CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de **Cibersegurança**

RELATÓRIO SOBRE OS **SETORES DOS OPERADORES DE SERVIÇOS ESSENCIAIS**

Transportes

Caracterização, Regulamentação e Recomendações no Âmbito do Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

Índice

Índice de Gráficos

Índice de Figuras

Índice de Tabelas

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 NIS[1], 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 societais 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 societais 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].

[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).

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 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 essencial[4] (...) 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 serviço[6].

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 de 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 (*Domain Name Services,* DNS)
		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.

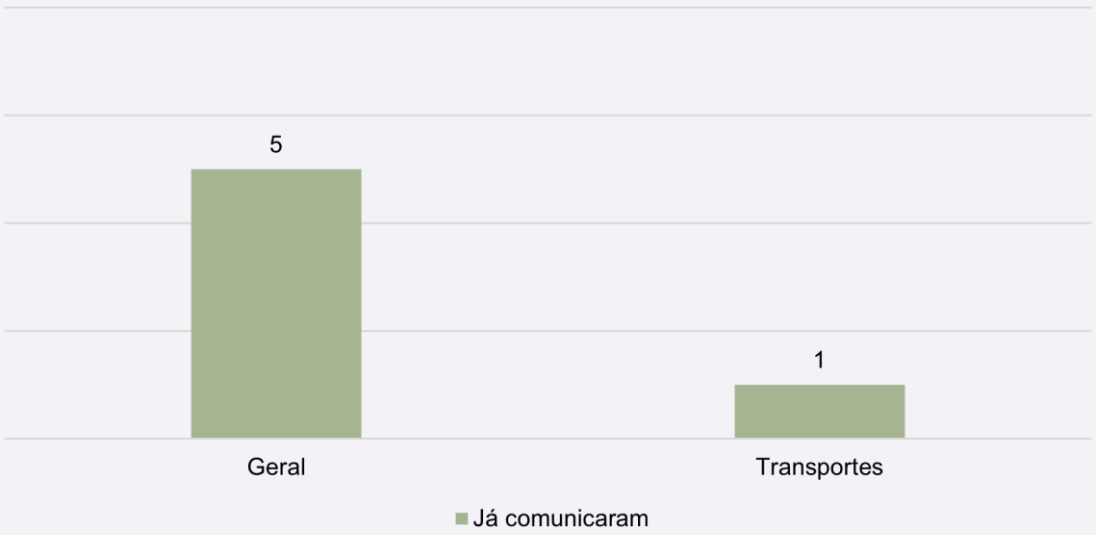
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez, 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.

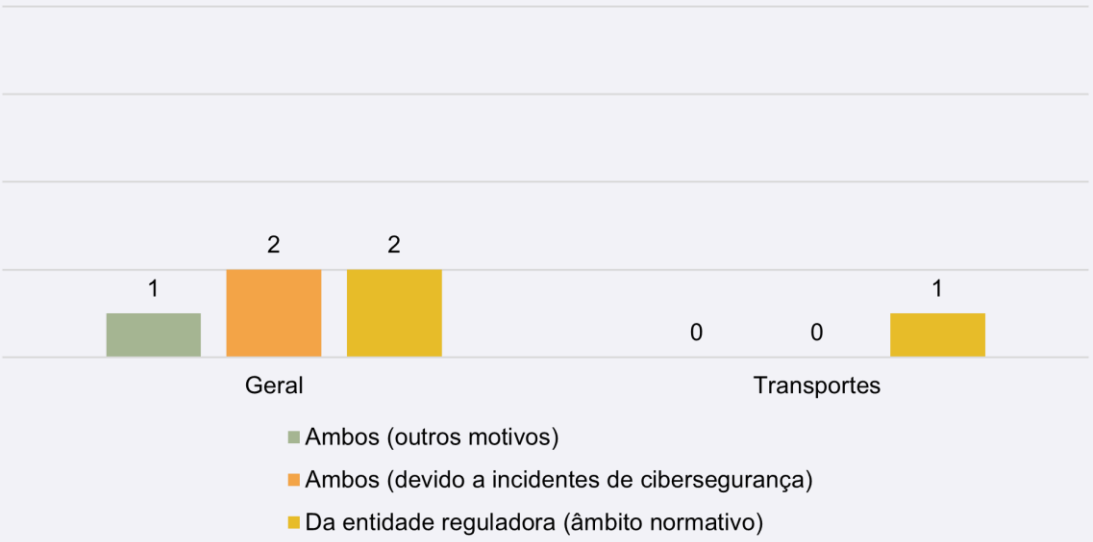
1. Comunicação entre OSE e respetivos Reguladores

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



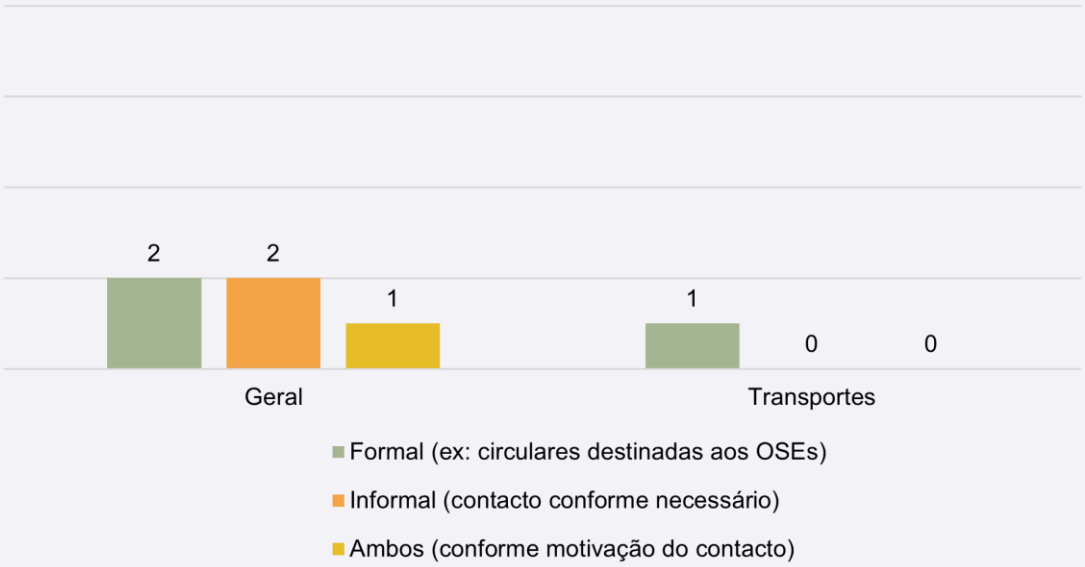
Entre os oito reguladores que responderam, cinco indicaram já ter comunicado com os OSE sobre questões de cibersegurança. Deve-se, no entanto, sublinhar que no setor dos transportes, registaram-se as respostas de três reguladores e que apenas um indicou já ter comunicado com os OSE sobre questões de cibersegurança.

Gráfico 2 - Origem da comunicação sobre questões de cibersegurança



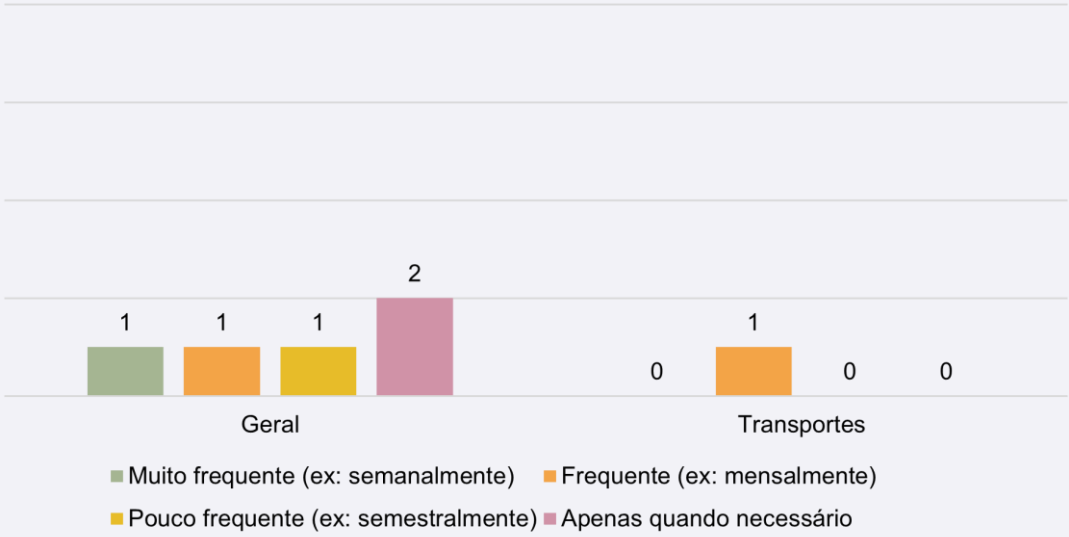
Relativamente à origem da comunicação sobre cibersegurança realizada por cinco dos reguladores, dois indicaram que a comunicação partiu dos próprios, em contexto de informação sobre normas do setor, outros dois responderam que houve comunicação que se gerou a partir dos dois lados, devido à ocorrência de incidentes de cibersegurança e apenas um respondeu que houve comunicação sobre cibersegurança a ser realizada com os OSE devido a outros motivos. O setor dos transportes mencionou que a comunicação teve origem da entidade reguladora.

Gráfico 3 - Formalidade da comunicação realizada



Entre os mesmos cinco reguladores, dois indicaram que a comunicação é geralmente feita de modo formal (incluído nestes o setor dos transportes, através de, por exemplo, circulares; outros dois responderam que a comunicação é sobretudo informal, consoante a necessidade e apenas um indicou haver comunicação tanto de caráter formal como mais informal.

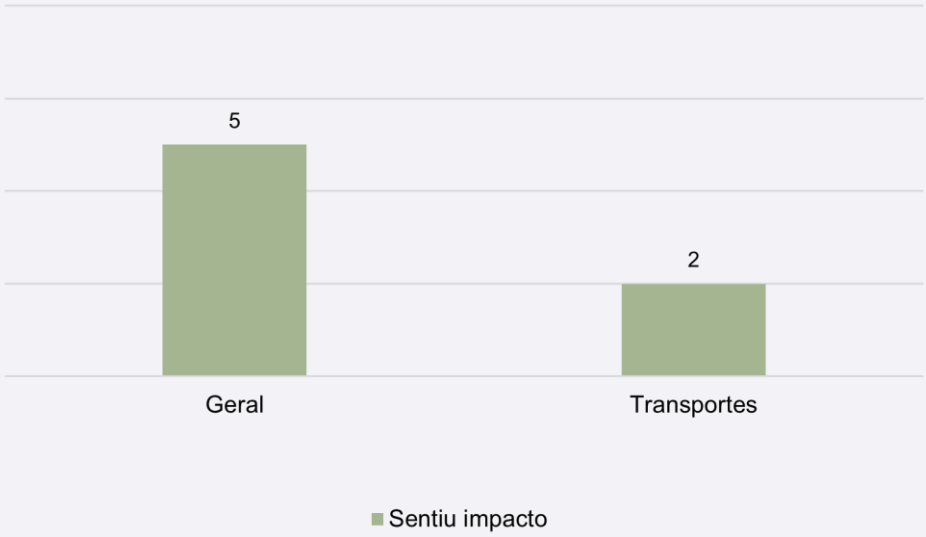
Gráfico 4 - Frequência da comunicação



No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. O regulador dos transportes indicou comunicar com os OSE sobre cibersegurança com uma frequência mensal.

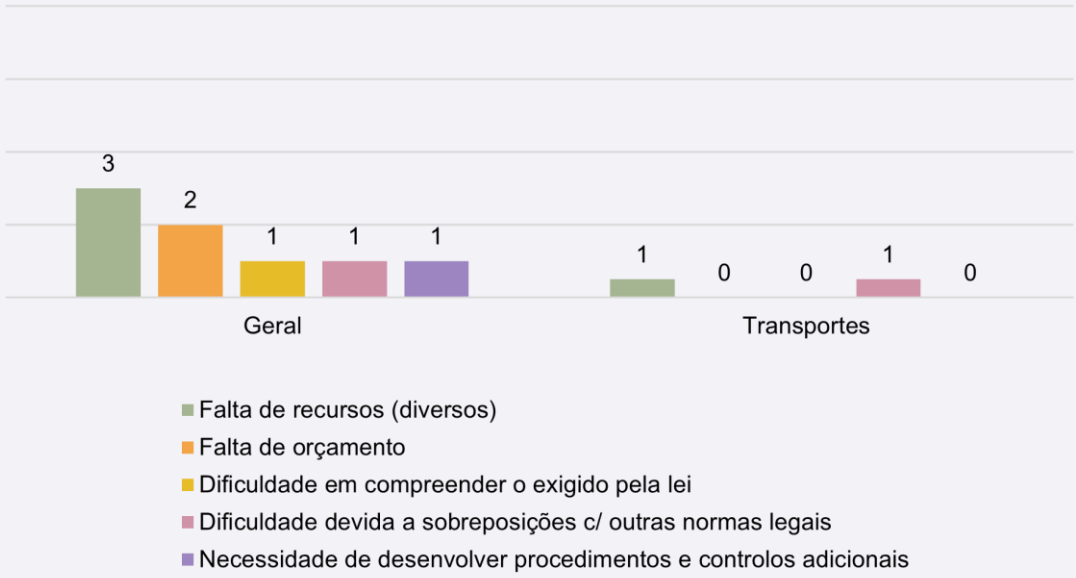
2. Impacto da publicação da Diretiva NIS ou da transposição da mesma (publicação da Lei n. º46/2018)

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. 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



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.

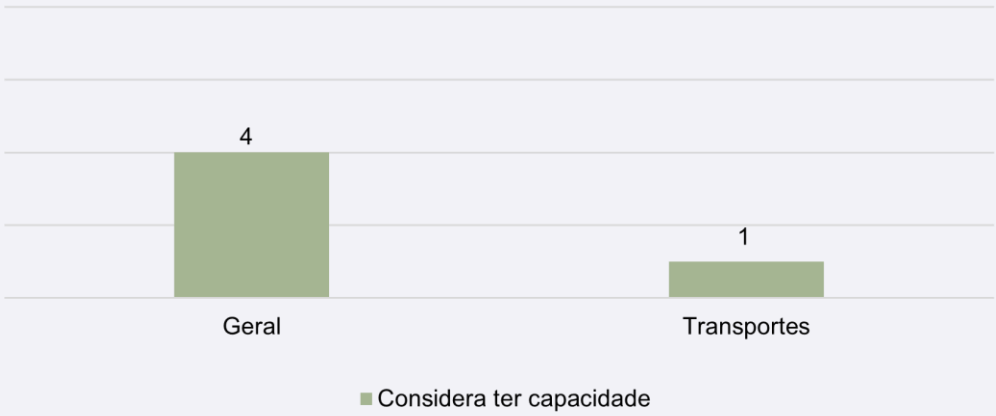
A falta de orçamento a conformidade com regime jurídico é outra das dificuldades sentidas. Soma-se ainda, a dificuldade em compreender o que era exigido pela nova legislação. Dificuldades relativas à sobreposição com outras normas legais foram indicadas apenas por um dos reguladores do setor dos transportes. Foi mencionada ainda a necessidade de desenvolver procedimentos e controlos adicionais.

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 mesma[7].

[7] 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.

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

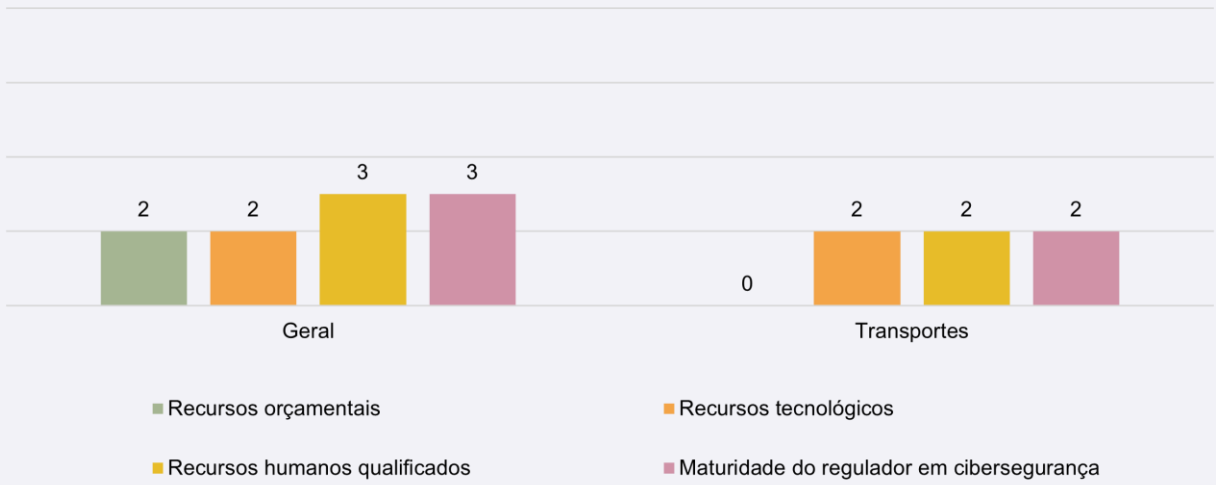
Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSE em matéria de cibersegurança, em caso de atribuição da competência



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).

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.

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.

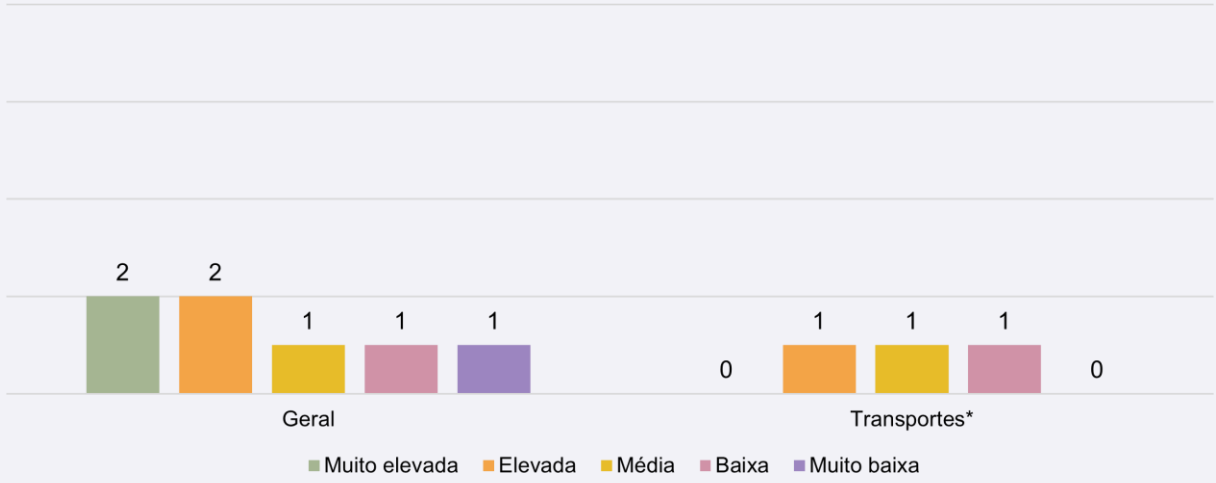
No setor dos transportes, os dois reguladores que consideram não ter capacidade para realizar a supervisão dos operadores em matéria de cibersegurança indicaram não ter suficientes recursos tecnológicos, recursos humanos e suficiente maturidade em cibersegurança.

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 cibersegurança[8], 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**.

[8] Banco Mundial, “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024, 4, https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

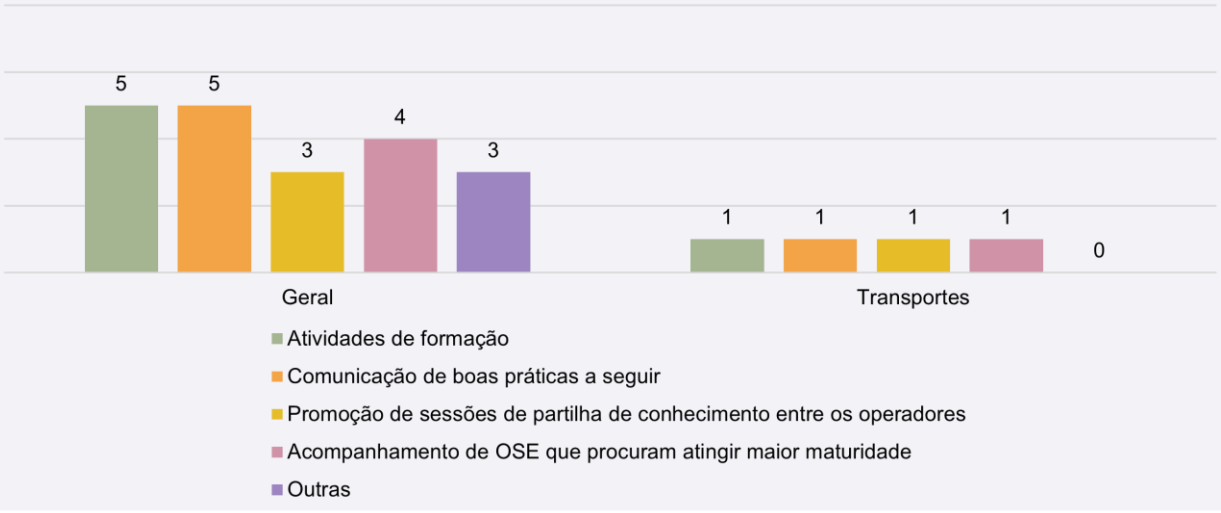
4. Maturidade em cibersegurança no setor

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



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. 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.

Gráfico 10 - 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, sendo um deles um dos inquiridos do setor dos transportes, 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.

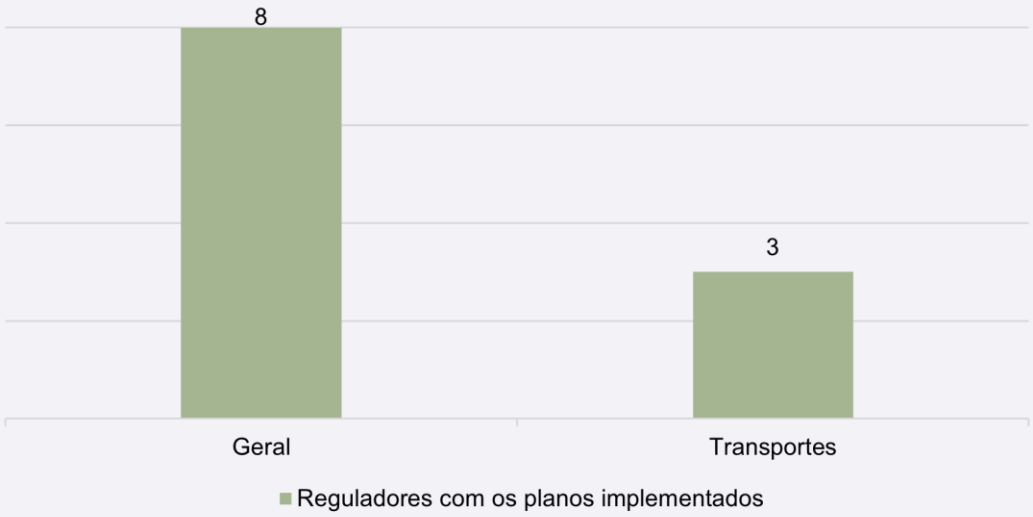
Relativamente à promoção de sessões de partilha de conhecimento, apenas três reguladores indicaram fazê-lo (novamente incluído um regulador do setor dos transportes). Quanto ao acompanhamento de OSE que procurem atingir maior maturidade em cibersegurança, quatro entidades referiram fazer esse acompanhamento, sendo uma delas das entidades reguladoras do setor dos transportes.

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

Apenas duas das entidades reguladoras inquiridas consideram ter suficientes profissionais capacitados em matéria de cibersegurança, enquanto os restantes seis (incluindo os três reguladores do setor dos transportes) 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**.

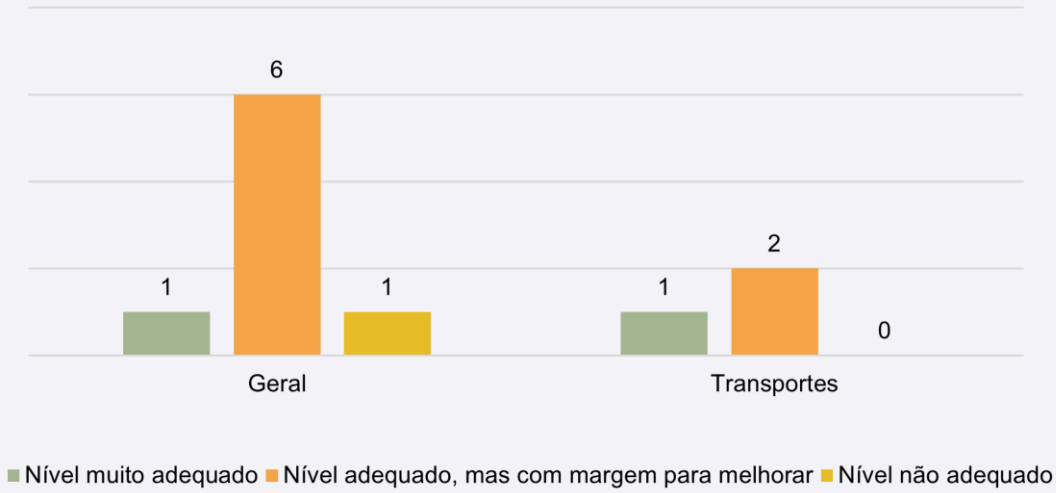
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados



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 considera que a Diretiva não leva os operadores a estabelecerem um nível adequado de cibersegurança face aos atuais perigos, desafios e ameaças.

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.

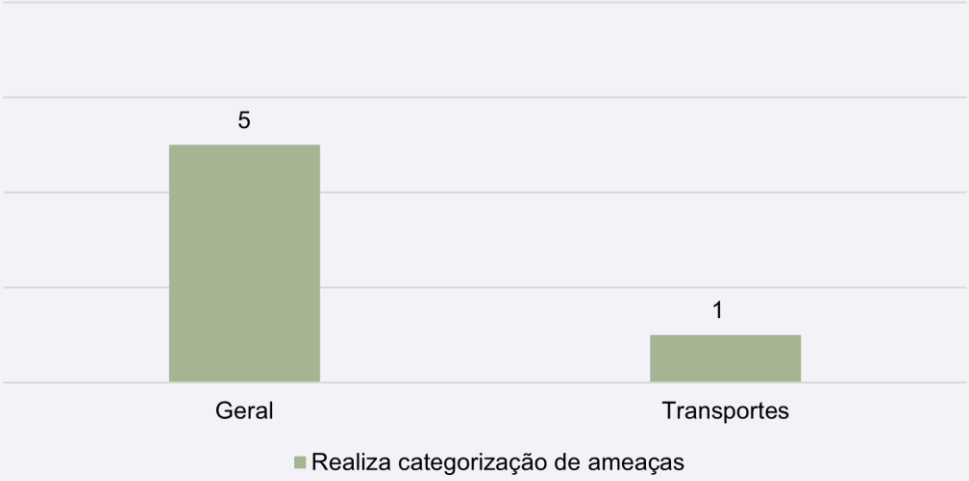
Uma questão semelhante foi colocada, em 2021, não aos reguladores, mas a diversos OSE na União Europeia, no âmbito do relatório *NIS Investments* 2021. As respostas recolhidas indicam que quase 50% (48,9%) dos operadores de serviços essenciais consideram que a Diretiva NIS teve um impacto positivo nas suas organizações e na União, aumentado o nível de cibersegurança das organizações, ao fortalecer as suas capacidades de deteção e de recuperação de incidentes[9].

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.

[9] ENISA, "NIS Investments", novembro de 2021, 5, https://www.enisa.europa.eu/publications/nis-investments-2021.

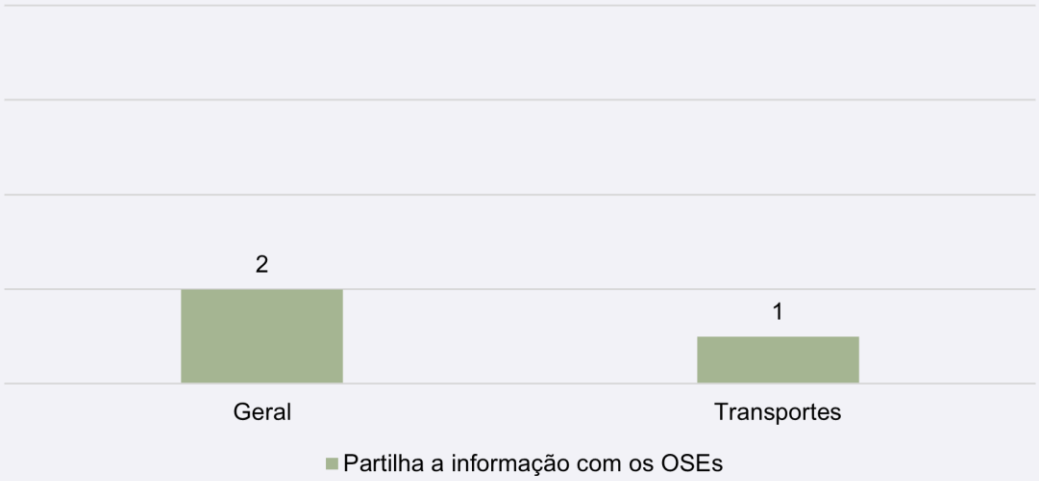
6. Categorização de ameaças

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



Cinco dos oito reguladores inquiridos, sendo um deles um dos três reguladores no setor dos transportes, realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores.

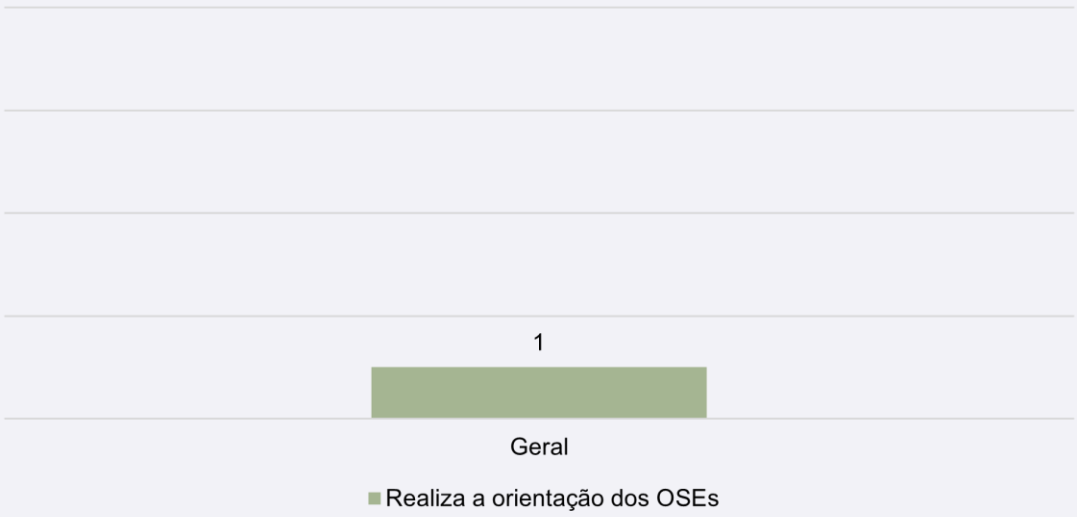
Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização



Dos cinco reguladores que realizam categorização de ameaças, apenas dois partilham informação relativa às ameaças com os OSE, sendo um destes, o regulador do setor dos transportes. Os restantes setores não efetuam a partilha de informação.

7. Orientação dos OSE por parte da entidade reguladora

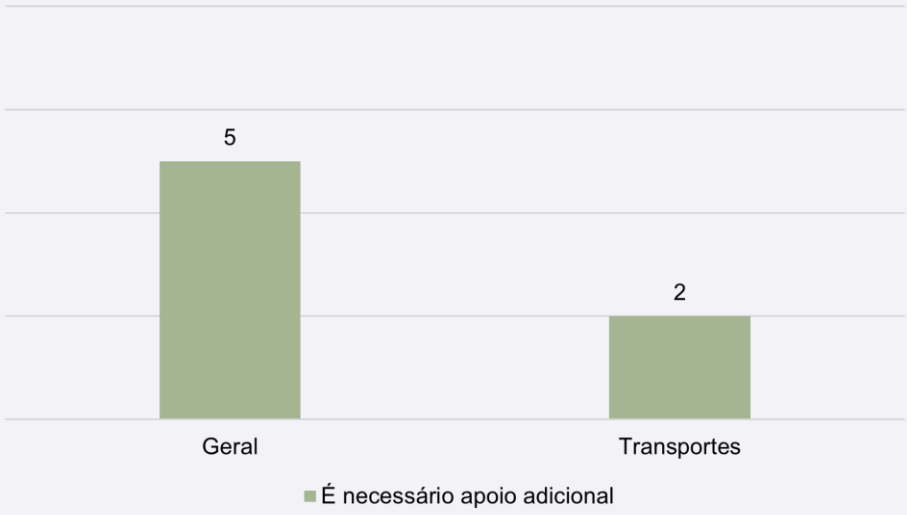
Gráfico 16 - Reguladores que orientam os OSE na digitalização de processos e na promoção de uma cultura digital



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



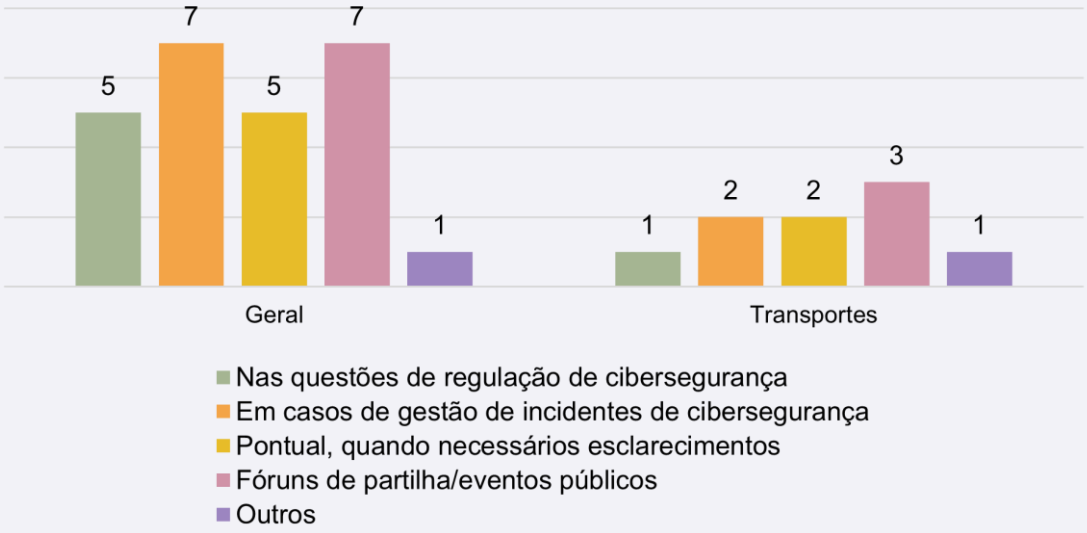
Entre os reguladores inquiridos, cinco (dois dos reguladores do setor dos transportes) têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional.

Gráfico 18 - 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, co-criação, 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.

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.

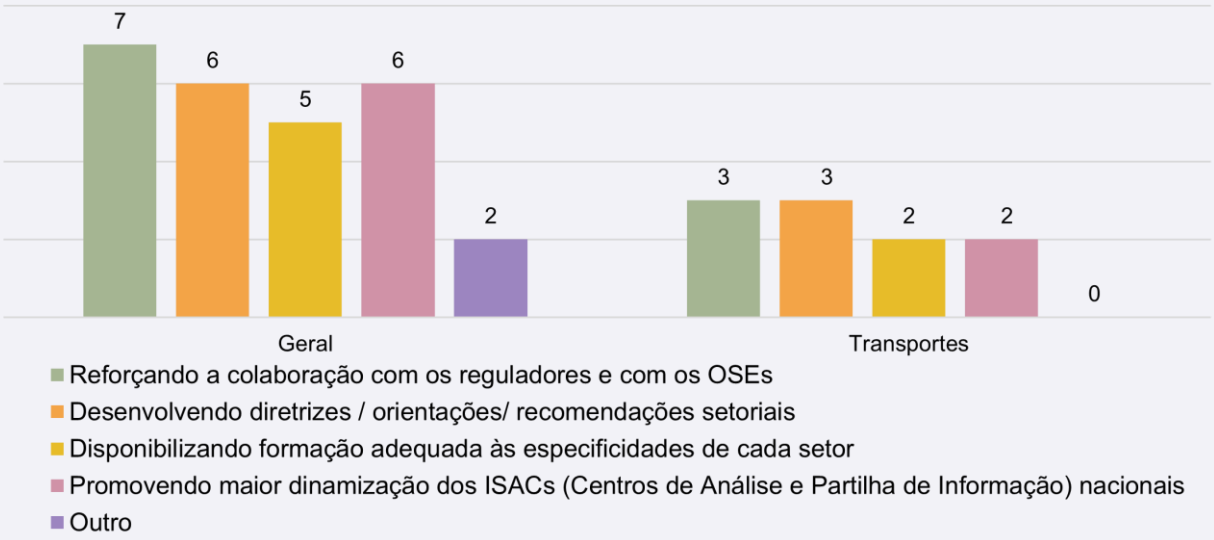
Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS



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.

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



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.

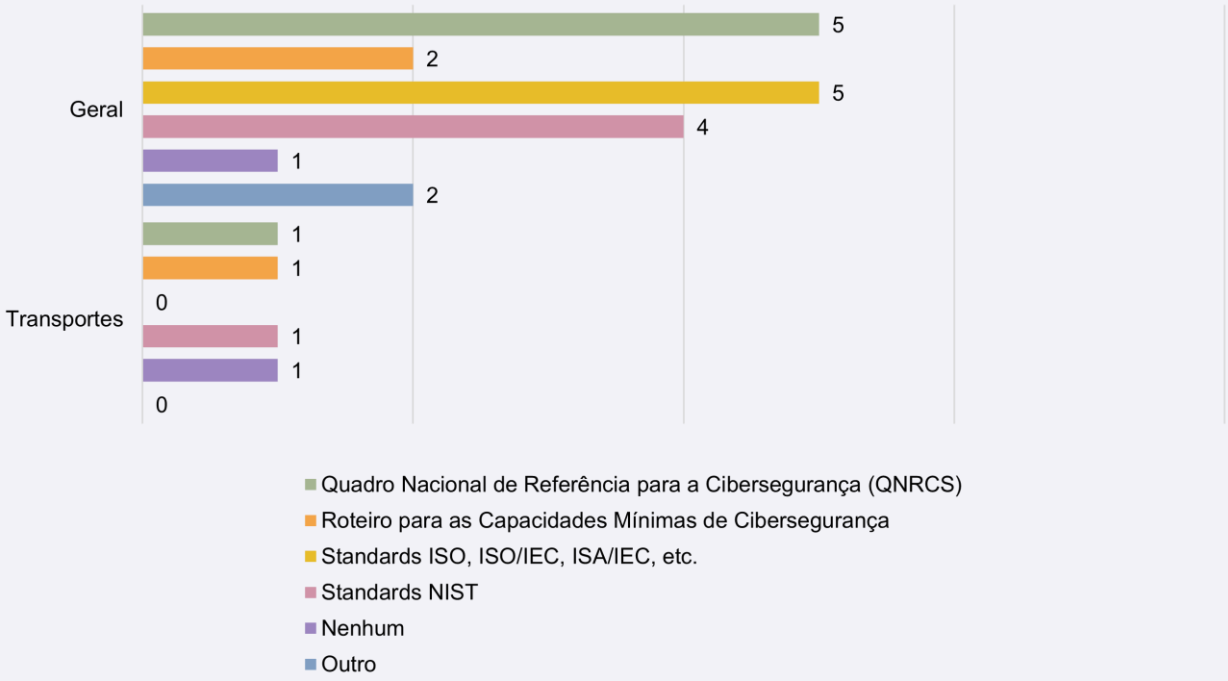
No setor dos transportes, os três reguladores inquiridos indicam que gostariam de ver o reforço da colaboração do CNCS com os reguladores e operadores, bem como o desenvolvimento de diretrizes, orientações ou recomendações setoriais. Dois dos três reguladores inquiridos referiram ainda que o CNCS poderia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

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”[10].

[10] CNCS, “Compromisso C-Academy”, https://www.cncs.gov.pt/pt/c-academy-compromisso/.

9. *Standards* e boas práticas recomendadas

Gráfico 21 - 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.

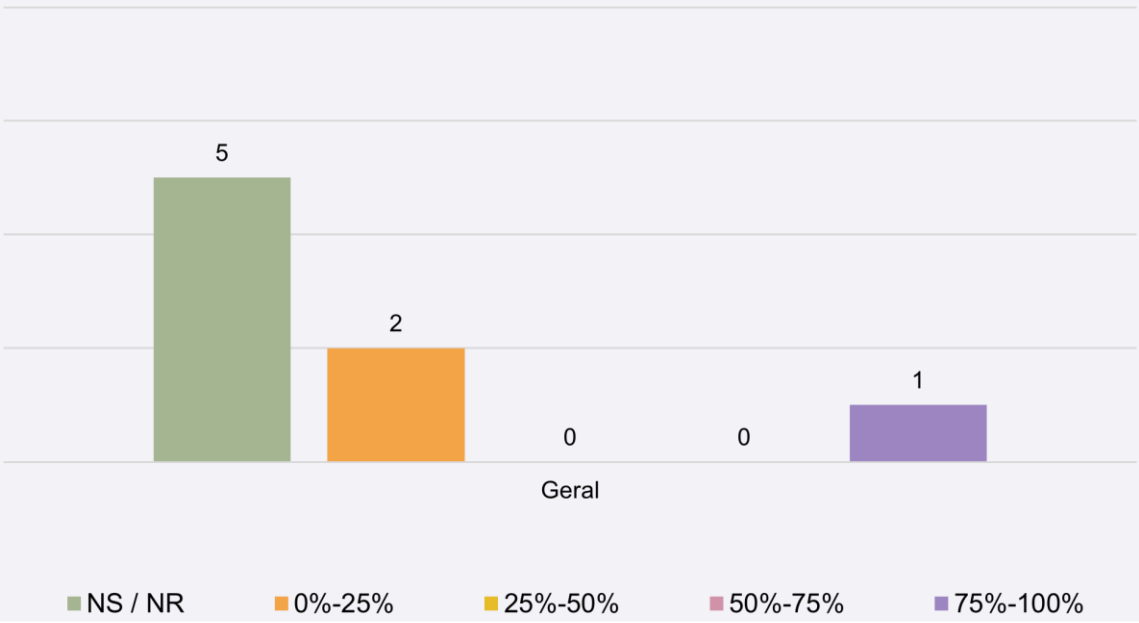
Na opção "outros", foram referidos *standards* da International Civil Aviation Organization (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain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

No setor 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.

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%[11].

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.

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.

