilidades_e_din%C3%A2micas_territoriais_na_Regi%C3%A3o_Norte_expectativas_interven%C3%A7%C3%B5es_e_resultantes?auto=download.
- Pacific Maritime Magazine. “European Oil Port Terminals Crippled by Cyberattack and Ransomware”. <https://pacmar.com/article/european-oil-port-terminals-crippled-by-cyberattack-and-ransomware/>.
- Paganini, Pierluigi. “BlackCat Gang Claimed Responsibility for Swissport Ransomware Attack”. *SecurityAffairs*, fevereiro de 2022. <https://securityaffairs.com/128039/cyber-crime/blackcat-swissport-ransomware-attack.html>.
- Pallardy, Richard. “The Unique Cyber Vulnerabilities of Medical Devices”. *Information Week*, 14 de novembro de 2023. <https://www.informationweek.com/cyber-resilience/the-unique-cyber-vulnerabilities-of-medical-devices#close-modal>.
- Palmié, Maximilian, Joakim Wincent; Vinit Parida e Umur Caglar. “The evolution of the financial technology ecosystem: an introduction and agenda for future research on disruptive innovations in ecosystems”. University of Vaasa, 2020. https://osuva.uwasa.fi/bitstream/handle/10024/10315/Osuva_Palmi%C3%A9_Wincent_Parida_Caglar_2020b.pdf?sequence=2&isAllowed=y.
- Parian, Christopher, Terry Guldemann, Sajal Bhatia. “Fooling the Master: Exploiting Weaknesses in the Modbus Protocol”. <https://www.sciencedirect.com/science/article/pii/S1877050920312576>.
- Poblete, Julio e Dr. Yoon. “Connected Automobiles and Cybersecurity”, março de 2018. http://cysecure.org/470/18sp/indiProject/Jpoblete-Project/indiO18julioPoblete_ConnectedAutomobiles.pdf.
- Polemi, Nineta e Christophe Maele. “Cibersegurança na Infraestrutura Marítima Crítica: Reflexão dos portos africanos”, Comissão Europeia, 20 de abril de 2023. <https://rusieurope.eu/wp-content/uploads/2024/02/cybersecurity-in-maritime-critical-infrastructure-crimson-report-portuguese.pdf>.
- PORDATA. “Acidentes de viação com vítimas: total e por tipo de acidente - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Acidentes_de_viacao_com_vitimas_total_e_por_tipo_de_acidente_-_Continente.xlsx.

- PORDATA. “Consumo de energia elétrica: total e por tipo de consumo”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Consumo_de_energia_eletrica_total_e_por_tipo_de_consumo.xlsx.
- PORDATA. “Consumo de energia primária: total e por tipo de fonte de energia”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-09/PORTUGAL_314.xlsx.
- PORDATA. “Consumo energético das famílias: total e por alguns produtos energéticos”, maio de 2024. https://www.pordata.pt/sites/default/files/202406/Portugal_Consumo_energetico_das_familias_total_e_por_alguns_produtos_energeticos.xlsx.
- PORDATA. “Empresas: total e por dimensão”, dados de 2022. <https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857>.
- PORDATA. “Estações de comboio e passagens de nível – Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Estacoes_de_comboio_e_passagens_de_nivel_-_Continente.xlsx.
- PORDATA. “Extensão da rede de autoestradas - Continente”, agosto de 2024. https://www.pordata.pt/sites/default/files/2024-08/Portugal_Extensao-da-rede-de-autoestradas.xlsx.
- PORDATA. “Extensão da rede rodoviária nacional em Portugal Continental”, agosto de 2024. https://www.pordata.pt/sites/default/files/2024-08/Portugal_Extensao-da-rede-rodoviaria-nacional.xlsx.
- PORDATA. “Importações de energia: total e por principais países de origem”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-10/Portugal_Importacoes-de-energia-por-principais-paises-de-origem.xlsx.
- PORDATA. “Mercadorias carregadas pelas empresas de transporte rodoviário: total e por principais países de destino - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_carregadas_pelas_empresas_de_transporte_rodoviario_total_e_por_principais_paises_de_destino_-_Continente.xlsx.
- PORDATA. “Mercadorias descarregadas pelas empresas de transporte rodoviário: total e por principais países de origem - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_descarregadas_pelas_empresas_de_transporte_rodoviario_total_e_por_principais_paises_de_origem_-_Continente.xlsx.
- PORDATA. “Mercadorias descarregadas por via marítima: total e por principais mercadorias”, julho de 2024. https://www.pordata.pt/sites/default/files/2024-09/PORTUGAL_601.xlsx.