[11] Departamento de Ciência, Tecnologia e Inovação do Governo do Reino Unido, "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

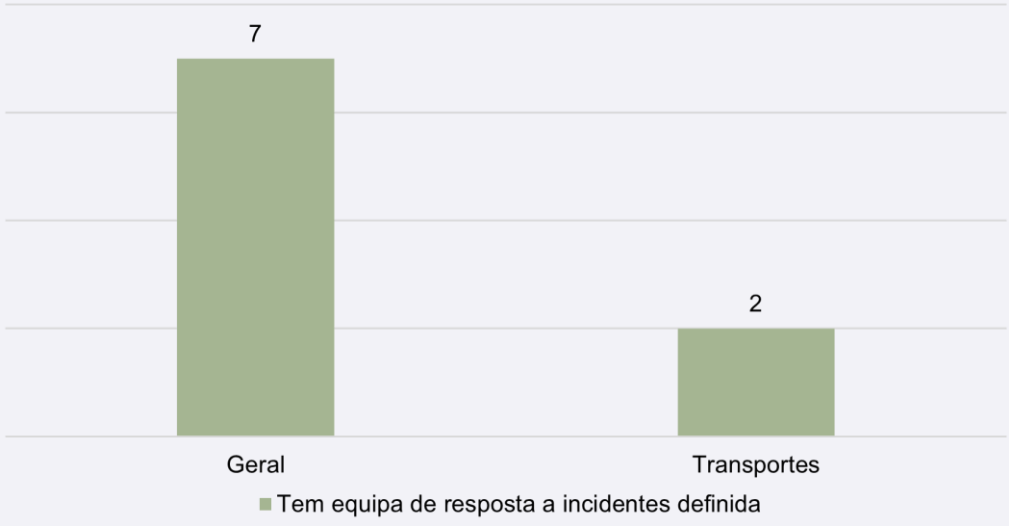
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança

Setores	Normativos
Energia	*Network Code on Cybersecurity (publicação pendente)*
Transporte	*Transport Cybersecurity Toolkit* (CE); 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 *(Digital Operation Resilience Act - DORA)*
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

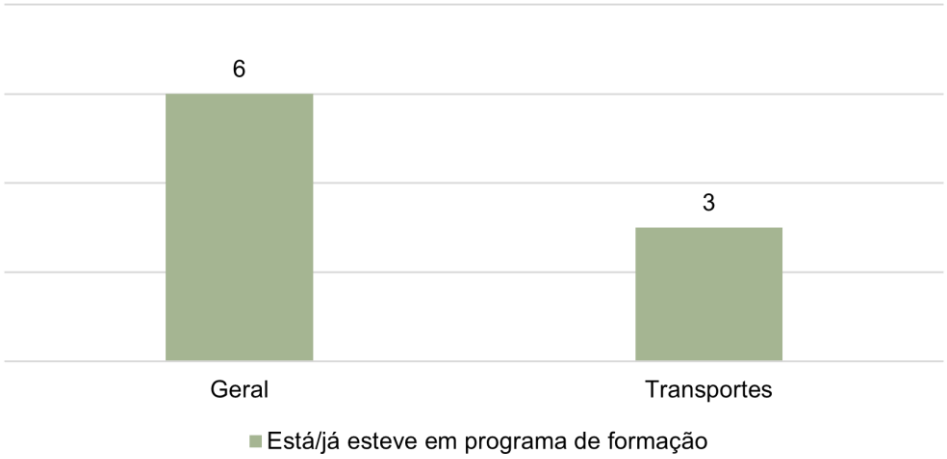
Gráfico 23 - Reguladores com equipa de resposta a incidentes definida



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.

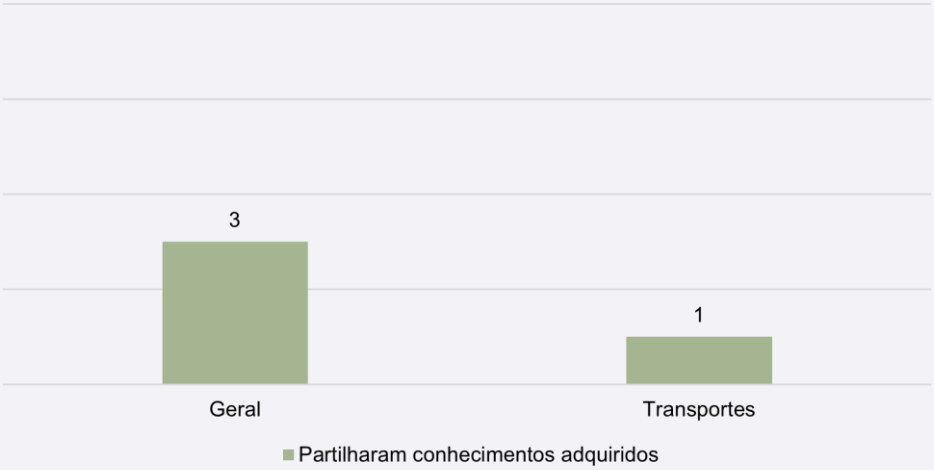
11. Sensibilização e consciencialização

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, nunca participaram em tais programas. No setor dos transportes, os três reguladores inquiridos indicaram estarem ou já terem estado em programas de formação e sensibilização sobre as matérias referidas.

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

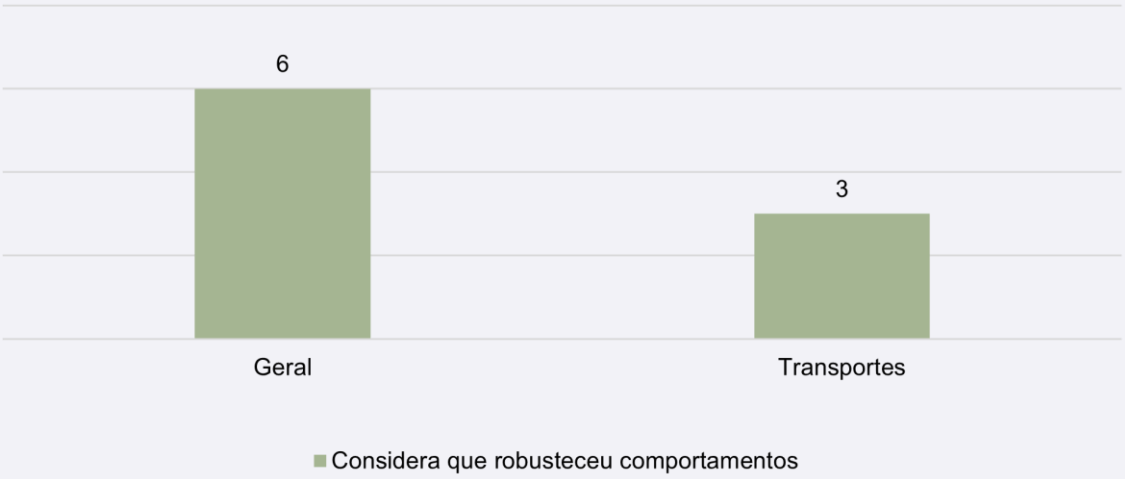


No seguimento da participação nos programas de formação e sensibilização para os riscos no ciberespaço, questionou-se se os conhecimentos adquiridos nesses programas foram partilhados com os OSE do setor. Os setores que fizeram essa partilha e os que não fizeram dividem-se igualmente.

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.

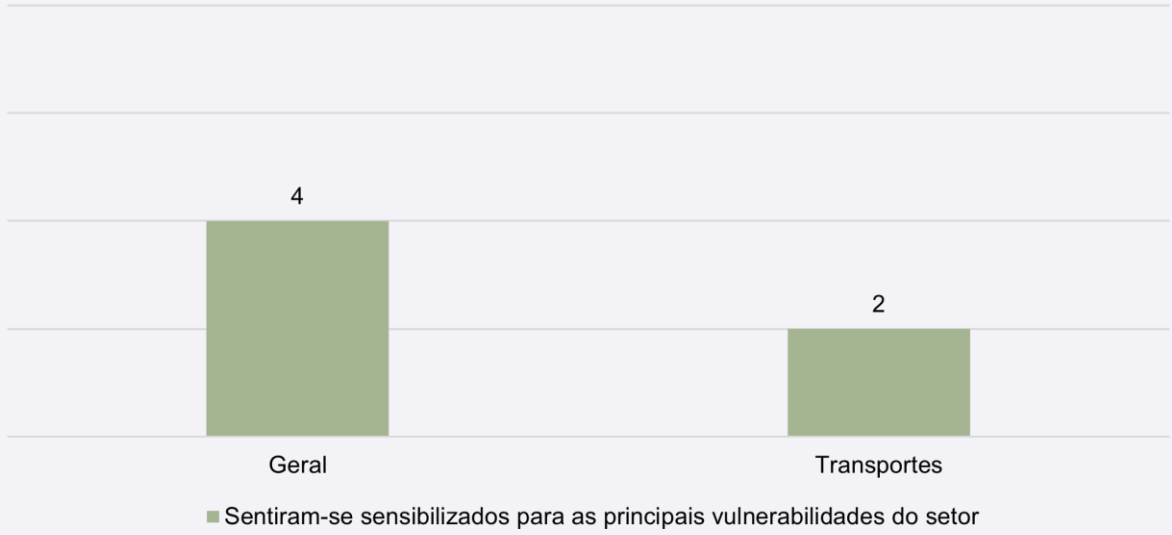
Relativamente ao setor dos transportes, apenas um dos três reguladores referiu ter partilhado os conhecimentos adquiridos na formação com os operadores, enquanto os outros dois reguladores não indicam ter feito essa partilha.

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.

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. Nos transportes, dois dos três

reguladores inquiridos consideram que a entidade formadora os sensibilizou para essas vulnerabilidades. O terceiro regulador discorda sobre ter sido sensibilizado acerca das mesmas.

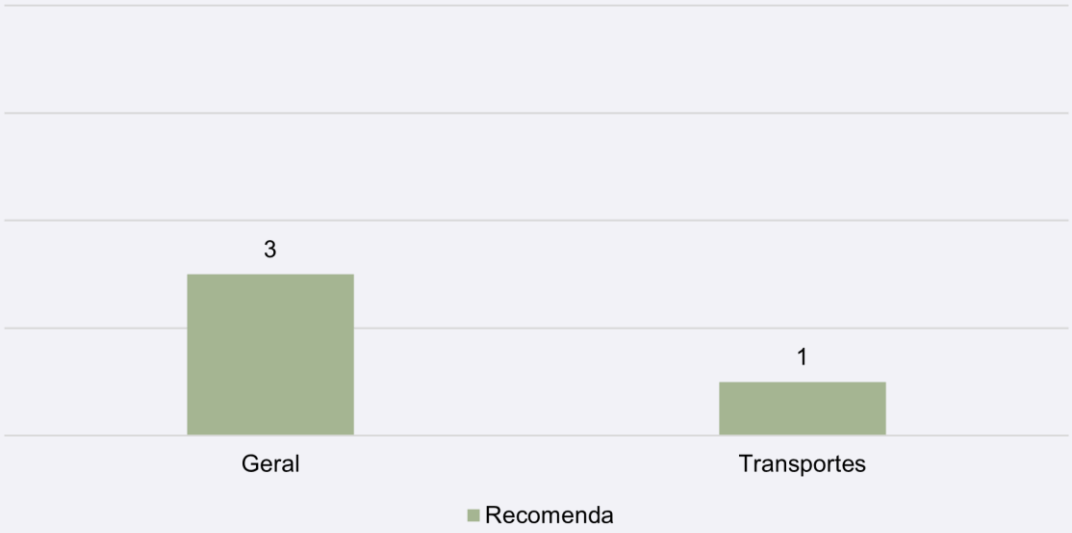
12. Cooperação nacional/internacional de proteção do ciberespaço

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.

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.

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 cincos indicaram não pertencer a qualquer estrutura do tipo.

Setorialmente, nos 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.

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

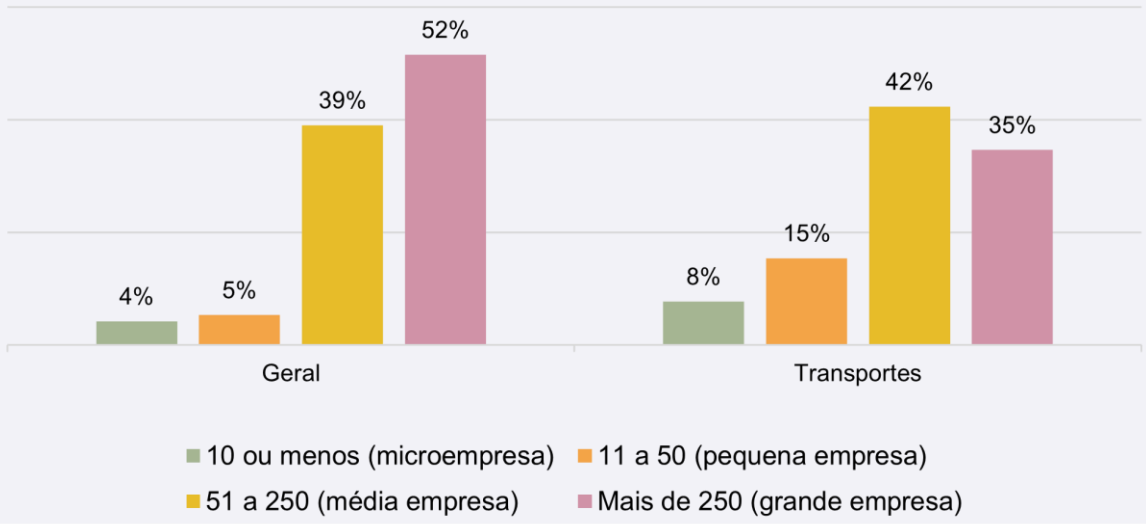
Setores	Estimativa
Energia	32
Transportes	> 19 000
Bancário	120
Infraestruturas do Mercado Financeiro	> 1 000
Distribuição de Água Potável	350
Infraestruturas Digitais	100

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

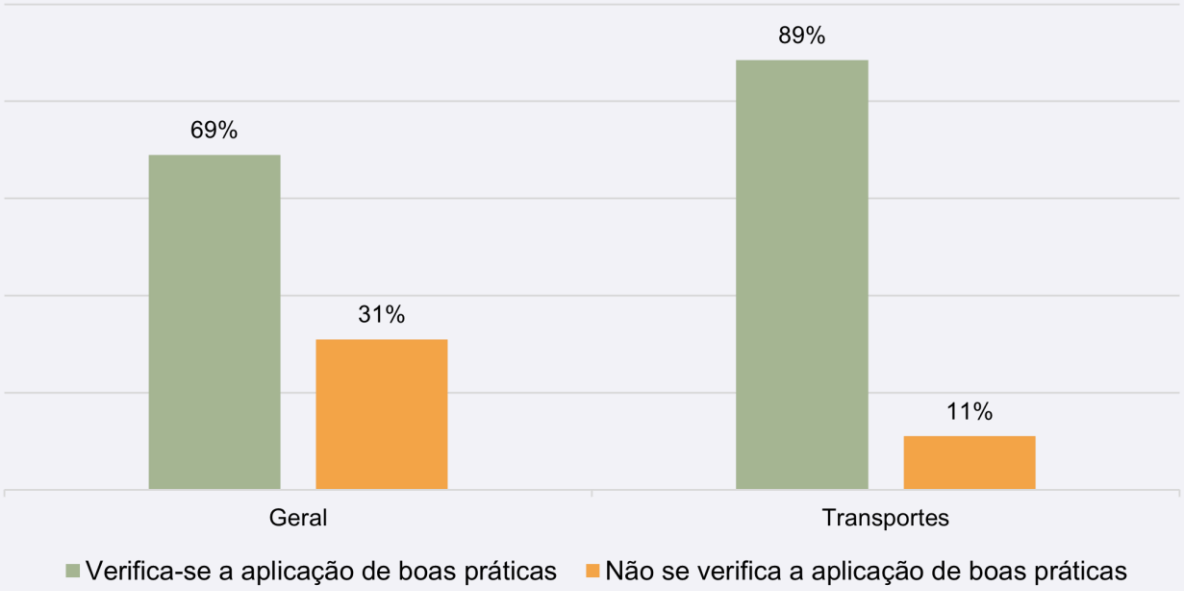
Gráfico 30 - Número de colaboradores na organização



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). No setor dos transportes, são mais comuns as médias 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 empresas[12].

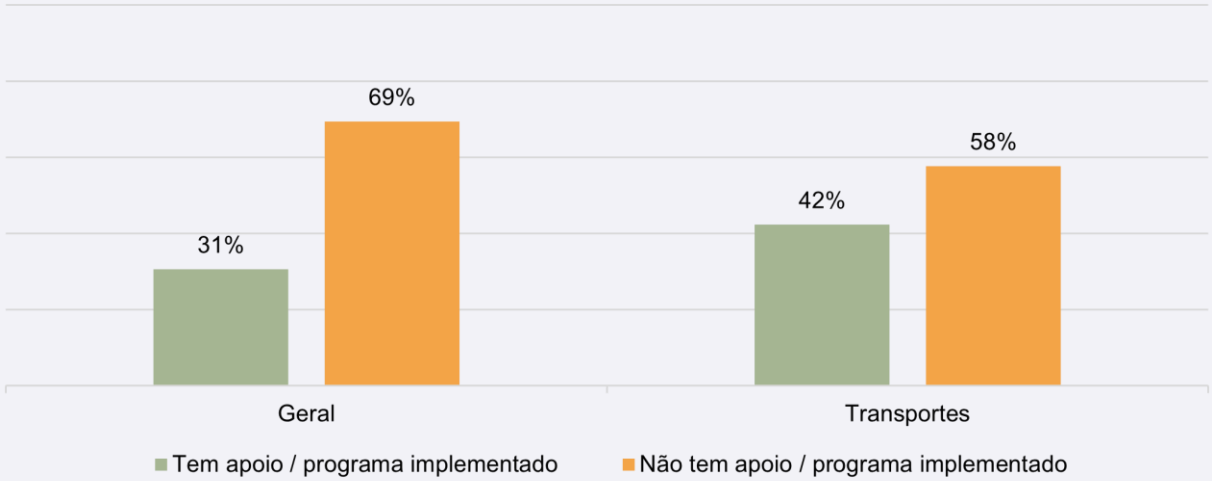
Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores



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.
O setor dos transportes destaca-se por ser um dos setores nos quais mais de 80% dos operadores consideram que boas práticas de cibersegurança são aplicadas pelos seus colaboradores.

[12] 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

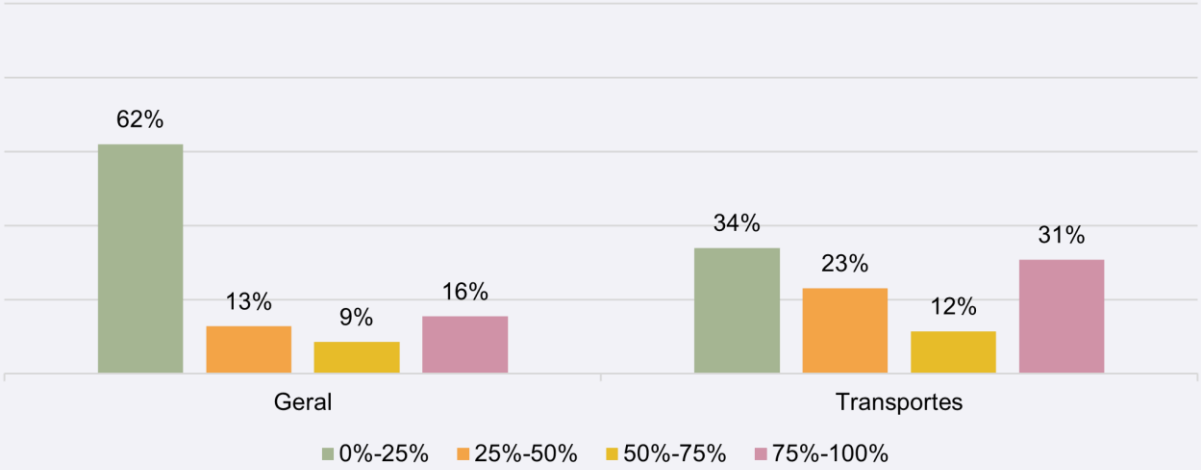


À data de realização do questionário, apenas um terço dos operadores tinham apoios ou programas próprios ou do Estado para colaboradores interessados em formação na área de cibersegurança.

No setor dos transportes predominam os OSE sem programas de apoio implementados, nomeadamente 58%.

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**.

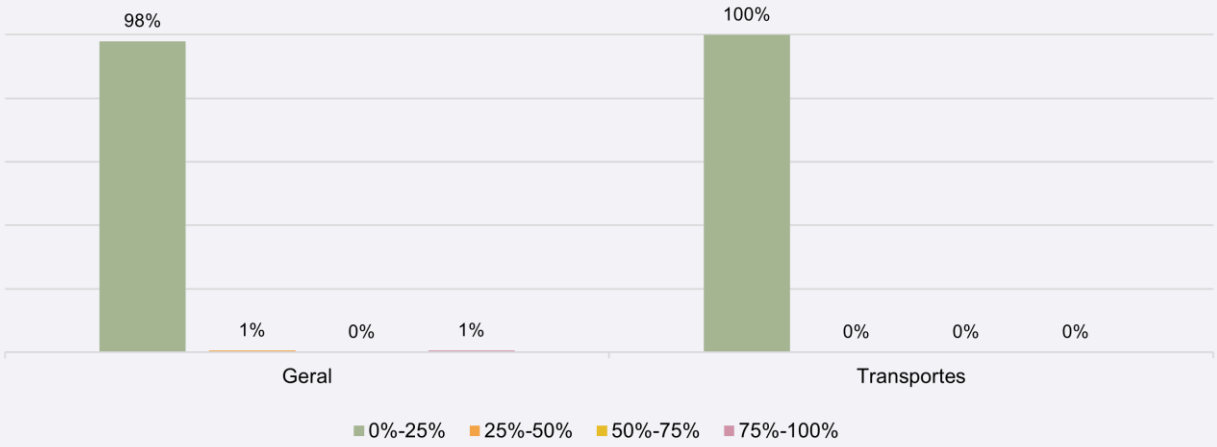
Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



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

No setor 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%.

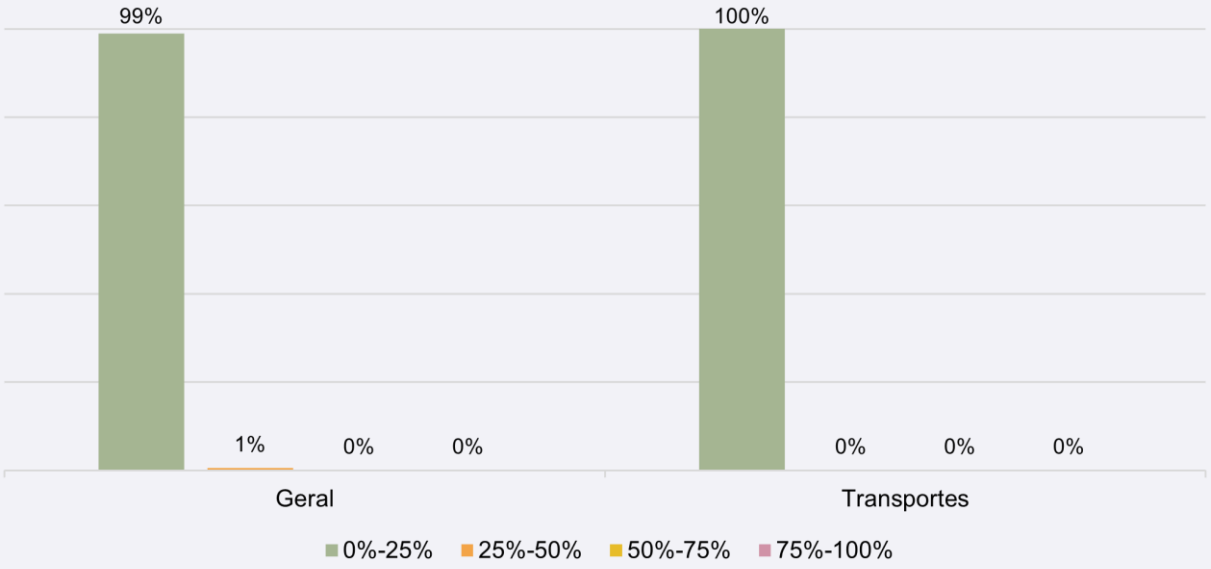
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



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. A totalidade dos operadores do setor dos transportes não ultrapassa os 25% com formação superior.

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

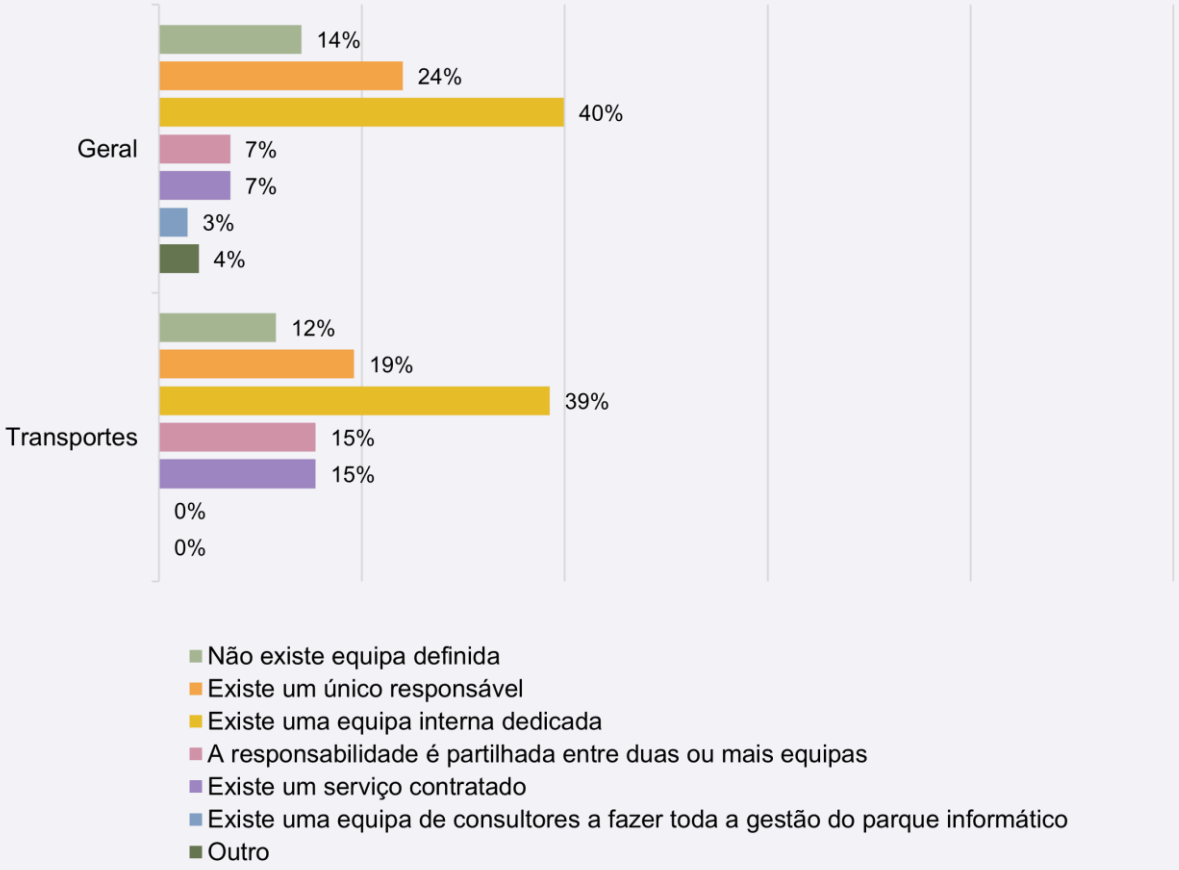


A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. Setorialmente, nos transportes, o resultado é idêntico ao anterior. Novamente, o resultado geral é um resultado expectável, uma vez que não se espera que colaboradores de outras áreas sejam 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 colaboradores[13].

[13] 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

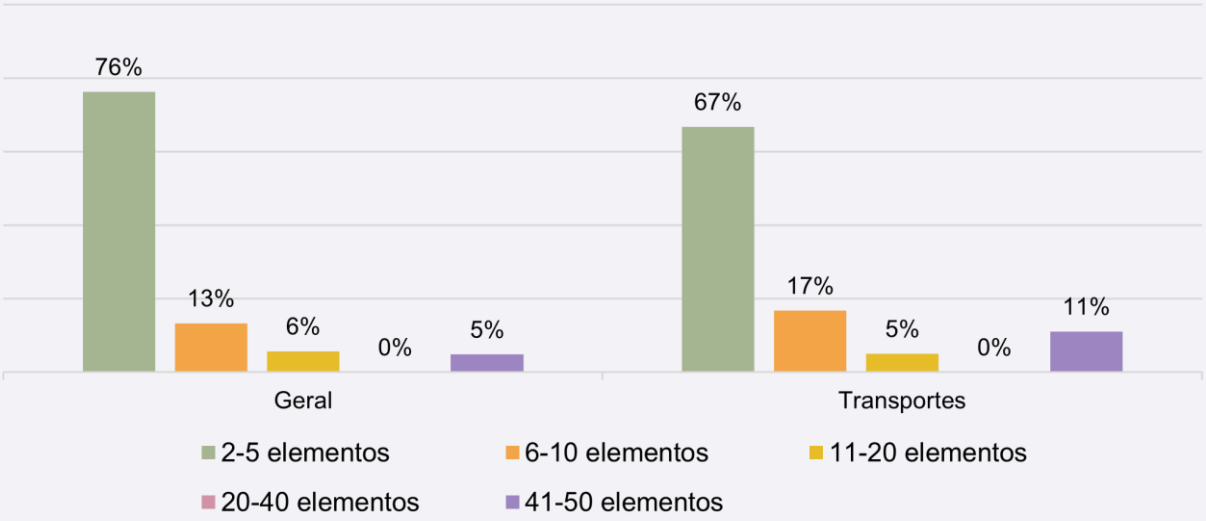


De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (25% dos casos).

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.

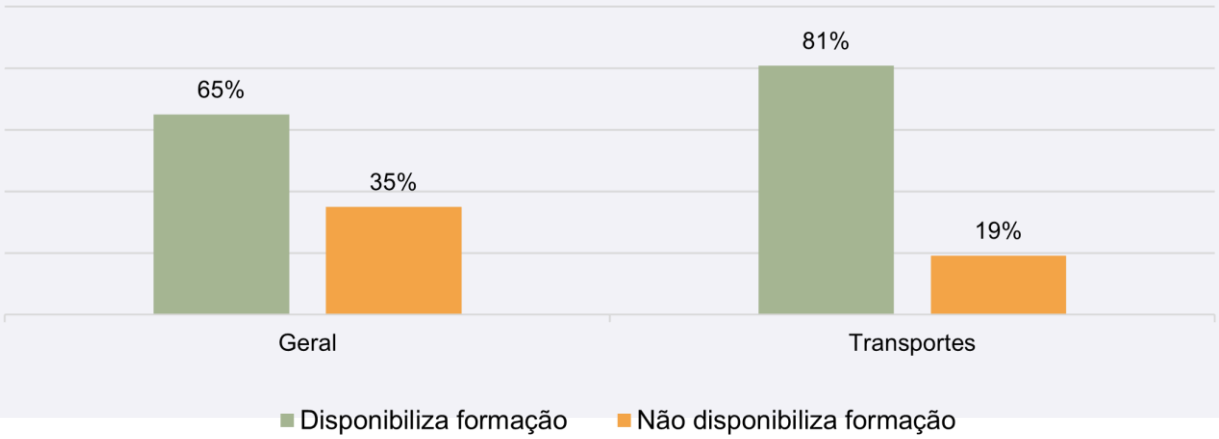
No setor dos transportes, prevalece a presença de uma equipa interna dedicada, com pelo menos 36% dos OSE a optarem por esta solução.

Gráfico 37 - 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.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

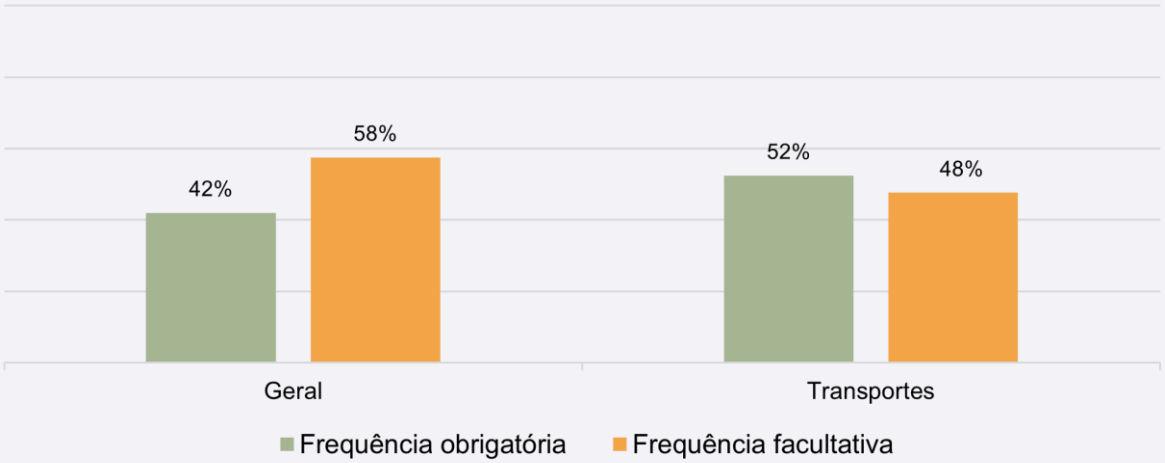


Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. No setor dos transportes apenas 19% dos operadores não disponibiliza formação.

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 2021[14]. 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.

[14] Instituto Nacional de Estatística, "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

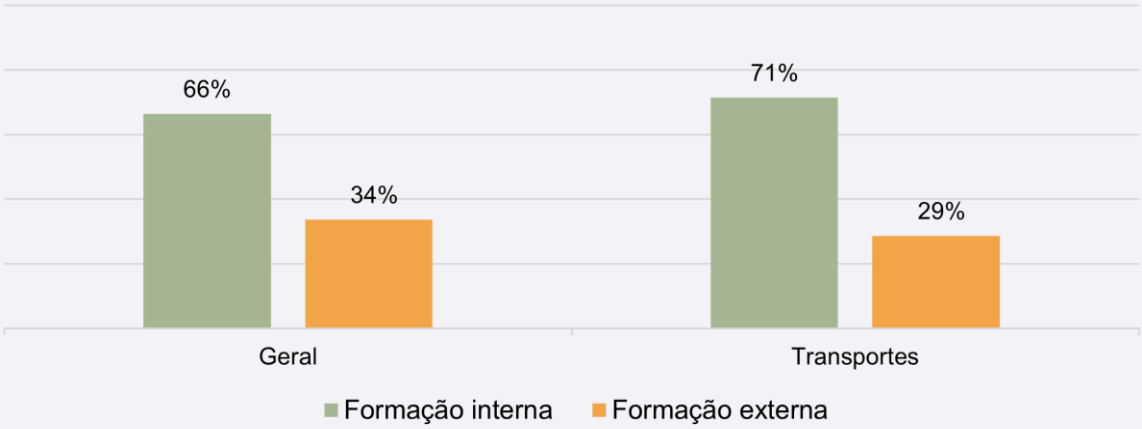


De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais esta tendência não se verifica. Por exemplo, no dos transportes, são mais os OSE nos quais a formação tem caráter obrigatório em vez de facultativo, mas com uma diferença pouco significativa.

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 inquérito[15].

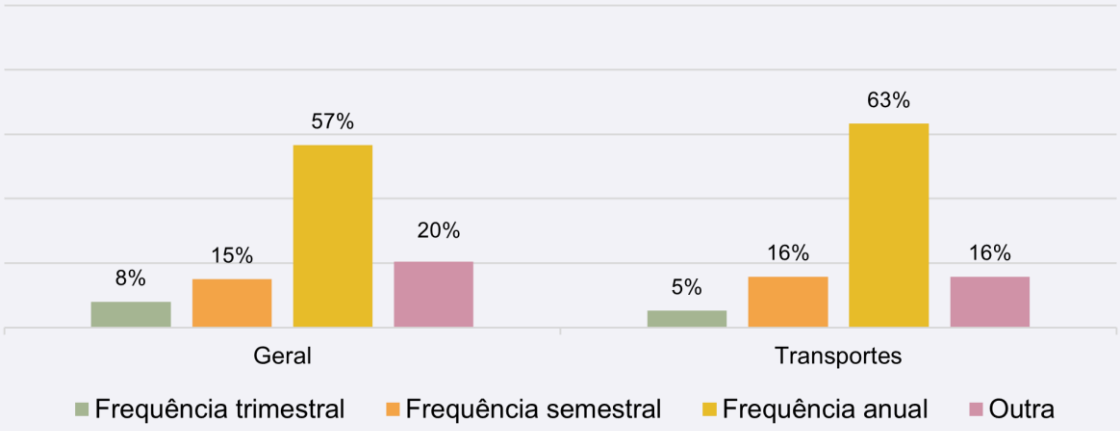
[15] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19.

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



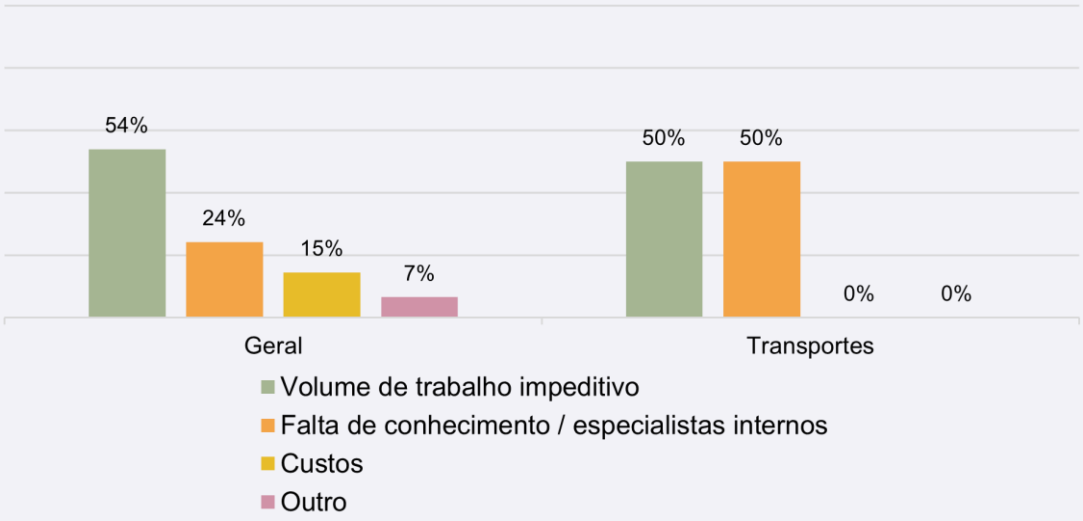
Neste gráfico, fica evidenciado o maior recurso à formação interna do que externa entre os OSE. A maioria dos inquiridos (66%) recorre aos meios internos para fins de formação aos colaboradores. Setorialmente, nos operadores do setor dos transportes, 29% recorre a formação externa.
Contudo, cerca de um terço dos OSE (34%) recorre a entidades externas para formar os seus colaboradores.

Gráfico 41 - 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. O setor dos transportes segue a tendência geral das formações, sendo maioritariamente anuais.
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*.

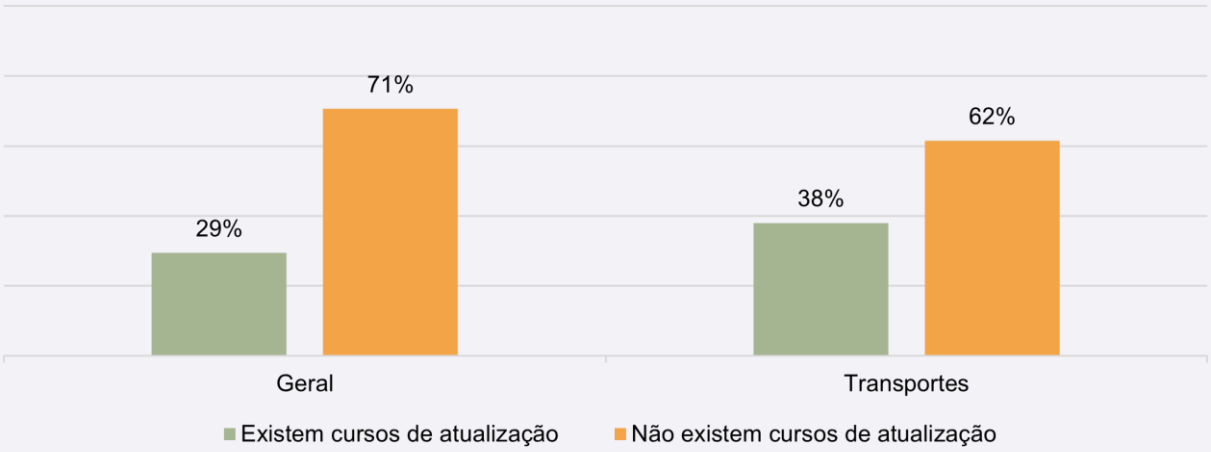
Gráfico 42 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam



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 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.

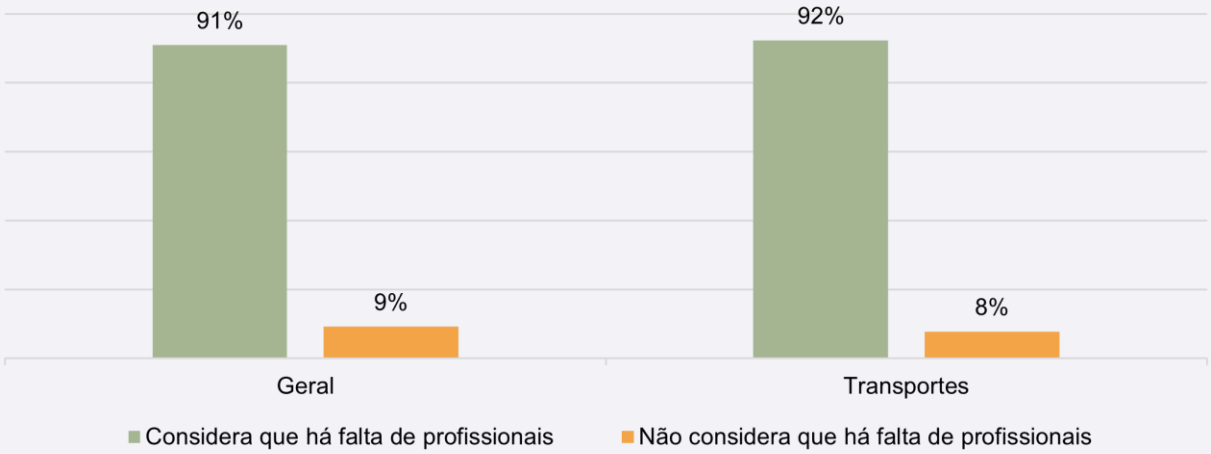
Os “outros” motivos mencionados passam, segundo os OSE, pela falta de planos de formação dentro das organizações e pela alocação de recursos financeiros a formação noutras áreas que não a cibersegurança.

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. No setor dos transportes, embora os valores de OSE superem a generalide, apenas 38% dispõe de cursos de atualização.

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, no setor dos transportes, 92% considera que há falta de profissionais, seguindo assim a generalidade.

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 profissionais[16] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[17]. 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 encontrados[18]. 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[19] [20].

[16] Banco Mundial, “Strategic Cybersecurity Talent Framework”, 5.

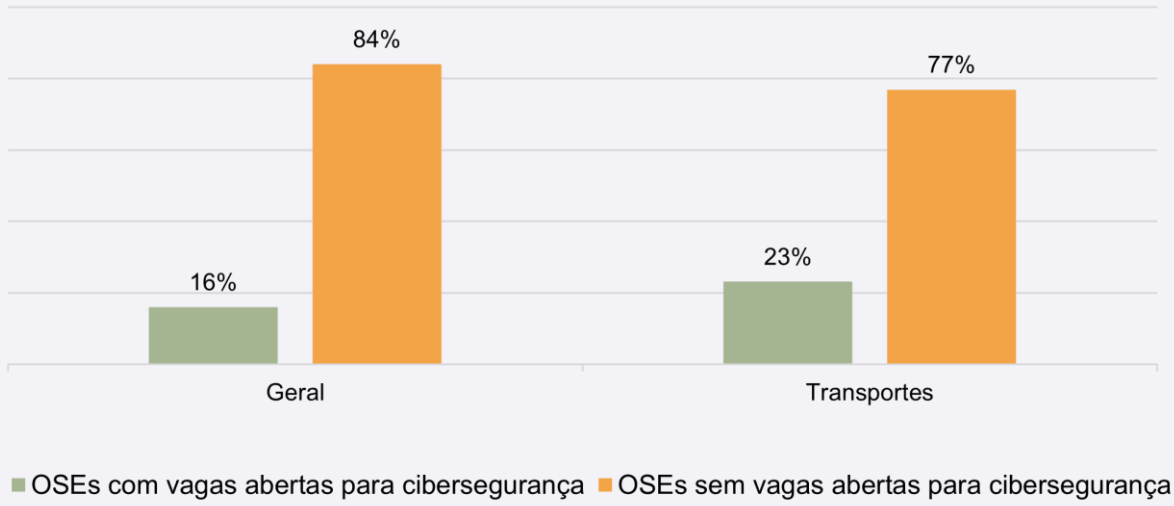
[17] ENISA, “Cybersecurity Skills Conference: Strengthening human capital in the EU”, https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.

[18] ENISA, “NIS Investments”, 2022, 16, https://www.enisa.europa.eu/publications/nis-investments-2022.

[19] ENISA, “NIS Investments”, 2022, 16-17.

[20] Banco Mundial, “Strategic Cybersecurity Talent Framework”, 22-25.

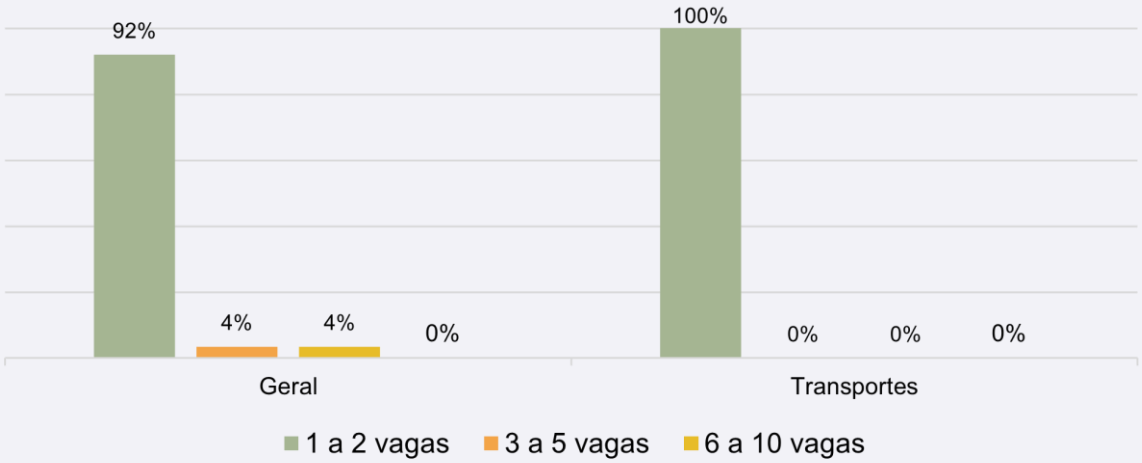
Gráfico 45 - Vagas abertas para a área de cibersegurança



À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. Apenas 23% dos OSE do setor dos transportes dispunham de vagas abertas para cibersegurança.

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 TIC[21].

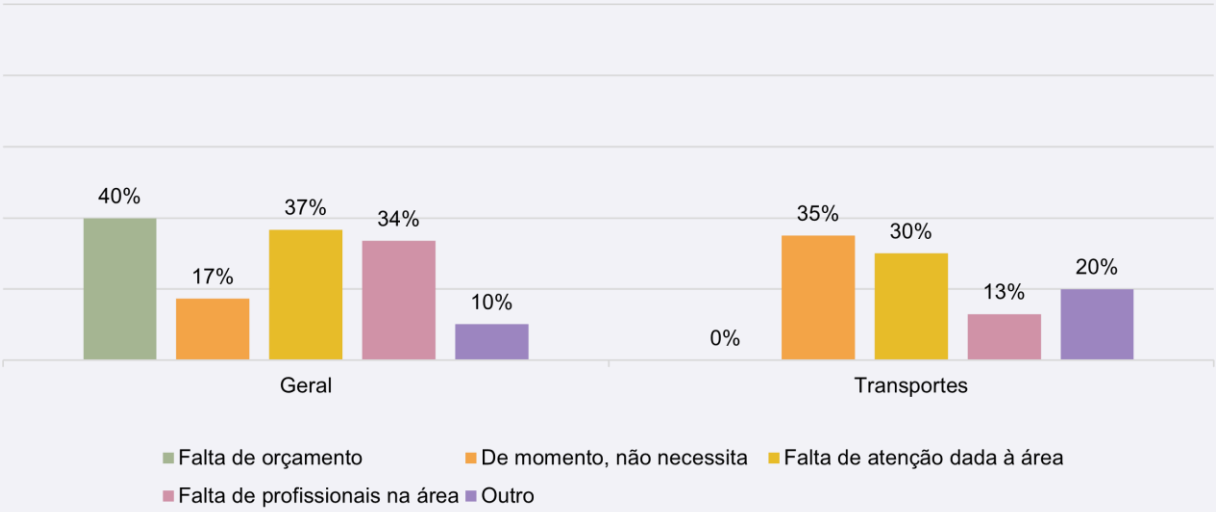
Gráfico 46 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança



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 no setor dos transportes.

[21] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 15.

Gráfico 47 - 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 elevadas[22].

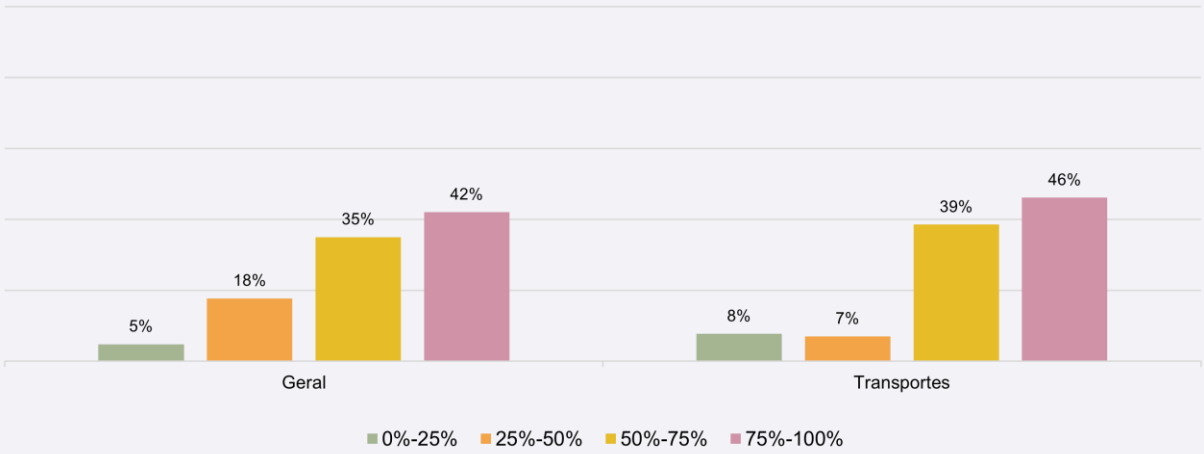
Voltando aos dados obtidos através do questionário realizado, a "falta de atenção dada à área" indicada por 37% dos OSE sem vagas em aberto é um dos aspetos mais preocupantes que surgem na análise. Um dos Objetivos Estratégicos (Objetivo 3) da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 passa por gerar e "garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço"[23], 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

[22] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 15-17.

[23] CNCS, "Estratégia Nacional de Segurança do Ciberespaço 2019-2023", 11, https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf.

informação e que esta assegure a alocação dos recursos necessários para cumprir esse desígnio[24].

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



Predomina entre os OSE o intervalo 75%-100% de colaboradores com acesso a equipamentos digitais (indicado por 42% dos OSE), sendo visível que há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos.

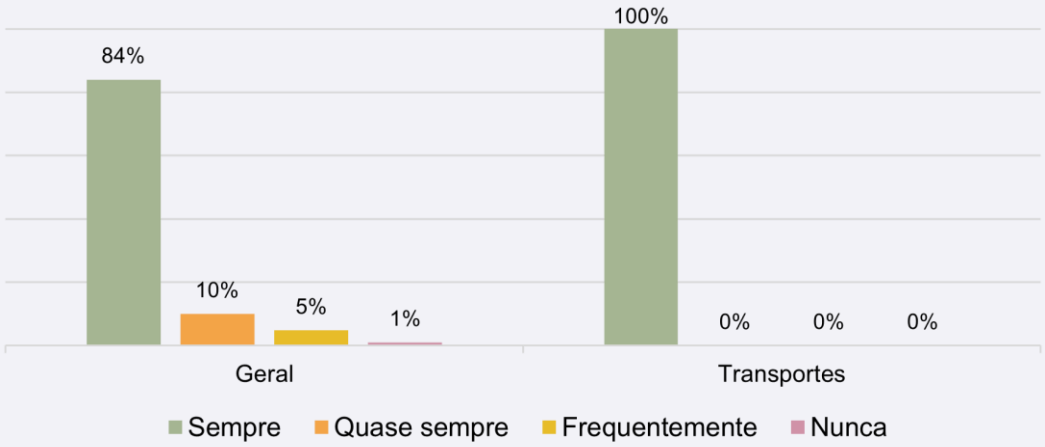
No setor dos transportes é acompanhada a tendência geral de ter entre 75% a 100% dos colaboradores com acesso a equipamentos digitais.

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 empresa[25].

[24] International Organization for Standardization, "International Standard ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements", 2.

[25] Instituto Nacional de Estatística, "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

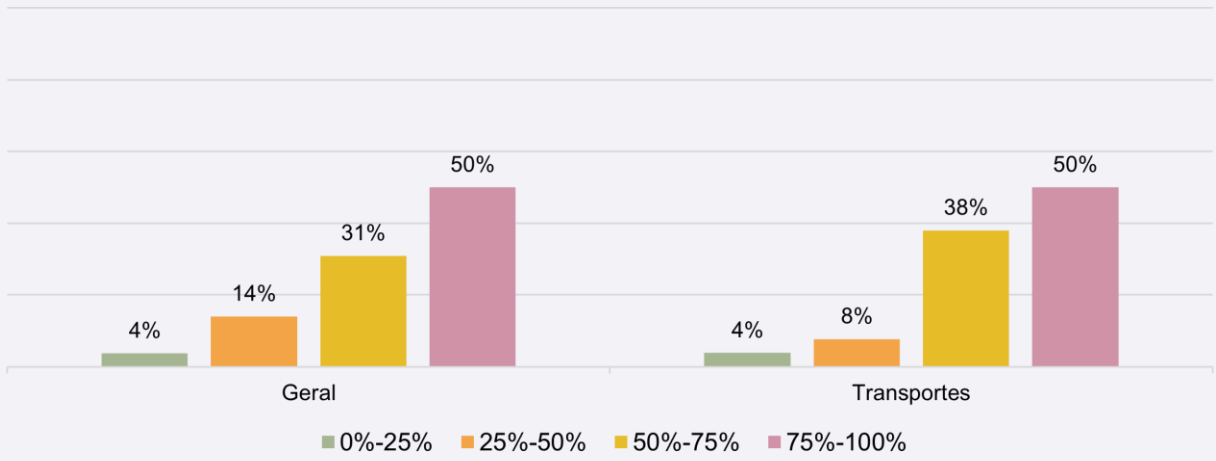


Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. Todos os operadores inquiridos no setor dos transportes indicaram ser os próprios a fornecer sempre os equipamentos necessários aos colaboradores.

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 serviço[26].

[26] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 4-5.

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

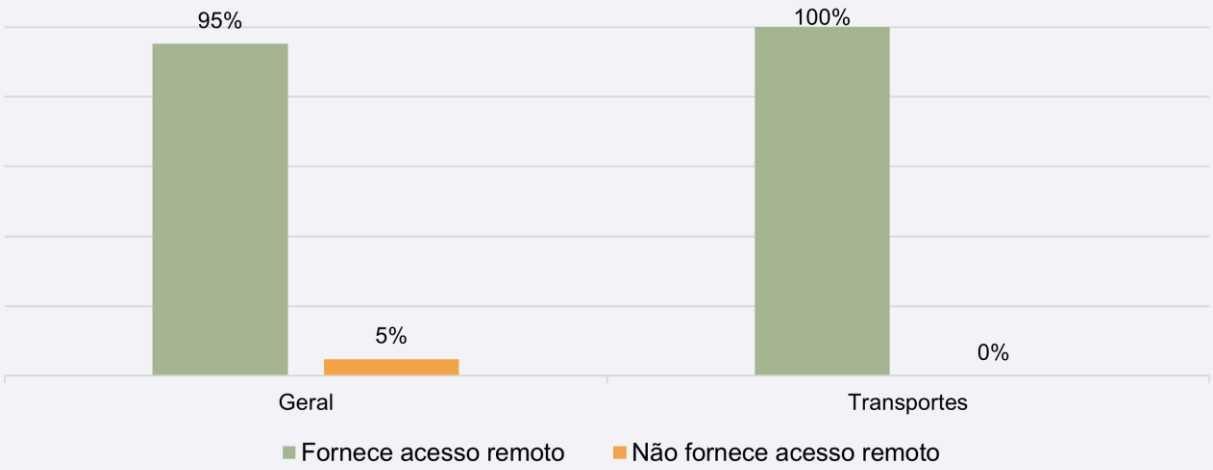


A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.
No setor dos transportes, verifica-se que faixa predominante continua a ser aquela em que 75%-100% dos colaboradores tem acesso à Internet no desempenho das suas funções, embora se registem operadores nos quais a percentagem de trabalhadores com acesso à Internet é menor.

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 setorialmente 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 trabalho[27].

[27] Instituto Nacional de Estatística, "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

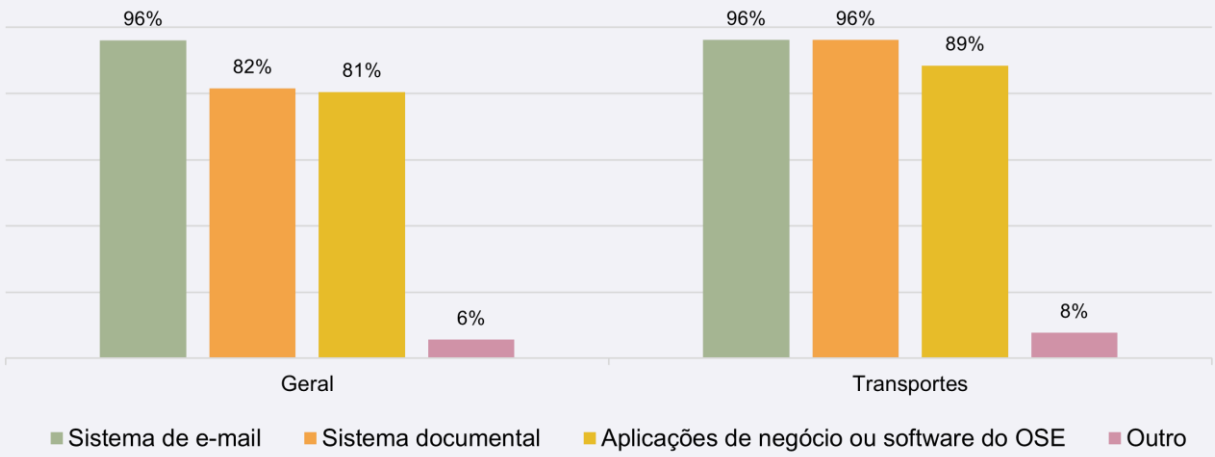


O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSE aos colaboradores é uma realidade em praticamente todos os OSE inquiridos (95%). No setor dos transportes, todos os OSE indicaram permitir o acesso remoto a esses sistemas por parte dos seus colaboradores.

Comparando mais uma vez 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-mail[28].

[28] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 6-7.

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

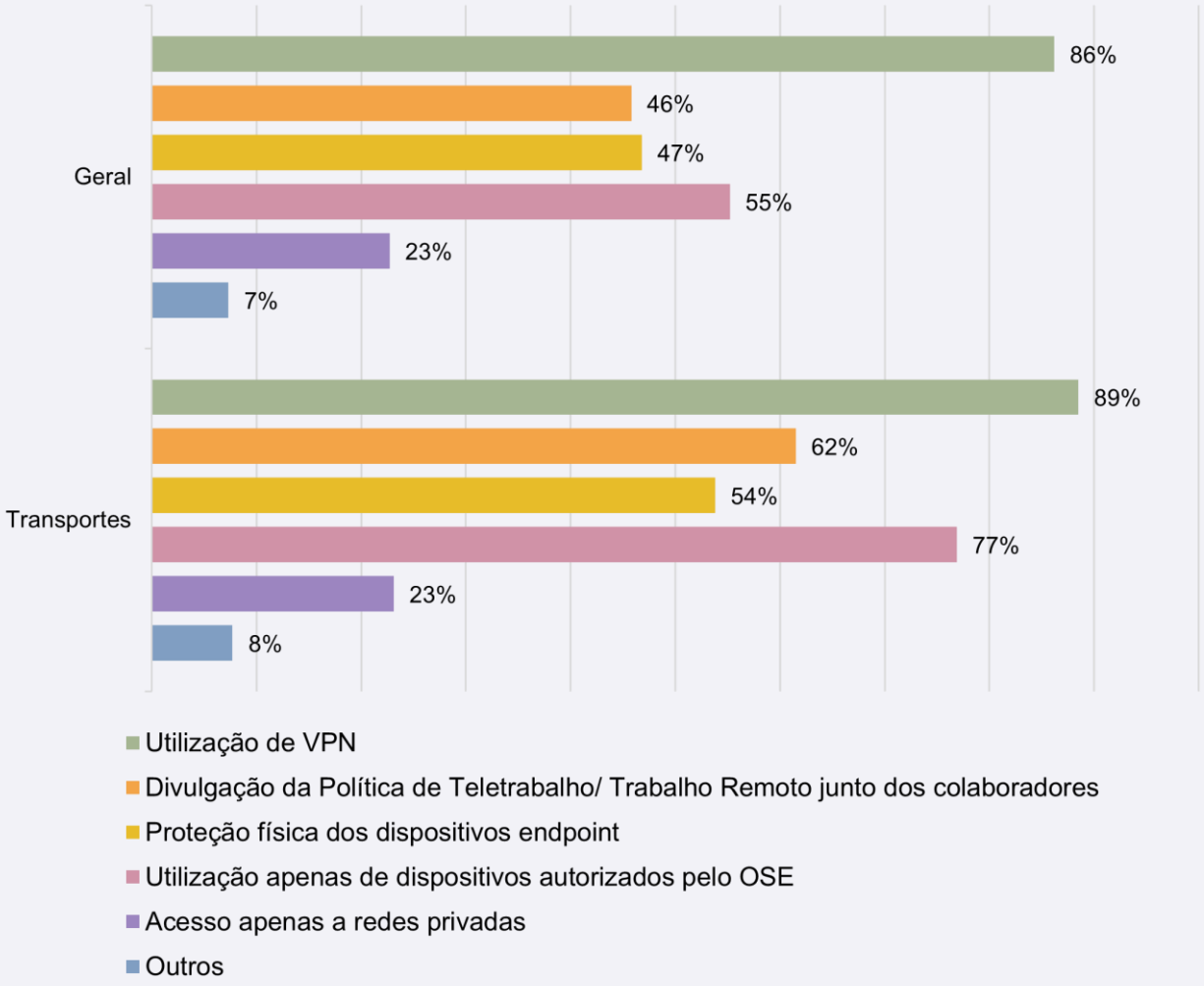


Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no a aplicações de negócio ou a *software* do operador. 6% refere conceder acesso remoto a outros tipos de sistemas, sem especificar quais. No setor dos transportes 96% dos OSE têm acesso ao sistema de email e ao sistema documental, 89% às aplicações de negócio ou software e 8% a outro tipo de sistemas.

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%)[29].

[29] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 6-7.

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

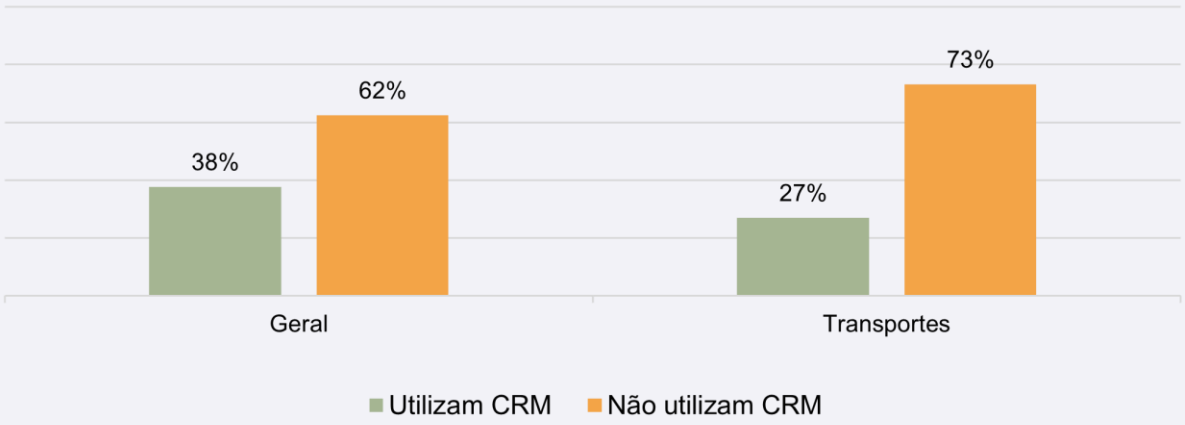


No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança 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.

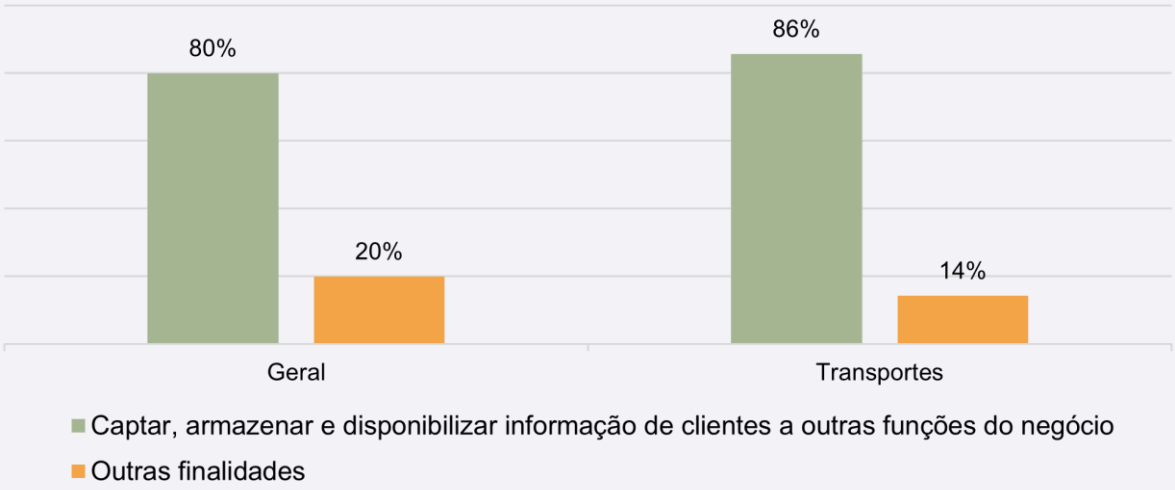
Gráfico 54 - OSE que utilizam Customer Relationship Management software (CRM)



São mais os operadores que não utilizam *software* de *Customer Relationship Management* (CRM)[30] - 62% - do que aqueles que utilizam - 38%. Quanto ao setor dos transportes, predominam os operadores que não utilizam CRM.

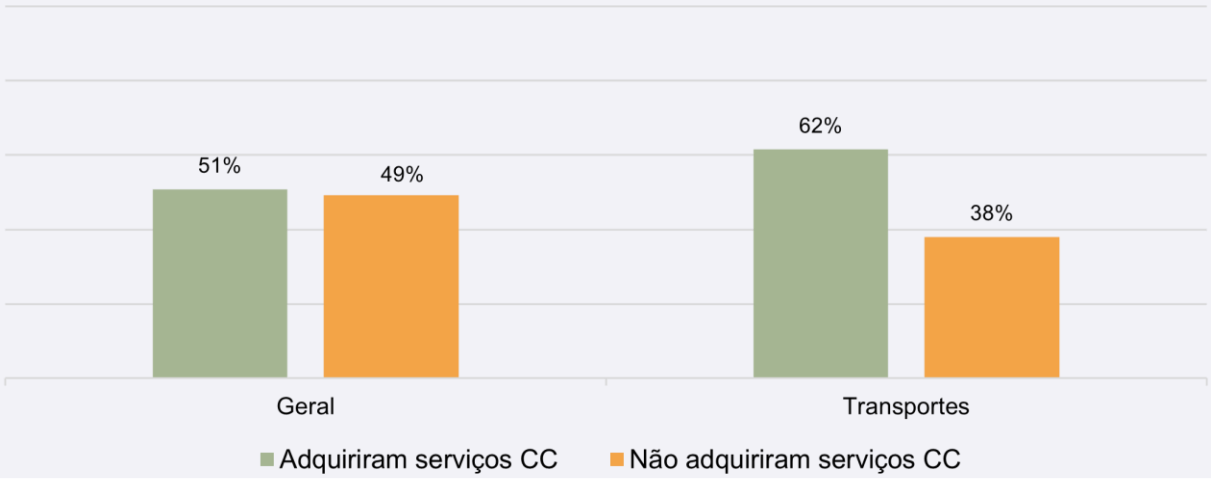
[30] *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos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

Gráfico 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. 86% dos OSE do setor dos transportes utilizam CRM para as funções especificadas.

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



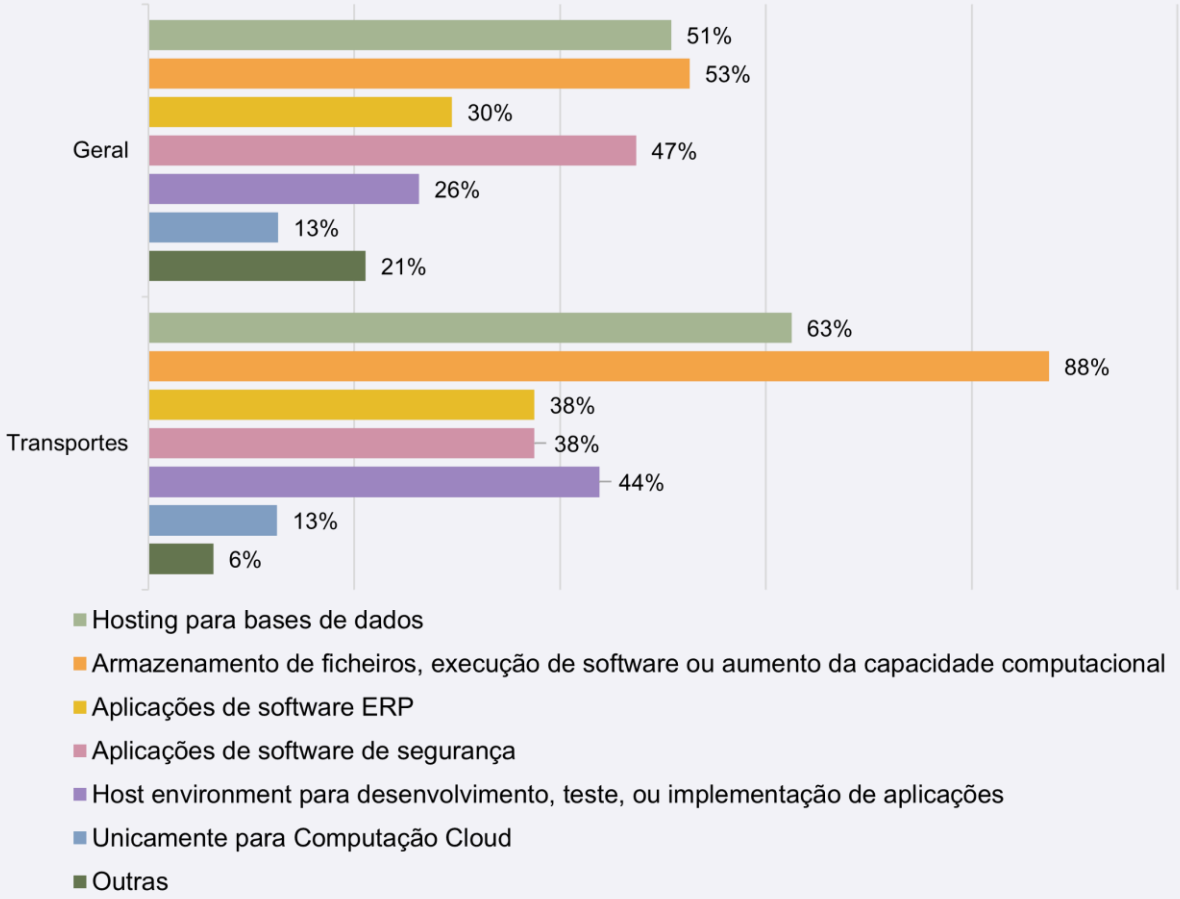
À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização.

No setor dos transportes, 62% dos OSE inquiridos adquiriram serviços *cloud.* 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 2021[31].

[31] ENISA, "NIS Investments", 2022, 11.

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*)[32]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[33].

Gráfico 57 - 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* ERP[34] aplicações de *software* de segurança; *host environment* para desenvolvimento, teste ou implementação de aplicações; e, por fim, exclusivamente para Computação *Cloud*.

[32] ENISA, "NIS Investments", 2023,10.

[33] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

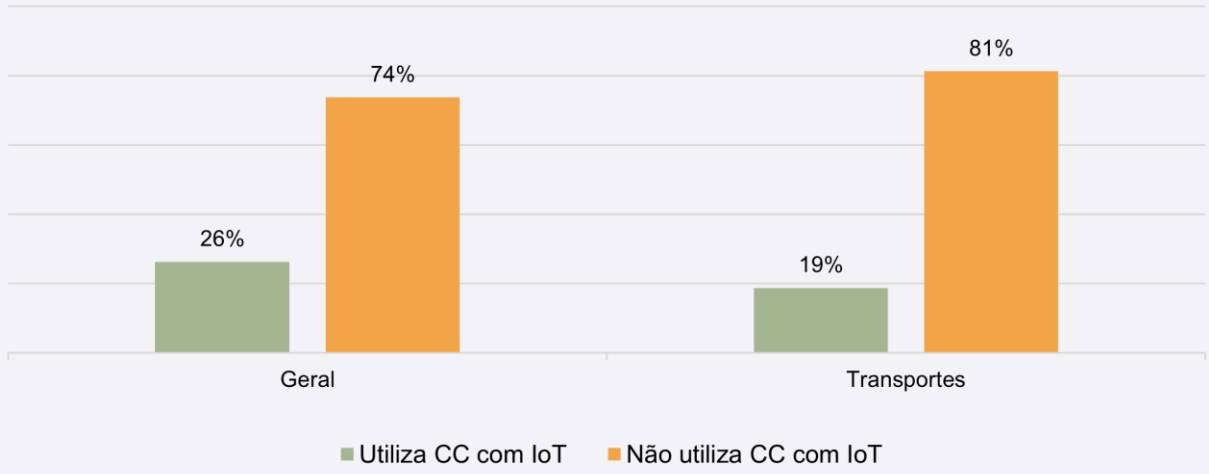
[34] *ERP (Enterprise Resource Planning)* refere-se a um tipo de *software* que as organizações utilizam para gerir os seus recursos e atividades do dia-a-dia, passando pela gestão de projetos, de recursos humanos e logística, entre outras áreas fundamentais para o funcionamento de uma organização. Uma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

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.

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. A utilização de serviços *cloud* para a utilização de *software* ou de aplicações de segurança é também uma das finalidades mais recorrentes entre este setor.

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%)[35].

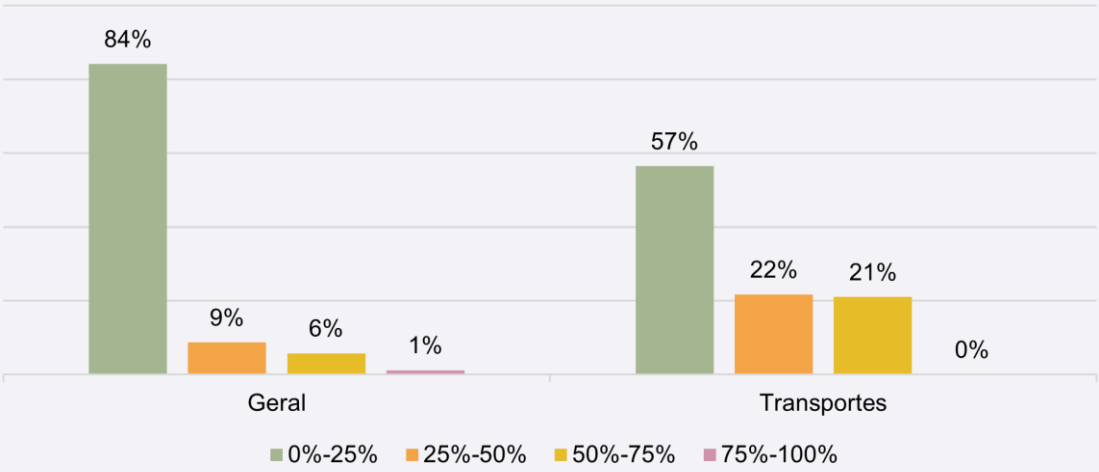
Gráfico 58 - Utilização de serviços de CC em conjunto com *Internet of Things* (IoT)



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, setor dos transportes fica aquém do limiar de 20%.

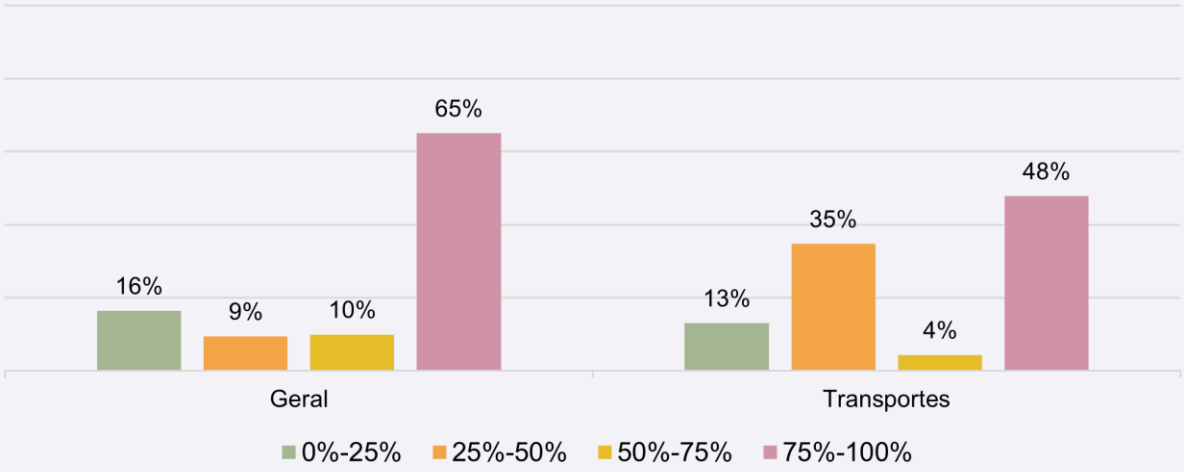
[35] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 59 - Percentagem de sistemas core em *cloud*



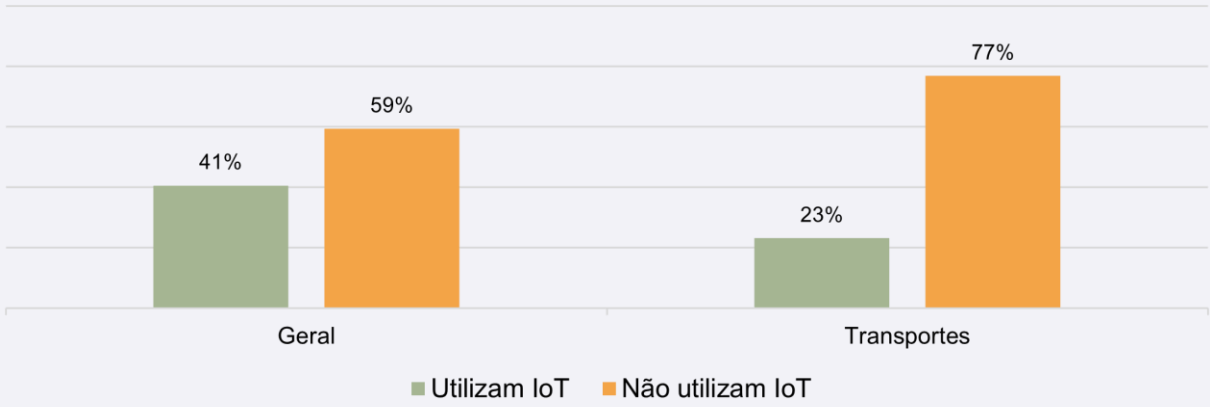
Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos. Há, no entanto, exceções. Por exemplo, no setor dos transportes, registam-se OSE cuja percentagem de sistemas *core* em *cloud* se encontra no intervalo de 25%-50% e 50%-75%.

Gráfico 60 - Percentagem de sistemas core on-perm



Contrastando com o gráfico anterior, aqui mostra-se 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 dos transportes prevalece a faixa de 75 a 100%.

Gráfico 61 - Utilização de IoT pelos OSE

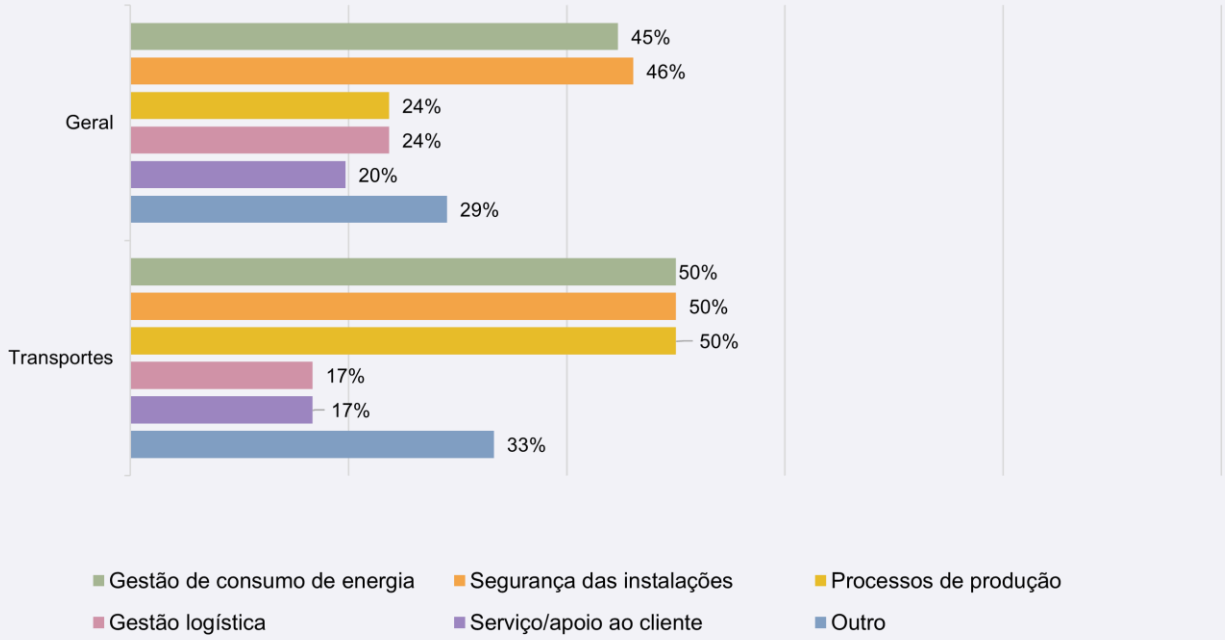


A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT. Setorialmente, nos transportes, prevalece a não utilização de IoT (77%).

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%[36].

[36] 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



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.

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%)"[37].

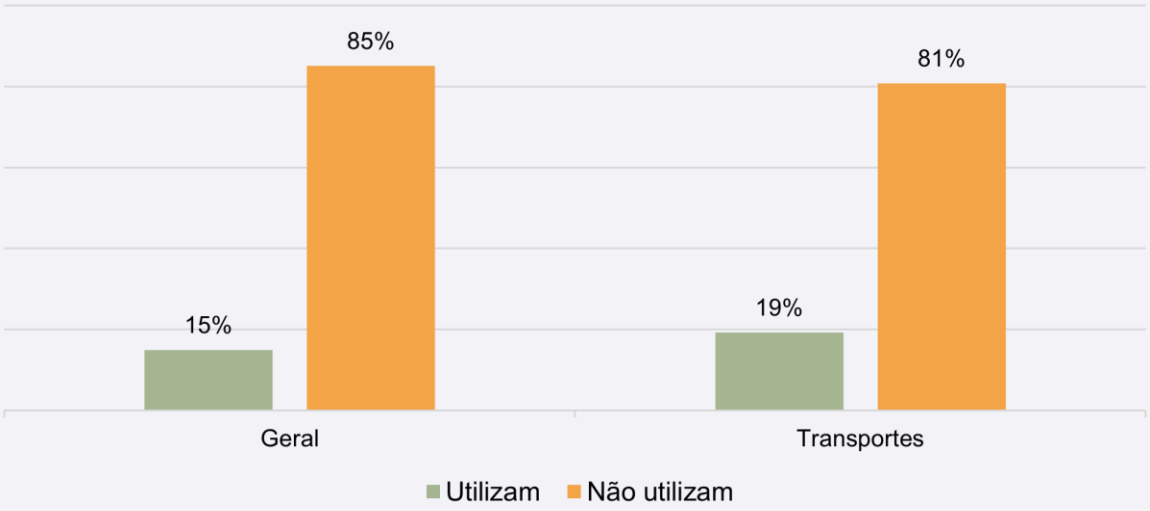
[37] ANACOM, "Utilização da Internet das Coisas (IoT - *Internet of Things*)", 2022, 17.