- PORDATA. “Mercadorias transportadas no sistema ferroviário: total e por principais mercadorias - Continente (2008-)", maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_transportadas_no_sistema_ferrovioario_total_e_por_principais_mercadorias_-_Continente_%282008-%29.xlsx.
- PORDATA. “Mercadorias transportadas no sistema ferroviário: total e por principais mercadorias - Continente (2008-)", maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Mercadorias_transportadas_no_sistema_ferrovioario_total_e_por_principais_mercadorias_-_Continente_%282008-%29.xlsx.
- PORDATA. “Número de linhas e extensão da rede de transporte metropolitano - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Numero_de_linhas_e_extensao_da_rede_de_transporte_metropolitano_-_Continente.xlsx.
- PORDATA. “Peões atropelados: total e mortos - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Peoes_atropelados_total_e_mortos_-_Continente.xlsx.
- PORDATA. “População empregada: total e por setor de atividade económica. Quantas pessoas trabalham na agricultura, indústria, comércio ou outros serviços?”, Indicador: Eletricidade, gás e água, 2023.

<https://www.pordata.pt/portugal/populacao+empregada+total+e+por+setor+de+atividade+economica-3384-304037>.

- PORDATA. “Preços médios de venda ao público dos combustíveis líquidos e gasosos - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Precos_medios_de_venda_ao_publico_dos_combustiveis_liquidos_e_gasosos_-_Continente.xlsx.
- PORDATA. “Produção bruta de energia elétrica: total e por tipo de produção de energia elétrica”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-10/Portugal_Producao-eletrica-por-fonte-de-energia.xlsx.
- PORDATA. “Produção de energia elétrica a partir de fontes renováveis (%)”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-10/Portugal_Producao-de-energia-eletrica-a-partir-de-fontes-renovaveis-percentagem.xlsx.
- PORDATA. “Produção de energia elétrica: total e a partir de fontes renováveis”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Consumo_de_energia_eletrica_total_e_por_tipo_de_consumo.xlsx.
- PORDATA. “Produto Interno Bruto (PIB): Quanta riqueza é criada em Portugal”, Estatísticas. <https://www.pordata.pt/pt/estatisticas/economia/crescimento-e-productividade/produto-interno-bruto-pib>.
- PORDATA. “Receitas do transporte metropolitano – Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Receitas_do_transporte_metropolitano_-_Continente.xlsx.
- PORDATA. “Veículos matriculados: total e por tipo de veículo”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Veiculos_matriculados_total_e_por_tipo_de_veiculo.xlsx.
- PORDATA. “Veículos matriculados: total e por tipo de veículo”. Temas em Construção. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Veiculos_matriculados_total_e_por_tipo_de_veiculo.xlsx?gl=1*13h5pmx*up*MQ..*ga*MTM0NTY3NzI1MS4xNzI4NDkxMTI5*ga_HL9EXBCVBZ*MTcyODQ5MTEyOC4xLjAuMTcyODQ5MTEyOC4wLjAuMA.
- PORDATA. “Venda de combustíveis para consumo”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Venda_de_combustiveis_para_consumo.xlsx.
- PORDATA. “Volume de negócios das empresas de transporte aéreo: total e por área”, Temas em Construção. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Volume_de_negocios_das_empresas_de_transporte_aereo_total_e_por_area.xlsx?gl=1*gu9zqo*up*MQ..*ga*MTI5OTY0OTE3NS4xNzI4OTI1Njk0*ga_HL9EXBCVBZ*MTcyODkyNTY5NC4xLjAuMTcyODkyNTY5NC4wLjAuMA.
- Port Economics, Management and Policy. “Petya Ransomware Cyber-Attack on Maersk”. <https://porteconomicsmanagement.org/pemp/contents/part2/digital-transformation/petya-ransomware-cyber-attack-maersk/>.
- Portugal 2030. “PT - Programa Regional de Lisboa 2021-2027”. https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_lisboa.pdf.
- Portugal 2030. “PT - Programa Regional do Alentejo 2021-2027”. https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_alentejo.pdf.
- Portugal 2030. “PT - Programa Regional do Algarve 2021-2027”. https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_algarve.pdf.
- Portugal 2030. “PT - Programa Regional do Centro 2021-2027”. https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_centro.pdf.
- Portugal Digital. “Plano de Ação para a Transição Digital de Portugal”, 5 de março de 2020. https://portugaldigital.gov.pt/wp-content/uploads/2022/01/Plano_Acao_Transicao_Digital.pdf.
- Portugal Digital. “Sobre nós”. <https://portugaldigital.gov.pt/sobre-nos/>.
- Portugal Energia. “Plano Nacional Energia e Clima 2021-2030”. <https://www.portugalenergia.pt/setor-energetico/bloco-3/>.