Gráfico 63 - 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



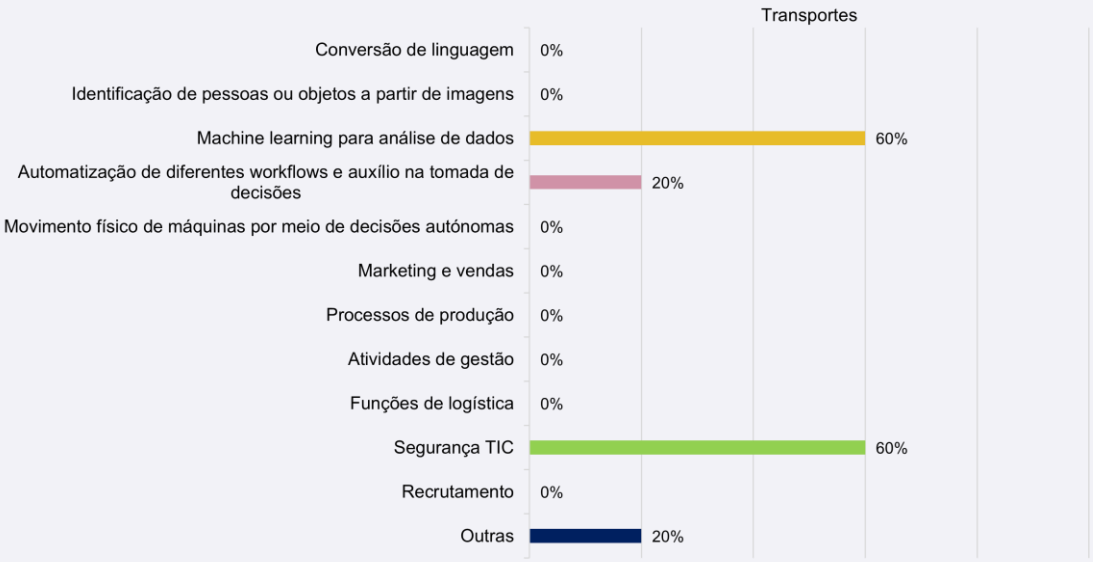
A utilização ou o recurso à IA é ainda reduzido entre os OSE. Apenas 15% dos inquiridos referem já utilizar ou recorrer a IA dentro das suas organizações.
Por norma, há pouca utilização de processos com recurso a Inteligência Artificial (IA) por parte dos operadores. Tal é verificável em todos os setores. No caso do setor dos transportes, segue-se a tendência geral, com a apenas 19% a utilizar IA.

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%)[38], 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%[39].

[38] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 16-17.
[39] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 16-17.

Gráfico 65 - Funções para as quais utilizam IA

Gráfico 65.1 - Funções para as quais utilizam IA



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.

No setor dos transportes mencionou-se a utilização de IA em *machine learing* para analise de dados, na automatização de fluxos de trabalho e auxílio na tomada de decisões, na segurança tic bem como em "outras".
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 IA[40].

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"[41]. 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%[42].

[40] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 17-18.
[41] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 9, https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
[42] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 9.

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança

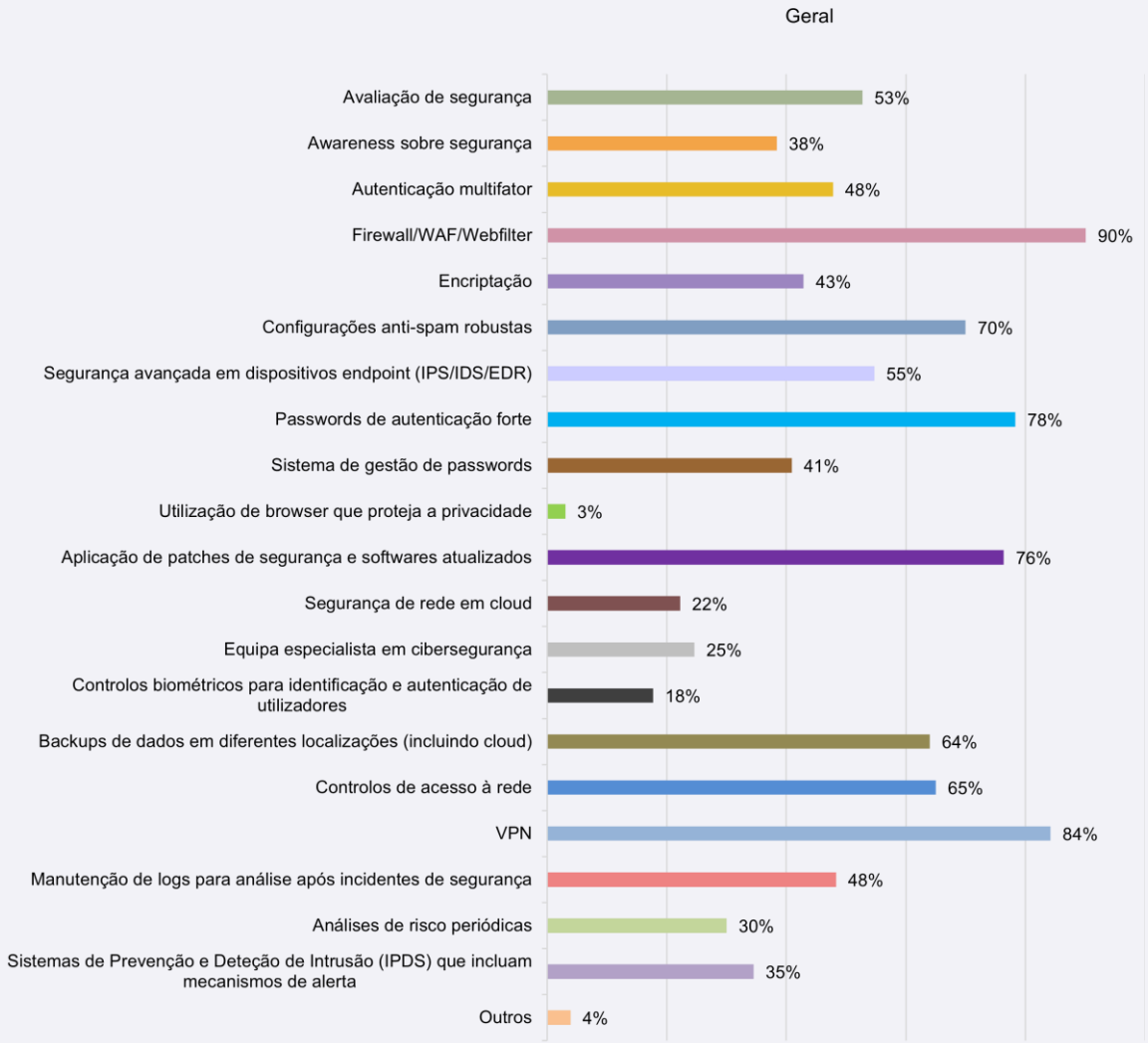


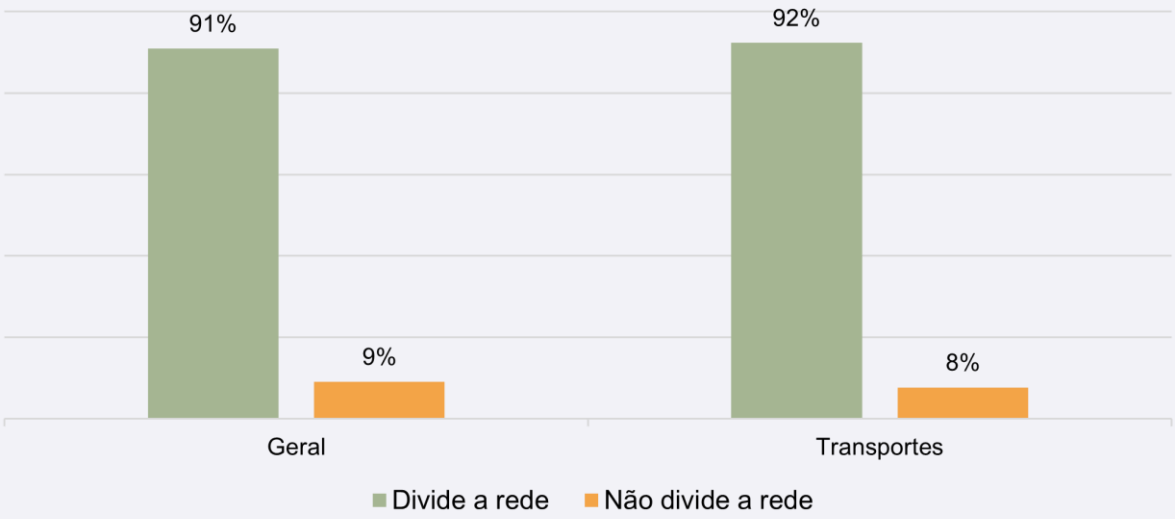
Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança

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%[43].

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%)[44].

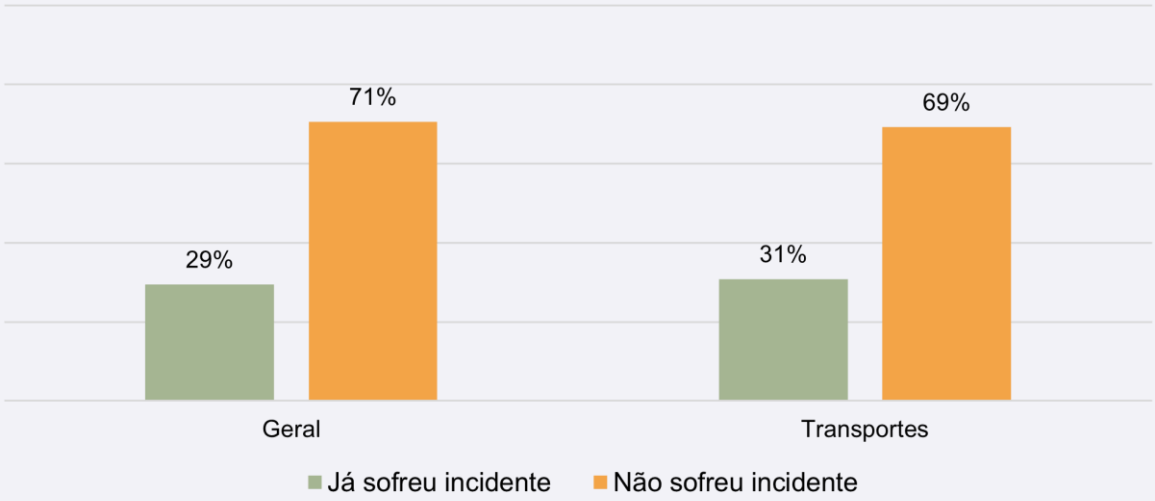
Gráfico 67 - Divisão entre rede dos colaboradores e rede para *guests*



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%.

[43] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 18.
[44] 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 setor dos transportes, 31% dos inquiridos mencionaram já sofrer incidentes de segurança em contexto TIC.

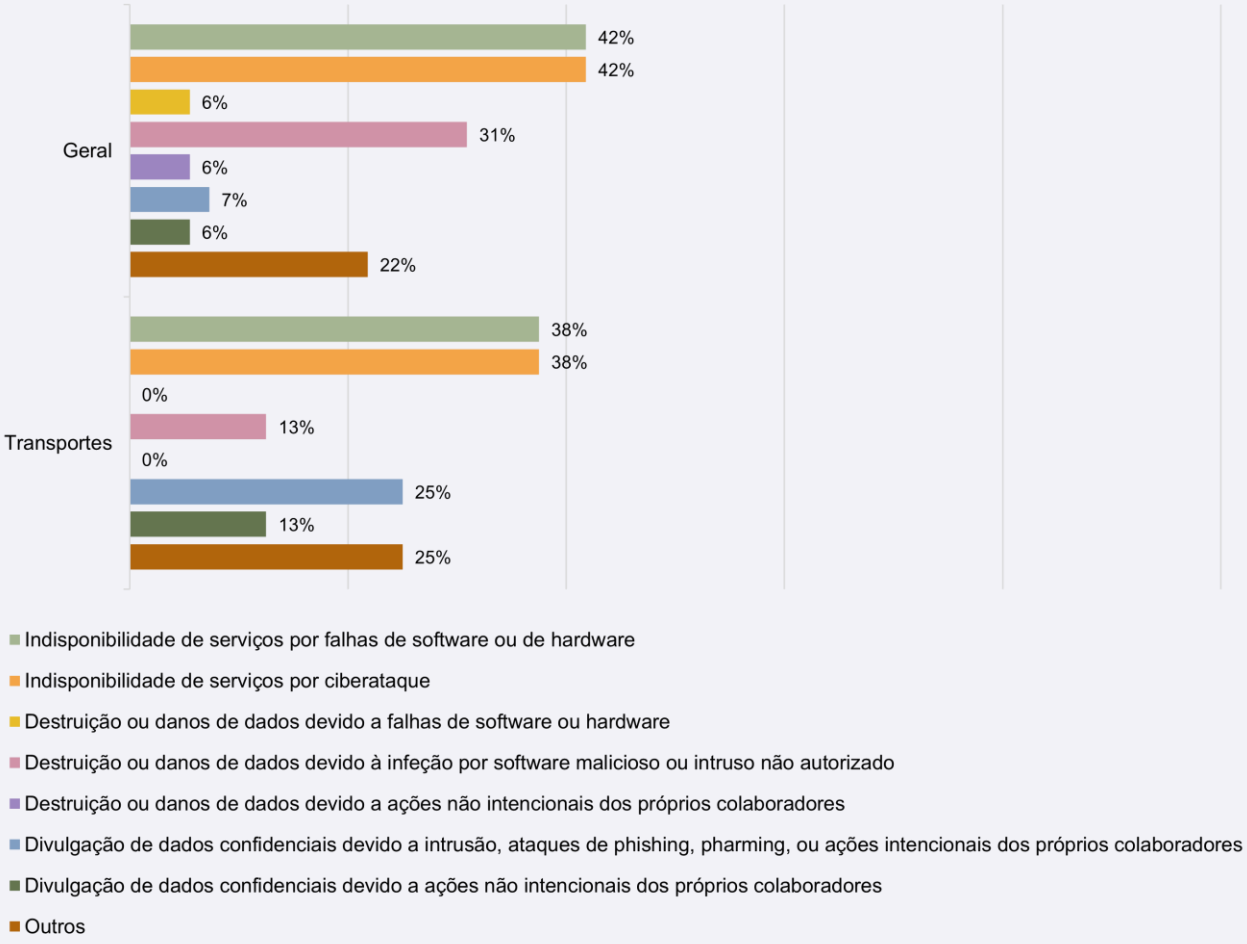
Sendo o IUTICE de 2022, Portugal registou a segunda menor proporção de empresas com incidentes de segurança das TIC na União Europeia (UE). Em 2021, 89,7% das empresas em Portugal, e 91,8% no total da UE, utilizaram pelo menos uma medida para garantir a integridade, a disponibilidade e a confidencialidade dos seus dados e sistemas de Tecnologias de Informação e Comunicação (TIC).[45]

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 terceiros.[46]

[45] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 18.

[46] Fórum Económico Mundial, "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



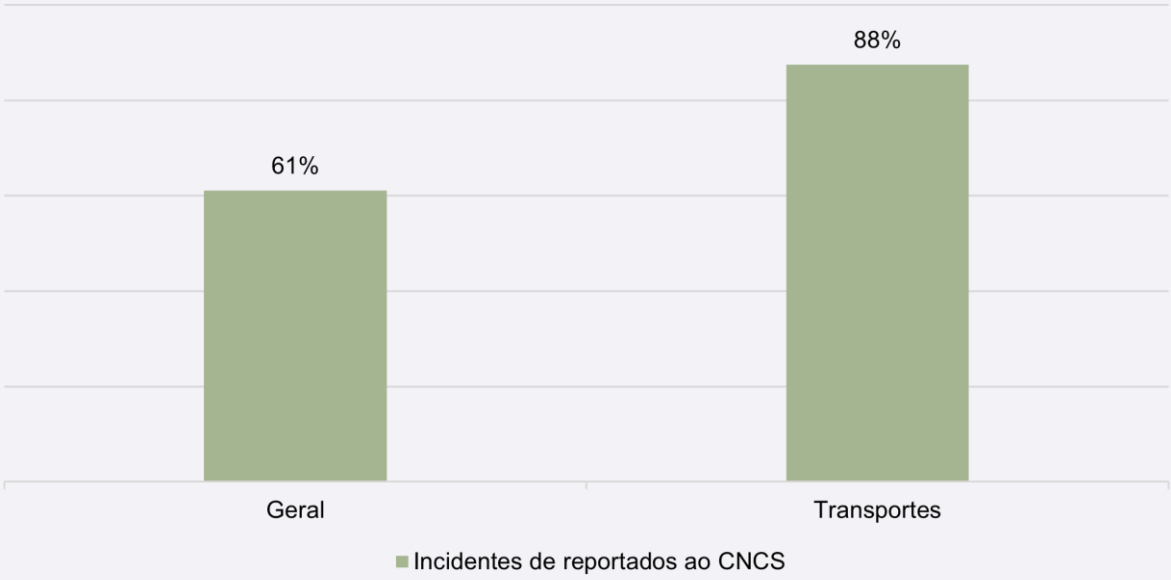
A grande maioria dos incidentes ocorridos afetou a disponibilidade dos serviços, quer por falha de *software* ou de *hardware*, quer por ciberataque. Depois destes, seguem-se os incidentes que resultaram na destruição de dados devido à infeção por *malware* ou devido a intrusão. Os operadores que referiram 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. No setor dos transportes os efeitos dos incidentes dividem-se entre a indisponibilidade de serviços por falha de *software* ou *hardware* e indisponibilidade de serviços por ciberataque.

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)[47].

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 aplicações[48].

Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS

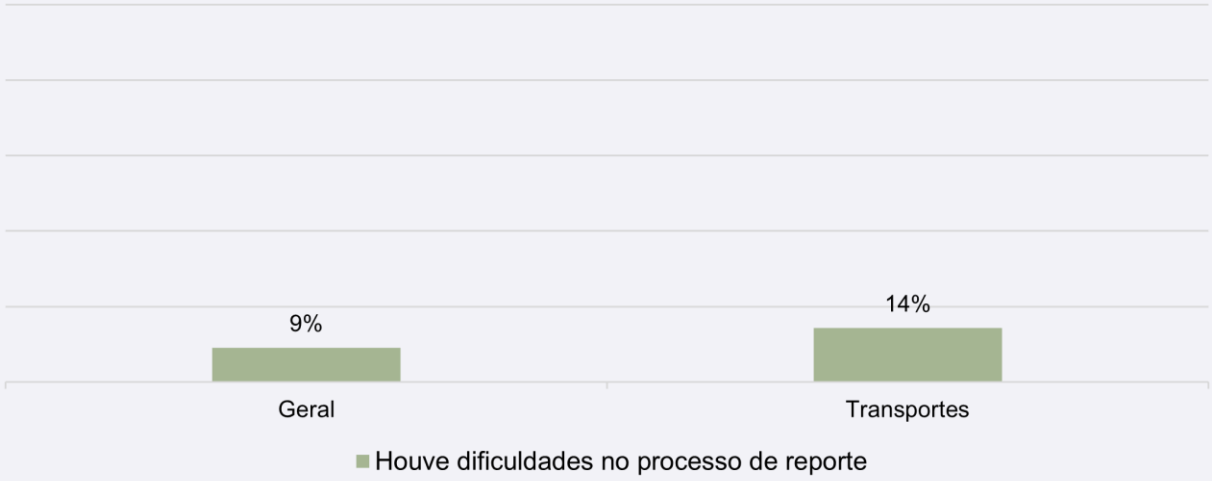


De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n. º1 do artigo 16.º da lei n. º46/2018, de 13 de agosto, os OSE estão apenas obrigados 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**. No setor dos transportes, observa-se mais reportes de incidentes que na generalidade, onde 88% 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.

[47] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 20.

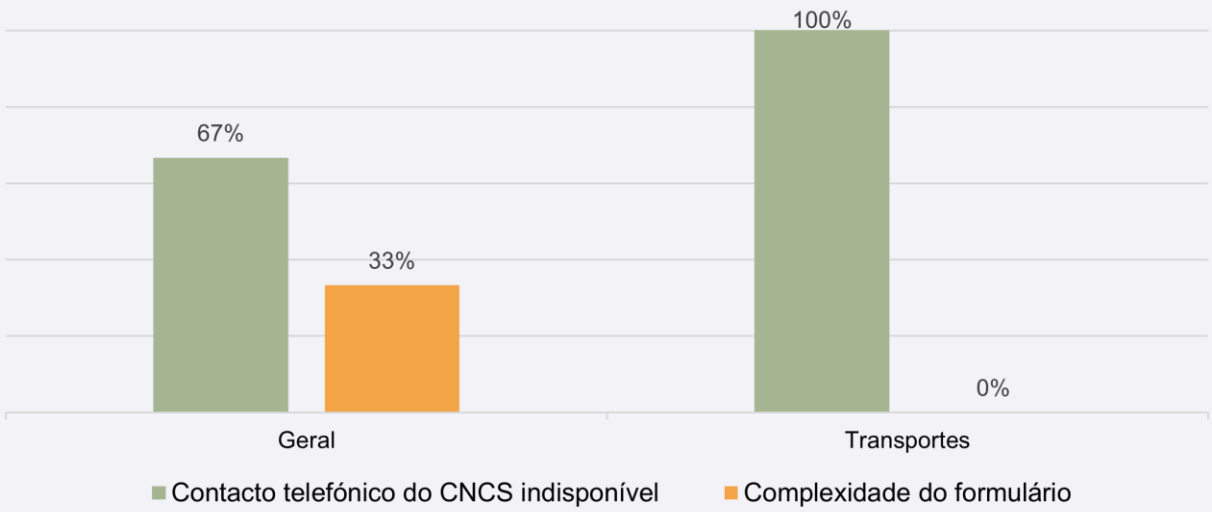
[48] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 6.

Gráfico 71 - Dificuldades no processo de notificação ao CNCS



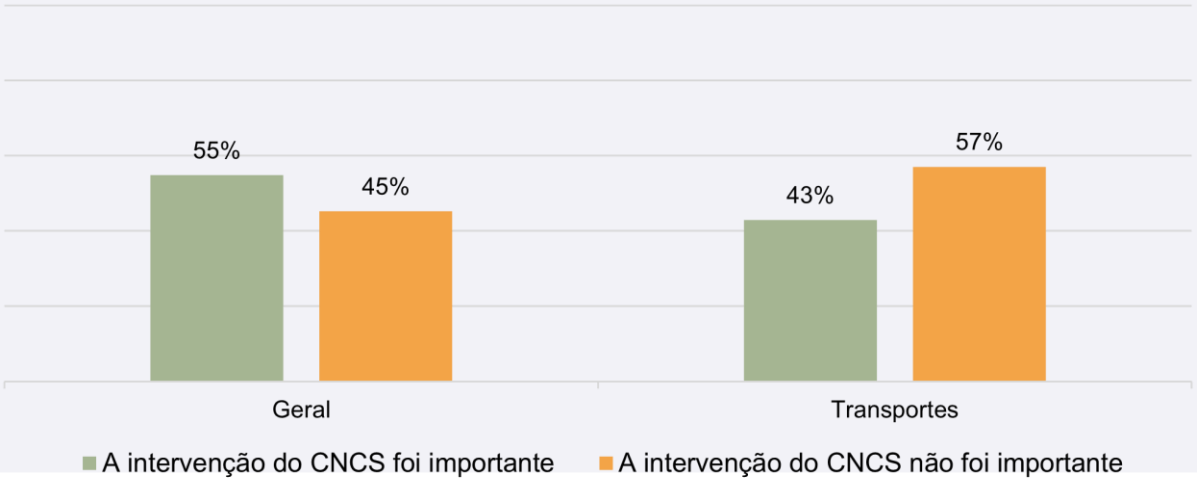
De modo geral, os operadores não tiveram dificuldades no processo de notificação de incidentes ao CNCS. No entanto, a nível geral, houve ainda cerca de 9% dos operadores a indicarem dificuldades na notificação. No setor dos transportes, 14% dos operadores afirmam ter dificuldades no processo de notificação ao CNCS.

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



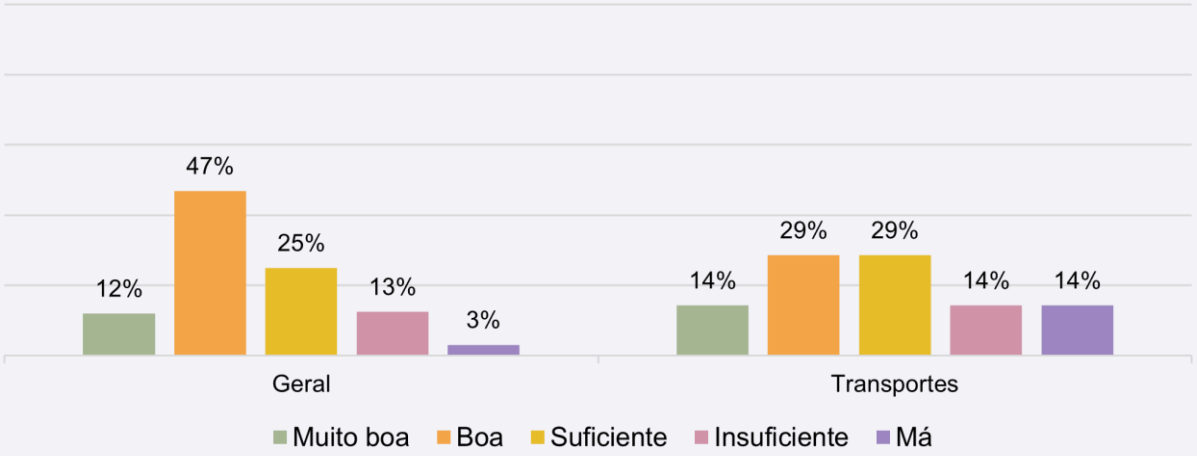
Entre os setores que identificaram dificuldades na notificação de incidentes ao CNCS, dois (sendo um deles o setor dos transportes) referiram que a principal dificuldade durante o processo de notificação foi a indisponibilidade do contacto telefónico e um atribuiu a principal dificuldade à complexidade do formulário de notificação. Os restantes 4 setores não identificaram 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%). Sectorialmente, nos transportes, predomina a opinião de que a intervenção do CNCS não foi relevante para a resolução do incidente notificado.

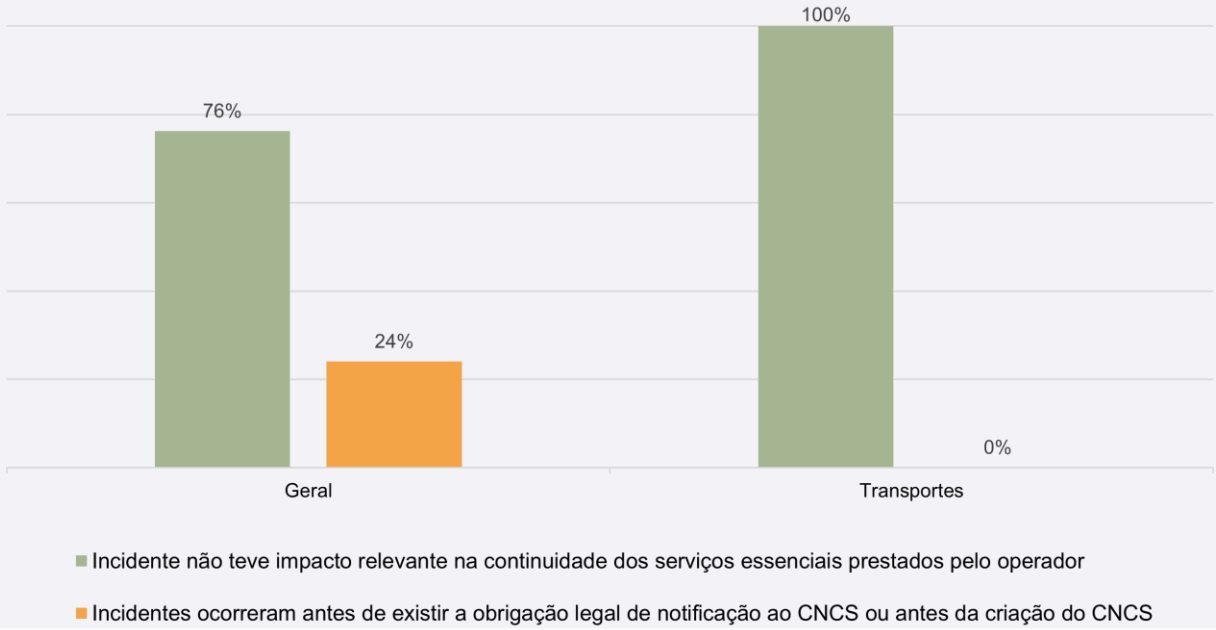
Gráfico 74 - Avaliação da resposta dada pelo CNCS



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%).

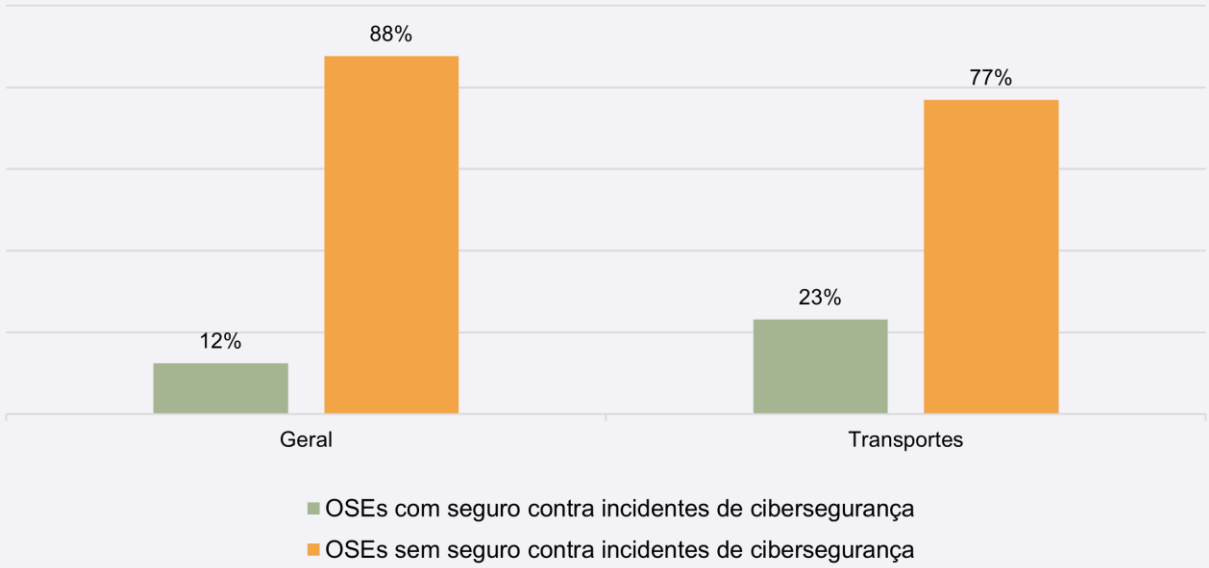
No setor de transportes existem algumas discrepâncias nas perspetivas dos diferentes operadores. Em geral, a opinião foi positiva, no entanto, 14% classificou a resposta do CNCS como insuficiente ou má.

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. A totalidade dos inquiridos do setor dos transportes indicou que o incidente não teve impacto relevante na continuidade dos serviços.

Gráfico 76 - Seguro contra incidentes de cibersegurança



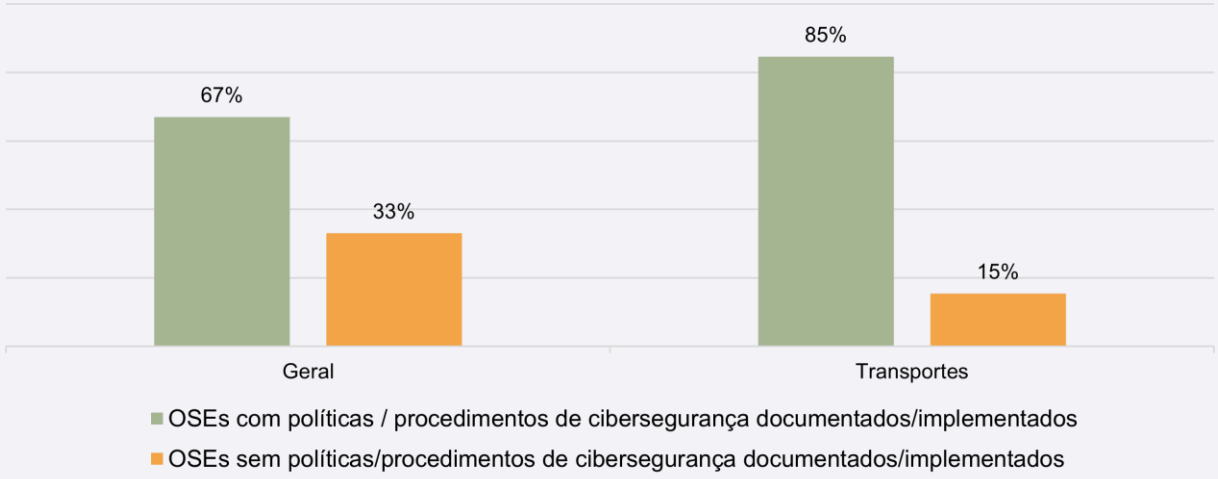
Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. A lógica geral mantém-se nos setores dos transportes, com a maior parte dos inquiridos a não possuírem este tipo de seguro.

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 essenciais[49].

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 cibersegurança[50].

[49] ENISA, "NIS Investments", 2023, 16 e 24.
[50] Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", 9.

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

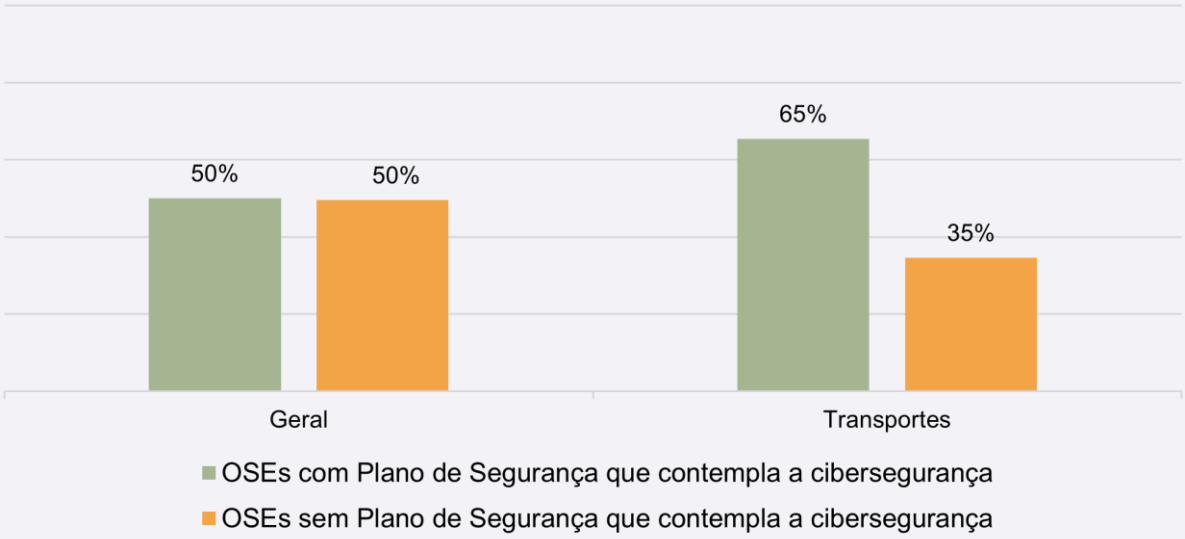


Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados. No setor dos transportes, esta proporção é maior que a geral, onde a maioria refere ter políticas ou procedimentos de cibersegurança documentados ou implementados.

Segundo dados do IUTICE, em 2022, cerca de 54.4% do total de empresas tinha documentos sobre medidas, práticas ou procedimentos em matéria de segurança[51].

[51] Instituto Nacional de Estatística, "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. No setor dos transportes, a maior parte dos operadores (65%) já tem um plano de segurança que contemple a área da cibersegurança.

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 real[52].

[52] Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024, 5.

Gráfico 79 - Políticas incluídas no Plano de Segurança

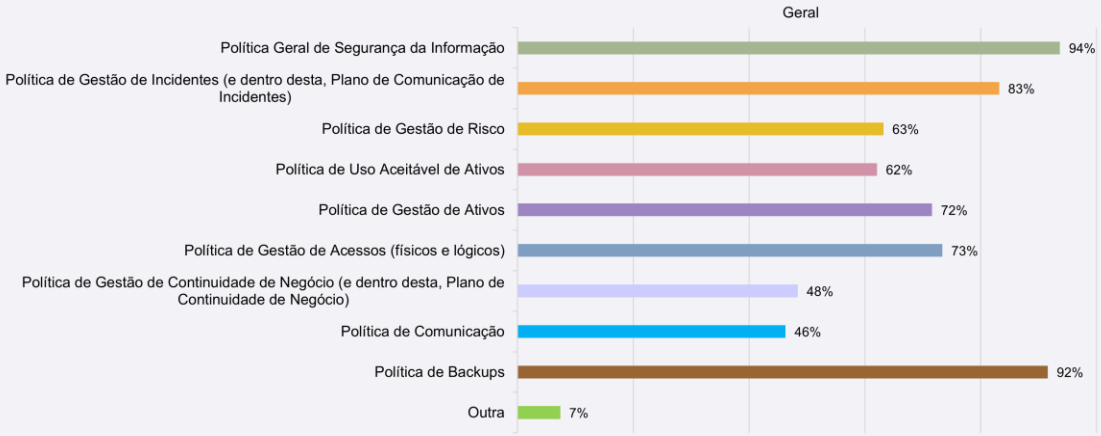
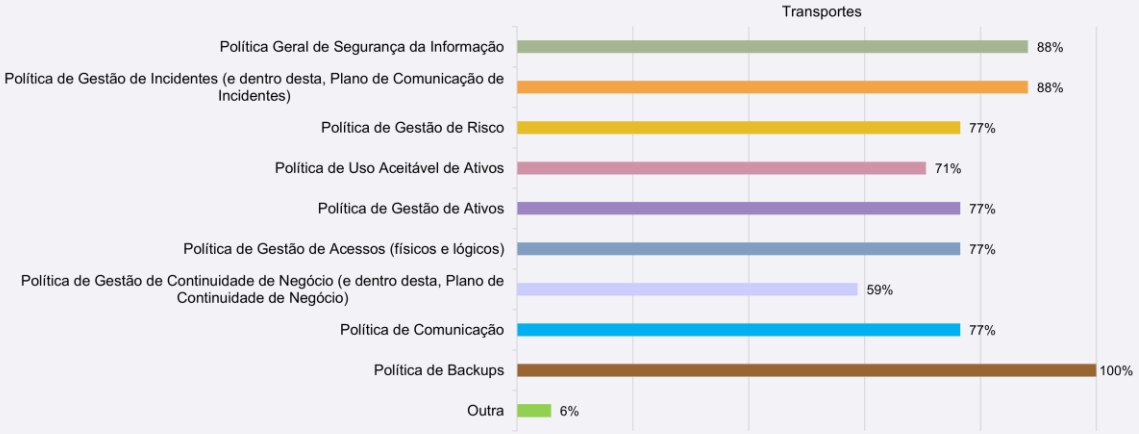


Gráfico 79.1 - Políticas incluídas no Plano de Segurança

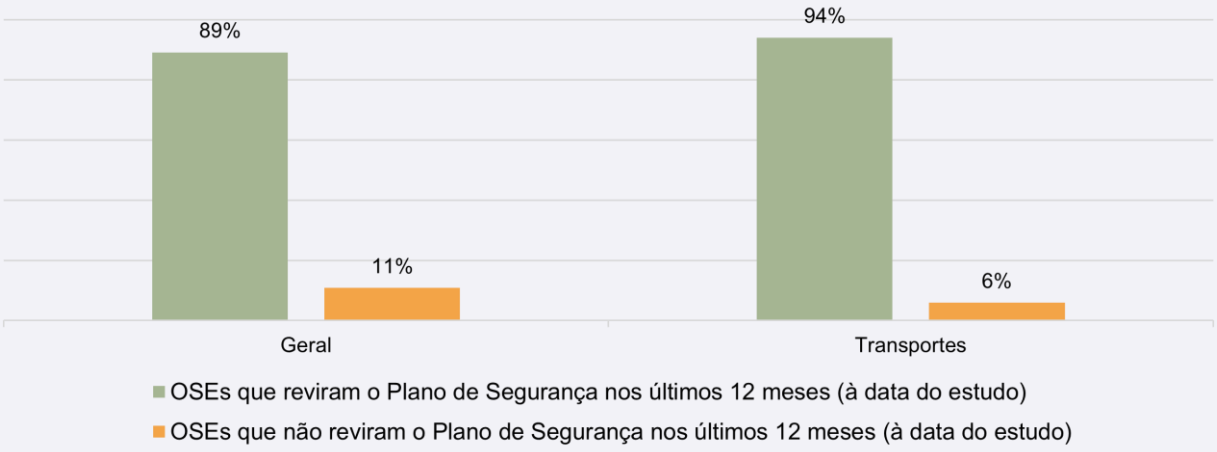


Os gráficos acima representam a percentagem de operadores com plano de segurança que tem as diversas políticas elencadas elaboradas no âmbito desse mesmo plano.

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 Electrónico, 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. No setor dos transportes, a grande maioria dos operadores com plano de segurança realizou a revisão do mesmo, apenas 6% refere não realizar o plano de segurança nos últimos 12 meses (à data do estudo).

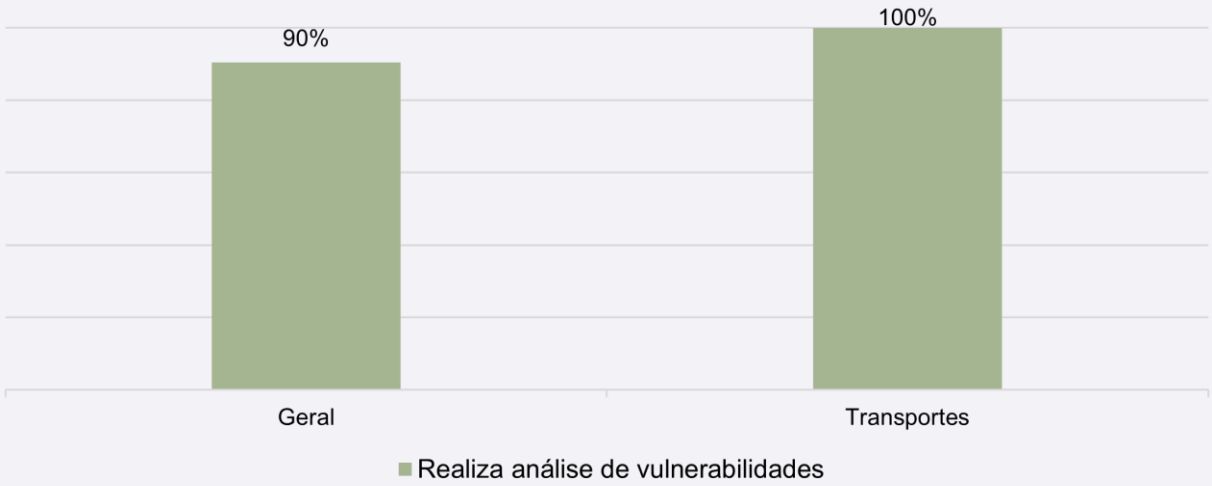
Segundo dados do IUTICE 2022, a maioria (61,7%) das empresas definiu ou fez uma revisão aos documentos sobre medidas, práticas ou procedimentos de segurança nos últimos 12 meses[53].

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.
No setor dos transportes, a percentagem de operadores que realiza estes procedimentos ultrapassa em 8 p.p a generalidade.

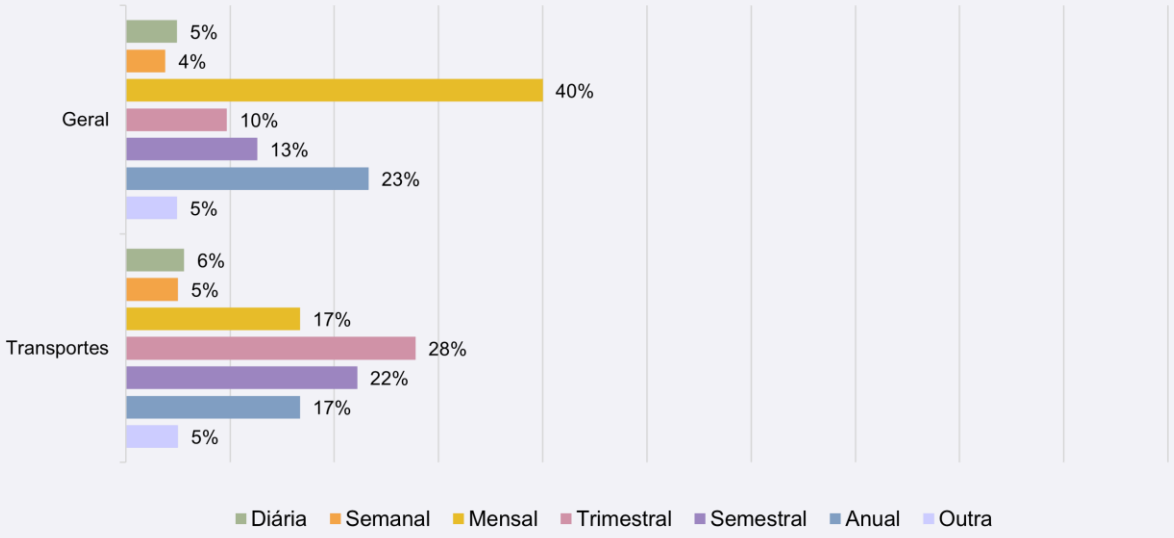
[53] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

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



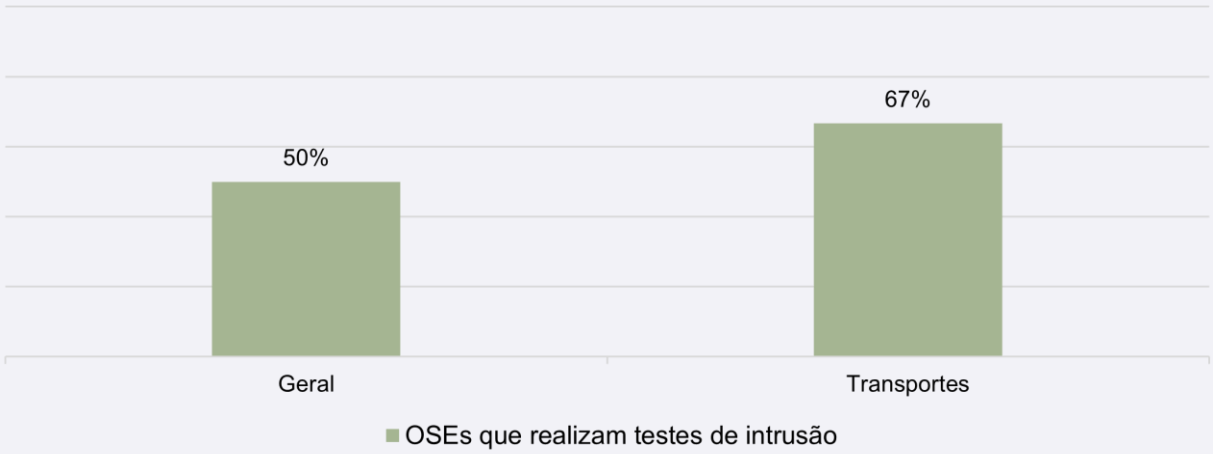
Entre os operadores que realizam procedimentos de deteção e gestão de vulnerabilidades, a vasta maioria (90%) faz também a análise das mesmas. No setor dos transportes, todos os operadores que já realizavam procedimentos de deteção e gestão de vulnerabilidades, fazem também a análise das mesmas.

Gráfico 83 - Frequência da análise de vulnerabilidades



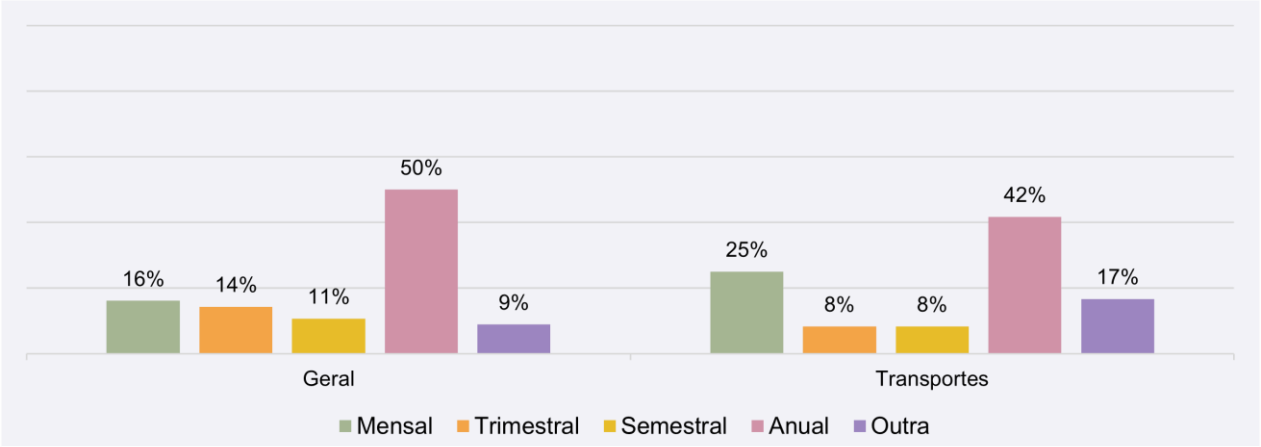
A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.
Há operadores, embora poucos, que realizam análise de vulnerabilidades diariamente, nomeadamente nos setores dos transportes.

Gráfico 84 - Realização de testes de intrusão



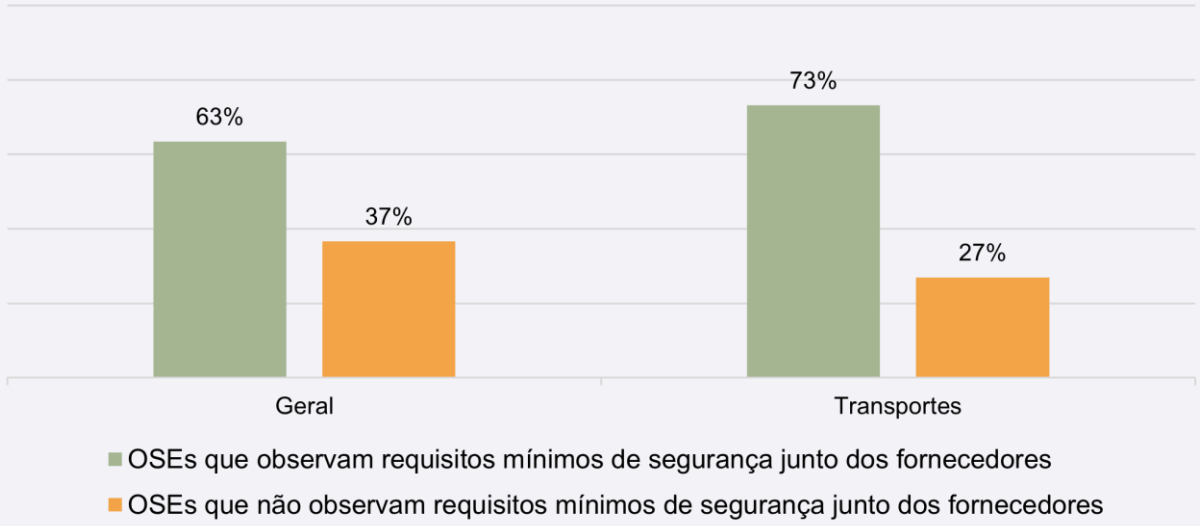
Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).
É de salientar o setor dos transportes, no qual 67% dos operadores realizam testes de intrusão.

Gráfico 85 - Frequência de testes de intrusão



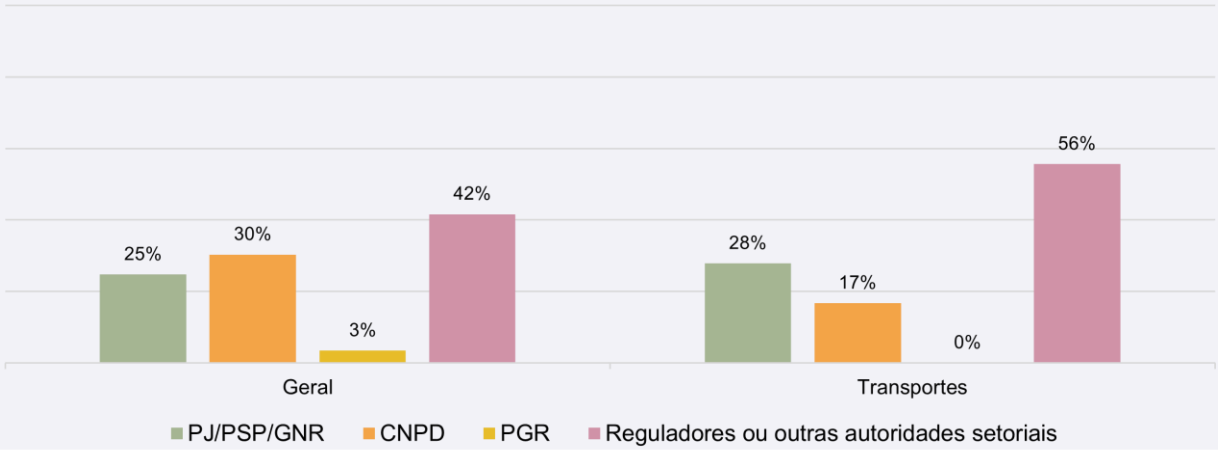
Com exceção dos operadores de serviços essenciais do setor da energia e do setor bancário, os operadores dos setores tendem a realizar testes de intrusão anualmente.
No setor dos transportes, embora prevaleça a periodicidade anual para estes testes, é possível verificar operadores a optar por períodos 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. Sectorialmente, nos transportes, 73% dos OSE observam os requisitos de segurança por parte dos fornecedores.

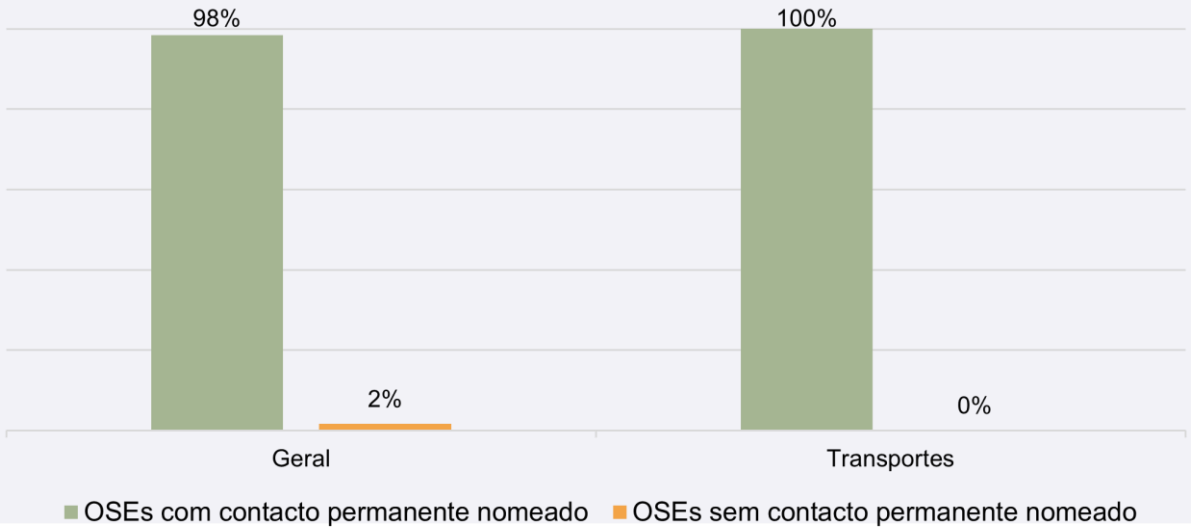
Gráfico 87 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS



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).

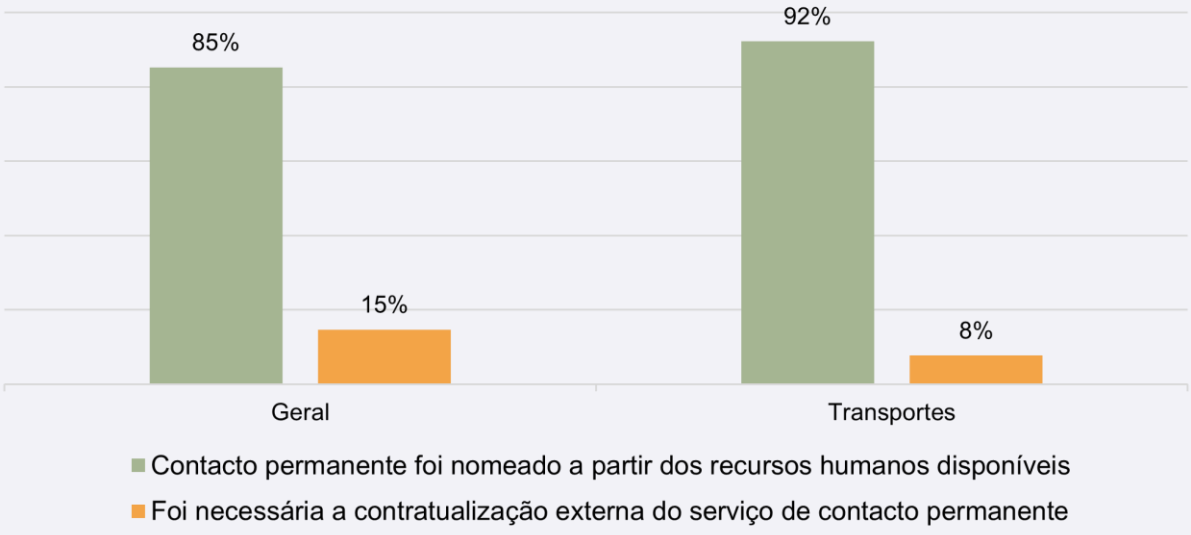
A Comissão Nacional de Proteção de Dados (CNPD) surge em 2º lugar nas intenções de notificação em caso de ciberataque/incidente dos inquiridos, estando em 3º lugar as intenções de notificação à PJ/PSP/GNR.
Em caso de ciberataque os OSE concordam em contactar, para além do CNCS, os reguladores ou outras entidades setoriais. Verifica-se que contactar a PGR foi a opção com menos destaque seguida do CNPD.
No setor dos transportes nenhum operador referiu, em algum caso, contactar a PGR, optando pela notificação aos reguladores, à PJ/PSP/GNR e à CNPD.

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



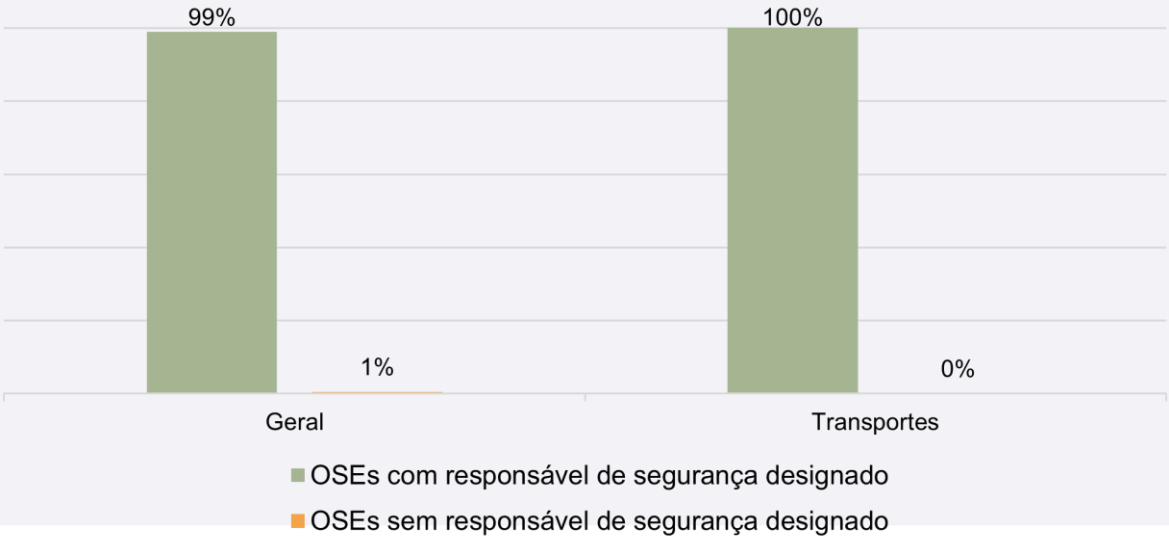
98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado.
No setor dos transportes a totalidade dos operadores respondeu ter contacto nomeado.

Gráfico 89 - Designação do contacto permanente



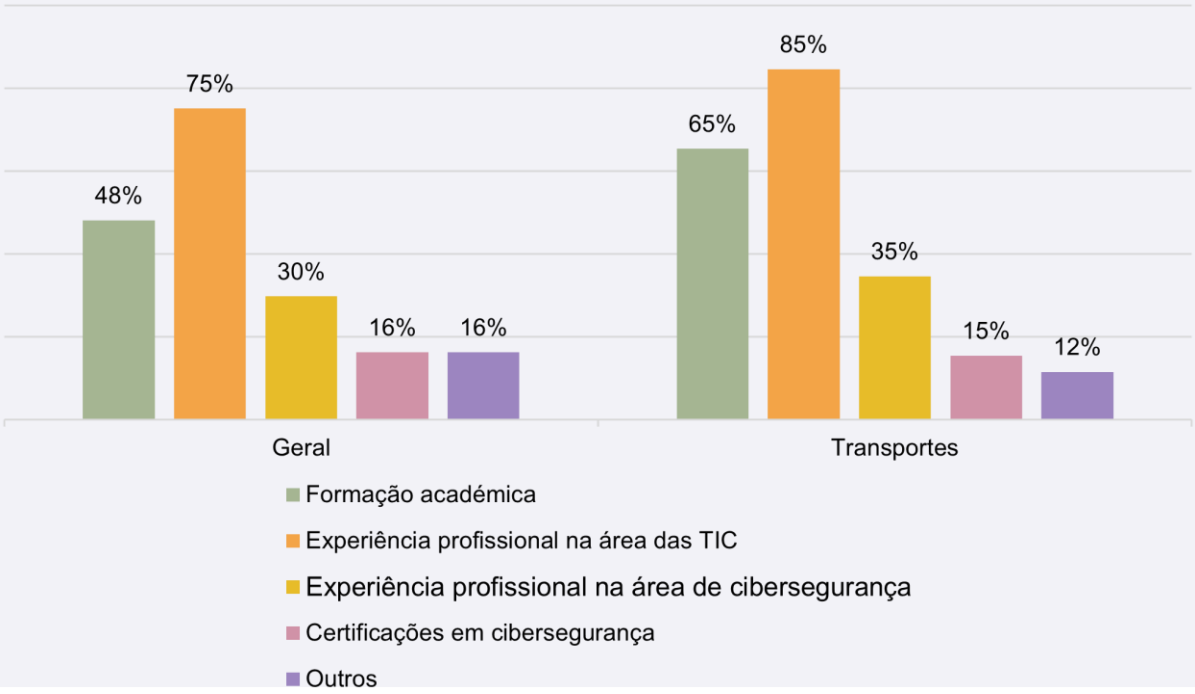
A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No setor dos transportes, 92% designou como contacto permanente alguém que fazia parte da organização.

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 em um setor 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

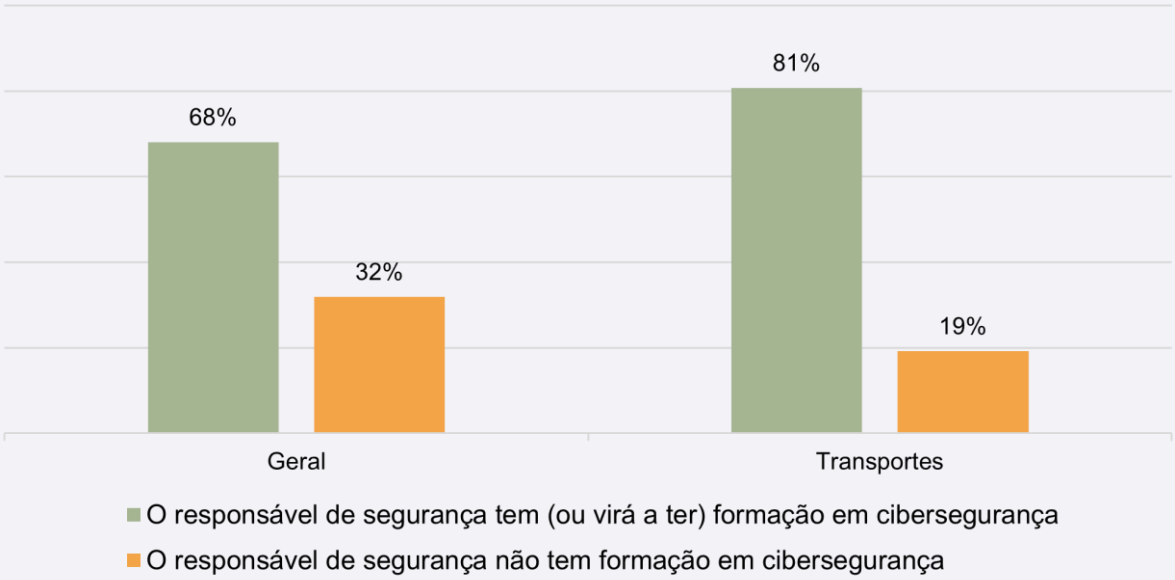


A formação académica e a experiência profissional na área das TIC e na área de cibersegurança foram os critérios mais importantes para a designação do responsável de segurança dos operadores. Na generalidade, a experiência profissional nas TIC foi um critério em 75% dos casos, a formação académica foi um critério em 43% dos casos e a experiência profissional em cibersegurança foi também critério em 30% dos casos.

No setor dos transportes, 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.

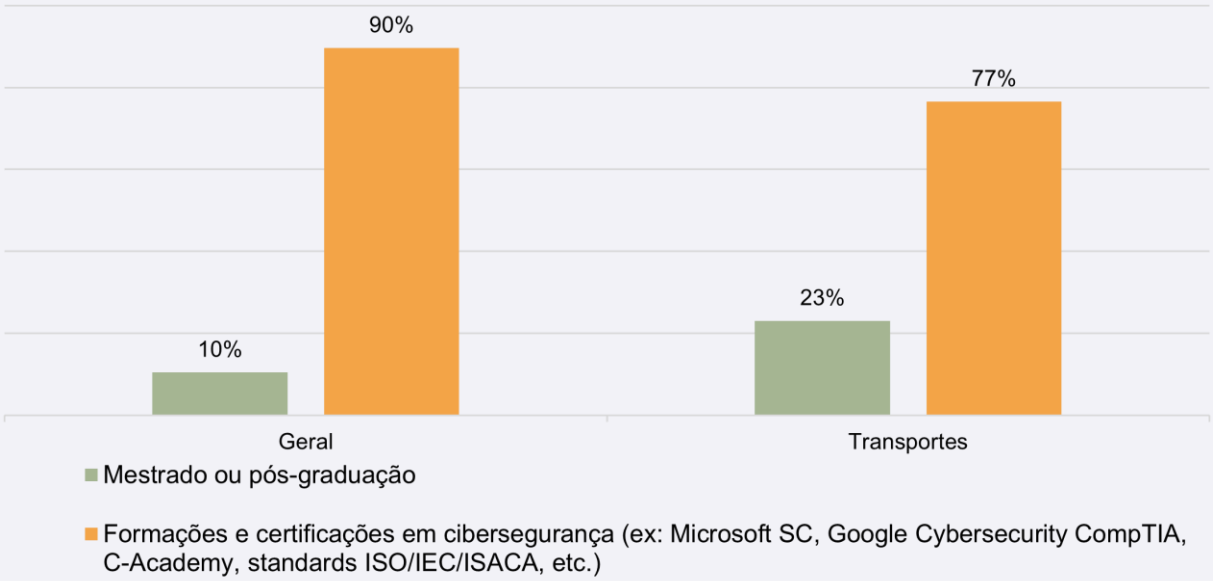
É também importante referir que se verificaram casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de câmara, como no caso de serviços municipalizados.

Gráfico 92 - Formação específica de cibersegurança do responsável de segurança



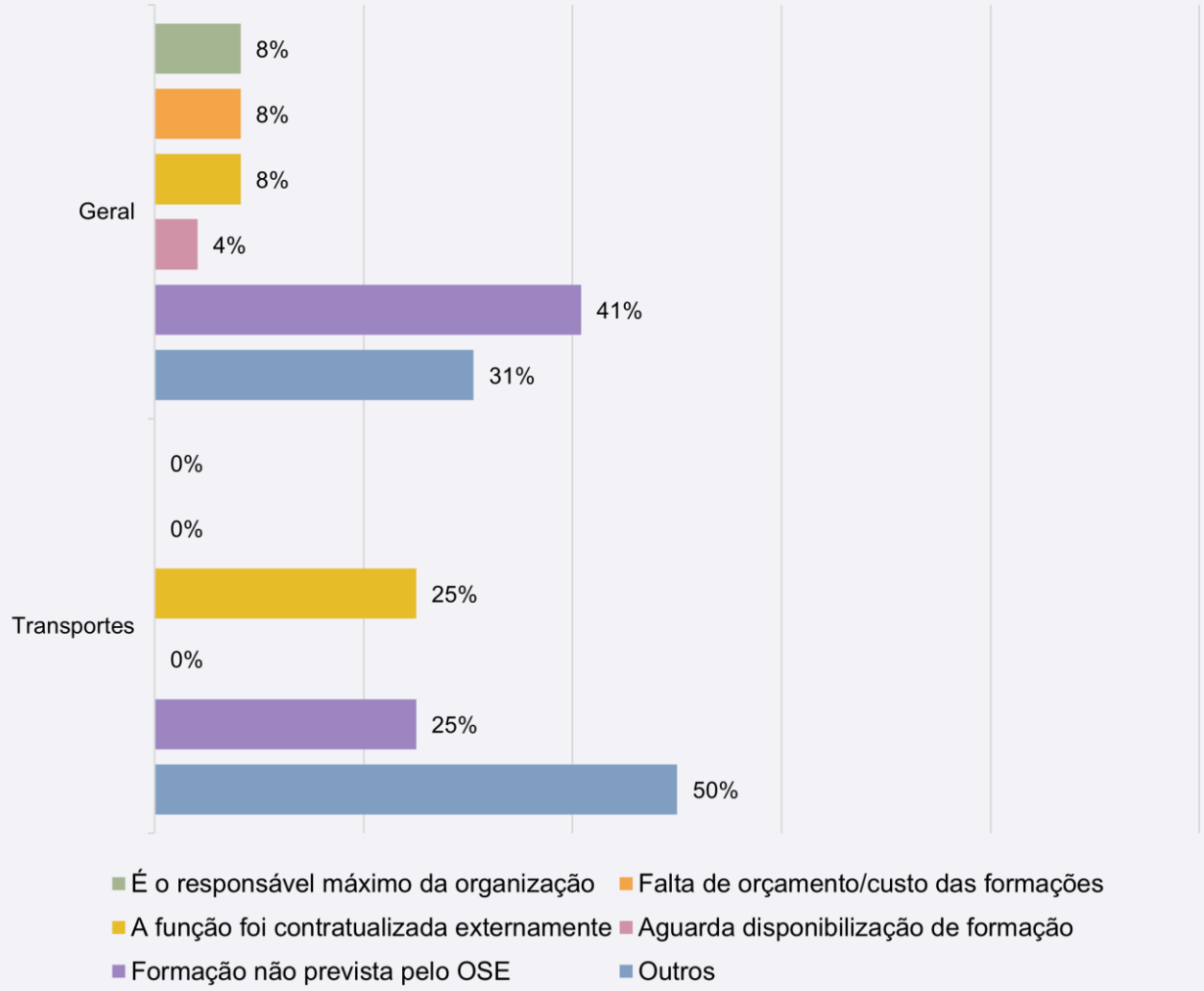
Em cerca de 70% dos casos, o responsável de segurança tem ou virá a ter formação específica em cibersegurança. No setor dos transportes, a maioria dos operadores (81%) refere que o responsável de segurança tem (ou virá a ter) formação em cibersegurança.

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. No setor dos transportes, essa percentagem não ultrapassa os 23%.

Gráfico 94 - 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.

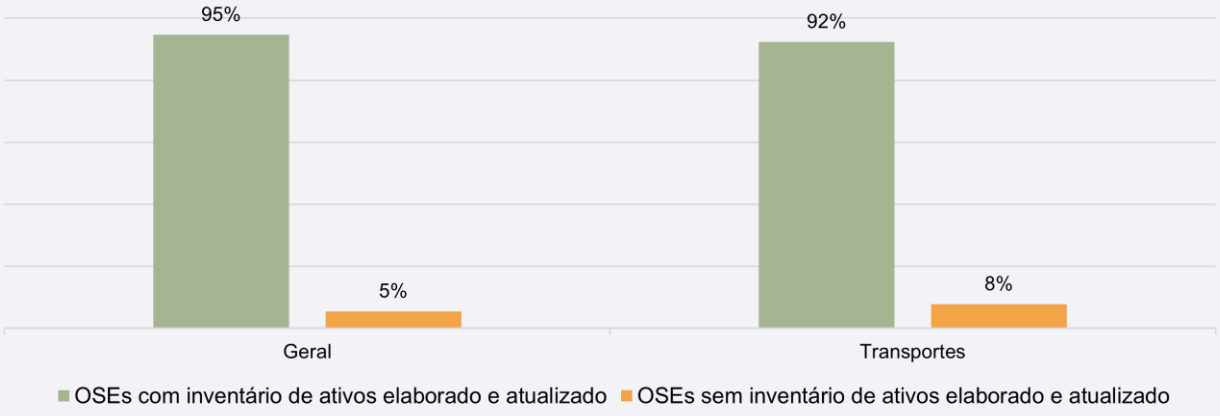
Em segundo lugar, surge a resposta “outros”, dada por cerca de 30% dos OSE onde o responsável de segurança não tem formação em cibersegurança. Entre esses “outros” motivos, encontram-se explicações tais como a falta de oportunidade ou disponibilidade de realizar a formação; tentativas de incluir formação 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 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.

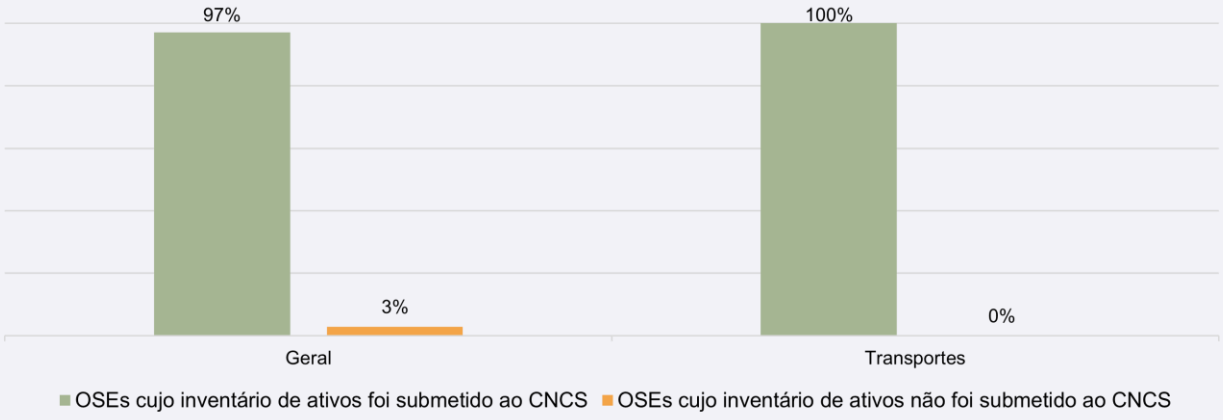
Tal como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado "Compromisso C-Academy" que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança 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



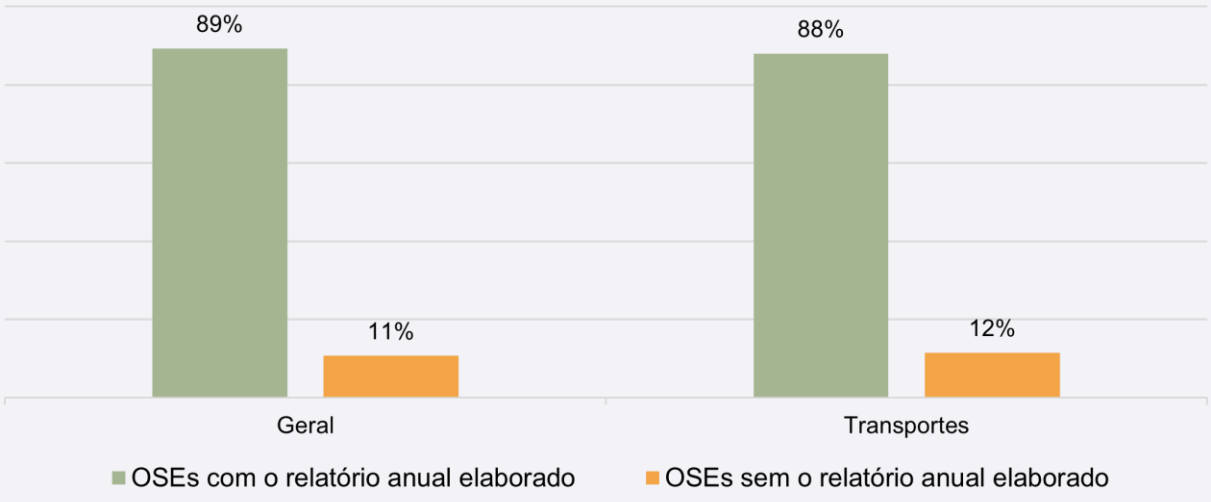
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. No setor dos transportes, a percentagem de operadores cujo inventário de ativos essenciais não está elaborado e atualizado é de 8%.

Gráfico 96 - Submissão do inventário de ativos ao CNCS



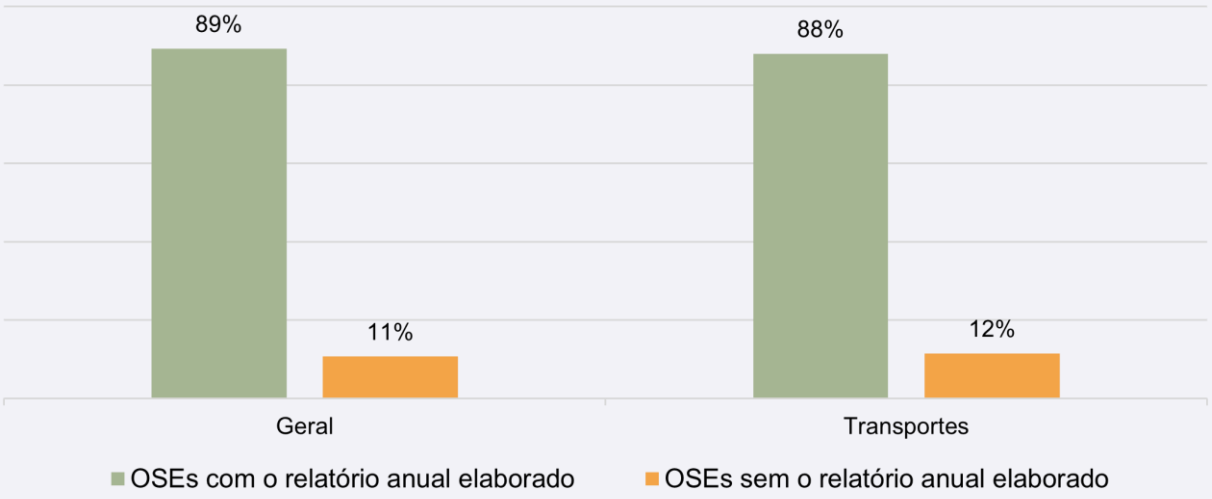
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. Destacam-se os setores dos transportes, onde todos os operadores com inventário de ativos elaborado efetuaram a submissão do mesmo.

Gráfico 97 - Elaboração do relatório anual previsto pelo decreto-lei n. º65/2021, de 30 de julho



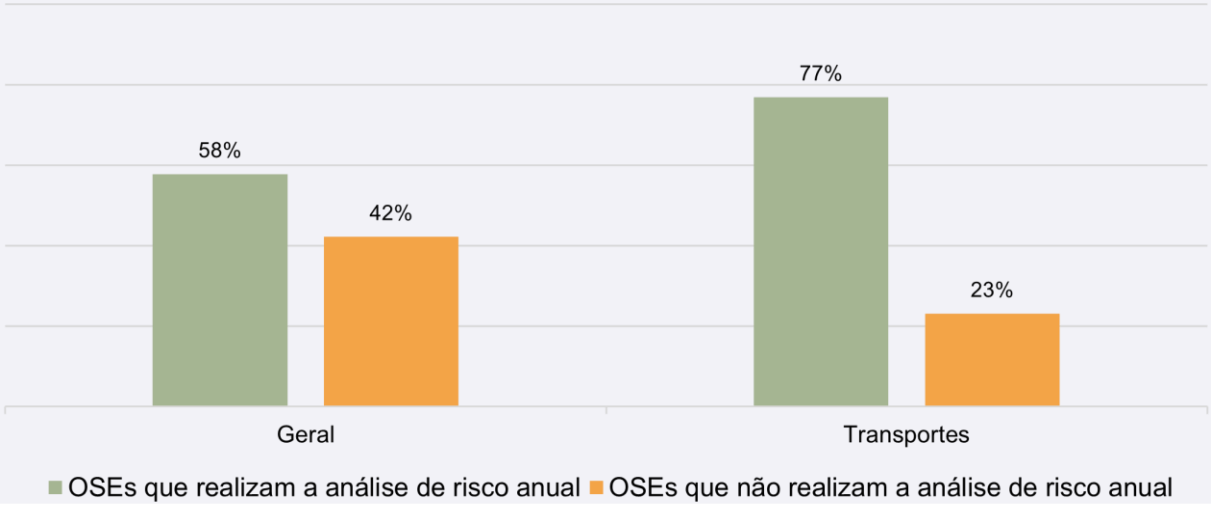
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. Nos transportes, 12% dos operadores não tinham relatório anual elaborado.

Gráfico 98 - Submissão do relatório anual ao CNCS



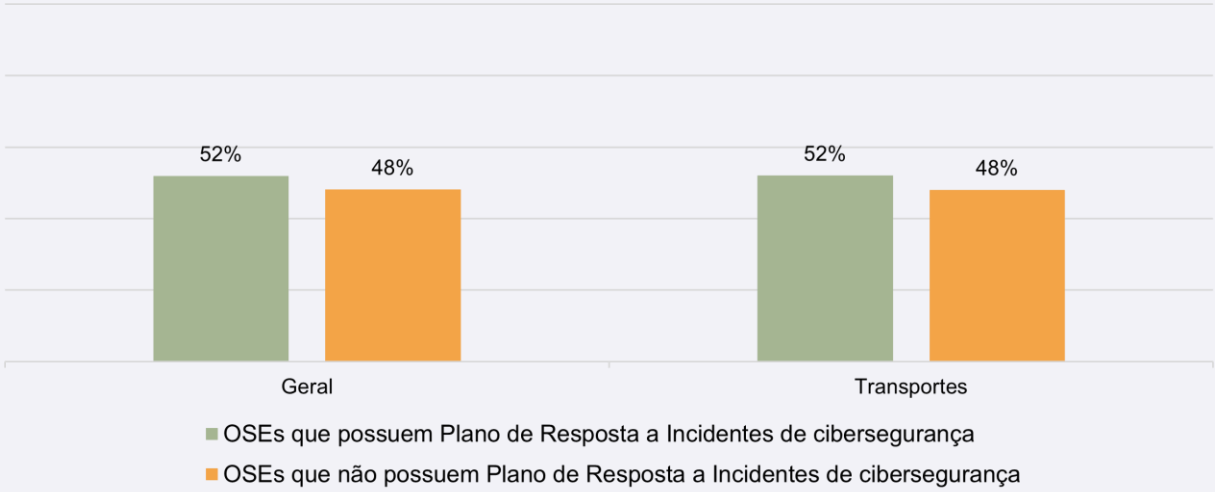
Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 97% submeteram-no ao CNCS. Destaca-se o setor dos transportes, no qual todos os operadores com relatório elaborado submeteram o mesmo ao CNCS.