- PORTUGAL.GOV.PT. “Estratégia de Longo Prazo de Combate à Pobreza Energética aprovada em Conselho de Ministros”, 23 de novembro de 2023. <https://www.portugal.gov.pt/pt/gc23/comunicacao/comunicado?i=estrategia-de-longo-prazo-de-combate-a-pobreza-energetica-aprovada-em-conselho-de-ministros>.
- PORTUGAL.GOV.PT. “Fibra ótica vai chegar a todo o país até 2027”, 12 de dezembro de 2023. <https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=esta-aberto-o-concurso-para-levar-a-fibra-otica-a-todo-o-pais>.
- Pousinho, Nuno. “A revolução do sistema de transportes”. *RTP Ensina*, 2021. <https://ensina.rtp.pt/explicador/a-revolucao-do-sistema-de-transportes-h70/>.
- Pplware. “ePark – App da Emel para pagamento do estacionamento”, 22 de setembro de 2014. https://pplware.sapo.pt/smartphones-tablets/windows_phone/epark-app-da-emel-para-pagamento-do-estacionamento/
- PplWare. “O maior banco do mundo sofreu ataque de ransomware e salvou-se graças a uma... pen USB”, 12 de novembro de 2023. <https://pplware.sapo.pt/internet/o-maior-banco-do-mundo-sofreu-ataque-de-ransomware-e-salvou-se-gracas-a-uma-pen-usb/>.
- Prado, Miguel. “EDP: imune à crise, mas não aos hackers”. *Expresso*, 18 de abril de 2020. <https://expresso.pt/economia/2020-04-18-EDP-imune-a-crise-mas-nao-aos-hackers>.
- PTSoc. Annual Report PTSOC 2023”. <https://ptsoc.pt.pt/en/relatorio-anual-ptsoc-2023/>.
- Public DNS. “DNS servers in Portugal”. <https://public-dns.info/nameserver/pt.html>.
- PwC. “A leadership agenda to take on tomorrow”, março de 2024. <https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf>.
- Qubole. “Platform”. <https://www.qubole.com/platform>.
- Railway Cybersecurity. “Cybersecurity training for the Railway Sector”. https://www.railway-cybersecurity.com/Railway_Cybersecurity_Training.html.
- Ramos, Graça. “A Escola de Aviação de Vila Nova da Rainha”. *RTP Ensina*, 2016. <https://ensina.rtp.pt/artigo/a-escola-de-aviacao-de-vila-nova-da-rainha/>.
- Rankia. “Cotação Galp Energia”. <https://www.rankia.pt/cotacao/galp-energia/>.
- Recomendação (UE) 2019/553 da Comissão de 3 de Abril de 2019 sobre a cibersegurança no setor da energia, 2019.
- Recuperar Portugal. “Investimento RE-C01-i06: Transição Digital da Saúde (300 M€)”, 8 de junho de 2021. <https://recuperarportugal.gov.pt/2021/06/08/investimento-re-c01-i06/>.
- Recuperar Portugal. “Monitorização”. <https://recuperarportugal.gov.pt/monitorizacao/>.
- Recuperar Portugal. “TD-C16-i05 CAPACITAÇÃO E TRANSFORMAÇÃO DIGITAL DAS EMPRESAS DOS AÇORES”. <https://recuperarportugal.gov.pt/transicao-digital/empresas-4-0/td-c16-i05-capacitacao-e-transformacao-digital-das-empresas-dos-acoresh/>.
- Redutskiy, Yuri. “Optimization of Safety Instrumented System Design and Maintenance Frequency for Oil and Gas Industry Processes”, março de 2017. https://www.researchgate.net/publication/315971691_Optimization_of_Safety_Instrumented_System_Design_and_Maintenance_Frequency_for_Oil_and_Gas_Industry_Processes.
- Regulamento (CE) n.º 2320/2002 do Parlamento Europeu e do Conselho de 16 de dezembro de 2002 relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil. *Jornal Oficial das Comunidades Europeias*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002R2320>.
- Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho de 11 de março de 2008 relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008R0300>.
- Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho de 31 de março de 2004 relativo ao reforço da proteção dos navios e das instalações portuárias. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:PT:PDF>.

- Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015R2120>.
- Regulamento (UE) 2017/1938 8 do Parlamento Europeu e do Conselho de 25 de outubro de 2017 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga o Regulamento (UE) n.º 994/2010. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017R1938>.
- Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32017R0745>.
- Regulamento (UE) 2019/1239 do Parlamento Europeu e do Conselho de 20 de junho de 2019 que estabelece um ambiente europeu de plataforma única para o setor marítimo e que revoga a Diretiva 2010/65/UE. *Jornal Oficial da União Europeia*, 25 de julho de 2019. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R1239>.
- Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho de 27 de novembro de 2019 relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) n.º 2015/166 da Comissão. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R2144>.
- Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho de 5 de junho de 2019 relativo à preparação para riscos no setor da eletricidade e que revoga a Diretiva 2005/89/CE. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0941>.
- Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554>.
- Regulamento (UE) n.º 185/2010 da Comissão de 4 de março de 2010 que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02010R0185-20140131>.
- Regulamento (UE) n.º 376/2014 do Parlamento Europeu e do Conselho de 3 de abril de 2014 relativo à comunicação, à análise e ao seguimento de ocorrências na aviação civil, que altera o Regulamento (UE) n.º 996/2010 do Parlamento Europeu e do Conselho e revoga a Diretiva 2003/42/CE do Parlamento Europeu e do Conselho, e os Regulamentos (CE) n.º 1321/2007 e (CE) n.º 1330/2007 da Comissão, *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0376&qid=1691222818840>.
- Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012R0648>.
- Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs). *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0909>.

- Regulamento (UE) n.º 994/2010 do Parlamento Europeu e do Conselho de 20 de outubro de 2010 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga a Diretiva 2004/67/CE do Conselho. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0001:0022:PT:PDF>.
- Regulamento da CMVM n.º 7/2023 Regulamentação do Regime da Gestão de Ativos. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/regulamento-cmvm/7-2023-835896543>
- Regulamento de Execução (UE) 2015/1998 da Comissão de 5 de novembro de 2015 que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação. *Jornal Oficial da União Europeia*, versão atualizada a 1 de setembro de 2024. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02015R1998-20240901>.
- Regulamento de Execução (UE) 2019/1583 da Comissão de 25 de setembro de 2019 que altera o Regulamento de Execução (UE) 2015/1998 da Comissão que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação, no que respeita às medidas de cibersegurança. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R1583>.
- Regulamento de Execução (UE) 2023/1695 da Comissão de 10 de agosto de 2023 relativo à especificação técnica de interoperabilidade para os subsistemas de controlo-comando e sinalização do sistema ferroviário da União Europeia e que revoga o Regulamento (UE) 2016/919. *Jornal Oficial da União Europeia*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023R1695>.
- Regulamento Geral sobre a Proteção de Dados, de 27 de abril de 2016. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis.
- Regulamento sobre circulação de automóveis. *Colecção Oficial de Legislação Portuguesa: Ano de 1901*. Lisboa: Imprensa Nacional, 1902, in Parlamento: Legislação Régia. <https://legislacaoregia.parlamento.pt/V/1/86/133/p733>.
- REN. “Produção de energia renovável bate recorde em 2023”, 2 de janeiro de 2024. <https://www.ren.pt/pt-pt/media/noticias/producao-de-energia-renovavel-bate-recorde-em-2023>.
- Repsol. “Formação”. <https://sines.repsol.pt/pt/comunidade/seguranca/formacao/index.cshtml>.
- Repsol. “Gás natural e gás propano e butano - conheça as diferenças”. <https://www.repsol.pt/particulares/assessoramento/gas-natural-e-gas-propano-e-butano/>.
- Repsol. “Integrated Management Report 2023”. https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/informes-anuales/2023/integrated-management-report-2023.pdf.
- República Portuguesa. “Domínio .pt cresceu 11% em 2021”. Comunicados, 25 de janeiro de 2022. <https://www.portugal.gov.pt/pt/gc22/comunicacao/comunicado?i=dominio-pt-cresceu-11-em-2021>.
- Resolução do Conselho de Ministros n.º 11/2024, de 8 de janeiro. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/11-2024-836222486>.
- Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho. *Diário da República*. <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/36-2015-67468089>.
- Reuters. “Bangladesh Bank hackers compromised SWIFT software, warning issued”, 25 de abril de 2016. <https://www.reuters.com/article/world/exclusive-bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DW/>
- Reuters. “German rail operator affected by global cyber attack”, 13 de maio de 2017. <https://www.reuters.com/article/technology/german-rail-operator-affected-by-global-cyber-attack-idUSKBN1890DM/>.
- Reuters. “Hong Kong exchange trading disrupted as hackers target website”. 10 de agosto de 2011. <https://www.reuters.com/article/technology/hong-kong-exchange-trading-disrupted-as-hackers-target-website-idUSTRE7792FT/>.
- Reuters. “Prague Airport says thwarted several cyber attacks; hospitals also targeted”, 18 de abril de 2020. <https://www.reuters.com/article/us-czech-cyber/prague-airport-says-thwarted-several-cyber-attacks-hospitals-also-targeted-idUSKBN2200GW/>.