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



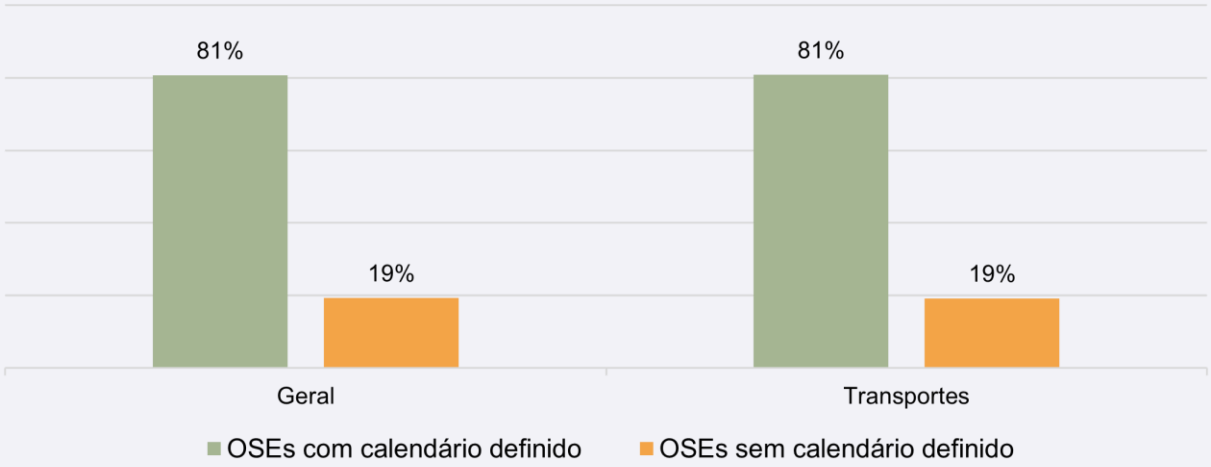
A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. Em destaque, o setor dos transportes, sendo um dos setores nos quais maior percentagem dos operadores realiza esta análise (77%).

Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança



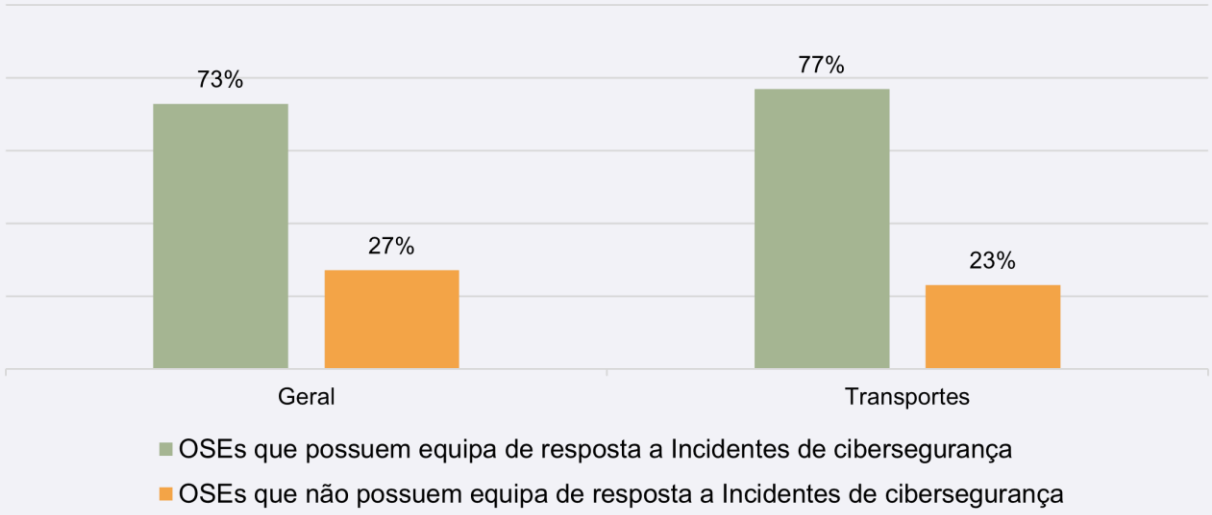
Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. Só nos setores dos transportes é que se verificam mais de 50% dos operadores com plano de resposta a incidentes.

Gráfico 101 - Definição de calendário para cumprimento das obrigações decorrentes do decreto-lei n. º65/2021, de 30 de julho



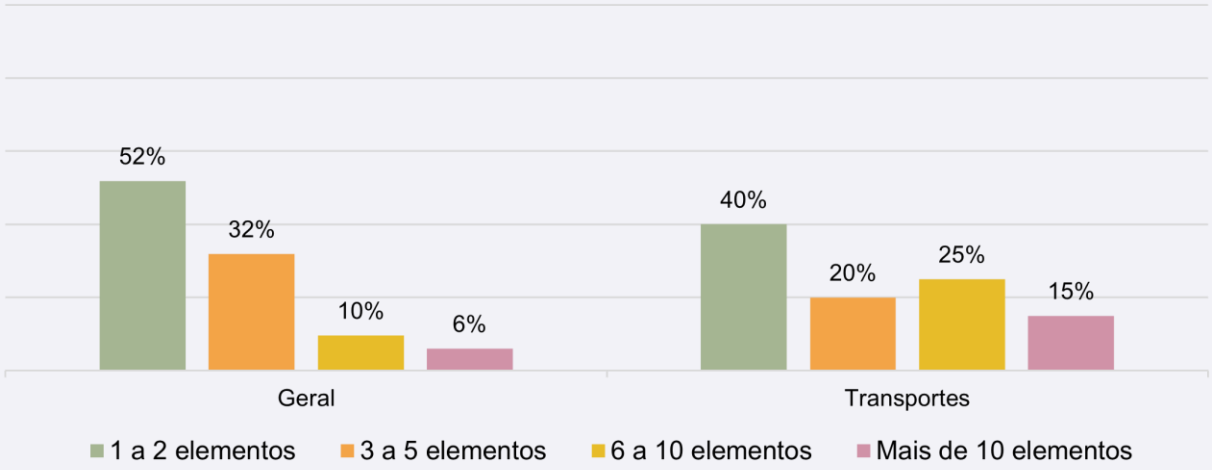
A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. No setor dos transportes, a percentagem de OSE sem calendário definido não ultrapassa os 19%. Há que salientar ainda que, tal como revelam os gráficos 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



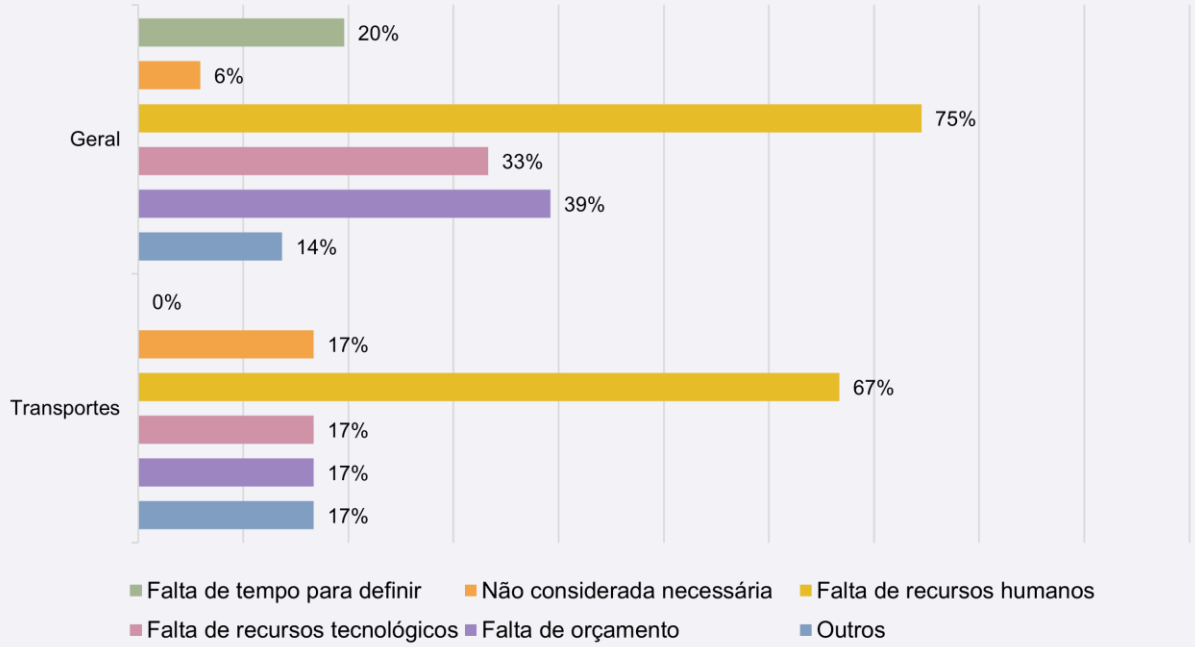
A nível geral, 73% dos operadores possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de operadores que possui tal equipa é sempre superior a 60%. Os operadores dos setores dos transportes ficam um pouco aquém desse limiar dos 80%, mas ainda acima dos 70%.

Gráfico 103 - 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%).
Em resumo, a composição das equipas de resposta a incidentes de cibersegurança tende a ser maioritariamente pequena.

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



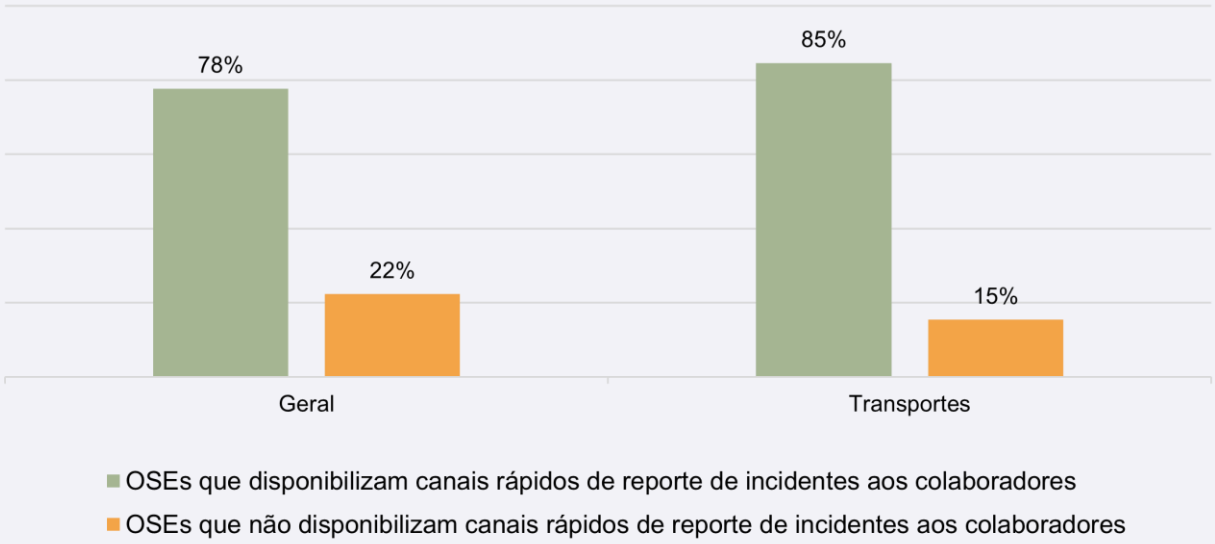
O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores.

A falta de tempo para definir a equipa surge com menos expressividade, sendo indicada por 20% dos operadores sem equipa.

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%.

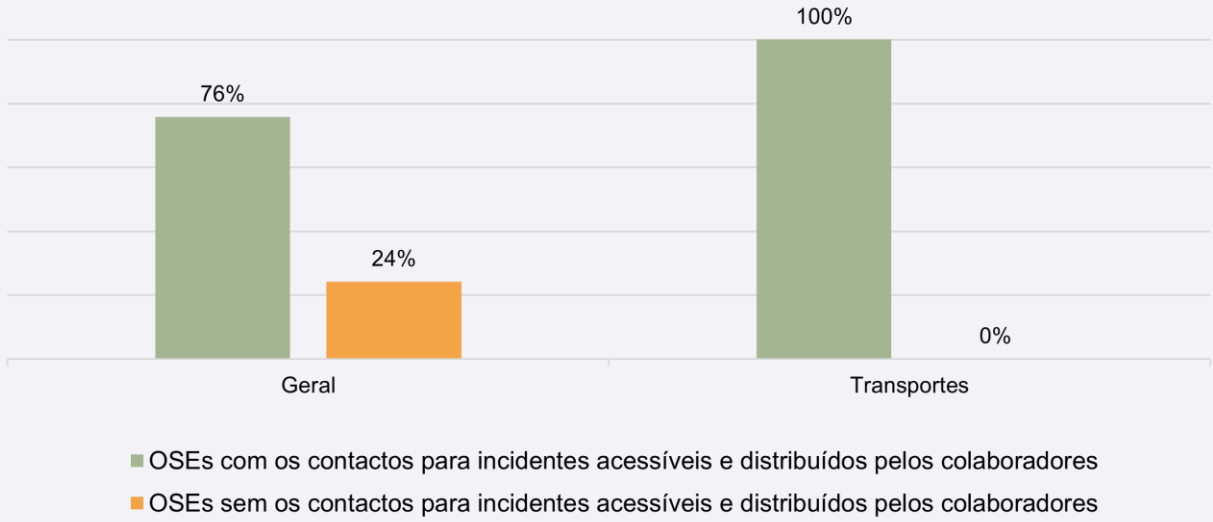
Os operadores que selecionaram a opção “outros” (14%) indicaram motivos tais como estar a ser planeada a criação da equipa, a equipa estar a receber formação, ou mesmo o descuido para com a área de cibersegurança.

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



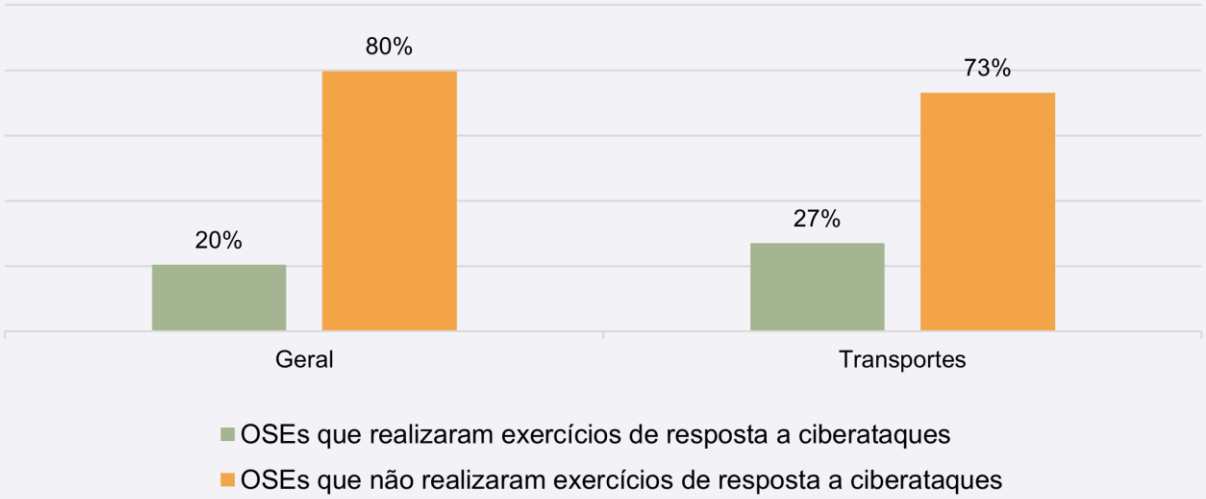
No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. O setor dos transportes, com 85%, apresentando assim um valor superior à média geral.

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



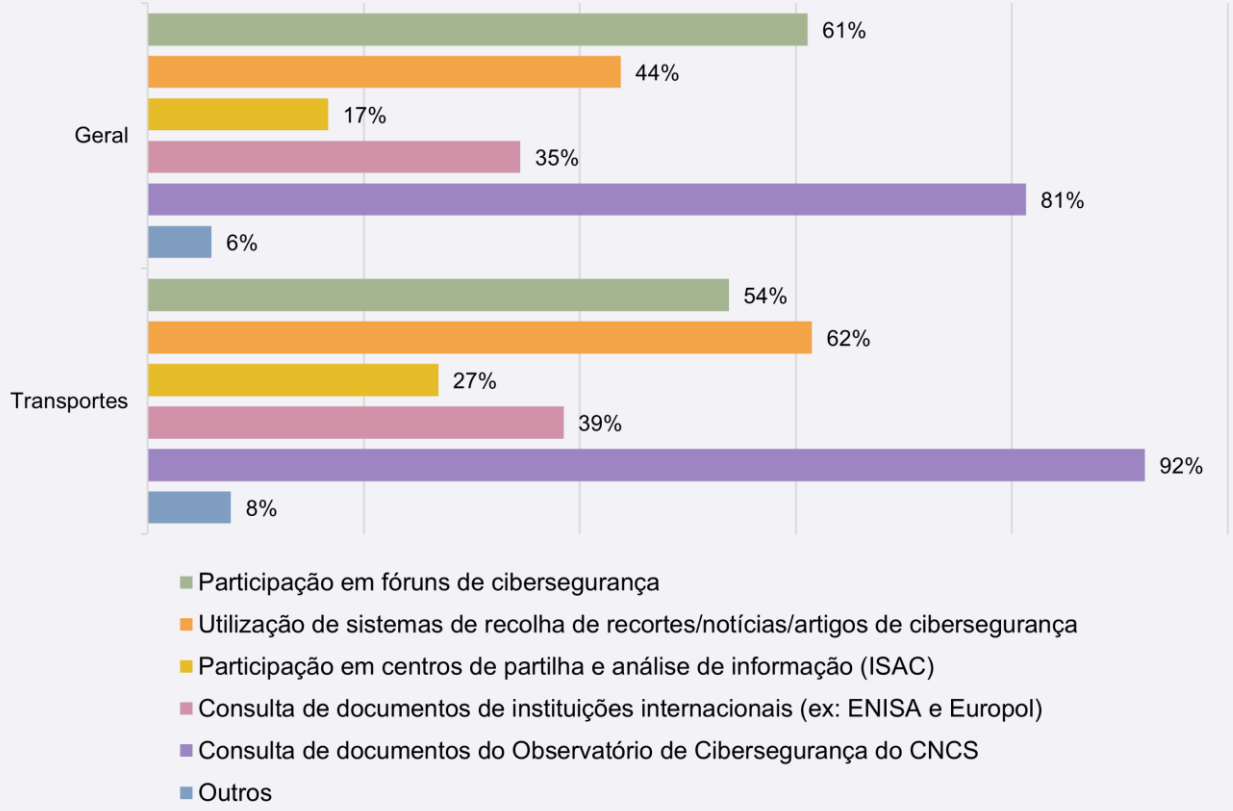
Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. Destaca-se o setor dos transportes, onde todos os inquiridos responderam positivamente a esta questão.

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. O setor dos transportes é o único onde ainda mais de 25% realizam tais exercícios.

Gráfico 108 - 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 comummente 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 ISACs[54]. 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.

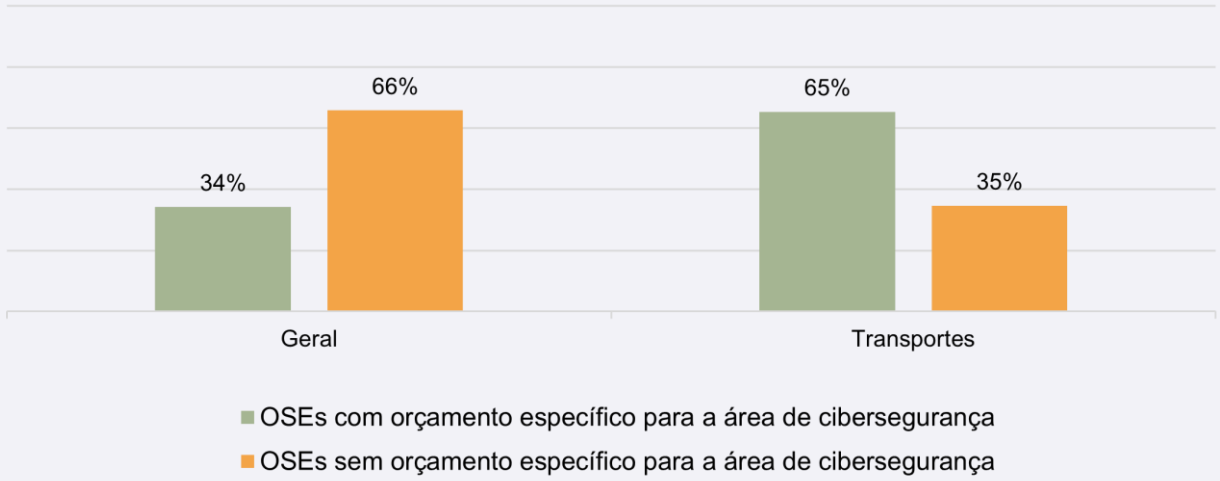
A baixa participação registada nos ISACs merece alguma reflexão. Estes centros de análise e partilha de informação "consistem em parcerias para troca de informação e experiência, assentes no pressuposto de que a partilha consistente de informação e análise de incidentes, ameaças, tendências e boas práticas favorece a resiliência digital individual e coletiva"[55].

[54] ENISA, "NIS Investments 2023", 59-61.
[55] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.

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 promotor[56].

Existem também diversos ISACs de nível europeu - no setor da energia, no setor dos transportes, havendo ISACs específicos para os subsetores 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 digitais[57]. 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*)[58]. 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 aplicável[59].

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, no setor dos transportes, são mais os operadores que possuem orçamento específico para essa área do que aqueles que não.

[56] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.

[57] Empowering EU ISACs, "European ISACs", https://www.isacs.eu/european-isacs.

[58] Exemplos retirados do European Energy Information Sharing & Analysis Centre (EE-ISAC), "Impact", https://www.ee-isac.eu/impact/#.

[59] Exemplo retirado do EE-ISAC, "Impact".

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 cibersegurança[60], 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 a ausência desses orçamentos específicos dificulta 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 cibersegurança[61]. 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 2023-2024[62]. 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 cibersegurança[63].

[60] ENISA, NIS Investments, 2021, 7-8.

[61] Comissão Europeia e Banco Europeu de Investimento, "European Cybersecurity Investment Platform", 2022, 29.

[62] 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.

[63] Conselho Europeu, "Horizonte Europa", https://www.consilium.europa.eu/pt/policies/horizon-europe/.

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

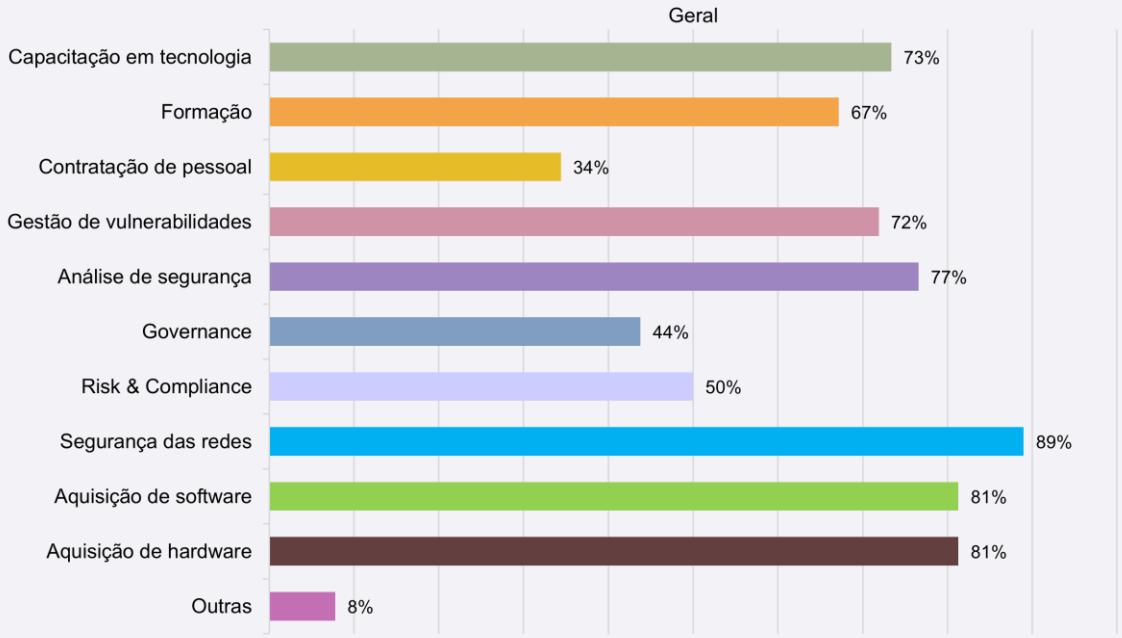
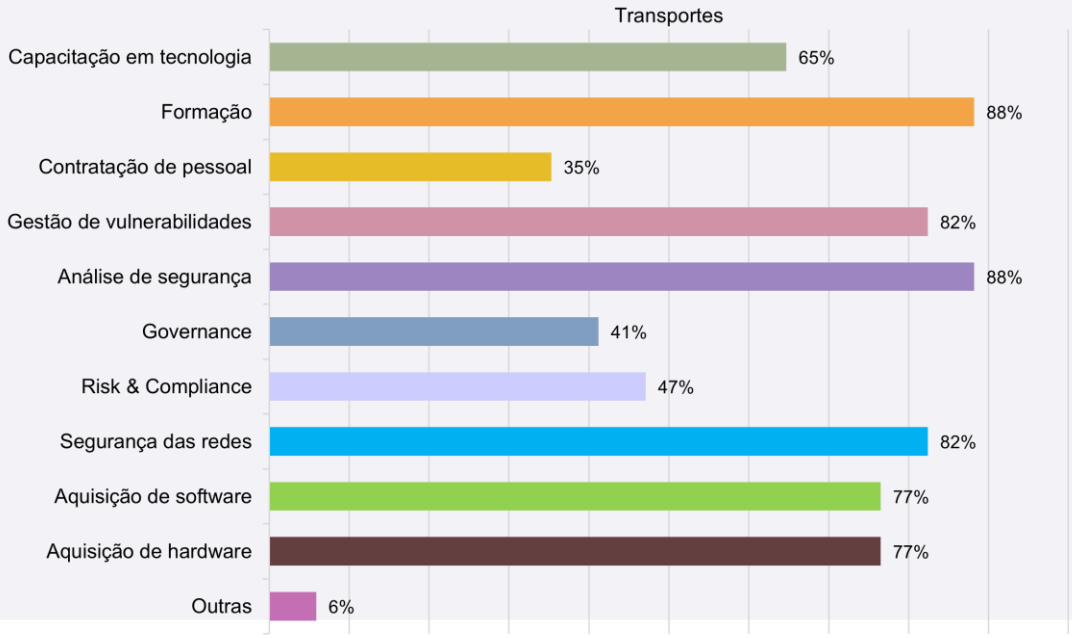


Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança



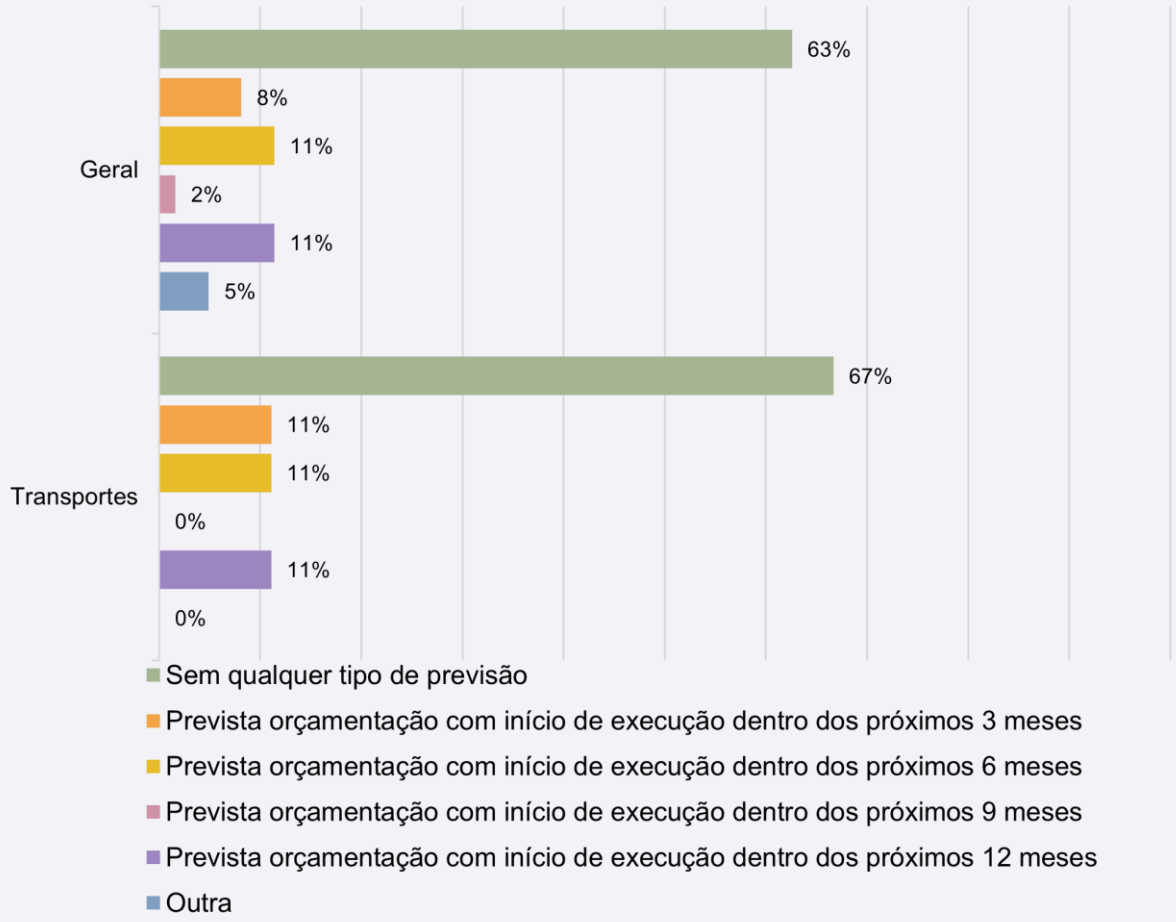
Entre os operadores que possuem orçamento específico para a cibersegurança, as áreas onde estes são mais comumente aplicados são a capacitação em tecnologia (73%), a formação dos colaboradores (67%), a gestão de vulnerabilidades (72%), análises de segurança (77%), *Risk &*

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[64].
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 entidades[65].

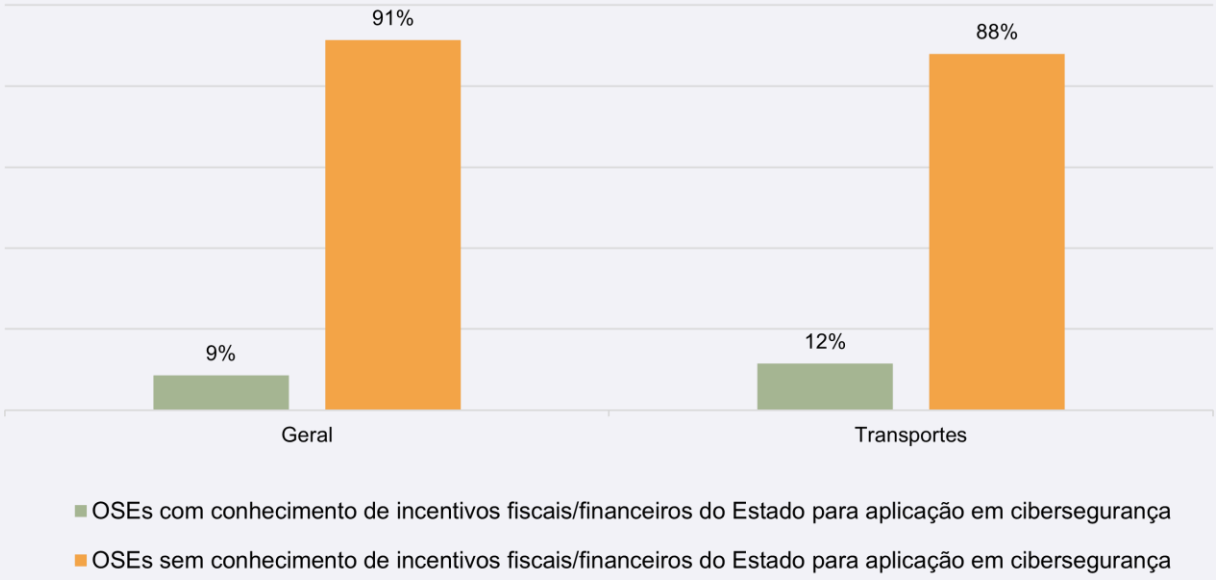
[64] ENISA, "NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist", 11 de dezembro de 2020, https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist.
[65] ENISA, "NIS Investments", 2023

Gráfico 111 - 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. No setor dos transportes, a previsão de vir a iniciar a execução de um orçamento específico para cibersegurança ainda durante o ano de 2024 existe para entre 11% 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

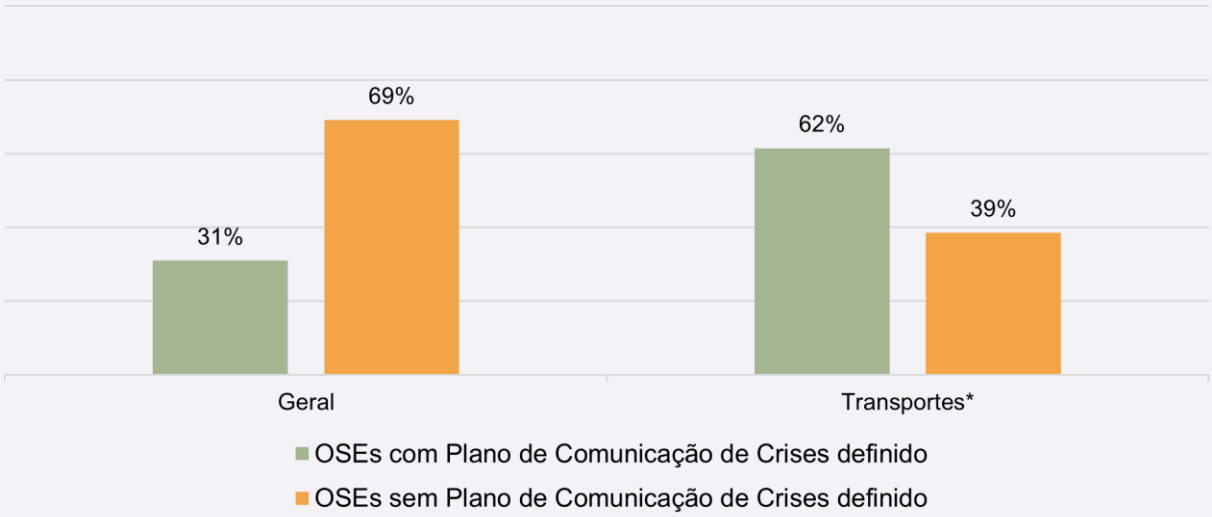


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No entanto, havia ainda alguns operadores no setor dos transportes, com conhecimento sobre tais incentivos.

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 cibersegurança[66].

[66] 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. Há que destacar setores como o dos transportes onde 62% dos operadores apresentam Plano de Crises definido.

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises

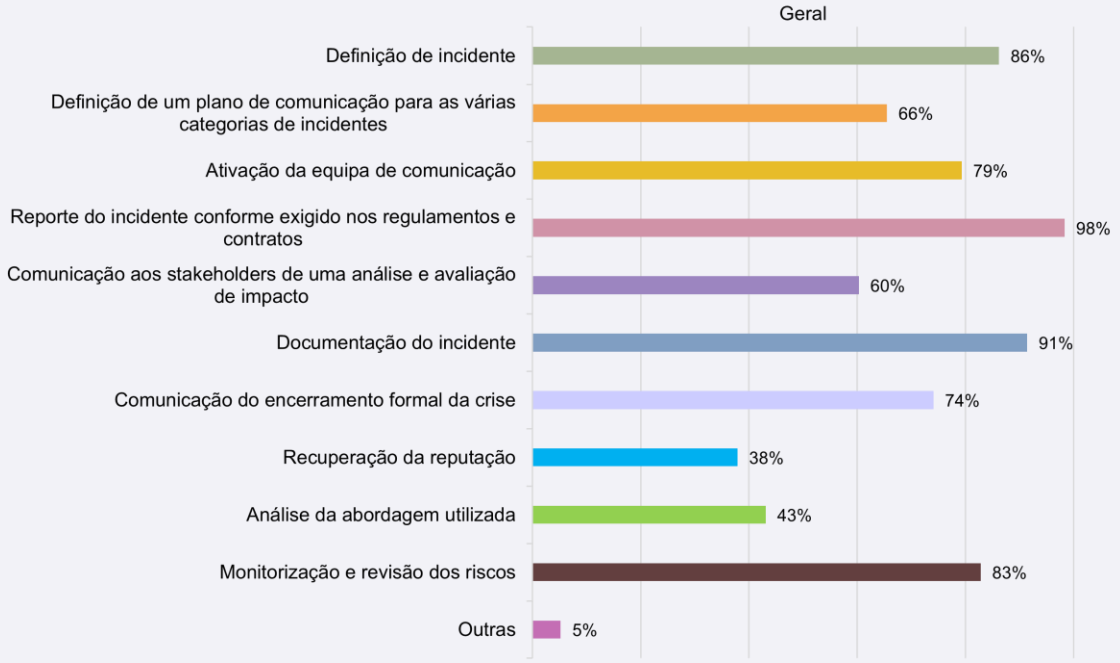
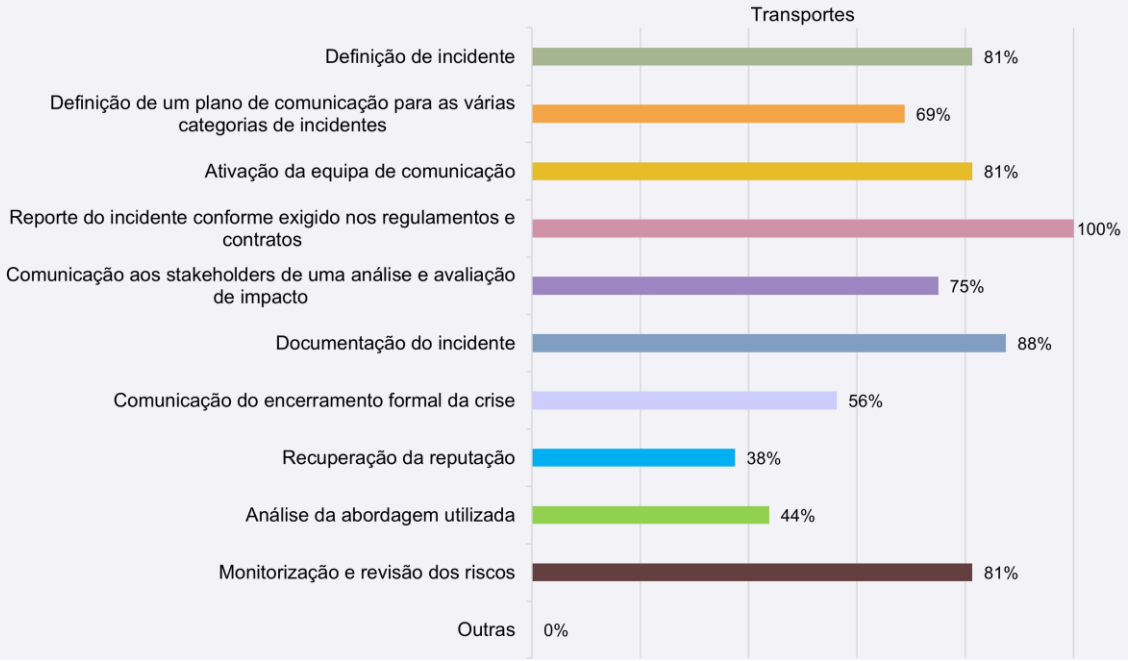


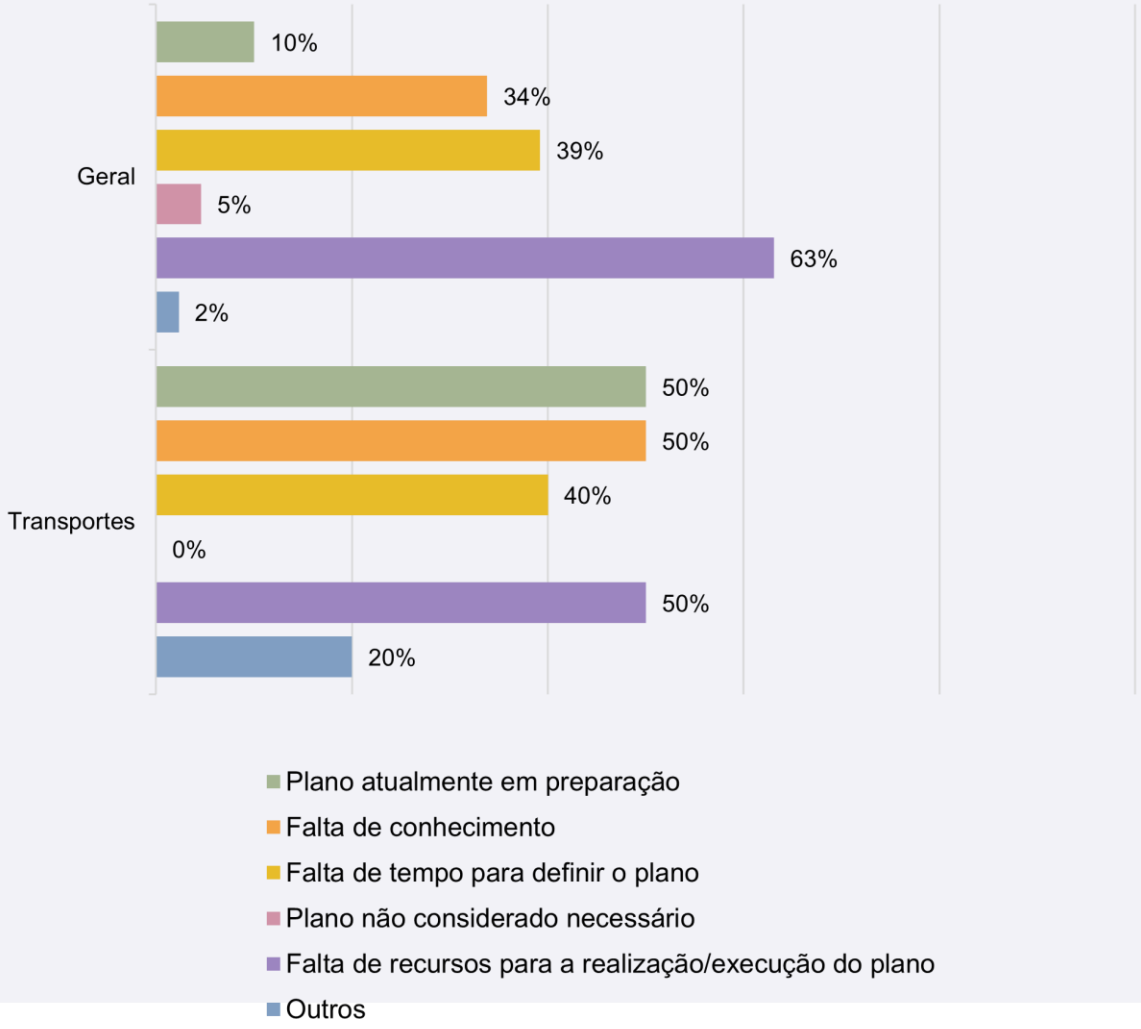
Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises



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.

Gráfico 115 - 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.

Análise Setorial

1. Transportes

1.1. Contextualização setorial

Geral

No âmbito da Diretiva 2016/1148[67] (NIS) e Lei n.º 46/2018[68], que transpõe a Diretiva e estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), o setor dos transportes abrange quatro subsetores: o transporte aéreo, o transporte marítimo, o transporte ferroviário e o transporte rodoviário. O setor dos transportes, bem como os quatro subsetores 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.

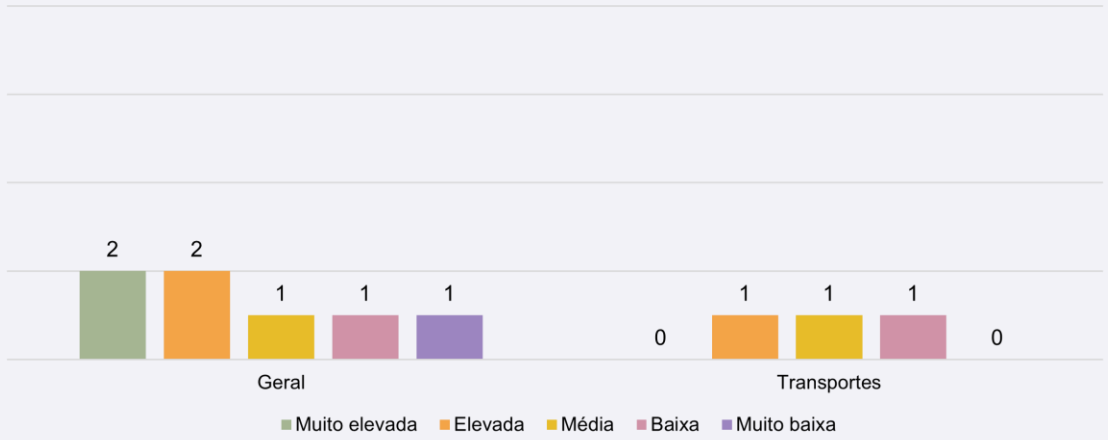
Todos estes transportes foram alvo de grande evolução ao longo de mais de um século, sendo-lhes integrados outros sistemas e mecanismos cada vez mais inteligentes, como por exemplo os de navegação. O crescimento e adaptação do **setor dos transportes** a processos e mecanismos inteligentes aumenta significativamente 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.

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**).

[67] 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

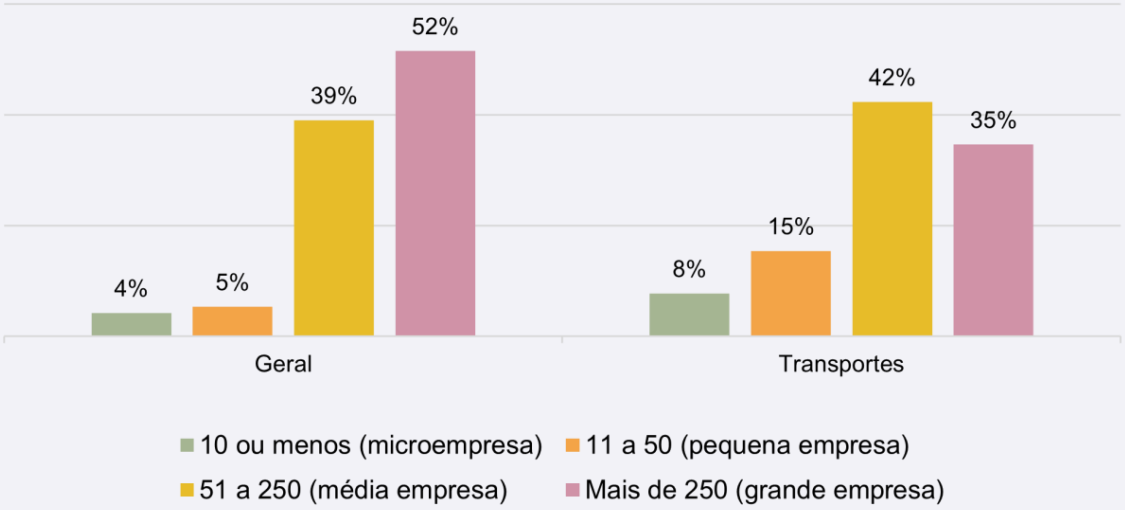
[68] Lei n.º 46/2018, de 13 de agosto, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.

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



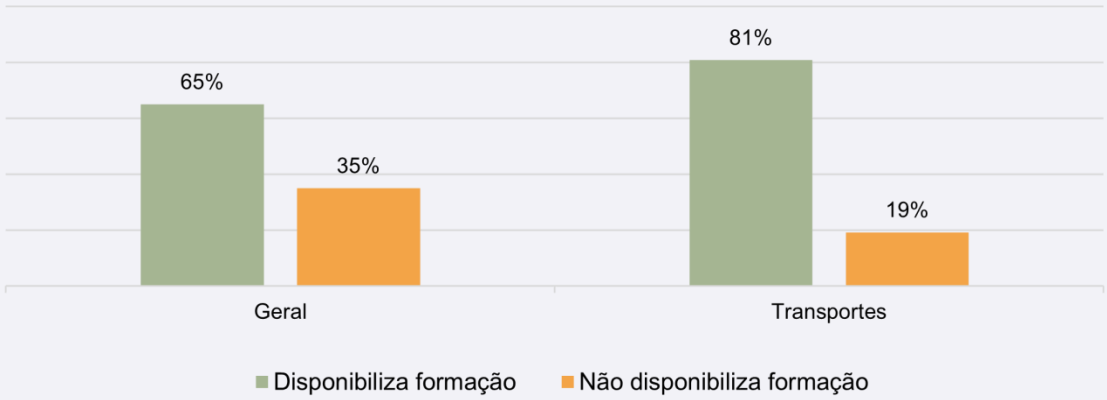
O tecido empresarial dos OSE do setor dos transportes é sobretudo composto por médias empresas, representando 42% dos operadores do setor, seguidas de grandes empresas com 35% e por fim pequenas e microempresas constituindo 23% dos operadores inquiridos. No âmbito geral, 52% dos OSE são grandes empresas, 39% são médias empresas e 9% são pequenas e microempresas (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



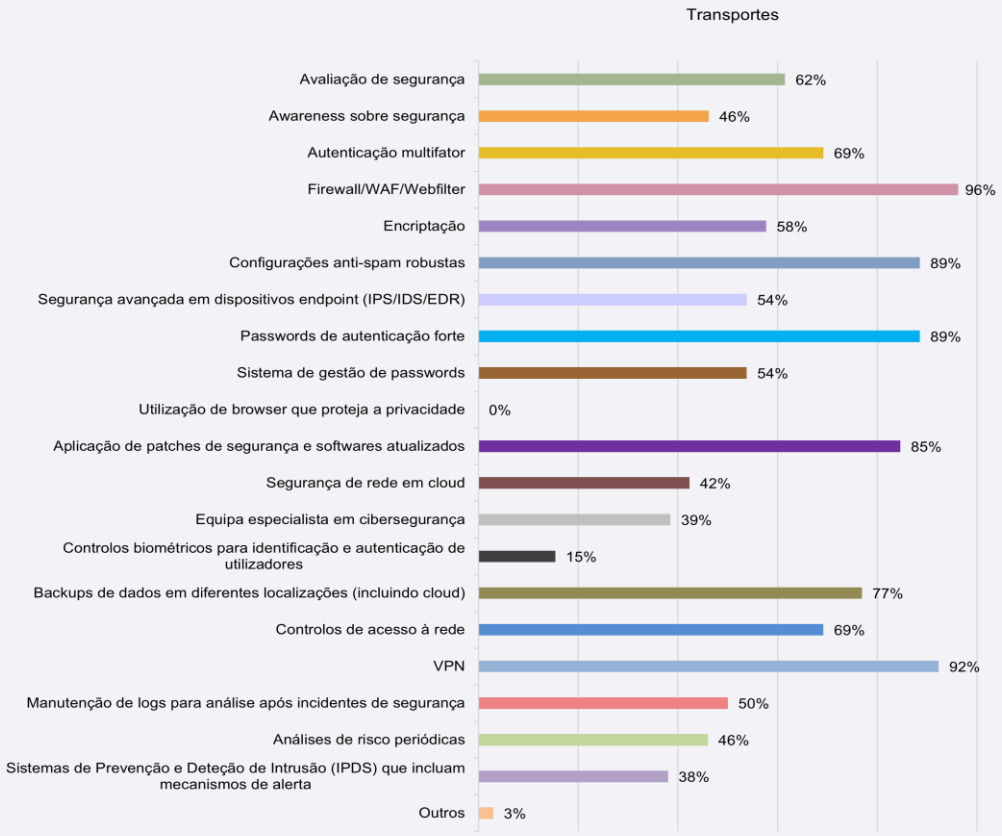
Esta perceção que pode ser suportada pelos 81% dos operadores que disponibiliza formação em cibersegurança aos seus colaboradores (vide **Gráfico 38**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



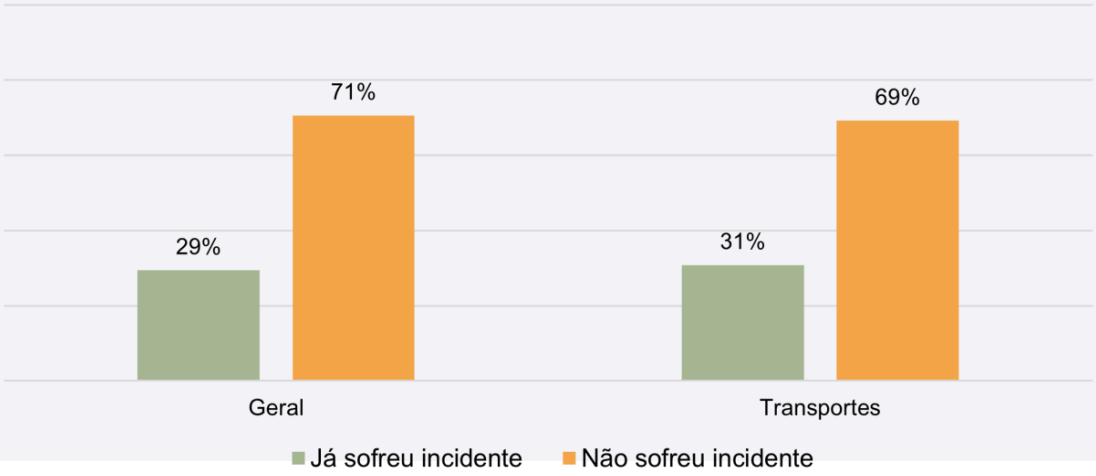
As medidas menos adotadas foram: Segurança de rede em *cloud* com 42%, Equipa especialista em cibersegurança com 39%, a implementação de controlos biométricos para identificação e autenticação com 15%, Análise de risco periódicas e *awareness* sobre segurança com 46% e Sistemas de Prevenção e Deteção de Intrusão (IPDS) com 38% (**Gráfico 66.2 A**).

Gráfico 66.2 A - Medidas de proteção contra ameaças de cibersegurança



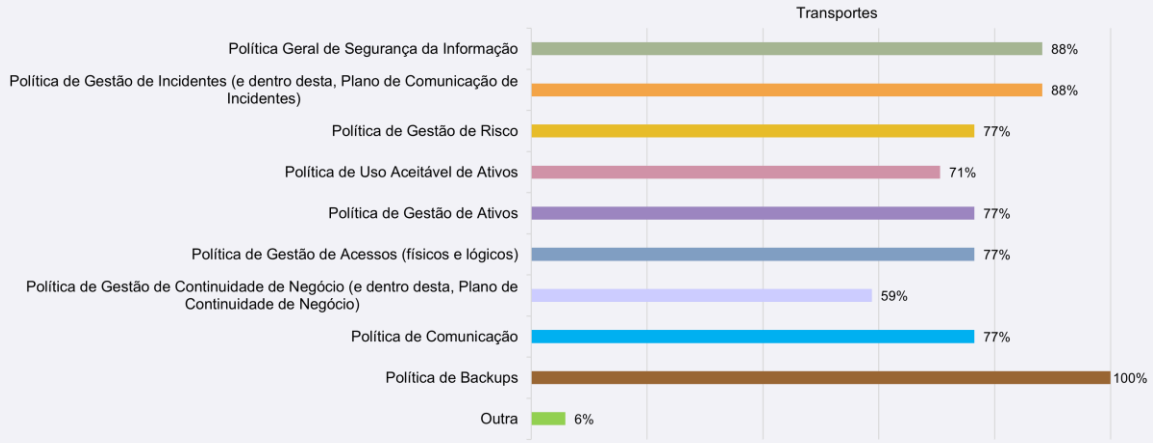
A taxa de incidência de incidentes de cibersegurança é apenas 2 p.p superior à média geral, onde 31% dos OSE sofreram incidentes em contexto TIC (**Gráfico 68**).

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



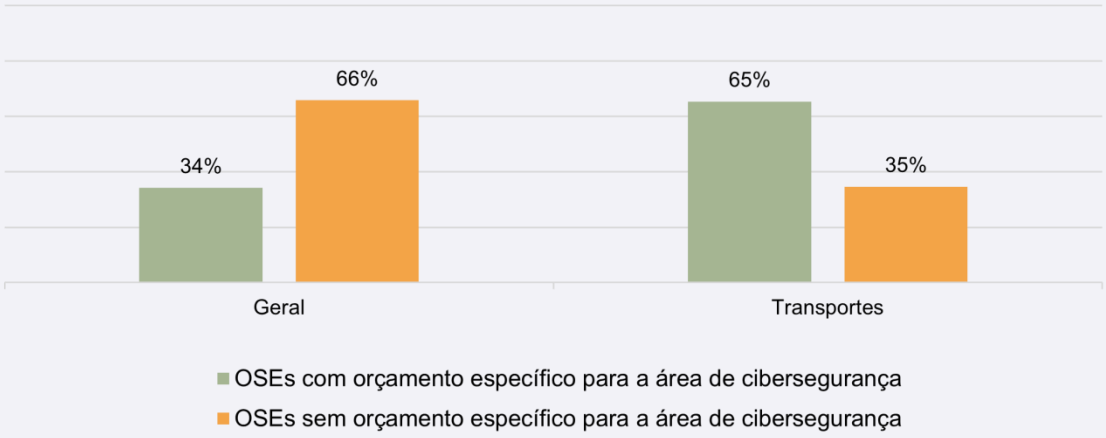
As políticas de cibersegurança e relacionadas menos implementadas foram: a política de gestão de continuidade de negócio com 59% e a política de uso aceitável de ativos com 71% (**Gráfico 79.2**).

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 antes[69]. 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)[70]. 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 Europa[71]. 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)[72].

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 janeiro[73].

[69] "Blériot XI", Museu do Ar, https://museudoar.pt/pagina-001.003.002.005-bl-riot-xi.
[70] 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/.
[71] 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.
[72] 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.
[73] Decreto-lei n.º 16:424, *Diário do Govêrno*, 26 de janeiro de 1929, https://files.diariodarepublica.pt/1s/1929/01/02200/02890290.pdf.

O Conselho Nacional do Ar foi a primeira estrutura formal e independente de regulação do setor do transporte aéreo no país[74]. A década de 30 via a aviação civil e comercial desenvolver-se.

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 1944[75] [76]. 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)[77]. 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 comercial[78].

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 1949[79].

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 computorizado 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 1996[80].

---

[74] "A nossa história", Autoridade Nacional da Aviação Civil (ANAC), https://www.anac.pt/vPT/Generico/ANAC/QuemSomos/Historia/Paginas/Historia.aspx.

[75] "A nossa história", ANAC.

[76] Decreto-lei n.º 33:967, *Diário do Govêrno*, 22 de setembro de 1944, https://files.diariodarepublica.pt/1s/1944/09/20800/09290931.pdf.

[77] "Cronologia", A Nossa História, TAP Air Portugal, https://www.tapairportugal.com/pt/a-nossa-historia/cronologia.

[78] "Cronologia", A Nossa História, TAP.

[79] "Cronologia", A Nossa História, TAP.

[80] "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 pessoas[81]. 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 reforma[82].

O setor do transporte aéreo tem continuado a evoluir e mantém-se, aos dias de hoje, como o meio de transporte mais seguro que existe[83], desempenhando um importante papel como uma força motriz da economia, gerando emprego e facilitando o grande comércio e turismo internacionais[84].

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 transporte[85].

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 navegar[86]. 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 continentes[87]. Atualmente, cerca de 80% do comércio mundial é realizado por transporte marítimo[88].

---

[81] "The Memorial", 9/11 Memorial and Museum, https://www.911memorial.org/visit/memorial.

[82] "Safeguarding and Securing Cyberspace", Press Release, News, CISA, 20 de julho de 2020, https://www.cisa.gov/news-events/news/safeguarding-and-securing-cyberspace.

[83] 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.

[84] Air Transport Action Group (ATAG) "Aviation: Benefits Beyond Borders", setembro de 2020, 4, https://atag.org/industry-topics/supporting-economic-social-development.

[85] 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.

[86] Nuno Pousinho, "A revolução do sistema de transportes", *RTP Ensina*, 2021, https://ensina.rtp.pt/explicador/a-revolucao-do-sistema-de-transportes-h70/.

[87] "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/.

[88] 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 317/89[89], de 22 de setembro. No mesmo ano, também foi criada a Direção-Geral dos Portos (DGP). Em 1993, através do Decreto-Lei n.º 319/93[90], 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) [91].

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 257/2002[92], 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/2012[93], 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 marítimo[94].

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 marítimos[95].

[89] Decreto-Lei n.º 317/89, de 22 de setembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/317-547635.
[90] Decreto-Lei n.º 319/93, de 21 de setembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/319-1993-655527.
[91] DGRM, "Breve História", https://www.dgrm.pt/breve-historia.
[92] Decreto-Lei n.º 257/2002, de 22 de novembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/257-2002-448755.
[93] 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.
[94] DGRM, "Breve História".
[95] 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 sistemas[96]. 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 comércio[97]. 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 decreto[98] 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/175[99], 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.

[96] James E. Vance e Thomas Clark Shedd, “Railroad history”, outubro de 2024, https://www.britannica.com/technology/railroad/Railroad-history.

[97] Nuno Pousinho, “A revolução do sistema de transportes”, *RTP Ensina*, 2021, https://ensina.rtp.pt/explicador/a-revolucao-do-sistema-de-transportes-h70/.

[98] Decreto-Lei n.º 143, de 26 de junho, *Diário da República*, https://legislacaoregia.parlamento.pt/V/1/35/9/p232.

[99] 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-B[100], 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 ferroviário[101]. 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 misto[102].

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 conetividade territorial e aumentar a descarbonização do setor dos transportes. Este projeto irá ter 3 fases[103]:

- **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 eficaz[104].

[100] Decreto-Lei n.º 299-B/98, de 29 de setembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/299-b-349923.
[101] Comboios de Portugal, "Cronologia da história dos caminhos de ferro em Portugal", https://www.cp.pt/institucional/pt/cultura-ferroviaria/historia-cp/cronologia.
[102] 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.
[103] Infraestruturas de Portugal, "Linha de Alta Velocidade Porto – Lisboa", https://www.infraestruturasdeportugal.pt/pt-pt/principais-investimentos/linha-de-alta-velocidade-porto-lisboa.
[104] 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"[105], tal como o Instituto da Mobilidade dos Transportes (IMT) ou as Infraestruturas de Portugal (IP), e operadores de sistemas de transporte inteligentes (STI)[106], 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 Paris[107]. 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 circulação[108]. 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 iniciar-se-ia 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"[109]. 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 estradas[110]. Também por esta altura começavam a surgir os primeiros transportes rodoviários coletivos, tendo, todavia, merecido menos atenção do Estado português nesta fase[111].

---

105 Diretiva (UE) 2016/1148, Anexo II, 28.

106 Diretiva (UE) 2016/1148, Anexo II, 28.

107 Ana Laura, "Os primeiros automóveis em Portugal", *RTP Ensina*, 1990, https://ensina.rtp.pt/artigo/os-primeiros-automoveis-em-portugal/.

108 "Regulamento sobre circulação de automóveis", Colecção Official de Legislação Portuguesa: Ano de 1901 (Lisboa: Imprensa Nacional, 1902), 701, in Parlamento: Legislação Régia, https://legislacaoregia.parlamento.pt/V/1/86/133/p733.

109 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.

110 Florbela Maré, "História das Infraestruturas Rodoviárias" (diss. mestrado, Universidade do Porto, 2011), 17, https://repositorio-aberto.up.pt/bitstream/10216/61562/1/000148960.pdf.

111 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 mesmas[112]. 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 concelhos[113]. 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[114] [115]. 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 estrada[116].

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 Abril[117], 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 terreno[118]. 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 1972[119]. 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.

---

[112] 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/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.

[113] Decreto-lei n.º 34:593: Plano Rodoviário, *Diário do Govêrno*, 11 de maio de 1945, https://files.dre.pt/1s/1945/05/10201/03730394.pdf.

[114] "História", A Carris, Carris, https://www.carris.pt/a-carris/historia/.

[115] "Origem", Sobre a STCP, STCP, https://www.stcp.pt/pt/institucional/sobre-a-stcp/origem/.

[116] Pacheco, "Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte", 126.

[117] Pacheco, "Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte", 128.

[118] Pacheco, "Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte", 129.

[119] "História", Sobre nós, Grupo Brisa, https://grupobrisa.pt/sobre-nos/historia/.

Entre 1969 e 1973, a cada ano havia cerca de mais 10 mil automóveis em circulação nas estradas portuguesas[120]. 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"[121]. 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 revisitar 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)[122]. A adesão formal à CEE, em 1986, juntamente como os novos fundos comunitários para o investimento em infraestruturas, terão sido a força motriz para uma nova fase de expansão da rede rodoviária em Portugal[123]. 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 é também nesta década que se conclui a ligação entre Porto e Coimbra e que se inaugura a primeira área de serviço em Portugal[124].

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 estacionamento[125]. Em 2014 é lançada a primeira aplicação móvel da Via Verde[126] 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 telemóvel[127]. Em 2016 a Via Verde lançava a aplicação Estacionar[128], com valências semelhantes à aplicação da EMEL.

[120] 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.
[121] Pacheco, "Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte", 130.
[122] Decreto-Lei n.º 380/85, de 26 de setembro, Diário da República, https://diariodarepublica.pt/dr/detalhe/decreto-lei/380-176998.
[123] Pacheco, "Alteração das Acessibilidades e Dinâmicas Territoriais na Região Norte", 135.
[124] "História", Grupo Brisa.
[125] "História", Grupo Brisa.
[126] "História", Grupo Brisa.
[127] "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/
[128] "História", Grupo Brisa.

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 ano[129]. 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 1.1.1. Impacto socioeconómico.

1.1.1. 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.

[129] "A Rede em Números", Infraestruturas, Infraestruturas de Portugal, https://www.infraestruturasdeportugal.pt/pt-pt/rede-rodoviaria-ip.

A tabela seguinte mostra a variação e evolução de alguns dos indicadores económicos e financeiros relevantes, em 2022[130]:

Tabela 5 - 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%

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 rendibilidade 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.

[130] Banco de Portugal, "Análise das empresas do setor dos transportes", 2022, https://bpstat.bportugal.pt/conteudos/publicacoes/1343.

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 subsetor 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 VVN[131].

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 públicos[132].

Dados de 2023 revelam que Portugal se encontra na 17º 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 tabela[133].

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 diminuiria[134].

[131] 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.
[132] "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
[133] Rui Martins, "Aumentar o uso dos transportes públicos", *Observador*, 2 de outubro de 2023, https://observador.pt/opiniao/aumentar-o-uso-dos-transportes-publicos/.
[134] 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 passageiros[135]. 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 toneladas[136]. O subsetor do transporte aéreo terá ainda tido, no mesmo ano, um volume de negócios na ordem dos 4,8 mil milhões de euros[137]. 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 setor[138]. 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 Portugal[139].

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 aeronaves[140]. 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 aeroporto[141]. 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 gravidez[142].

---

135 INE, “Estatísticas dos Transportes e Comunicações 2022”, novembro de 2023, 63.

136 INE, “Estatísticas dos Transportes e Comunicações 2022”, novembro de 2023, 65.

137 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

138 Banco de Portugal, “Análise das empresas do setor dos transportes”, BPstat, https://bpstat.bportugal.pt/conteudos/publicacoes/1343.

139 INE, “Estatísticas dos Transportes e Comunicações 2022”, novembro de 2023, 65.

140 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.

141 Seters, Grebe e Faber, “Health Impacts of Aviation”, maio de 2024, 36.

142 Seters, Grebe e Faber, “Health Impacts of Aviation”, maio de 2024, 24.

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 Luxemburgo[143]. Cerca de 15% da população estará sujeita a níveis de ruído médios na ordem dos 66,5 dB quando o máximo permitido por lei está fixado nos 55 dB[144]. 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 crianças[145].

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 toneladas[146]. 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 anterior[147].

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 EBITDA[148] nestes setores subiu 35,9% em 2022, após um crescimento de 31,85% em 2021[149].

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 GT[150]. No total, movimentaram-se cerca de 20 milhões de toneladas de mercadorias[151].

---

143 Lília Alexandre, "Mobilizar Rumo à Poluição Zero – Ruído", *Associação Zero*, janeiro de 2022, 15, https://zero.ong/wp-content/uploads/2023/06/MobilizAR-Ruido_.pdf.

144 Alexandre, "Mobilizar Rumo à Poluição Zero – Ruído, janeiro de 2022, 15.

145 Alexandre, "Mobilizar Rumo à Poluição Zero – Ruído, janeiro de 2022, 17-18.

146 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.

147 INE, "Estatística dos Transportes e Comunicações 2022", novembro de 2023, 8.

148 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).

149 Banco de Portugal, "Análise das empresas do setor dos transportes".

150 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).

151 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.

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 de 5,3%) e no tráfego nacional alcançou 2,9 milhões de toneladas diminuindo 11,4%[152]. Podemos dividir as mercadorias carregadas em sete categorias[153]:

- 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 categorias[154]:

- 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.

[152] INE, “TRANSPORTE DE PASSAGEIROS CONTINUOU A AUMENTAR NO 1º TRIMESTRE DE 2024”, 1.

[153] 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_ferroviario__total_e_por_principais_mercadorias_-_Continente_%282008-%29.xlsx.

[154] 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.

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 Iémen 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 Norte e a Europa, houve um aumento de 26% no tempo de trânsito, sendo a principal causa o colapso da ponte Francis Scott Key[155].

A proteção do transporte marítimo é assegurada globalmente por meio de normas estabelecidas no Decreto-lei n.º 226/2006[156], 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 simulacros[157].

[155] 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.
[156] Decreto-Lei n.º 226/2006, de 15 de novembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/226-2006-544783.
[157] 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.

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 passageiros[158]. 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 modalidade[159]. 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 nível[160].

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 km[161]. 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 euros[162].

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 internacional[163]. No total, no ano de 2022, foram transportadas cerca de 9,3 milhões de toneladas de mercadoria no transporte ferroviário, dos quais cerca de 6,6 milhões de toneladas é referente a tráfego nacional[164]. Podemos dividir as mercadorias transportadas em cinco categorias[165]:

- 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.

[158] AMT, "Transporte Ferroviário em Portugal – 2022", dezembro de 2023, 2,https://observatorio.amt-autoridade.pt/storage/100/8jtMIB1Gfmvaf20hBO1DofNpYO1DxF-metaRmVycm92aWFfMjAyMl9Ob3RhX2VzdGF0aXN0aWNhLnBkZg==-.pdf.

[159] INE, "Transportes e Comunicações 2022", novembro de 2023, https://www.ine.pt/xportal/xmain?xpgid=ine_inst_infografia&INST=637341691&xpid=INE.

[160] 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.

[161] 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.

[162] 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.

[163] INE, "Estatística dos Transportes e Comunicações 2022", 6.

[164] 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.

[165] 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_ferroviario__total_e_por_principais_mercadorias_-_Continente_%282008-%29.xlsx.

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 2016/798[166] 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, incluindo[167]:

- 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 2020/700[168] 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 como[169]:

- O quadro regulamentar é muito complexo e, devido a isso, é necessário colocar para esforços de forma a garantir os benefícios económicos e operacionais;
- 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-Alcafache, e é considerado o pior acidente ferroviário de que há memória em Portugal, tendo um grande impacto social.

---

166 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.

167 Eur-Lex,“ Segurança ferroviária à escala da União Europeia”,https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:320305_1.

168 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.

169 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.

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 controlo[170].

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%)[171].

Em 2023, Portugal Continental contava com aproximadamente 3 mil km de autoestradas[172], totalizando 14 339 km de estradas[173]. No ano anterior, 2022, foram exportadas 6 957 mil toneladas de cargas, sendo que Espanha foi o principal destino, recebendo 4 367 mil toneladas[174]. Quanto às importações, o volume total atingiu 7 767 mil toneladas, com a Espanha novamente em destaque, enviando 5 488 mil toneladas[175]. 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 tratores[176].

[170] Luciano Lourenço, “Alcafache: 30 anos depois”, maio de 2017, 102-115, https://www.riscos.pt/wp-content/uploads/2018/SRC_V/Ebook_Alcafache._30_anos_depois.pdf.
[171] INE, “Estatística dos Transportes e Comunicações 2022”, novembro de 2023, 6-7.
[172] 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.
[173] 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.
[174] 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.
[175] 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.
[176] 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.

Em 2023, registaram-se 34 974 acidentes de viação em Portugal, resultando em 43 495 feridos e 467 mortos[177]. No mesmo ano, ocorreram 4 873 atropelamentos de peões, dos quais 57 resultaram em mortos[178]. 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 mortos[179].

Os acidentes de viação geram anualmente elevados custos económicos, sociais e humanos, sendo crucial quantificá-los para informar políticas de segurança rodoviária em Portugal[180]. O custo económico e social dos acidentes rodoviários pode ser dividido em dois componentes:

- **Danos patrimoniais**: Incluí 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 vítimas[181].

1.1.2. 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 congestionamentos[182].

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 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 **1.2. Ameaças**.

---

[177] 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.

[178] 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.

[179] Ricardo Felner, "Maior choque de sempre", *Público*, fevereiro de 2000, https://www.publico.pt/2000/02/22/jornal/maior-choque-de-sempre-140333.

[180] 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.

[181] ANSR, "O Impacto Económico e Social da Sinistralidade Rodoviária em Portugal", outubro de 2021, 18.

[182] "Sistemas de Transporte Inteligentes", Infracontrol, https://www.infracontrol.com/pt-pt/sistemas-de-transporte-inteligentes-its/ .

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 aviação[183].

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 entidades[184].

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 mundo[185].

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 satisfatória[186].

[183] EASA, "Aviação sustentável: rumo a uma aviação com emissões zero", https://www.easa.europa.eu/pt/light/topics/sustainable-aviation-towards-zero-emission-aviation.
[184] EuroControl, "Automatic dependent surveillance – broadcast", https://www.eurocontrol.int/service/automatic-dependent-surveillance-broadcast.
[185] Flightradar24, "How flight tracking works", https://www.flightradar24.com/how-it-works.
[186] 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 possuí 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, previr 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 comportamento[187].

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 subsetor[188].

[187] EASA, “Artificial Intelligence and Aviation”, https://www.easa.europa.eu/en/light/topics/artificial-intelligence-and-aviation-0.
[188] 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*[189], cuja missão principal é fornecer, quase em tempo real, as localizações dos navios e iates, utilizando uma rede de recetores *Automatic Identification System*[190](*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 clientes[191].

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/2012[192], 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 eficiente[193].

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 2050[194].

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.

---

189 MarineTraffic, https://www.marinetraffic.com/.

190 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).

191 "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.

192 Decreto-Lei n.º 49-A/2012, de 29 de fevereiro, *Diário da* República, https://dre.pt/application/file/a/551481.

193 DGRM, "Sistema VTS", https://www.dgrm.pt/sistema-vts.

194 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.

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 real[195].

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 portuário[196].

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 eficazes[197].

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 navegação[198].

[195] 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.
[196] Luca Braidotti et al., "On the Automation of Ports and Logistics Chains in the Adriatic Region", setembro de 2020, 104-105.
[197] Luca Braidotti et al., "On the Automation of Ports and Logistics Chains in the Adriatic Region", setembro de 2020, 99.
[198] 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 2016/797[199], 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 ferroviárias[200].
- 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 níveis[201]:
- **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 velocidade[202].

[199] 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%3AOJ.L_.2016.138.01.0044.01.POR.

[200] 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.

[201] 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.

[202] 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 UE[203].

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 termo 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 adaptada[204]. 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 outros[205].

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 comboios[206].

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 combustível[207].

[203] 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.
[204] Siemens, “Connected Driver Advisory System (C-DAS)”, https://www.mobility.siemens.com/uk/en/portfolio/rail-infrastructure/connected-driver-advisory-system.html.
[205] UIC, “FRMCS: Future Railway Mobile Communication System”, setembro de 2023, https://uic.org/rail-system/telecoms-signalling/frmcs.
[206] 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.
[207] 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.

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 circulação[208].

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 emergência[209].

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 total[210]. 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 elétricos[211].

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 colisões[212].

---

[208] 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/.

[209] 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/.

[210] 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.

[211] Margarita Martínez-Díaz e Francesc Soriguera, “Autonomous Vehicles: theoretical and practical challenges”, Transportation Research Procedia, 2018, https://www.sciencedirect.com/science/article/pii/S2352146518302606.

[212] 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.

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 contribuí 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 tráfego[213].

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 inteligente[214]. 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 operacional[215].

Como mencionado anteriormente, a congestão do tráfego é um problema comum em grandes cidades. Esta situação resulta não apenas na perde 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 lugares[216].

[213] Intel, “Estradas Inteligentes Começam com Infraestrutura Inteligente”, https://www.intel.com.br/content/www/br/pt/transportation/smart-road-infrastructure.html.
[214] European Commission, “Smart Mobility”, https://transport.ec.europa.eu/transport-themes/smart-mobility_en.
[215] 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.
[216] 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.

1.2. Ameaças

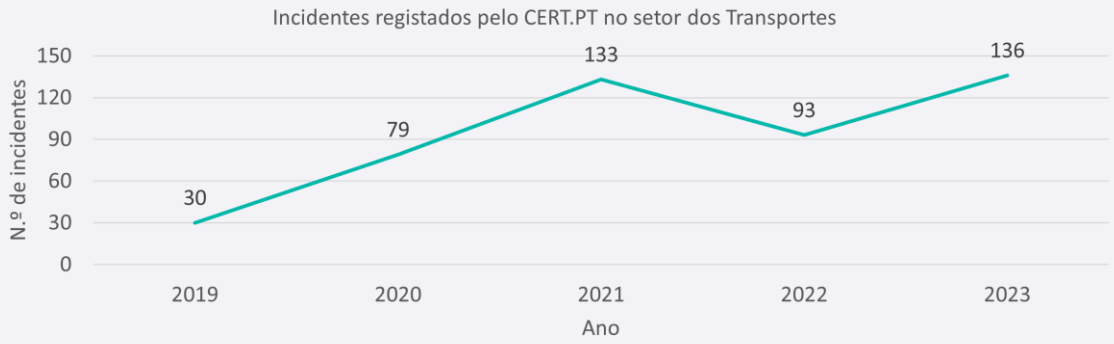
Quando se analisa as ameaças a que o **setor dos transportes** se encontra exposto, as consequências podem ir muito além de perdas financeiras ou materiais, podendo interferir na segurança humana. Esta é uma das principais razões que deve servir de base para que seja dada a devida importância e atenção 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 **1.1.2. 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 transportes[217].

Figura 1 - Número de incidentes no setor dos Transportes anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, Obtido a 10 de outubro de 2024, https://www.cncs.gov.pt/pt/estatistica/)

[217] 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 subsetores do transporte aéreo, marítimo, ferroviário e rodoviário. Cada um destes subsetores 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 subsetor é essencial, pois um incidente pode comprometer toda a cadeia, afetando desde os dados utilizados no desenvolvimento das infraestruturas até aos componentes eletrónicos das aeronaves[218].

Relativamente ao subsetor 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 subsetor 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 marítimos[219].

Nos subsetores do transporte ferroviário e rodoviário, a cadeia de abastecimento também é uma preocupação crescente devido à forte interligação entres os sistemas e à dependência da tecnologia nas operações diárias. Nestes subsetores, 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.

[218] 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.

[219] 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 abastecimento[220];
- **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 intelectual[221];
- ***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 inadequada[222].

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%[223]. Como mencionado anteriormente, este setor enfrenta ameaças constantes, tornando essencial a análise dos impactos de ataques passados para compreender possíveis incidentes futuros.

[220] Civil Aviation Cybersecurity Subcommittee, “Civil Aviation Supply Chain”, 6-7.
[221] Civil Aviation Cybersecurity Subcommittee, “Civil Aviation Supply Chain”, 13-14.
[222] Civil Aviation Cybersecurity Subcommittee, “Civil Aviation Supply Chain”, 15-16.
[223] ENISA, “ENISA Threat Landscape: Transport Sector”, março de 2023, 26, https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape.

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 evitada[224];
- 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 clientes[225];
- 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 indianas[226];
- 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 identificação[227];
- 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 clientes[228].

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-Russo[229].

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.

---

[224] "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/.

[225] Jane Wakefield, "EasyJet admits data of nine million hacked", *BBC*, 19 de maio de 2020, https://www.bbc.com/news/technology-52722626.

[226] Campbell Kwan, "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/

[227] 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.

[228] 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/.

[229] ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 28.

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 Cairo[230]. 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 terrestre[231].

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 Conflitos[232], 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 Estatal[233].
- **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 intuitos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa[234].
- ***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 responsável[235].
- **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* malicioso[236]. No caso, consideraram-se os colaboradores internos maliciosos.

---

230 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/.

231 ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 29.

232 CNCS, "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança, https://www.cncs.gov.pt/pt/observatorio/#relatorios.

233 CNCS, "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021", maio de 2021, 74, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf.

234 CNCS, "Relatório Riscos & Conflitos 2021", maio de 2021, 75.

235 CNCS, "Relatório Riscos & Conflitos 2021", maio de 2021, 75-76.

236 CNCS, "Relatório Riscos & Conflitos 2021", maio de 2021, 76-77.

Tabela 6 - Agentes de ameaça mais prováveis (Transporte Aéreo)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Ransomware	■	■	■	■
Malware	■	■	■	■
Vulnerabilidades	■	■	■	■
Phishing	■	■	■	
Acesso indevido a dados pessoais	■	■	■	■
DDoS		■	■	
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*, *phising*, intrusões, furto de credenciais, ataques *DDoS*, *spoofing*, vulnerabilidades nas cadeias de abastecimento e no geral[237].

[237] ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 30.

A ENISA também propõe uma taxonomia detalhada de ameaças, relacionando-as com os principais impactos de incidentes que podem ocorrer em ativos e serviços portuários[238]:

Tabela 7 - 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%[239].

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.

[238] ENISA, "Cyber Risk Management for ports - Guidelines for Cybersecurity in the Maritime Sector", dezembro de 2020, 17.
[239] 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 receitas[240];
- 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 supersónico[241];
- 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 dólares[242];
- 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 empresa[243];
- 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 proximidade[244].

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 leme[245].

[240] Port Economics, Management and Policy, "Petya Ransomware Cyber-Attack on Maersk", https://porteconomicsmanagement.org/pemp/contents/part2/digital-transformation/petya-ransomware-cyber-attack-maersk/.
[241] 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.
[242] Hydro, "Cyber-attack on Hydro", março de 2019, https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/.
[243] Maritime Cybersecurity, "Mediterranean Shipping Company (MSC) hit by a malware attack in Geneva, Switzerland", abril de 2020, https://maritimecybersecurity.nl/incident/KPgm1rZz5r.
[244] 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/.
[245] 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 8 - 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 abastecimento[246]. 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%[247].

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 indisponíveis[248].

[246] ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 33.
[247] ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 34.
[248] 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 ferroviários[249]:

Tabela 9 - 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%[250]. 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-Russia e anti-NATO, especialmente direcionados às companhias de transporte ferroviário. Alguns exemplos são:

- Em abril de 2022, um grupo pró-Russia lançou um ataque contra a operadora de transportes CFR Calatori, derrubando o *website* da companhia[251];
- Em junho do mesmo ano, o *website* da Lithuanian railways fica fora do ar, sendo o incidente reivindicado por atacantes russos[252];
- 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 Killnet[253].

[249] ENISA, "Railway Cybersecurity", novembro de 2021, 20.
[250] ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 34.
[251] 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.
[252] 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/.
[253] Vera Novais, "Estónia alvo de maior ciberataque desde 2007. Grupo russo reinvindica ataque", *Observador*, 18 de agosto de 2022, https://observador.pt/2022/08/18/estonia-alvo-de-maior-ciberataque-desde-2007-grupo-russo-reinvindica-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 comboios[254];
- 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 resgate[255];
- A Ucrânia, em 2017, sofreu um ataque aos seus sistemas do setor ferroviário, resultando na interrupção das operações, causando alguns atrasos nos comboios[256];
- 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 passageiros[257];
- A infraestrutura ferroviária belga foi alvo de um incidente de cibersegurança em 2021, este incidente afetou os sistemas dos comboios, levando a atrasos nos mesmos[258];
- 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 comboio[259].

[254] Carles Llorach, "Cyber-attacks received in the railway sector", Phoeniix, 2024, https://phoeni2x.eu/2024/02/29/cyber-attacks-received-in-the-railway-sector/.
[255] 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.
[256] 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/.
[257] "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/.
[258] 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/.
[259] "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 10 - Agentes de ameaça mais prováveis (Transporte Ferroviário)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Ransomware	■	■	■	■
Malware	■	■	■	■
Vulnerabilidades	■	■	■	■
Phishing	■	■	■	
DDoS		■	■	
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*, *phising*, intrusões, ataques *DDoS* e vulnerabilidades nas cadeias de abastecimento[260].

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 outros[261].

Tabela 11 - 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 *software*	Modificação do comportamento do *software* 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 diretos[262]. 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.

[260] ENISA, “ENISA Threat Landscape: Transport Sector”, março de 2023, 36.
[261] Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, “Conjunto de ferramentas de cibersegurança para o setor dos transportes”, 9.
[262] ENISA, “ENISA Threat Landscape: Transport Sector”, março de 2023, 38.

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 cibergurança, 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 manuais[263];
- 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 imediações[264]. 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 transportados[265].

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 desenvolvimento[266].

[263] ENISA, "ENISA Threat Landscape: Transport Sector", março de 2023, 36-37.

[264] 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.

[265] 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/.

[266] 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 12 - 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

1.3. 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"[267], enquadrado na Estratégia Nacional de Segurança do Ciberespaço (ENSC) de 2015 aprovada pela Resolução do Conselho de Ministros nº36/2015, 12 de junho[268].

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 vivemos[269].

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 setor[270].

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 dia[271].

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

[267] 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/.

[268] Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/36-2015-67468089.

[269] 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/.