- RISI. “CIA Trojan Causes Siberian Gas Pipeline Explosion”. <https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion>.
- RISI. “Hacker Takes Over Russian Gas System”. <https://www.risidata.com/Database/Detail/hacker-takes-over-russian-gas-system>.
- Roos, Dave. “How Airplanes Were Used in World War I”. *History*, 10 de fevereiro de 2022, atualizado a 10 de maio de 2024. <https://www.history.com/news/world-war-i-aviation-airplanes>.
- Rosalino, Hélder. “Desafios da transformação digital para o Setor Bancário”. *Fintech House Lisboa*, janeiro de 2020. <https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20200123.pdf>
- RTCA. “Introducing RTCA's Security Standards and Training Partnership”. <https://www.rtca.org/security/>.
- RTP. “Introdução do gás natural em Portugal”, 25 de setembro de 1990. <https://arquivos.rtp.pt/conteudos/introducao-do-gas-natural-em-portugal/>.
- SAE International. “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”, junho de 2016. https://nmi.org.uk/wp-content/uploads/2016/6/4_SAE-J3061-and-friends-for-NMI-Jun-16.pdf.
- SAE International. “CYBERSECURITY GUIDEBOOK FOR SAE, “COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK ARINC811”, dezembro de 2005, <https://www.sae.org/standards/content/arinc811/>.
- SAE International. “Hardware Protected Security for Ground Vehicles”. https://www.sae.org/standards/content/j3101_202002/.
- Sarbanes Oxley Act. “The Sarbanes-Oxley Act”, <https://sarbanes-oxley-act.com/>.
- SCADA INFO. “SCADA and Energy Management System”. <https://www.scadainfo.com/scada-and-energy-management-system/>.
- Schizas, Emmanuel, Rui Hao, Keith Bear, Massimo Preziuso, Elizabeth Seger, Robert Wardrop, Raghavendra Rau, Pradeep Debata, Philip Rowan, Nicola Adams, Mia Gray e Nikos Yerolemou. “Transforming Paradigms: A Global AI in Financial Services Survey”. *World Economic Forum*, 29 de fevereiro de 2020. https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf.
- Schmeken, Holger. “Automotive Cyber Security: New mandatory regulations”. DQS, 6 de dezembro de 2022. <https://www.dqsglobal.com/intl/learn/blog/automotive-cyber-security-new-mandatory-regulations>.
- Seacord, Robert, Daniel Plakosh e Grace Lewis. *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices*. Boston: Addison-Wesley, 2003.
- Security Boulevard. “Securing Legacy OT Systems: Challenges and Strategies”, 24 de abril de 2023. <https://securityboulevard.com/2023/04/securing-legacy-ot-systems-challenges-and-strategies/>.
- Security Magazine. “App Cybercomm já está em funcionamento na TAP”, junho de 2023. <https://www.securitymagazine.pt/2023/06/07/ciberseguranca-app-cybercomm-ja-esta-em-funcionamento-na-tap-e-ctt/>.
- Security Magazine. “GALP dá mais um passo na sua segurança e integra rede nacional CSIRT”, 20 de julho de 2021. <https://www.securitymagazine.pt/2021/07/20/galp-da-mais-um-passo-na-sua-seguranca-e-integra-rede-nacional-csirt/>.
- Security Magazine. “Galp Energia mantém segurança dos serviços críticos com plataforma xDR com M365 E5”, 6 de setembro de 2024. <https://www.securitymagazine.pt/2024/09/06/galp-energia-mantem-seguranca-dos-servicos-criticos-com-plataforma-xdr-com-m365-e5/>.
- Security Standards Council. “PCI Data Security Standard (PCI DSS)”. Standards. <https://www.pcisecuritystandards.org/standards/pci-dss/>.
- Séneca, Hugo. “Hackers publicam passwords de milhares de médicos e enfermeiros do SNS na internet”. *Expresso*, 20 de julho de 2020. <https://expresso.pt/sociedade/2020-07-20-Hackers-publicam-passwords-de-milhares-de-medicos-e-enfermeiros-do-SNS-na-internet>.

- Seters, Daan, Stefan Grebe e Jasper Faber. “Health Impacts of Aviation UFP Emissions in Europe”. CE Delft, maio de 2024. https://www.transportenvironment.org/uploads/files/CEdelft_Final_Study.pdf.
- SIBS. “Relatório e Contas 2023: Contas Consolidadas”, julho de 2024. https://sibs-sites.sibs.pt/sibs/wp-content/uploads/sites/13/2024/07/RC_2023_SIBS_CONSOLIDADO.pdf.
- Siemens. “Connected Driver Advisory System (C-DAS)”. <https://www.mobility.siemens.com/uk/en/portfolio/rail-infrastructure/connected-driver-advisory-system.html>.
- Silva, Alina, Ana Correia, Carolina Guimarães, Josefina Gomes, José Maria Azevedo, Manuela Oliveira, Paula Araújo da Silva, Paula Lopes, Paulo Santos, Pedro Figueiredo, Raquel Meira, Ricardo Sousa, Ruben Fernandes, Susana Pinto e Vasco Leite. “Estratégia de Desenvolvimento do Norte para Período de Programação 2021-27 das Políticas da União Europeia”. PT - Programa Regional do Norte 2021-2027, Portugal 2030. <https://www.ccdr-n.pt/storage/app/media/2021/CCDRN%202030-compactado.pdf>.
- Silva, Douglas, Caio Catarina e Eric Battle. “Advanced oil recovery associated with carbon capture and storage”. *Research, Society and Development*, vol. 11, n.º 1, janeiro de 2022. <http://dx.doi.org/10.33448/rsd-v11i1.24599>.
- Silver-Greenberg, Jessica Matthew Goldstein e Nicole Perlroth. “JPMorgan Chase Hacking Affects 76 Million Households”. *The New York Times*, outubro de 2014. <https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>.
- Simão, Mafalda. “A Prestação de Cuidados de Saúde em Função do Território”. Publicado no Repositório Científico da Universidade de Coimbra, 2022. <https://estudogeral.uc.pt/handle/10316/102463>.
- Skaves, Peter. “FAA Aircraft Systems Information Security Protection (ASISP) Overview”. Federal Aviation Administration, abril de 2015. <https://ieeexplore.ieee.org/iel7/7118533/7121207/07121273.pdf>.
- SNS, “Portugal lidera Grupo Europeu criado para o setor da saúde”, 30 de janeiro de 2020. <https://www.sns.gov.pt/noticias/2020/01/31/saude-ciberseguranca/>.
- SNS. “História do SNS”. <https://www.sns.gov.pt/sns/servico-nacional-de-saude/historia-do-sns/>.
- Soltani, Reza, Marzia Zaman, Rohit Joshi e Srinivas Sampalli. “Distributed Ledger Technologies and Their Applications: A Review”, *Applied Sciences* 12, 2022. <https://doi.org/10.3390/app12157898>.
- SPMS. “Alertas e Segurança”. <https://www.spms.min-saude.pt/alertaseseguranca/>.
- SPMS. “BI CSP – Bilhete de Identidade dos Cuidados de Saúde Primários”. <https://www.spms.min-saude.pt/2020/07/bi-csp-bilhete-de-identidade-dos-cuidados-de-saude-primarios/>.
- SPMS. “Cibersegurança”, abril de 2019. <https://www.spms.min-saude.pt/2019/04/ciberseguranca-2/>.
- SPMS. “Circular Normativa n.º 03/2017: medidas excecionais de segurança”, 19 de maio de 2017. <https://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA3-Medidas-Excecionais-de-Ciberseguran%C3%A7a.pdf>.
- SPMS. “Conteúdos de Sensibilização de Cibersegurança”, Academia SPMS. <https://academia.spms.min-saude.pt/atis-de-sensibilizacao-de-ciberseguranca/>.
 - SPMS. “Exames Sem Papel”, julho de 2020. <https://www.spms.min-saude.pt/2020/07/exames-sem-papel/>.
- SPMS. “FAQs PEM - Receita sem papel”, novembro de 2015. <https://spms.min-saude.pt/wp-content/uploads/2015/11/FAQs1.pdf>.
- SPMS. “PEM | Prescrição Eletrónica Médica”, julho de 2020. <https://www.spms.min-saude.pt/2020/07/pem/>.
- SPMS. “Plano de Atividades e Orçamento 2022”, 76, setembro de 2021. https://www.spms.min-saude.pt/wp-content/uploads/2022/09/Plano-de-Atividades-e-Orcameto-2022_Assinado_09092022.pdf.

- SPMS. “Prescrição Eletrónica Médica: Especificação dos Serviços para integração com o Sistema Central de Prescrições”, janeiro de 2018. [SPMS \(min-saude.pt\)](https://www.spms.min-saude.pt/).
- SPMS. “Receita Sem Papel”, abril de 2019. <https://www.spms.min-saude.pt/2019/04/receita-sem-papel-2/>.
- SPMS. “RNU: Registo Nacional de Utentes”, outubro de 2015. <https://www.spms.min-saude.pt/2015/10/rnu/>.
- SPMS. “SCLínico | Cuidados de Saúde Hospitalares (CSH)”, julho de 2020. <https://www.spms.min-saude.pt/2020/07/sclinico-hospitalar/>.
- SPMS. “SCLínico | Cuidados de Saúde Primários (CSP)”, julho de 2020. <https://www.spms.min-saude.pt/2020/07/sclinico-cuidados-de-saude-primarios-csp/>.
- SPMS. “SINAVE | Sistema Nacional de Vigilância Epidemiológica”. <https://www.spms.min-saude.pt/2020/07/sinave-2/>.
- SPMS. “Sistema Central de Prescrições”, janeiro de 2018. https://spms.min-saude.pt/wp-content/uploads/2018/10/PEM_ServicosPrescri%C3%A7%C3%A3o_ET-2.5.pdf.
- Stankizai, Abdul e Munam Shah. “Evaluation of Cyber Security Threats in Banking Systems”. Paper apresentado no 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, EUA, de 5 a 7 de dezembro 2021. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9659862>.
- STCP. “Origem”. Sobre a STCP. <https://www.stcp.pt/pt/institucional/sobre-a-stcp/origem/>.
- Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman. “NIST Special Publication NIST SP 800-82r3: Guide to Operational Technology (OT) Security”. *National Institute of Standards and Technology*, setembro de 2023. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf>.
- Sulaiman Asif. “Cyber Threat Analysis: Types, Benefits, Tools, Approaches”, *Knowledge Hut*, 5 de setembro de 2023. <https://www.knowledgehut.com/blog/security/threat-analysis>.
- Swiss National Bank. “The SNB’s legal basis”. <https://www.snb.ch/en/the-snb/organisation/legal-framework>
- Sytas, Andrius. “Russian group claims hack of Lithuanian sites in retaliation for transit ban”. *Reuters*, 27 de junho de 2022. <https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27/>.
- Tamplin, True. “Advantages of Financial Information Exchange (FIX)”. *Finance Strategists*, 12 de julho de 2023. <https://www.financestrategists.com/wealth-management/investment-management/financial-information-exchange-fix/#advantages-of-financial-information-exchange-fix>.
- TAP Air Portugal. “Cronologia”. A Nossa História. <https://www.tapairportugal.com/pt/a-nossa-historia/cronologia>.
- TAP. “Apresentação de resultados 2023”, março de 2024. <https://www.tapairportugal.com/pt/sobre-nos/investidores/informacao-financeira?accordionid=12943eea-2400-4b17-ad20-487d8c4f8635>.
- TAP. “Relatório de Sustentabilidade 2023”, 2024. <https://www.tapairportugal.com/pt/-/media/Institucional/PDFs/Relatorios/2023/Relatorio-de-Sustentabilidade-TAP-2023.pdf?la=pt-PT&hash=A15B2D9DA1DBF21D101AFE8F24258F5DB60BAE98>.
- TAP. “Relatório de Sustentabilidade de 2023”. <https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais>.
- Teixeira, Alberto. “Banca com lucros recorde em 5 gráficos”. *Eco*, 15 de março de 2024. <https://eco.sapo.pt/2024/03/15/banca-com-lucros-recorde-em-5-graficos/>.
- Teixeira, Rui, Ofer Carmi, Peter Gattinesi e Philipp Hohenblum. “JRC Technical Report: Water Security Plan Implementation Manual for Drinking Water Systems”, Comissão Europeia. <https://ec.europa.eu/newsroom/cipr/items/738662/en>.
- Telecommunications Industry Association. “ANSI/TIA-942 Standard”. <https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/>.
- The Apache Software Foundation. “Apache Hadoop”. <https://hadoop.apache.org/>.

- The Geography of Transport Systems. “Geographical Impacts of the Suez and Panama Canals”. <https://transportgeography.org/contents/chapter1/emergence-of-mechanized-transportation-systems/suez-panama-canal-geography-impacts/>.
- The Guardian. “New Zealand stock exchange disrupted by fourth 'offshore' cyber attack”, 28 de agosto de 2020. <https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack>.
- The New York Times, “Hackers Attacked California Power”, 10 de junho de 2001. <https://www.nytimes.com/2001/06/10/us/hackers-attacked-california-power.html>.
- Timu, Andra. “Pro-Russian Hacking Group Killnet Attacks Romanian Websites”. *Bloomberg*, abril de 2022. <https://www.bloomberg.com/news/articles/2022-04-29/romanian-government-border-police-websites-hit-by-ddos-attack>.
- TORRES VEDRAS WEB. “História da Exploração Petrolífera em Portugal: Avanços e Desafios na Indústria”, 14 de fevereiro de 2024. <https://torresvedrasweb.pt/historia-da-exploracao-petrolifera-em-portugal-avancos-e-desafios-na-industria/>.
- Três Em Um. “Sobre”. <https://3em1.pt/>.
- Turhune, Chad. “UCLA Health System data breach affects 4.5 million patients”, *Los Angeles Times*, 17 de julho de 2015. <https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html>.
- U.S. Department of Homeland Security. “OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)”, fevereiro de 2014. <https://www.energy.gov/oe/articles/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014>.
- U.S. Securities and Exchange Commission. “OCIE Cybersecurity and Resiliency Observations”. <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>.
- UIC. “FRMCS: Future Railway Mobile Communication System”, setembro de 2023. <https://uic.org/rail-system/telecoms-signalling/frmcs>.
- United States Department of Education. “Handbook OCIO-05, Handbook for Information Technology Security Certification and Accreditation Procedures”, março de 2006. <https://www.ed.gov/media/document/acshbocio05doc>.
- United States Federal Trade Commission. “Gramm-Leach-Bliley Act”. Business Guidance: Privacy and Security. <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>.
- United States Government Accountability Office. “Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination”. Report to Congressional Committees, dezembro de 2023. <https://www.gao.gov/assets/d24106683.pdf>.
- Vance, James e Thomas Shedd. “Railroad history”, outubro de 2024. <https://www.britannica.com/technology/railroad/Railroad-history>.
- Vujičić, Dejan, Dijana Jagodić e Siniša Randić. “Blockchain technology, bitcoin, and Ethereum: A brief overview”. Paper apresentado no 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), Sarajevo, Bósnia e Herzegovina, de 21 a 23 de março de 2018. <https://ieeexplore.ieee.org/abstract/document/8345547/>.
- Wakefield, Jane. “EasyJet admits data of nine million hacked”, *BBC*, 19 de maio de 2020. <https://www.bbc.com/news/technology-52722626>.
- Wall, Tyler. “Throwback Attack: Ukrainian railway hit by cyberattack, stranding passengers”. *Industrial Cybersecurity Pulse*, 24 de março de 2023. <https://www.industrialcybersecuritypulse.com/hacks-attacks/throwback-attack-ukrainian-railway-hit-by-cyberattack-stranding-passengers/>.
- Wang, Jun, Li Zhang, Yanjun Huang, Jian Zhao. “Safety of Autonomous Vehicles”. *Journal of Advanced Transportation*, outubro de 2020. <https://onlinelibrary.wiley.com/doi/full/10.1155/2020/8867757>.
- Warrick, Joby e Ellen Nakashima. “Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran”. *Washington Post*, 8 de maio de 2020. <https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted->

[cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html](https://www.cncs.pt/pt/actualidades/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html).

- Watanabe, Ikuo e Tetsuo Takashige. “Advanced ATP System for Improving Train Traffic Density and Control Efficiency”, 1991. <https://onlinepubs.trb.org/Onlinepubs/trr/1991/1314/1314-023.pdf>.
- Wongthongtham, Pornpit, Daniel Marrable, Bilal Abu-Salih, Xin Liu e Greg Morrison. “Blockchain-enabled Peer-to-Peer energy trading”. *Computers & Electrical Engineering* 94, setembro de 2021. <https://doi.org/10.1016/j.compeleceng.2021.107299>.
- Wood, Johny. “Global financial stability at risk due to cyber threats, IMF warns. Here's what to know”. *World Economic Forum*, 15 de maio de 2024. <https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/>.
- Woodroof, Nicholas. “TOTEX: commercial creativity and the supply chain of the future”. *OilField Technology*, 12 de agosto de 2019. <https://www.oilfieldtechnology.com/special-reports/12082019/totex-commercial-creativity-and-the-supply-chain-of-the-future/>.
- World Bank. “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.
- World Economic Forum, “Strengthening cybersecurity in the oil and gas industry”, janeiro de 2023. www.weforum.org/impact/cyber-resilience-oil-and-gas/.
- World Economic Forum. “Global Cybersecurity Outlook 2024”, janeiro de 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.
- *World Population Review*. “Euro Health Consumer Index by Country 2024”. <https://worldpopulationreview.com/country-rankings/euro-health-consumer-index-by-country>.
- Zetter, Kim. “Meet ‘Flame’. The Massive Spy Malware Infiltrating Iranian Computers”. *Wired*, 28 de maio de 2012. <https://www.wired.com/2012/05/flame/>.
- Zhou, Haibo, Wenchao Xu, Jiacheng Chen e Wei Wang. “Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities”, janeiro de 2020. <https://ieeexplore.ieee.org/abstract/document/8967260>.

www.cncs.gov.pt/