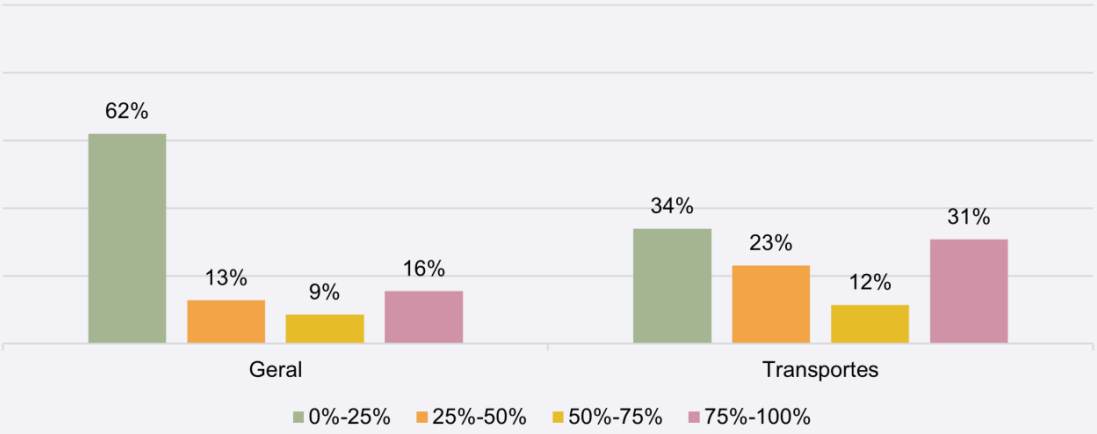
[270] AMT, "AMT promoveu debate sobre "Transição digital, ambiental e energética - impacto na gestão dos modelos de concessão"", 22 de novembro de 2022, https://www.amt-autoridade.pt/comunica%C3%A7%C3%A3o/not%C3%ADcias/amt-promoveu-debate-sobre-transi%C3%A7%C3%A3o-digital-ambiental-e-energ%C3%A9tica-impacto-na-gest%C3%A3o-dos-modelos-de-concess%C3%A3o/.

[271] 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/.

em estudo no presente relatório. A C-Academy tem como objetivo abranger 9,8 mil formandos até ao primeiro trimestre de 2026[272].

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.

[272] "C-Academy", Sensibilização e Formação, CNCS, https://www.cncs.gov.pt/pt/c-academy/.

A TAP também implementa autenticação multifator (MFA) e mantém uma equipa de gestão de incidentes disponível 24 horas, focada em detetar e responder a ameaças[273]. 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 cibersegurança[274].

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 cibersegurança[275].

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 internacional[276].

[273] 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.
[274] 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/.
[275] 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/.
[276] "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 informação[277]. 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 informáticas[278].

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 emergentes[279]. 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 euros[280].

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 colaboradores[281]. 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"[282].

---

[277] 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.
[278] CP, "Relatório do Governo Societário 2023", 145.
[279] Infraestruturas de Portugal, "A IP promove ações sobre Cibersegurança", outubro de 2019, https://www.infraestruturasdeportugal.pt/pt-pt/ip-promove-acoes-sobre-ciberseguranca.
[280] 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.
[281] 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.
[282] OPT, "Empresa", https://www.opt.pt/empresa/.

1.4. 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 local[283].

O programa "Horizonte 2020"[284] 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 inteligentes[285];

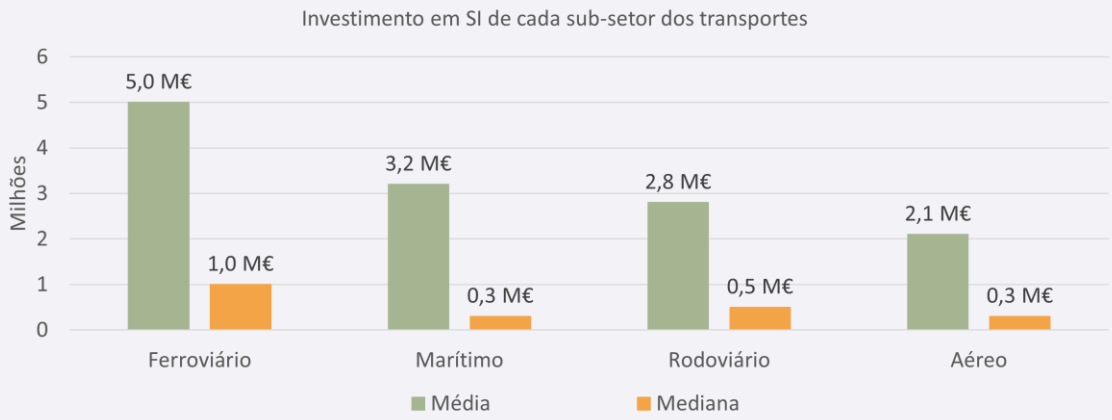
Consequentemente a todas estas iniciativas, projetos e implementações, cresce a relevância e preocupação relativamente à cibersegurança. Como já foi referido, a evolução tecnológica é acompanhada de crescimento de atividade maliciosa que pode resultar no efeito contrário ao pretendido pela implementação 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 UE[286].

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 ambientais[287]. 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-19[288].

[283] 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.
[284] 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.
[285] Comissão Europeia, "Tecnologias-chave para impulsionar a digitalização dos transportes", https://digital-strategy.ec.europa.eu/pt/policies/technologies-digitalisation-transport.
[286] Comissão Europeia, "Tecnologias-chave para impulsionar a digitalização dos transportes".
[287] Comissão Europeia, "European Digital Innovation Hubs", https://digital-strategy.ec.europa.eu/en/activities/edihs.
[288] 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 subsetores apresentam valores entre 300 mil e 500 mil euros de gastos com SI[289].

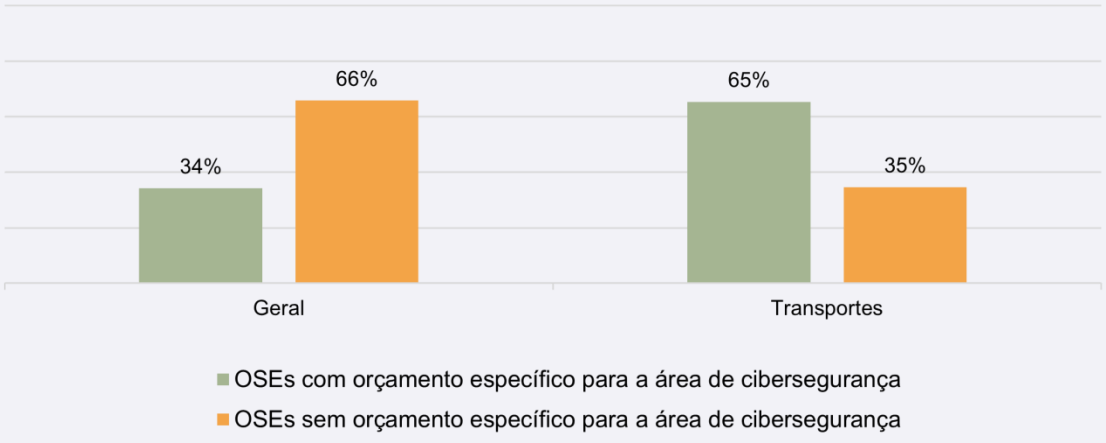
Figura 2 - Investimento em SI de cada subsetor dos transportes



(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



[289] 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 valore 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

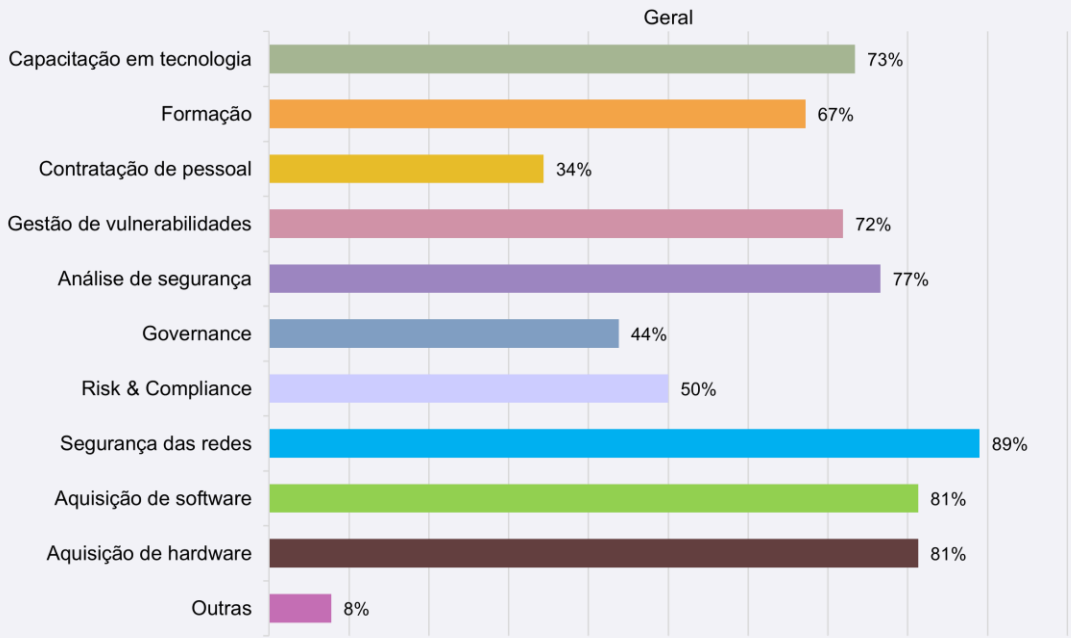
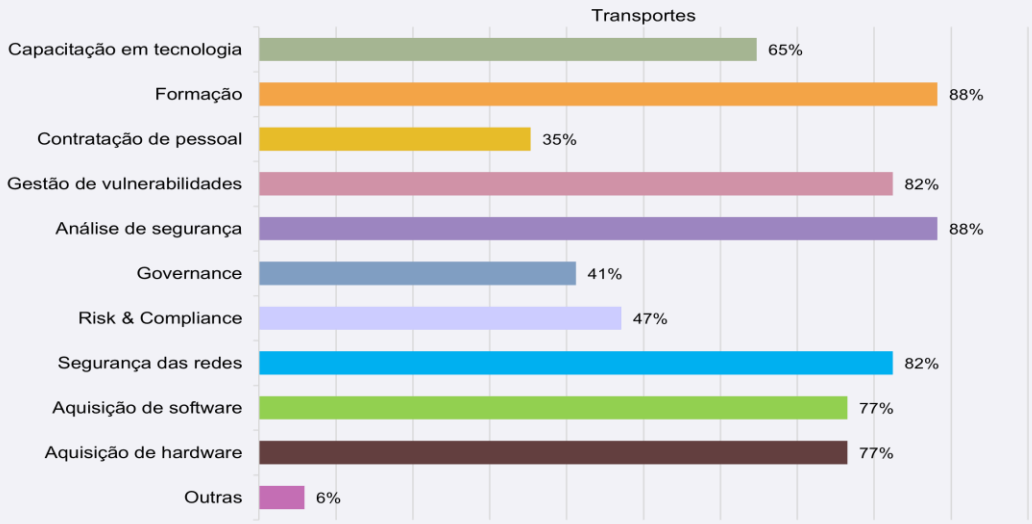
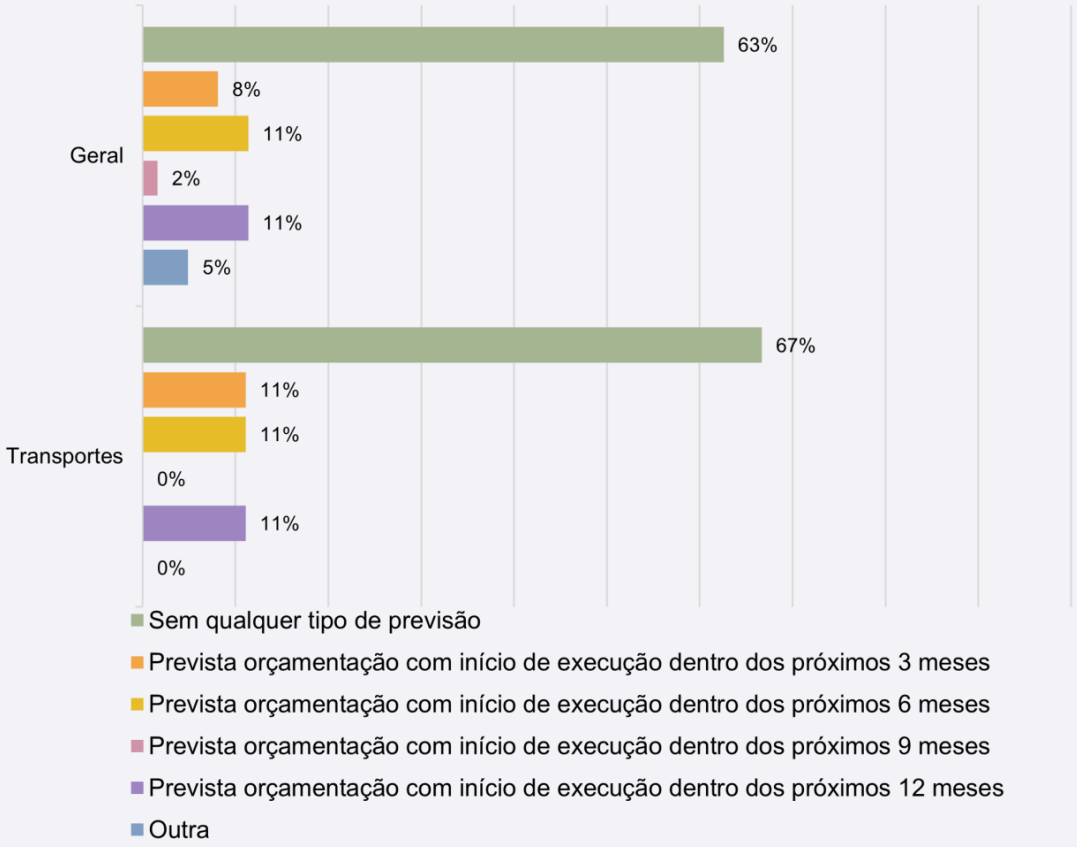


Gráfico 110.2 - Áreas de aplicação dos orçamentos específicos para cibersegurança



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 operações[290].

[290] 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 ativos[291].

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 navios[292].

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 dias[293].

Transporte Ferroviário

O Relatório de Governo Societário de 2023 estabelece como diretriz a ampliação da eficiência, segurança e sustentabilidade dos processos. Isto incluí 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 milhão[294].

[291] 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.

[292] 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.

[293] 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.

[294] 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.

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 empresa[295].

Transporte Rodoviário

No relatório do Governo Societário de 2023, observamos a contratação de serviços de consultoria em informática[296]. O Relatório e Contas de 2023 revelou um aumento no licenciamento de *software*, com um total aproximado de 2 milhões de euros[297]. 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 projetos[298]:

- 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 informáticos[299].

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 valores[300].

- 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 euros[301].

[295] 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.
[296] Carris, "Relatório Governo Societário 2023", março 2024, 87, https://www.carris.pt/media/3g1lrm01/relatorio-governo-societario-2023.pdf.
[297] Carris, "Relatório e Contas 2023", 116, https://www.carris.pt/media/lwsixqty/relatorio-e-contas-2023.pdf.
[298] Carris, "Plano de Atividades e Orçamento 2024", 20-22, https://www.carris.pt/media/4duh1ymp/carris_pao-2024-2027.pdf.
[299] Carris, "Relatório e Contas 2022", 61.
[300] Carris, "Plano de Atividades e Orçamento 2024", 20.
[301] Sociedade de Transportes Colectivos do Porto (STCP) "Instrumentos Previsionais de Gestão 2023-2027", 12 de setembro de 2022, 11.

1.5. RJSC e legislação setorial

Os OSE dos quatro subsetores 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 subsetores 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 civil[302]. 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 voos[303].

Este regulamento viria a ser revogado pelo Regulamento (CE) n.º 300/2008, de 11 de março[304] e, este, posteriormente revogado pelo Regulamento (UE) n.º 185/2010, de 4 de março[305], ambos ainda sem menções específicas à cibersegurança, segurança informática ou outras expressões associadas. Seria apenas com o Regulamento de Execução (UE) 2015/1988, 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 aviação[306]. 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 visadas[307].

---

[302] 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.

[303] Regulamento (CE) n.º 2320/2002, Anexo, 8.

[304] 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.

[305] 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.

[306] 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.

[307] 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.

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 Regulamento[308]. 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 à Europeia)[309].

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 operacional[310].

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)"[311]. 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"[312] 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"[313].

[308] Regulamento de Execução (UE) 2015/1998, 1-2.

[309] "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.

[310] 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.

[311] 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.

[312] 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.

[313] ANAC, "Plano Nacional de Segurança", 49.

Transporte marítimo e por vias navegáveis interiores

Um importante documento ao nível da segurança no subsetor 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 ISPS[314]. 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"[315]. 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 sistemas[316].

Em 2005, foi publicada a Diretiva 2005/65/CE, de 26 de outubro, relativa ao reforço da segurança nos portos[317]. 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 passageiros[318]. Seria depois transposta para o ordenamento jurídico português através do Decreto-Lei n.º 226/2006, de 15 de novembro[319].

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-Membros[320]. 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-membros[321].

---

[314] 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.

[315] Regulamento (CE) n.º 725/2004, Apêndice 2, 8.3.5.

[316] Regulamento (CE) n.º 725/2004, Artigo 3.º, n.º 8.

[317] 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.

[318] Diretiva 2005/65/CE, Anexo II, 36.

[319] Decreto-Lei n.º 226/2006, de 15 de novembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/226-2006-544783.

[320] 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.

[321] Regulamento (UE) 2019/1239, artigos 5.º, 10.º e 12.º.

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) 2017/2110[322]. 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)[323]. A DGRM deve ainda proceder a verificações periódicas e aleatórias do correto funcionamento dos sistemas de registo de dados[324].

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)[325]. 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"[326], 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 ferroviário[327]. 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"[328], bem como demonstrar a "forma como a empresa executa e mantém o sistema de gestão da segurança"[329] e demonstrar a "forma como a empresa controla a aplicação de regras técnicas de segurança e procedimentos para situações de emergência"[330].

[322] Decreto-Lei n.º 93/2020, de 3 de novembro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/93-2020-147432950.
[323] Decreto-Lei n.º 93/2020, artigo 29.º, n.º 2 e Capítulo II, Parte A, ponto 9.1.15.
[324] Decreto-Lei n.º 93/2020, artigo 29.º, n.º 3.
[325] Lei n.º 10/90, de 17 de março, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/10-1990-333167.
[326] Lei n.º 10/90, artigo 2.º, n.º 3.
[327] 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.
[328] Decreto-Lei n.º 270/2003, de 28 de outubro, *Diário da República*, artigo 14.º, alínea l).
[329] Decreto-Lei n.º 270/2003, artigo 14.º, n.º 2, alínea n).
[330] Decreto-Lei n.º 270/2003, artigo 14.º, n.º 2, alínea o).

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 Europeia[331], 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"[332].

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/UE[333], 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 veículos[334].

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 geral[335]. 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"[336].

[331] 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*, 1, 8 de setembro de 2023, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023R1695.

[332] Regulamento de Execução (UE) 2023/1695, Anexo I, 4.2.1.1. Segurança, 399.

[333] 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.

[334] Diretiva 2010/40/EU, artigos 10.º, Anexo 1, 4.1.

[335] 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.

[336] Regulamento (UE) 2019/2144, artigo 4.º, n.º 5, alínea d).

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"[337].

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 46/2018[338], 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)[339].

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 subsetores 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"[340], entre outros elementos.

[337] Regulamento (UE) n.º 2019/2144, artigo 11.º.
[338] Lei n.º 46/2018, de 13 de agosto, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
[339] Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.
[340] 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.

Passados seis anos sobre a publicação da Diretiva NIS, foi publicada a Diretiva (UE) 2022/2555[341], ou NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: "setores de importância crítica"[342] e "outros setores críticos"[343]. 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.

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. Quantos 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 mesmos[344]. 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 texto[345].

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"[346].

[341] 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

[342] Diretiva (UE) 2022/2555, Anexo I.

[343] Diretiva (UE) 2022/2555, Anexo II.

[344] Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

[345] Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

[346] Diretiva (UE) 2022/2555, artigo 29.º, n.º 1.

1.6. 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"[347]. 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 aéreo[348]:

Tabela 13 - Standards e Boas Práticas (Transportes Aéreo)

Standards	Boas práticas
• 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.

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 colaboradores[349];

[347] Comissão Europeia - Direção Geral da Mobilidade e dos Transportes, "Conjunto de ferramentas de cibersegurança para o setor dos transportes", 2.
[348] ENISA, "Mapping of OES Security Requirements to Specific Sectors", 18 de janeiro de 2018, 20.
[349] ICAO, "Aviation Security Manual (Doc 8973 – Restricted)", https://www.icao.int/security/sfp/pages/securitymanual.aspx.

- **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 comerciais[350].
- **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 críticos[351];
- **RTCA DO-326 Airworthiness security process specifications:** Estabelece especificações para processos de segurança relacionados com a aeronavegabilidade[352];
- **ISO 4170:1995:** Conjunto de normas que definem métodos de teste para determinar a resistência à corrosão de materiais metálicos utilizados nas estruturas das aeronaves[353];
- **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 desempenho[354];
- **ISO 24113:2023:** Fornece diretrizes para a avaliação e gestão de riscos relacionados com a segurança dos sistemas de informações aeronáuticos[355];
- **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 espacial[356];
- **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 seguros[357];
- **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 autorizados[358];
- **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 proteção[359].

[350] SAE International, “COMMERCIAL AIRCRAFT INFORMATION SECURITY CONCEPTS OF OPERATION AND PROCESS FRAMEWORK ARINC811”, dezembro de 2005, https://www.sae.org/standards/content/arinc811/.

[351] 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-aiss-framework-guidance/.

[352] RTCA, “Introducing RTCA's Security Standards and Training Partnership”, https://www.rtca.org/security/.

[353] ISO, “ISO 4170:1995”, https://www.iso.org/standard/20263.html.

[354] ISO, “ISO 6772:2012”, https://www.iso.org/standard/54516.html.

[355] ISO, “ISO 24113:2023”, https://www.iso.org/standard/83494.html.

[356] 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.

[357] 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.

[358] 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.

[359] 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 ferroviários[360].

Tabela 14 - 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.

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 informações[361];
- **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 riscos[362].
- **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 interessadas[363];

[360] ENISA, "Mapping of OES Security Requirements", 23.
[361] ISO, "ISO/IEC 27001:2022", https://www.iso.org/standard/27001.
[362] ISA, "ISA/IEC 62443 Series of Standards", https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
[363] ISO, "ISO 20138-2:2019",https://www.iso.org/standard/68443.html.

- **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 operações[364];
- **ISO 22888:2020:** Específica os requisitos para a gestão de risco em projetos de construção ferroviária[365];
- **ISO 27002 e 27005**: A ISO 27002 é focada em estabelecer, implementar, manter e melhorar a gestão da informação e a ISO é focada na gestão de risco[366];
- **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 ameaças[367];
- **CLC/TS 50701**: É uma norma técnica que fornece informações de cibersegurança nos sistemas do transporte ferroviário[368];
- **UK Rail Cyber Security Guidance to Industry:** Estabele orientações sobre cibersegurança para a indústria ferroviária, assim como proteger sistemas e dados contra ameaças de cibersegurança[369];
- **NIS Directive Cooperation Group guidelines**: Documento que resume as principais descobertas sobre medidas de cibersegurança para OSE[370].

[364] ISO, "ISO 22163:2023",https://www.iso.org/standard/79427.html.

[365] ISO, "ISO 22888:2020",https://www.iso.org/standard/74080.html.

[366] ENISA, "Railway Cybersecurity", 11.

[367] ISA, "ISA/IEC 62443 Series of Standards", https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[368] European Standards, "CLC/TS 50701:2023", https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/?srsltid=AfmBOorDKQDhbsSznI-J4WKrvDMc6xbxHRStGpKIGvUiP344XdenbQwR.

[369] 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.

[370] 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 marítimo[371]:

Tabela 15 - 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.

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 marítimas[372];
- **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 cibersegurança[373].

[371] ENISA, "Mapping of OES Security Requirements", 23-24.

[372] Clarksons, "What is the International Safety Management Code?", https://www.clarksons.com/glossary/international-safety-management-code.

[373] IMO, "Maritime cyber risk", https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

- **International Ship and Port Facility Security (ISPS) Code:** Estabelece medidas de segurança para proteger navios e portos contra atos de interferência ilícita[374];
- **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 informações[375];
- **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 riscos[376];
- **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 informações[377];
- **IEC 61162 - Digital interfaces for navigational equipment within a ship:** Define padrões para as interfaces digitais nos equipamentos de navegação a bordo de navios[378];
- **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 navios[379];
- **ISO 14885:2014 - Large yachts - Diesel engines for main propulsion and essential auxiliaries - Safety requirements:** Define requisites de segurança para motores a diesel utilizados em grandes iates, tanto para propulsão principal como para auxiliar[380];
- **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 cibersegurança[381];
- **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*[382];
- **Cyber-enabled ships: ShipRight procedure – autonomous ships**: Aborda as diretrizes de segurança para embarcações autónomas, focando-se na integração de tecnologias de cibersegurança[383];
- **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 marítimo[384];
- **United States coast guard – Cyber Strategy Draft guidelines on maritime cyber risk**

[374] LR, "ISPS Code", https://www.lr.org/en/services/statutory-compliance/isps-code.

[375] ISO, "ISO/IEC 27001:2022".

[376] ISA, "ISA/IEC 62443 Series of Standards".

[377] IEC, "IEC 62351-7", https://webstore.iec.ch/en/publication/30593.

[378] IEC, "IEC 61162-1:2024", https://webstore.iec.ch/en/publication/72729.

[379] ISO, "ISO 13613:2011", https://www.iso.org/standard/54090.html.

[380] ISO, "ISO 14885:2014", https://www.iso.org/standard/55259.html.

[381] 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.

[382] 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.

[383] LR, "Out of the box – Implementing autonomy and assuring AI", https://www.lr.org/en/knowledge/research-reports/2023/ai-and-autonomy/?creative=708188340864.

[384] 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/.

management: Aborda a gestão de riscos de cibersegurança no setor marítimo[385];

- **Tanker Management and Self Assessment 3 – OCIMF**: É uma *framework* com o objetivo de melhorar a gestão de navios *tank*[386];

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. A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor dos transportes rodoviários[387]:

Tabela 16 - Standards e Boas Práticas (Transporte Rodoviário)

Standards	Boas práticas
• 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;

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 dados[388];

[385] 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/.

[386] 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.

[387] ENISA, "Mapping of OES Security Requirements", 27.

[388] 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.

- **SAE J3101 - Requirements for Hardware- Protected Security for Ground Vehicle Applications (WiP):** Estabelece requisitos para a segurança no *hardware* dos veículos[389];
- **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 emissões[390];
- **ISO 15764: Road Vehicles - Extended data link security**: Define os padrões na segurança da ligação de dados nos veículos rodoviários[391];
- **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 veículo[392];
- **ISO 26262-1:2011 - Road vehicles - Functional safety:** Aborda a segurança funcional nos veículos rodoviários[393];
- **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 veículos[394];
- **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 dados[395];
- **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 automobilísticos[396];
- **ENISA Cyber Security and Resilience of smart cars:** Aborda os desafios e riscos associados à conectividade nos veículos modernos[397];
- **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 automobilística[398];
- **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 veículos[399];

---

389 SAE International, “Hardware Protected Security for Ground Vehicles”, https://www.sae.org/standards/content/j3101_202002/.

390 ISO, “ISO 15031-7:2013”, https://www.iso.org/standard/62489.html.

391 ISO, “ISO 15764:2004”, https://www.iso.org/standard/28775.html.

392 ISO, “ISO/SAE 21434:2021”, https://www.iso.org/standard/70918.html.

393 ISO, “ISO 26262-1:2011”, https://www.iso.org/standard/43464.html.

394 ETSI, “Intelligent Transport Systems (ITS)”, https://cdn.standards.iteh.ai/samples/59261/357d2dcaa38c4977b9b395c643b2114c/ETSI-TS-102-940-V2-1-1-2021-07-.pdf.

395 ETSI, “ETSI TS 103 096-3”, https://www.etsi.org/deliver/etsi_ts/103000_103099/10309603/01.04.01_60/ts_10309603v010401p.pdf.

396 ETSI, “ETSI TR 103 061-6”, https://www.etsi.org/deliver/etsi_tr/103000_103099/10306106/01.01.01_60/tr_10306106v010101p.pdf.

397 ENISA, “Cyber Security and Resilience of smart cars”, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

398 ISAC, “Best Practices”, https://automotiveisac.com/best-practices.

399 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.

1.7. 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)[400].

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 inteligentes[401].

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 críticas[402].

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 contínuas[403].

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 fraca[404].

---

[400] ENISA, “Securing Smart Airports”, 2016, 25.
[401] ENISA, “Securing Smart Airports”, 2016, 47
[402] ENISA, “Securing Smart Airports”, 2016, 48
[403] ENISA, “Securing Smart Airports”, 2016, 49
[404] 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 TO[405].

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 complexos[406].

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 sensíveis[407].

[405] ENISA, “ENISA Guidelines - Cyber Risk Management for Ports”, 2020,16-18.
[406] ENISA, “Railway Cybersecurity”, novembro de 2021, 18.
[407] 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 carbono[408].

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 veículos[409].

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 automóvel[410].

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 rodoviários[411]. 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 elétricos[412].

---

[408] 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.
[409] 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.
[410] 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.
[411] 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.
[412] International Energy Agency, "World Energy Outlook 2023", 200, https://iea.blob.core.windows.net/assets/ed1e4c42-5726-4269-b801-97b3d32e117c/WorldEnergyOutlook2023.pdf.

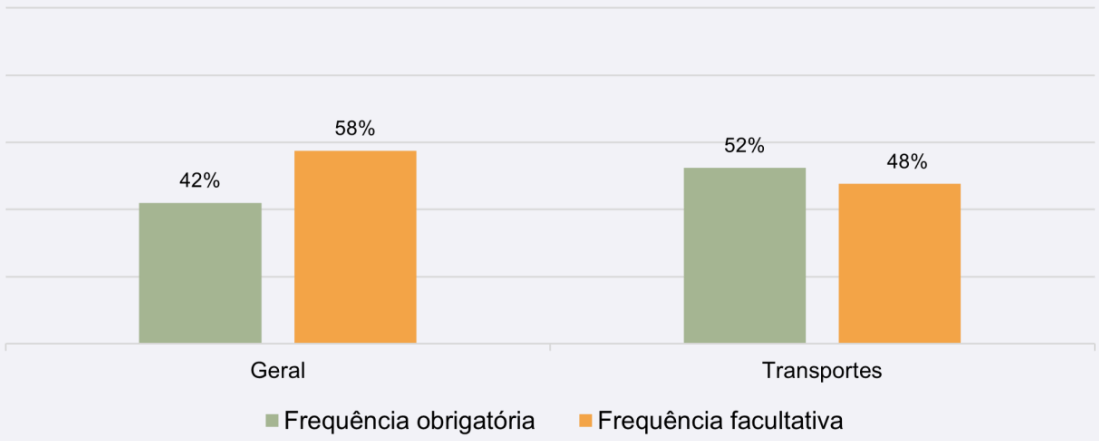
1.8. Recomendações

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 subsetores, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

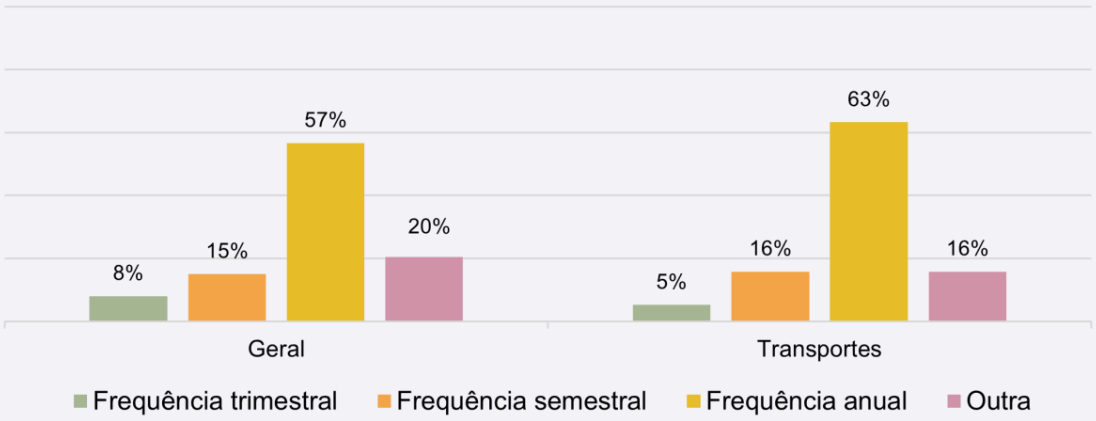
Como abordado inicialmente, os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor dos transportes disponibilizarem formação em cibersegurança aos seus colaboradores, quase metade das formações são de caráter facultativo, e não obrigatório (**Gráfico 39**).

Gráfico 39 - Caráter 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 Deteção 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 17 - 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 *phishing*, 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 Monitorização Contínua	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 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 *softwares* e sistemas de TI e TO minimiza o risco de exploração de vulnerabilidades conhecidas. Assegurar que componentes de *hardware*, 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 proactivamente, 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*[413].

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos[414]:

[413] Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 4.
[414] Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 6.

Tabela 18 - Controlos de Segurança da CIS (Transportes)

Categoria	Controlo de segurança
Controlos básicos	Inventário e Controlo de Ativos
	Inventário e Controlo de Ativos de *Software*
	Proteção de Dados
	Configuração Segura de Ativos e *Software*
	Gestão de Contas
	Gestão de Controlo de Acessos
	Gestão Contínua de Vulnerabilidades
	Gestão de Logs de Auditoria
Controlos fundacionais	Proteções de *e-mail* e de Navegadores
	Defesas Contra *Malware*
	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 *Software*
	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 indústria[415].

Tabela 19 - 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 *stakeholders* no desenvolvimento de *standards* específicos para soluções de cibersegurança; • Trabalhar com operadores aeroportuários para desenvolver produtos e/ou soluções alinhados com os requisitos mínimos de cibersegurança.

[415] 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 20 - 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 elas[416]:

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 setor[417]:

- 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 (EMSWe, 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."

[416] ENISA, "Guidelines - Cyber Risk Management for Ports", 2016, 14.
[417] 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 21 - 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-observatoriocibersegurancа-cncs.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)[418].

Algumas das medidas levantadas foram as seguintes:

- Sessões de sensibilização e formação (especialmente contra *ransomware* e *phishing*);
- Proteção de *endpoints*, segregação da rede e controlo de acessos em sistemas críticos;
- Adaptação de sistemas *legacy* (embora seja um grande desafio no que respeita à complexidade de atualização de sistemas com longos ciclos de vida);
- Realização de auditorias técnicas e auditorias de *governance* (ISO compliance);
- 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.

[418] ENISA, “Railway Cybersecurity”, 2020, 30.

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 22 - 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 *URL* malicioso ou *script* malicioso que direciona um colaborador 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.
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 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-observatoriocibersegurancа-cncs.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 seguintes[419]:

Tabela 23 - 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 *software* 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 *software*	● Instalar sempre *software* fidedigno; ● Atualizar sempre o *software* instalado em conformidade com as políticas e práticas de organização.

[419] 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 seguintes[420]:

Tabela 24 - Medidas de segurança (Transporte Rodoviário)

Âmbito	Medidas de segurança adaptadas
Governação	• Atribuir papéis e responsabilidades de gestão e comunicação em matéria de cibersegurança e segurança TI e TO; • Assegurar a governação da cibersegurança em toda a cadeia de prestação de serviços de segurança; • Definir mecanismos de governação para cumprimento regulamentar e legislativo.
Gestão dos riscos	• Identificar claramente vários sistemas de *hardware* e *software* 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.

[420] 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 25 - 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-observatoriocibersegurança-cncs.pdf)

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

- 9/11 Memorial and Museum. “The Memorial”. https://www.911memorial.org/visit/memorial.
- 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.
- Alexandre, Lília. “Mobilizar Rumo à Poluição Zero – Ruído”. Associação Zero, janeiro de 2022. https://zero.ong/wp-content/uploads/2023/06/MobilizAR-Ruido_.pdf.
- 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-metaRmVycm92aWFfMjAyMl9Ob3RhX2VzdGF0aXN0aWNhLnBkZg==-.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, “Utilização da Internet das Coisas (IoT - Internet of Things)”, 2022. https://www.anacom.pt/streaming/relatorioInternet_dasCoisas_IoT2022.pdf?contentId=1737940&field=ATTACHED_FILE.

- 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/.
- Autoridade Nacional da Aviação Civil (ANAC). “A nossa história”. https://www.anac.pt/vPT/Generico/ANAC/QuemSomos/Historia/Paginas/Historia.aspx.
- Banco de Portugal. “Análise das empresas do setor dos transportes”, BPStat, 2022. https://bpstat.bportugal.pt/conteudos/publicacoes/1343.
- 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.
- 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.
- 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.
- 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.
- Center for Internet Security. “The 18 CIS Critical Security Controls”, CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list.
- CISA. “Safeguarding and Securing Cyberspace”. Press Release, News, 20 de julho de 2020. https://www.cisa.gov/news-events/news/safeguarding-and-securing-cyberspace.
- 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.
- 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/cncs-ensc-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, ISAC. https://www.cncs.gov.pt/pt/isac/.
- CNCS. “C-Academy: Sensibilização e Formação”. https://www.cncs.gov.pt/pt/c-academy/.
- 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-observatoriocibersegurancacncs.pdf.
- CNCS. “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança. https://www.cncs.gov.pt/pt/observatorio/#relatorios.
- 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_Relatorio_Contas/2023/relatorio-governo-societario-2023.pdf.
- 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. “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. “Smart Mobility”. https://transport.ec.europa.eu/transport-themes/smart-mobility_en.
- 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 Europeu, “Horizonte Europa”. https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Conselho Europeu. “Cibersegurança: Como combate a UE as ciberameaças”. https://www.consilium.europa.eu/pt/policies/cybersecurity/.
- 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 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 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 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 Govêrno, 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 Govêrno. 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 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.
- 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 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. “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.
- 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) 2018/1972 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 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 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 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.
- 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.
- 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.
- Empowering EU ISACs, “European ISACs”. https://www.isacs.eu/european-isacs.
- 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, “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”, 2022. https://www.enisa.europa.eu/publications/nis-investments-2022.
- ENISA. “NIS Investments”, 2023. https://www.enisa.europa.eu/publications/nis-investments-2023.
- ENISA. “Cyber Security and Resilience of smart cars”. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
- ENISA. “ENISA Threat Landscape: Transport Sector”, março de 2023. https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape.
- 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. “NIS Investments”, 2021. https://www.enisa.europa.eu/publications/nis-investments-2021.

- 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. “ETSI TS 103 096-3”. 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-aiss-framework-guidance/.
- EuroControl. “Automatic dependent surveillance – broadcast”. https://www.eurocontrol.int/service/automatic-dependent-surveillance-broadcast.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), “Impact”. https://www.ee-isac.eu/impact/#.
- European Standards. “CLC/TS 50701:2023”. https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/?srsltid=AfmBOorDKQDhbsSznI-J4WKrvDMc6xbxHRStGpKIGvUiP344XdenbQwR.
- 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.
- Felner, Ricardo. “Maior choque de sempre”. Público, fevereiro de 2000. https://www.publico.pt/2000/02/22/jornal/maior-choque-de-sempre-140333.
- Flightradar24. “How flight tracking works”. https://www.flightradar24.com/how-it-works.
- ForeNova, “Cyber Threat Analysis Done the Right Way”. https://www.forenova.com/threat-detection/how-to-conduct-a-cyber-threat-analysis.
- Fórum Económico Mundial, “Global Cybersecurity Outlook 2024”, janeiro de 2024.
- Garmin, “Funcionalidades úteis que distinguem os pilotos automáticos Garmin”. https://www.garmin.com/pt-PT/garmin-technology/marine-technology/autopilot/advanced-autopilot-features/.
- 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/.
- 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.
- Hassanzadeh, Amin, Amin Rasekhb, Stefano Galellic, Mohsen Aghashahid, Riccardo Taorminae, Avi Ostfeldf e Katherine Banksg. “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.
- 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.

- https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=594883237&DESTAQUESmodo=2.
- Hydro. “Cyber-attack on Hydro”, março de 2019. https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/.
- 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.
- 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. “IEC 61162-1:2024”. https://webstore.iec.ch/en/publication/72729.
- IEC. “IEC 62351-7”. https://webstore.iec.ch/en/publication/30593.
- 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, “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. “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. “Metainformação”, janeiro de 2007, atualizado em junho de 2024. https://www.ine.pt/bddXplorer/htdocs/minfo.jsp?var_cd=0002613&lingua=PT.
- 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.

- 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 Energy Agency. “World Energy Outlook 2023”. https://iea.blob.core.windows.net/assets/ed1e4c42-5726-4269-b801-97b3d32e117c/WorldEnergyOutlook2023.pdf.
- 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.
- 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, “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- 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/SAE 21434:2021”. https://www.iso.org/standard/70918.html.
- 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.
- Kontas, Vasilis. “What is the Automatic Identification System (AIS)?”, MarineTraffic. https://support.marinetraffic.com/en/articles/9552859-what-is-the-automatic-identification-system-ais.
- 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 46/2018, de 13 de agosto, Diário da República. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- 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/.
- Llorach, Carles. "Cyber-attacks received in the railway sector", Phoeniix, 2024. https://phoeni2x.eu/2024/02/29/cyber-attacks-received-in-the-railway-sector/.
- Lourenço, Luciano. "Alcafache: 30 anos depois". Riscos, maio de 2017. https://www.riscos.pt/wp-content/uploads/2018/SRC_V/Ebook_Alcafache._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/.
- 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/KPgm1rZz5r.
- 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/.
- 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.

- 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/.
- 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.
- Novais, Vera. “Estónia alvo de maior ciberataque desde 2007. Grupo russo reinvindica ataque”. Observador, 18 de agosto de 2022. https://observador.pt/2022/08/18/estonia-alvo-de-maior-ciberataque-desde-2007-grupo-russo-reinvindica-ataque/.
- 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/.
- 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.
- 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.
- OPT, “Empresa”. https://www.opt.pt/empresa/.
- 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.
- 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, “Empresas: total e por dimensão”, dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- 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. “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. “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_ferroviario__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. “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. “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*gu9zgo*_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/.
- 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/.

- 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/.
- 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) 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) 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 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 sobre circulação de automóveis. Colecção Official de Legislação Portuguesa: Ano de 1901. Lisboa: Imprensa Nacional, 1902, in Parlamento: Legislação Régia. https://legislacaoregia.parlamento.pt/V/1/86/133/p733.
- 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. “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/.
- 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.
- RTCA. “Introducing RTCA's Security Standards and Training Partnership”. https://www.rtca.org/security/.
- 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/.
- 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/.
- 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.
- Siemens. “Connected Driver Advisory System (C-DAS)”. https://www.mobility.siemens.com/uk/en/portfolio/rail-infrastructure/connected-driver-advisory-system.html.
- 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.
- STCP. “Origem”. Sobre a STCP. https://www.stcp.pt/pt/institucional/sobre-a-stcp/origem/.
- Sulaiman Asif, “Cyber Threat Analysis: Types, Benefits, Tools, Approaches”, Knowledge Hut, September 5, 2023. https://www.knowledgehut.com/blog/security/threat-analysis.
- 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/.
- 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.
- 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/.
- 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.
- 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.
- Vance, James e Thomas Shedd. “Railroad history”, outubro de 2024. https://www.britannica.com/technology/railroad/Railroad-history.
- 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.
- 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.
- World Bank. “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.
- 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/

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Observatório
de **Cibersegurança**

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU