CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de **Cibersegurança**

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

Infraestruturas Digitais

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].

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

[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).

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 OSEs, 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 OSEs 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 OSEs.

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 OSEs, indicando setores e subsetores a incluir, bem como realizando remissões para outras Diretivas de modo a caracterizar o tipo de entidades a considerar.

[4] Lei n.º 46/2018, artigo 3.º, alínea g).
[5] Lei n.º 46/2018, artigo 3.º, alínea t).

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:

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

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

		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 (OSEs), 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.

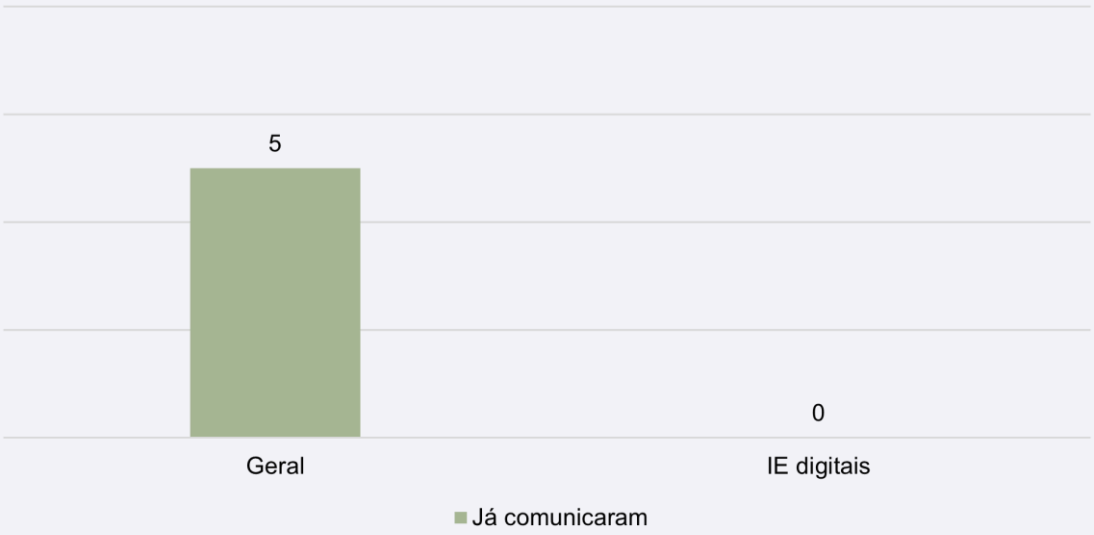
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez,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

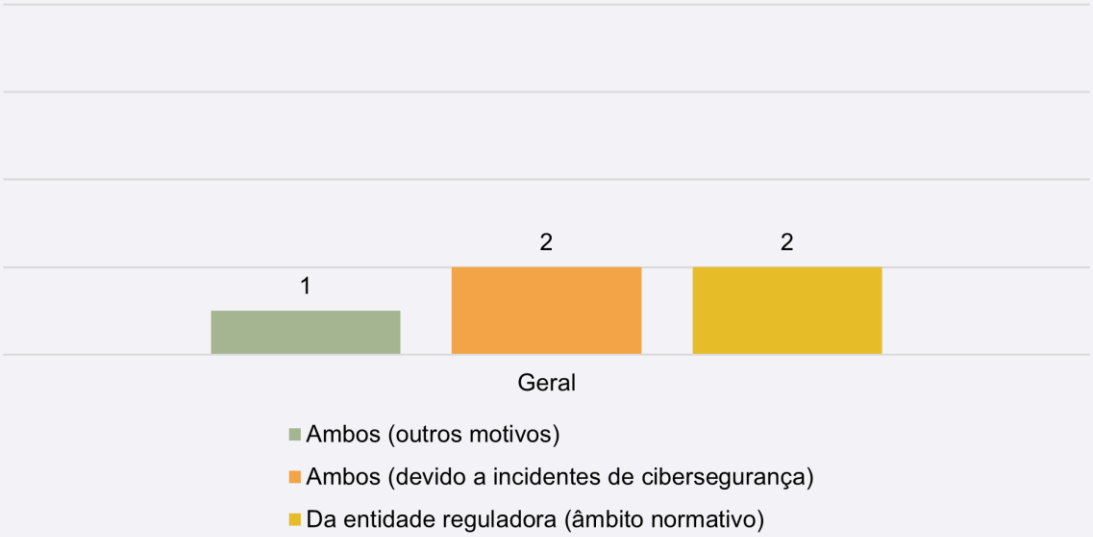
1. Comunicação entre OSEs e respetivos Reguladores

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



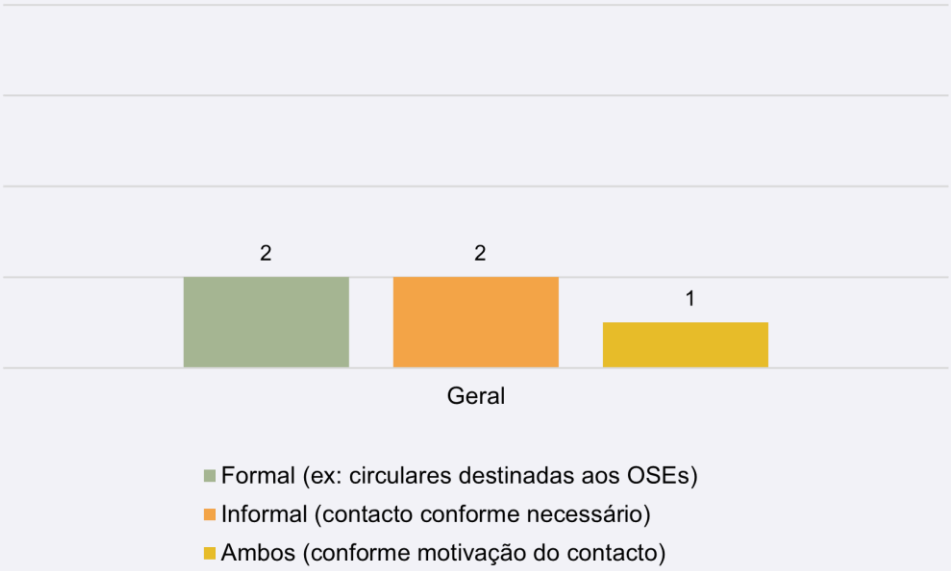
Entre os oito reguladores que responderam, cinco indicaram já ter comunicado com os OSEs sobre questões de cibersegurança. Deve-se, no entanto, sublinhar que no setor dos transportes, registaram-se as respostas de três reguladores e que apenas um indicou já ter comunicado com os OSEs sobre questões de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

Gráfico 2 - Origem da comunicação sobre questões de cibersegurança



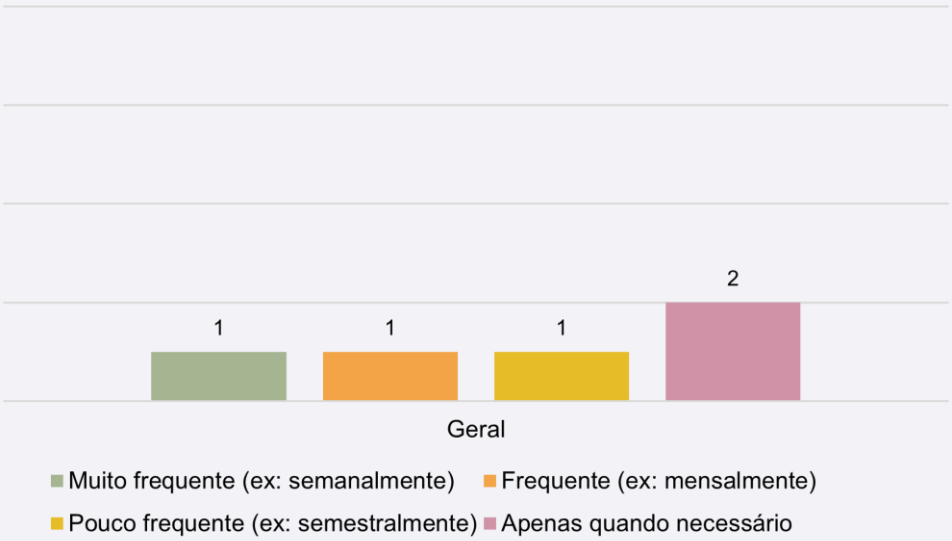
Relativamente à origem da comunicação sobre cibersegurança realizada por cinco dos reguladores, dois indicaram que a comunicação partiu dos próprios, em contexto de informação sobre normas do setor, outros dois responderam que houve comunicação que se gerou a partir dos dois lados, devido à ocorrência de incidentes de cibersegurança e apenas um respondeu que houve comunicação sobre cibersegurança a ser realizada com os OSEs devido a outros motivos. A questão não é aplicável ao setor das infraestruturas digitais pois o setor nunca efetuou qualquer comunicação.

Gráfico 3 - Formalidade da comunicação realizada



Entre os mesmos cinco reguladores, mantendo a exclusão do setor das infraestruturas digitais, dois indicaram que a comunicação é geralmente feita de modo, 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.

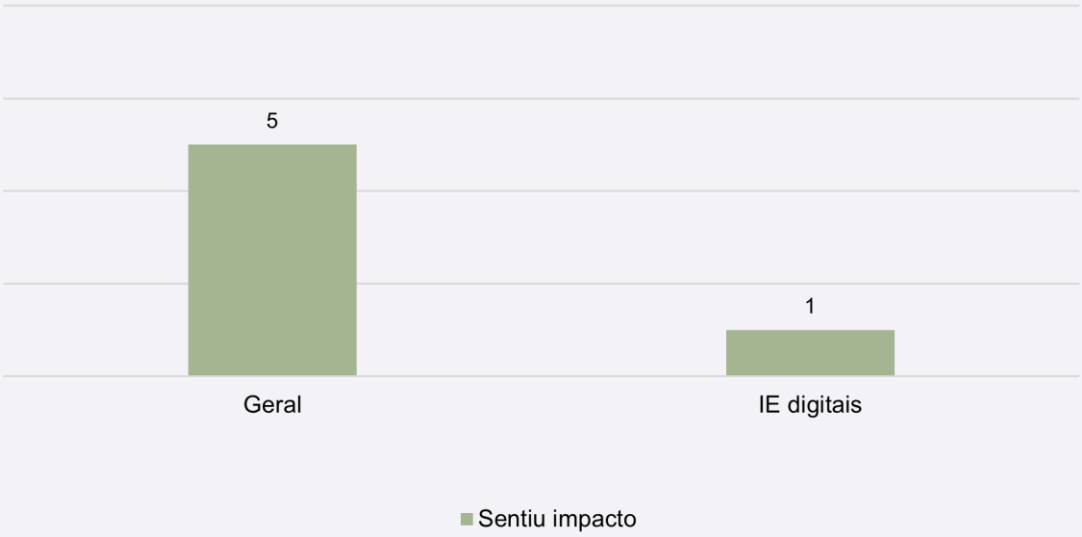
Gráfico 4 - Frequência da comunicação



No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. Mantém-se a exclusão do setor das infraestruturas digitais.

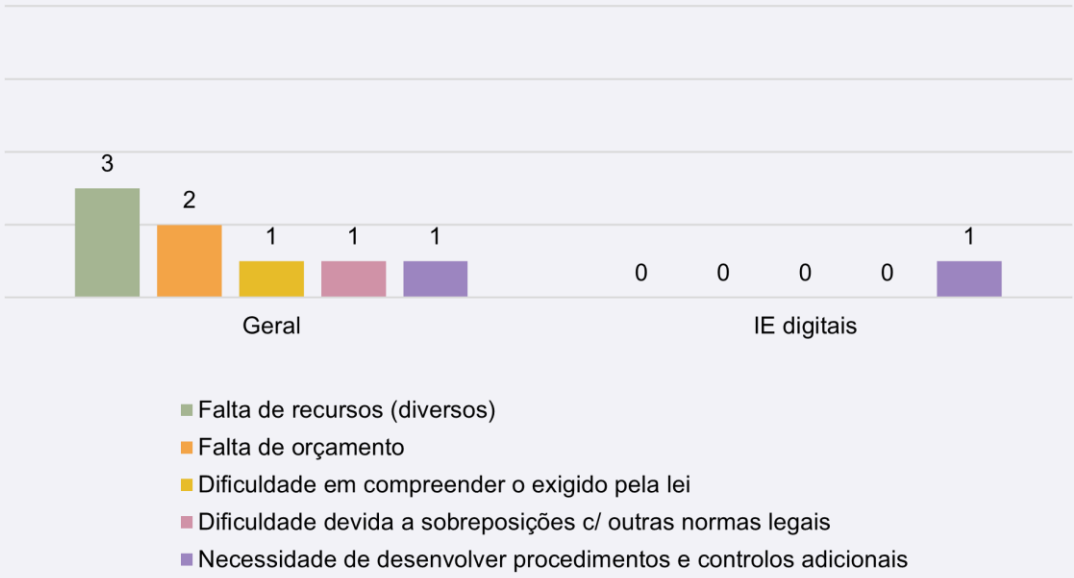
2. Impacto da publicação da Diretiva NIS ou da transposição da mesma (publicação da Lei n. º46/2018)

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



Questionou-se aos reguladores se sentiram impacto nas suas organizações e nos OSEs 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 feito sentir no setor das infraestruturas digitais. Ver-se-á, de seguida, quais foram os impactos sentidos.

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



Três dos cinco reguladores que indicaram ter sentido impacto na sua organização ou nos OSEs 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.

Dois reguladores indicaram também a falta de orçamento a conformidade com regime jurídico, como outra das dificuldades sentidas. Soma-se ainda, a dificuldade em compreender o que era exigido pela nova legislação, tendo este sido o único setor a apontar esta dificuldade.

Dificuldades relativas à sobreposição com outras normas legais foram indicadas apenas por um dos reguladores, já a necessidade de desenvolver procedimentos e controlos adicionais foi unicamente indicada pelo regulador do setor das infraestruturas digitais.

De acordo com um inquérito realizado pela ENISA, a implementação da diretiva NIS tem, normalmente, um efeito positivo nos OSEs 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[15].

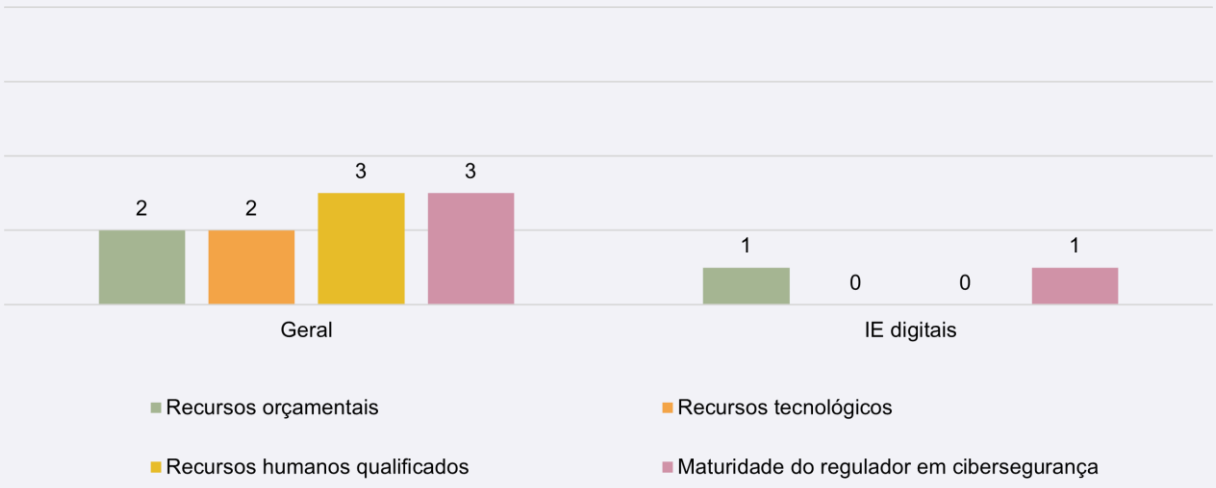
3. Supervisão dos OSEs em matéria legislativa de cibersegurança por parte dos Reguladores

Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSEs 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.

O regulador do setor das infraestruturas digitais, indicara não considerar ter essa capacidade.

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.

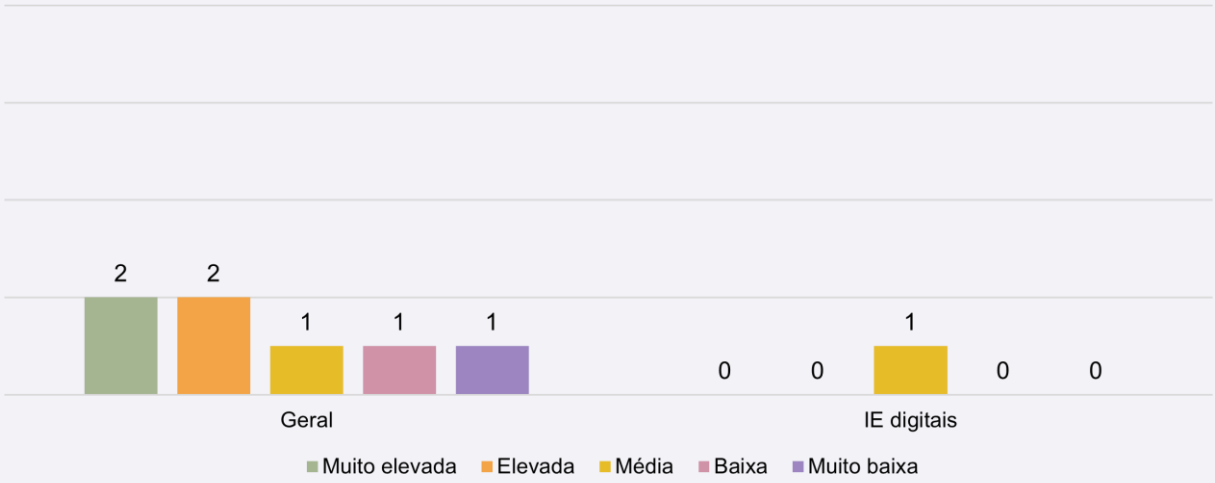
Além destes, três das entidades que consideram não ter a capacidade de realizar essa supervisão entendem não ter os recursos humanos suficientes para tal.

Nas infraestruturas digitais, os principais recursos em falta indicados foram os recursos orçamentais e os recursos humanos qualificados.

A falta de recursos humanos qualificados em cibersegurança é um tema que surge repetidamente nas respostas tanto dos reguladores como dos OSEs. Dados do Fórum Económico Mundial evidenciam uma escassez global de cerca 4 milhões de profissionais em cibersegurança[7], escassez essa que coloca diversas dificuldades não só aos reguladores e aos OSEs dos setores em análise, mas também noutras organizações e setores de atividade. Este tema é explorado em maior detalhe na análise do **Gráfico 44**.

4. Maturidade em cibersegurança no setor

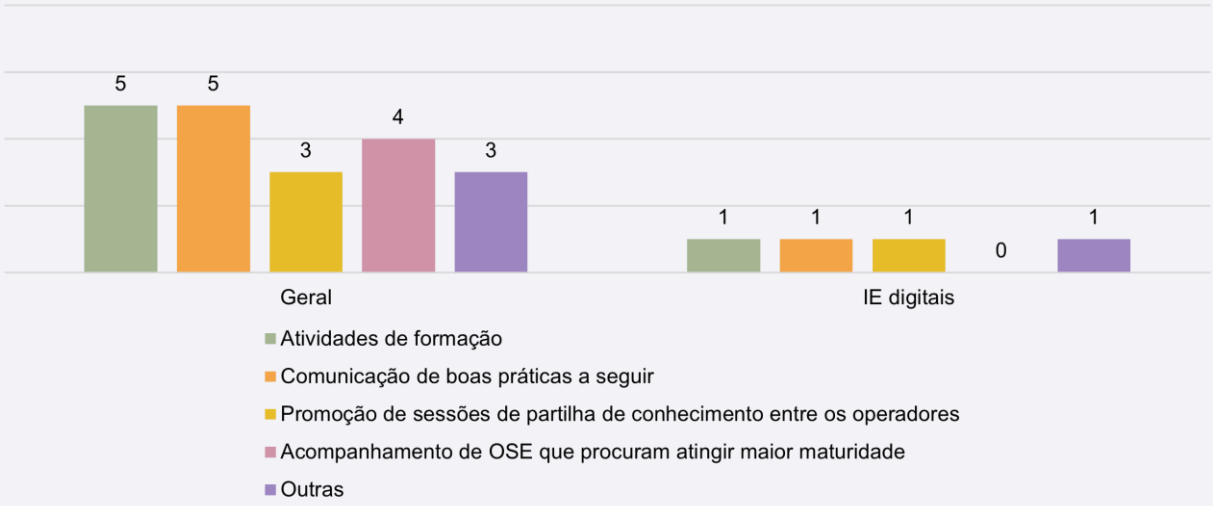
Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores



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 elevada. O regulador do setor das infraestruturas digitais considera que a maturidade no setor é média.

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

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, incluído as infraestruturas digitais, promovem atividades de formação num esforço para aumentar a maturidade no setor. Verifica-se o mesmo número de reguladores a recomendar boas práticas a seguir.

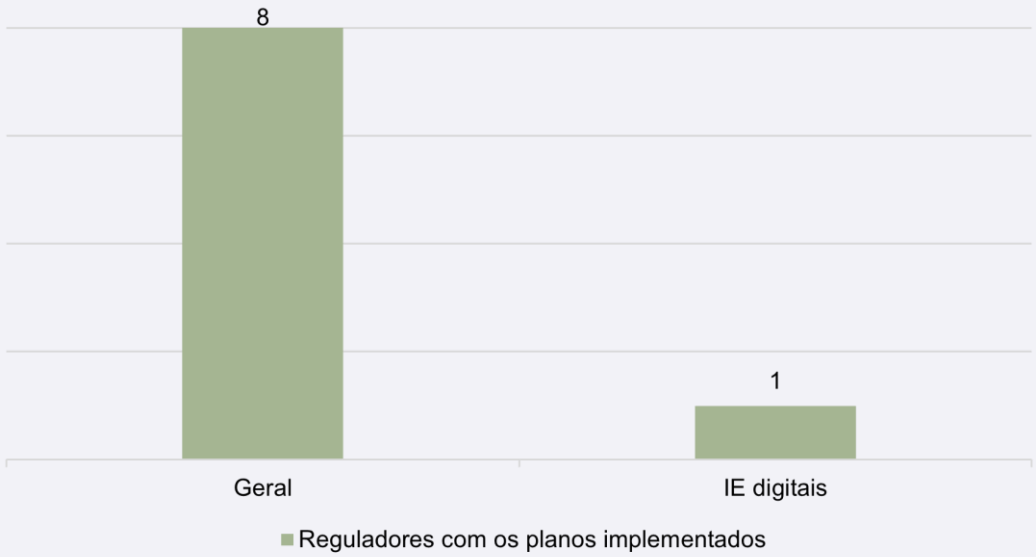
Relativamente à promoção de sessões de partilha de conhecimento, apenas três reguladores indicaram fazê-lo incluindo novamente o setor das infraestruturas digitais. Quanto ao acompanhamento de OSEs que procurem atingir maior maturidade em cibersegurança, quatro entidades referiram fazer esse acompanhamento. O setor das infraestruturas digitais menciona ainda outras medidas.

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

Apenas duas das entidades reguladoras inquiridas, sendo uma delas o setor das infraestruturas digitais, consideram ter suficientes profissionais capacitados em matéria de cibersegurança, enquanto os restantes seis 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**.

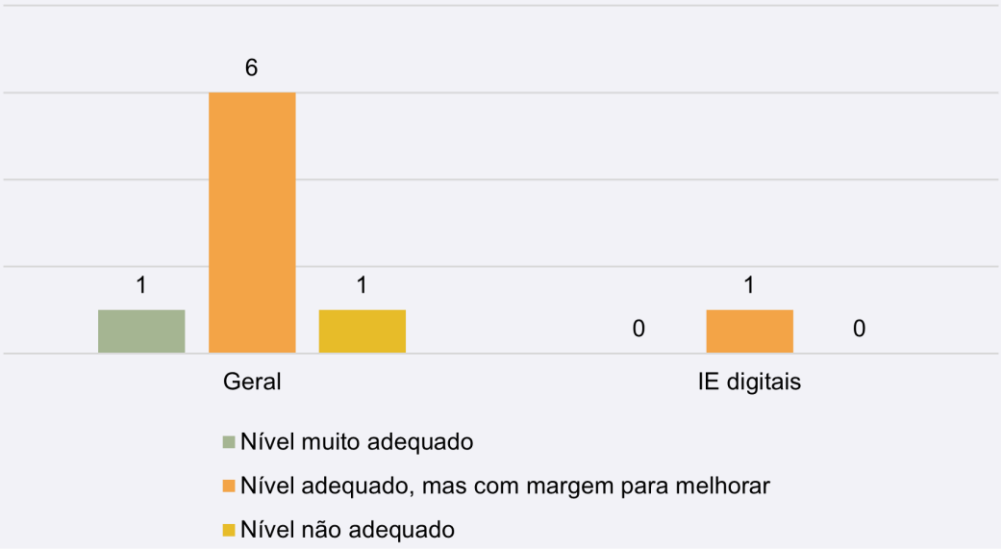
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados



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 OSEs, 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, entre eles encontra-se o setor das infraestruturas digitais.

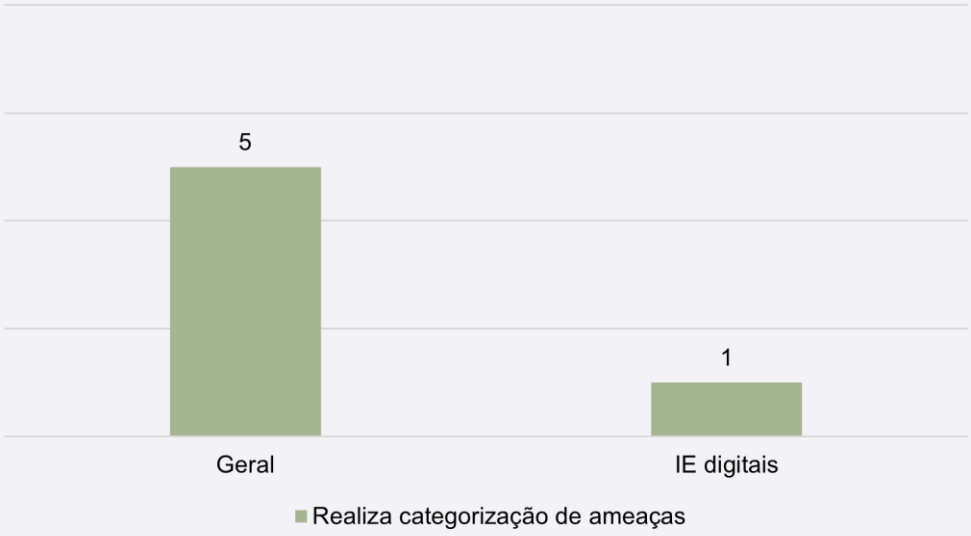
Uma questão semelhante foi colocada, em 2021, não aos reguladores, mas a diversos OSEs na União Europeia, no âmbito do relatório *NIS Investments* 2021. As respostas recolhidas indicam que quase 50% (48,9%) dos operadores de serviços essenciais consideram que a Diretiva NIS teve um impacto positivo nas suas organizações e na União, aumentado o nível de cibersegurança das organizações, ao fortalecer as suas capacidades de deteção e de recuperação de incidentes[8].

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.

[8] 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



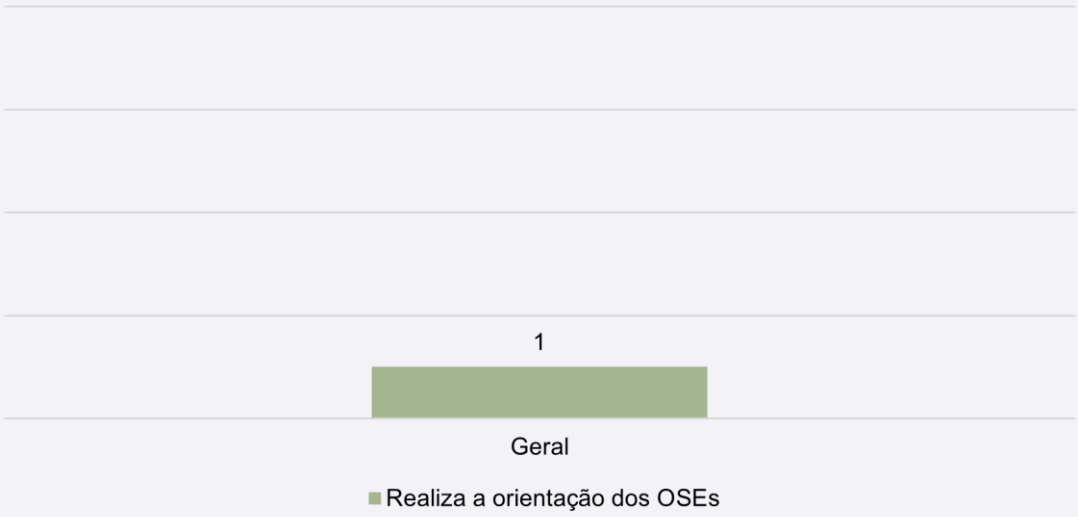
Cinco dos oito reguladores inquiridos, fazendo parte o setor das infraestruturas digitais, realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores.

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

Dos cinco reguladores que realizam categorização de ameaças, apenas dois partilham informação relativa às ameaças com os OSEs. O setor das infraestruturas digitais não efetua a partilha de informação.

7. Orientação dos OSEs por parte da entidade reguladora

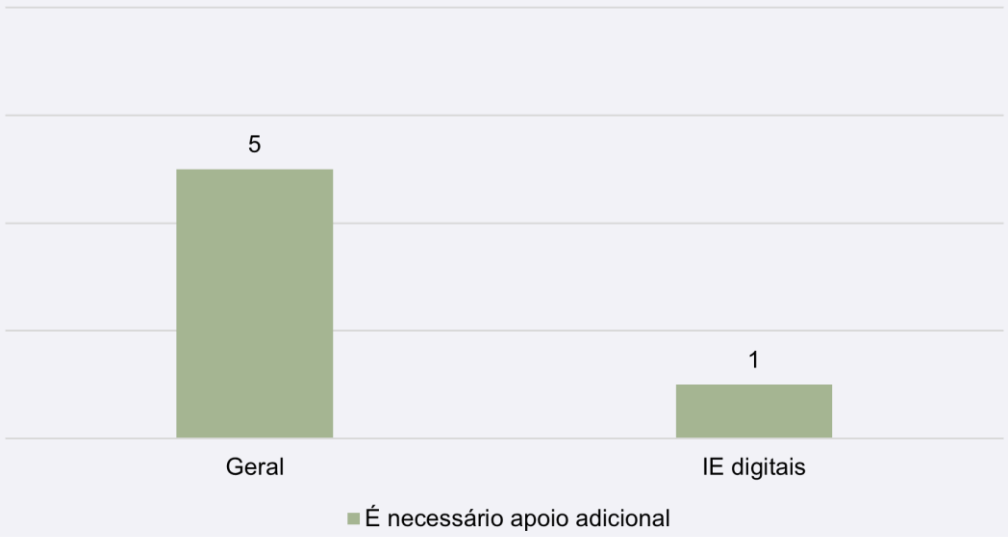
Gráfico 16 - Reguladores que orientam os OSEs na digitalização de processos e na promoção de uma cultura digital



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



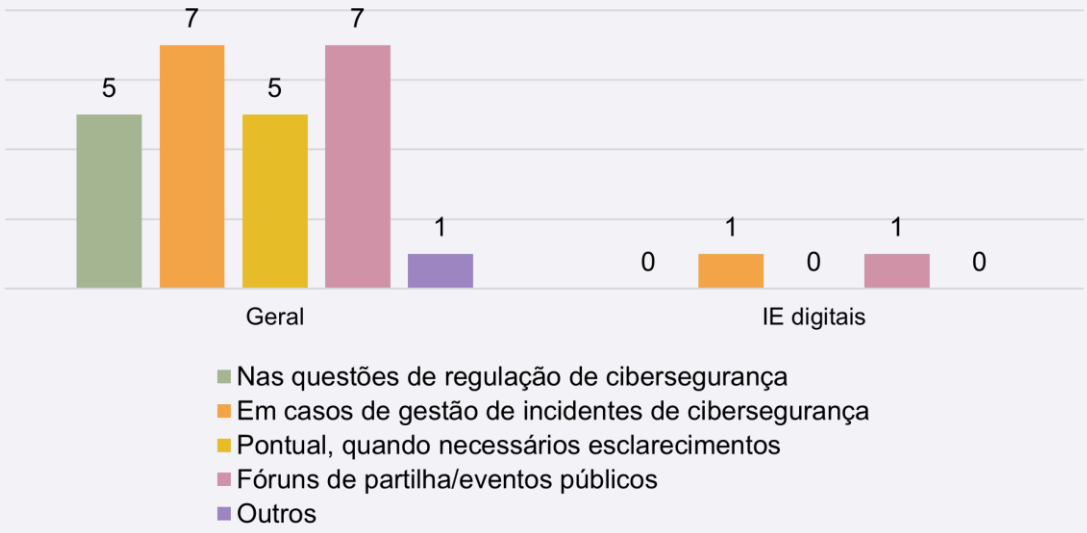
Entre os reguladores inquiridos, cinco têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional. O setor das infraestruturas digitais menciona ser necessário apoio adicional.

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 OSEs com base em casos concretos ocorridos no setor como por exemplo um ataque a uma infraestrutura e como proteger.

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

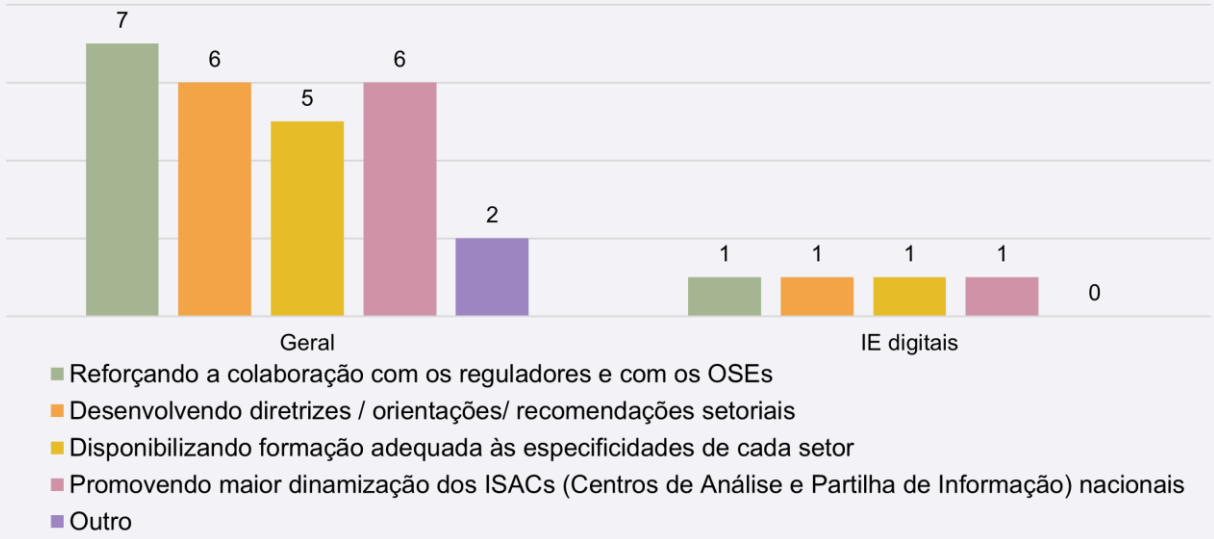
Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS



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.

O setor das infraestruturas digitais indica por norma interagir com o CNCS no âmbito de questões relacionadas com a cibersegurança e em fóruns de partilha e eventos públicos.

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



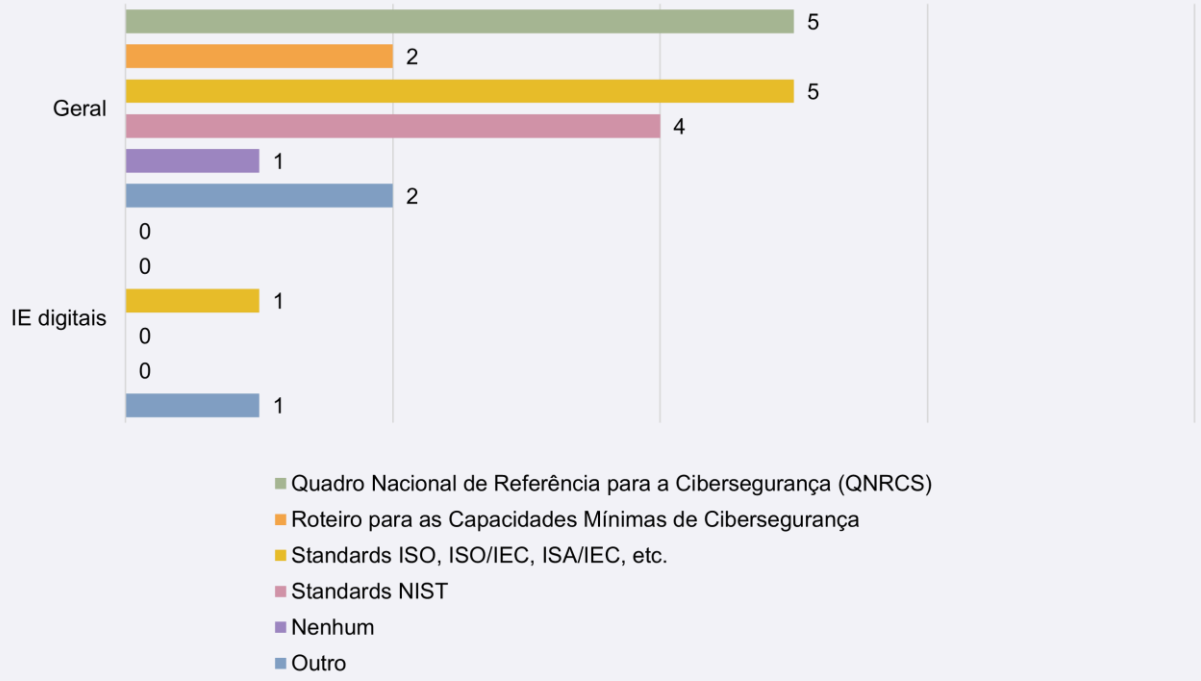
Relativamente às áreas através das quais o CNCS poderia prestar mais auxílio, sete dos reguladores (excetua-se o regulador do setor bancário) indicaram que este poderia reforçar a colaboração realizada com os reguladores e com os OSEs, as áreas de desenvolvimento de diretrizes/orientações/recomendações 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. O setor das infraestruturas digitais menciona todos os pontos anteriores, excluindo apenas o apoio ao nível do desenvolvimento 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"[9].

[9] 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 OSEs 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.

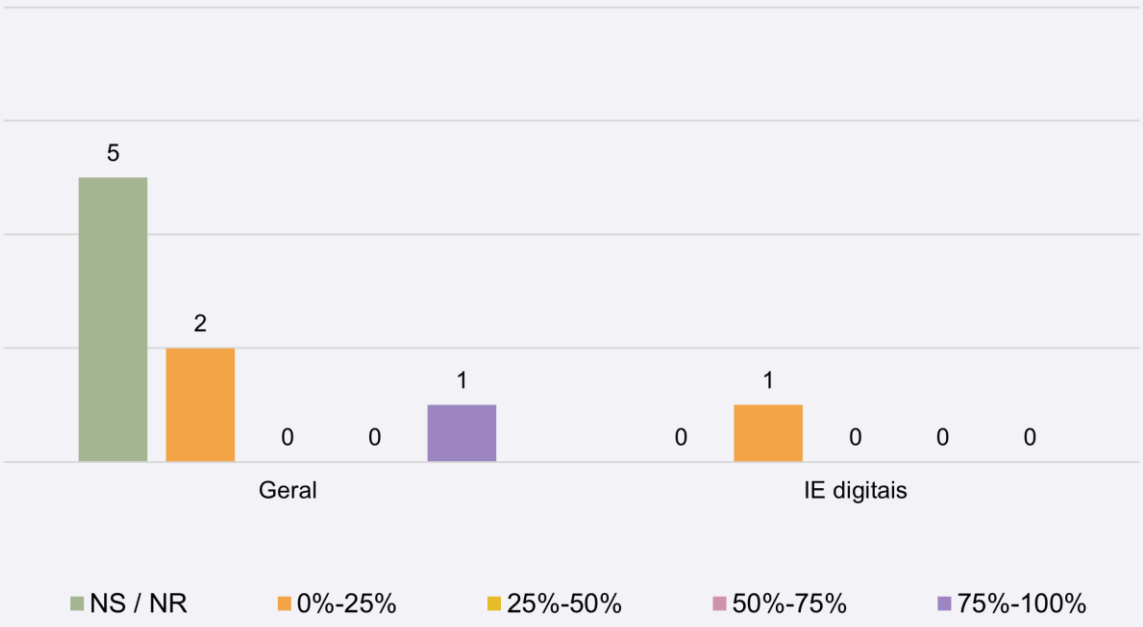
Na opção "outros", foram referidos *standards* da International Civil Aviation Organization (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain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

O regulador do setor das infraestruturas digitais indicara recomendar aos operadores *standards* ISO, sendo que este último também indicou boas práticas como a utilização de DNSSEC, DKIM e DMARC.

De acordo com um estudo realizado em 2023 pelo Departamento de Ciência, Tecnologia e Inovação do Governo do Reino Unido, o uso de boas práticas de cibersegurança diminuiu de 2021 para 2023. Nesta diminuição podem ser nomeados o decréscimo no uso de políticas de palavras-passe, onde se verificou uma redução de utilização pelos inquiridos de 79% para 70%, enquanto no uso de *Firewalls* se registou uma diminuição de 78% para 66%[10].

[10] 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

Gráfico 22 - Percentagem aproximada de OSEs 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. No setor das infraestruturas digitais, os reguladores identificam entre 0%-25% de operadores certificados em normas internacionais ISO ou semelhantes.

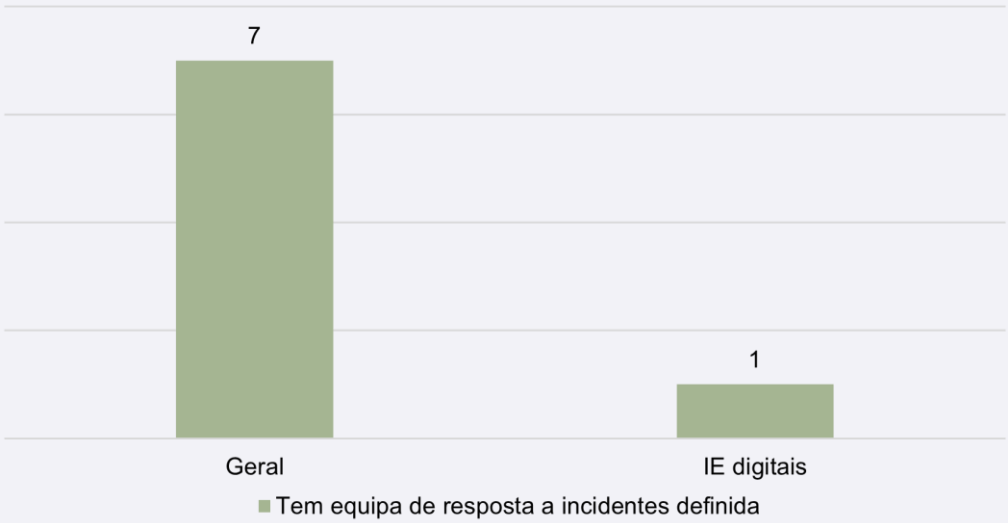
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança

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 1.

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 das infraestruturas digitais, o regulador inquirido informa ter definido a equipa de resposta a incidentes.

11. Sensibilização e consciencialização

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

Relativamente à participação em programas de formação e sensibilização para os riscos no ciberespaço, seis dos reguladores inquiridos, indicaram que participam ou já participaram em programas do género promovidos pelo CNCS ou outra entidade, enquanto dois nunca participaram em tais programas.

O regulador do setor das infraestruturas digitais insere-se no grupo dos 25%, tendo indicado que nunca participaram em programas do tipo.

Gráfico 25 - Reguladores recipientes de formação que partilharam os conhecimentos adquiridos com os OSEs 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 OSEs 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.

Nas infraestruturas digitais, o regulador não terá feito essa partilha com os operadores.

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

Entre os reguladores que frequentaram os programas de formação e sensibilização, todos consideram que ter frequentado os programas robusteceu os comportamentos relativos à cibersegurança dentro da sua organização. Como indicado no gráfico anterior, esta questão também não se aplica ao regulador do setor das infraestruturas digitais, que não participou em programas do género.

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

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

sensibilizados sobre as principais vulnerabilidades do setor. Quanto ao setor das infraestruturas digitais a situação aplicável é a mesma que a anterior.

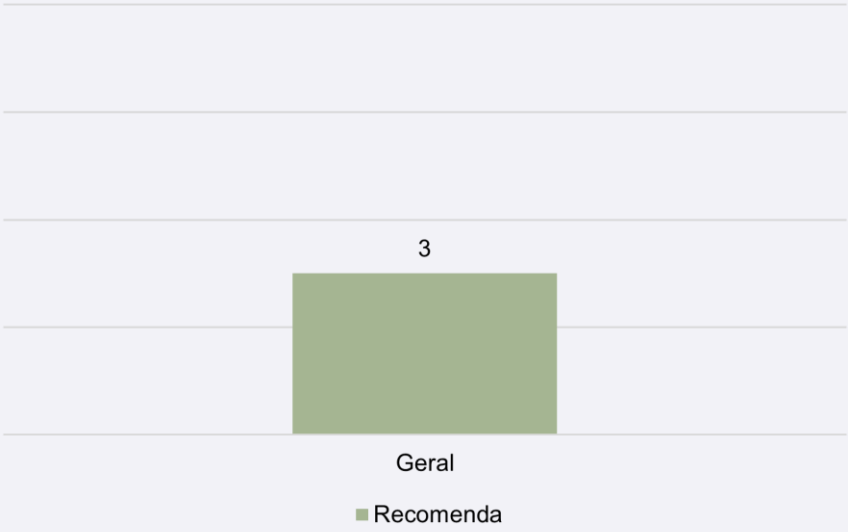
12. Cooperação nacional/internacional de proteção do ciberespaço

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

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

O regulador dos setores das infraestruturas digitais insere-se no grupo da maioria, não fazendo parte de nenhuma estrutura do tipo.

Gráfico 29 - Reguladores que recomendam a participação dos OSEs 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.

No caso do regulador inquirido das infraestruturas digitais, este não recomenda aos operadores a participação em centros de partilha de informação.

13. Regulação de entidades e OSEs

Por fim, questionou-se aos reguladores dos setores em análise qual o número de entidades por si reguladas e quantas destas eram OSEs. Das respostas obtidas foram criadas as Tabelas 2 e 3.

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

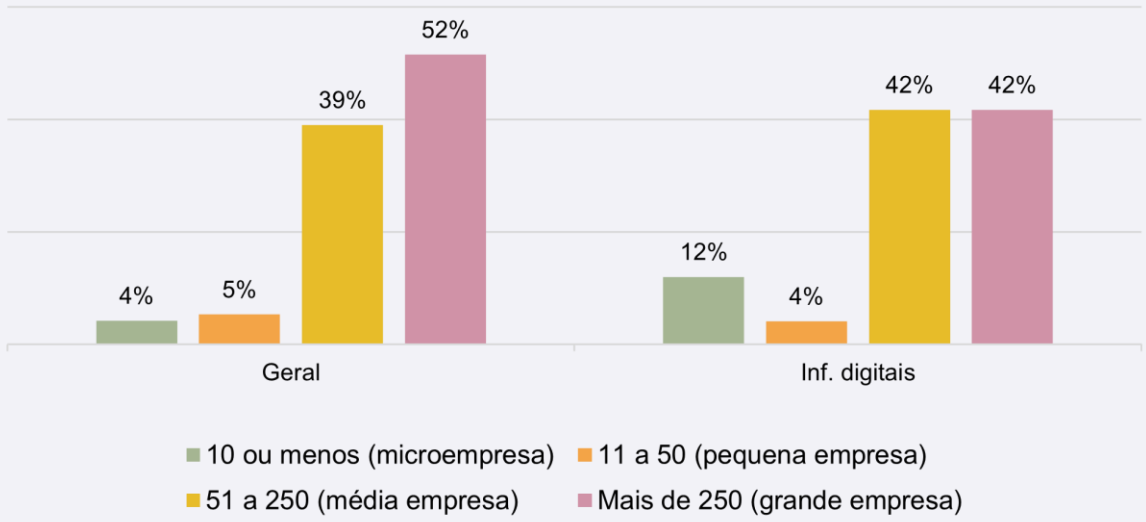
Tabela 4 - Número estimado das entidades reguladas que são OSEs

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



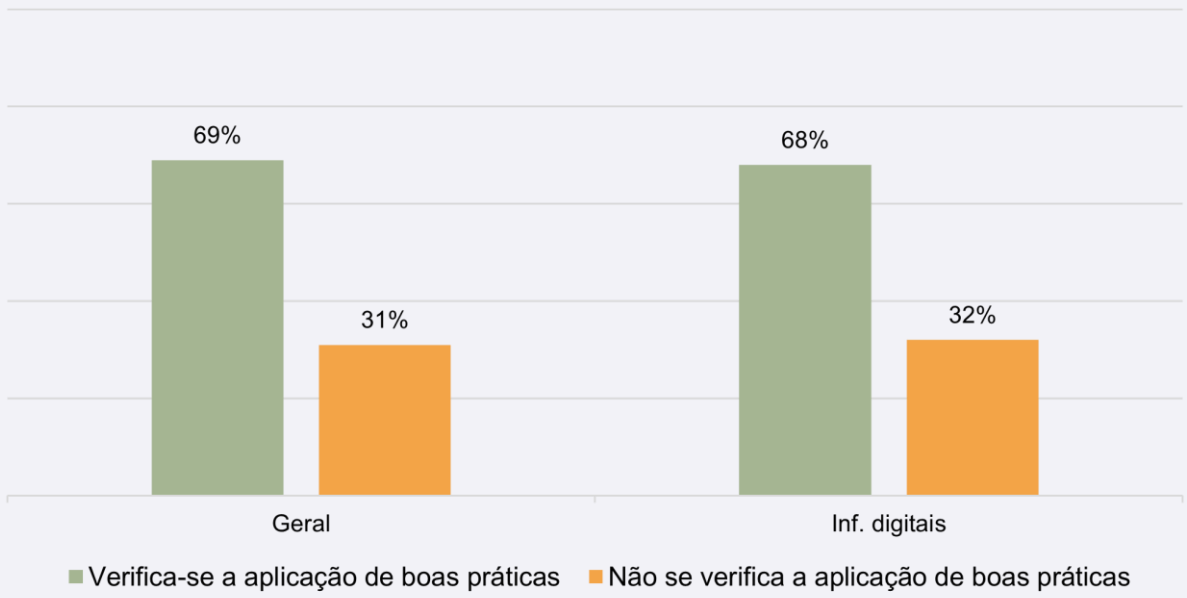
O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSEs. As médias empresas representam 39% dos OSEs, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas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

No setor das infraestruturas digitais observa-se uma igual distribuição entre médias empresas e grandes empresas (42% cada).

A composição do tecido empresarial dos OSEs difere grandemente daquele que é o tecido empresarial geral das empresas portuguesas. Enquanto entre os OSEs 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[11].

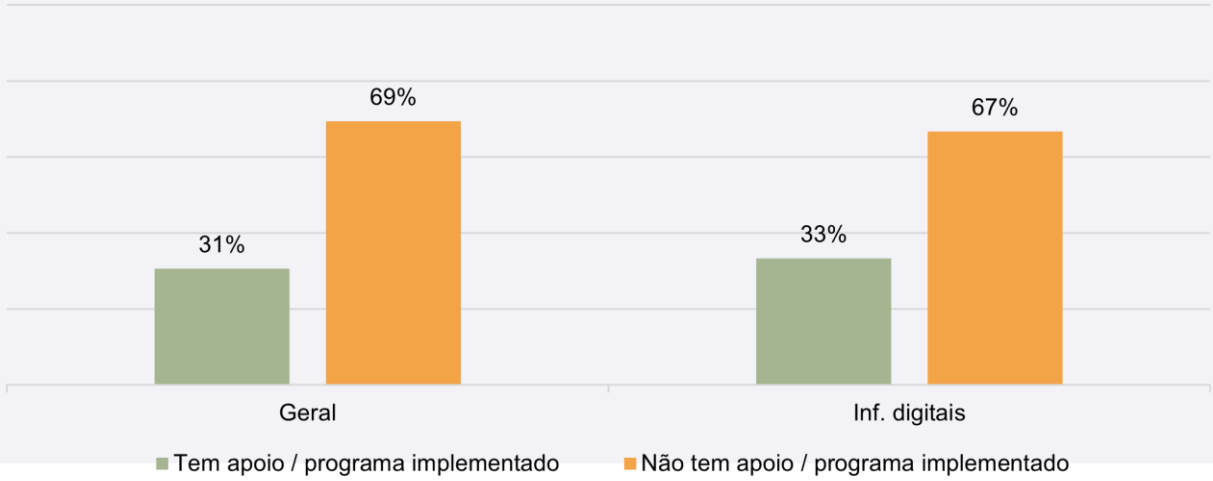
[11] PORDATA, "Empresas: total e por dimensão", dados de 2022, https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.

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



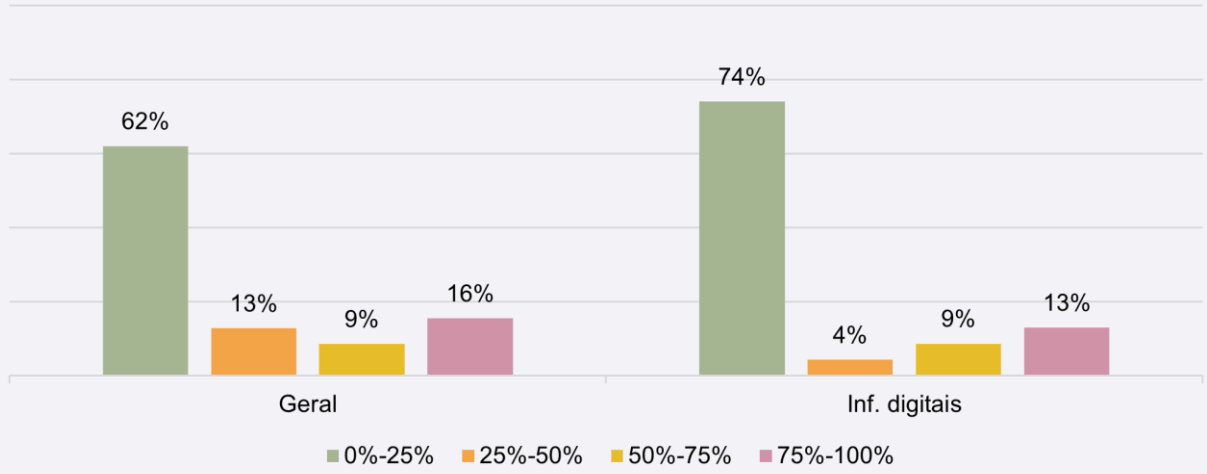
De um modo geral, os operadores percecionam a adoção de boas práticas de cibersegurança por parte dos seus colaboradores. Alguns exemplos dessas boas práticas são a não partilha de palavras-passe, o bloqueio do computador durante momentos de ausência da estação de trabalho, o cuidado com a informação 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.
No setor das infraestruturas digitais, a perceção de que estas boas práticas são aplicadas varia 1 ponto percentual dos valores gerais.

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

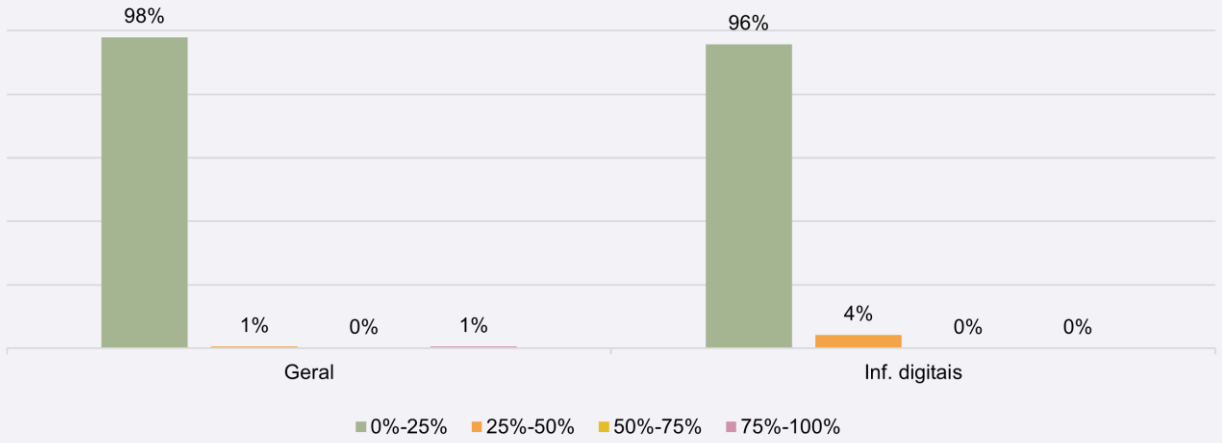
Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



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

No setor das infraestruturas digitais, a percentagem de operadores onde três quartos dos colaboradores ou mais têm formação básica em cibersegurança é relativamente baixa, nunca ultrapassando os 13%.

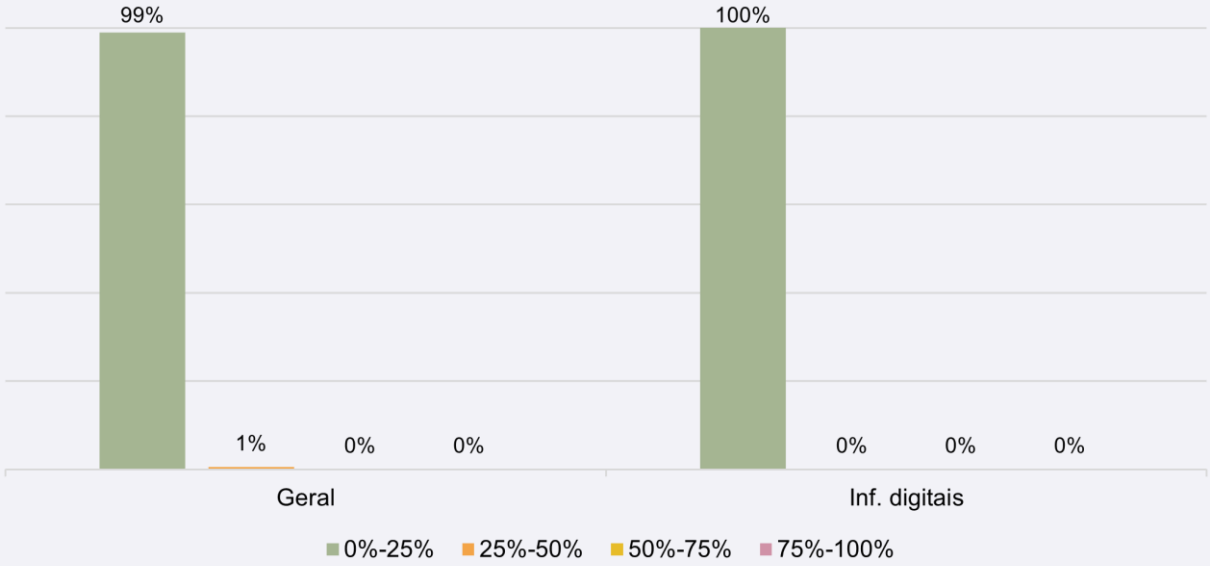
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



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

Em termos gerais, a percentagem de trabalhadores dos operadores com formação superior em cibersegurança situa-se predominantemente na faixa entre 0%-25% em todos os operadores de todos os setores. Existe um número reduzido de colaboradores dos operadores inquiridos, com formação superior em cibersegurança. Destaca-se o setor das infraestruturas digitais, nos quais se registam operadores com percentagens de colaboradores com formação superior em cibersegurança nas faixas acima dos 25%.

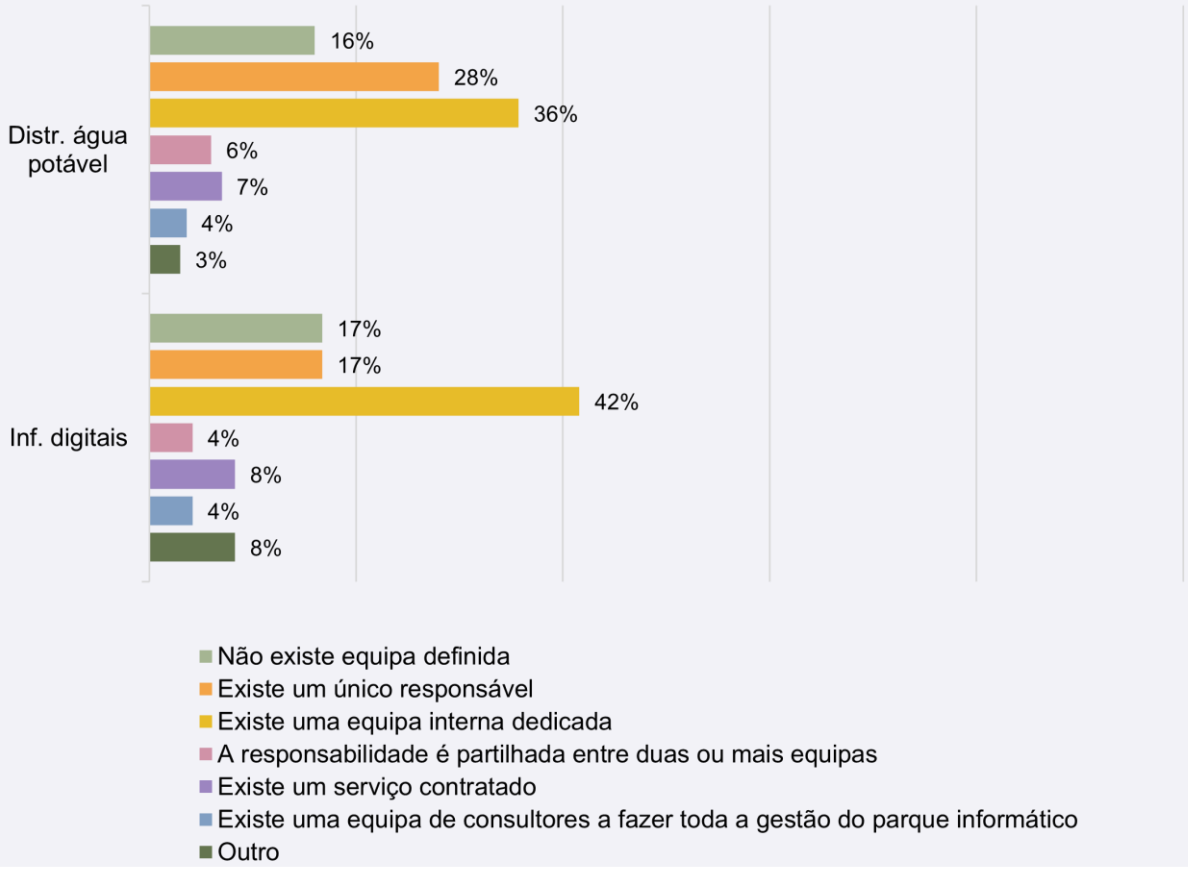
Gráfico 35 - Percentagem aproximada de trabalhadores do operador com certificações em cibersegurança



A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos, no setor das infraestruturas digitais situa-se nos 100%. 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 OSEs 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 OSEs a certificar os seus próprios colaboradores[12].

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).

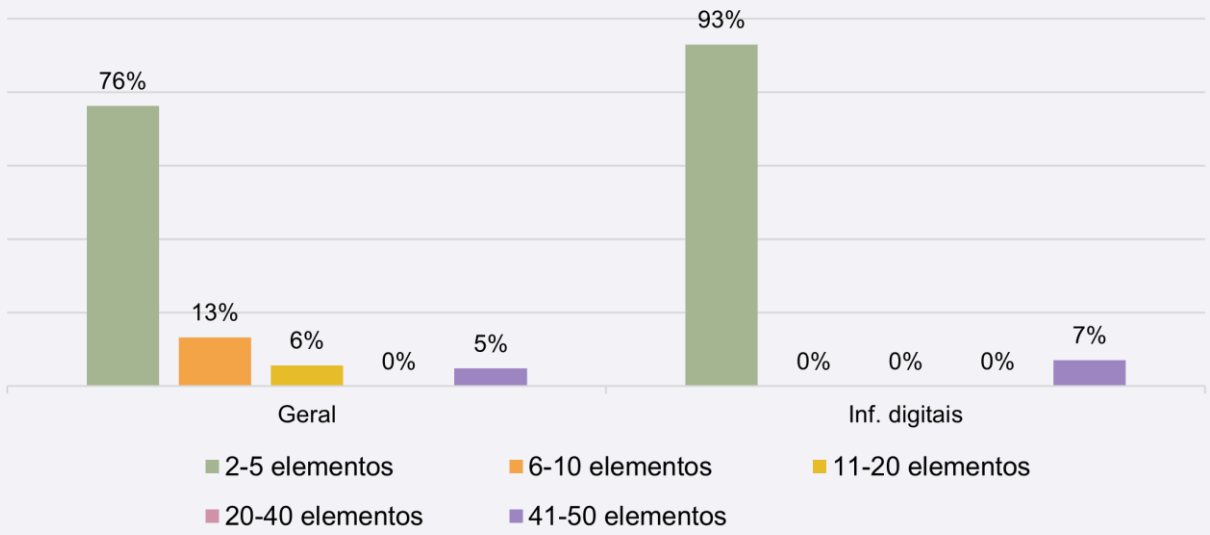
Verificam-se ainda outras situações, como a não existência de equipa definida (em 14% dos operadores inquiridos), a partilha de a responsabilidade entre duas ou mais equipas (7%), a existência um serviço contratado (7%), aquelas onde uma equipa de consultores faz toda a gestão do parque informático (3%). Entre os que responderam "outro", as principais soluções indicadas

[12] ENISA, "NIS Investments", novembro de 2021, 73.

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.

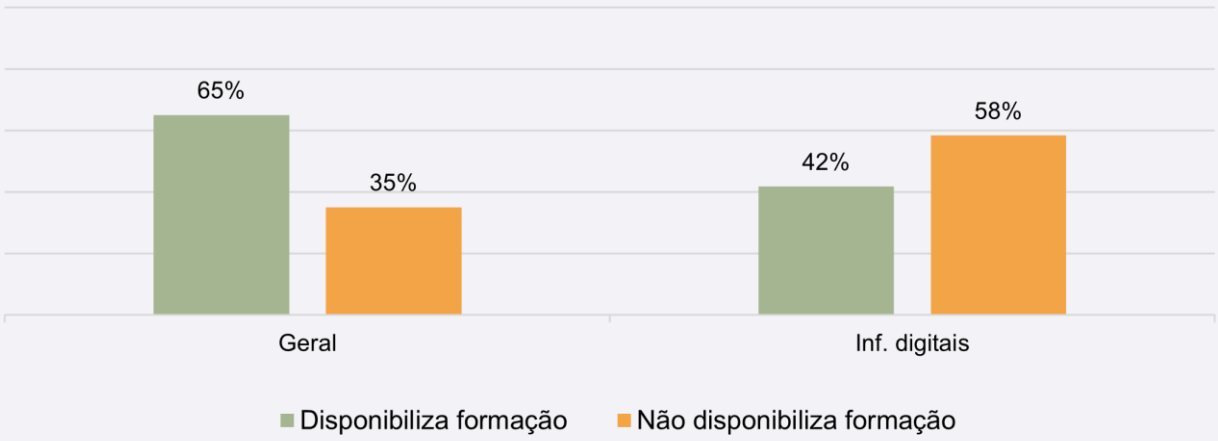
No setor das infraestruturas digitais, prevalece a presença de uma equipa interna dedicada, com pelo menos 42% dos OSEs a optarem por esta solução.

Gráfico 37 - Composição das equipas de helpdesk



Na sua larga maioria, as equipas de *helpdesk* são compostas por 2-5 elementos. Entre os OSEs 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 OSEs 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. Sectorialmente, nas infraestruturas digitais, 93% das equipas são de 2-5 elementos e os restantes 7% de 41-50 elementos.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

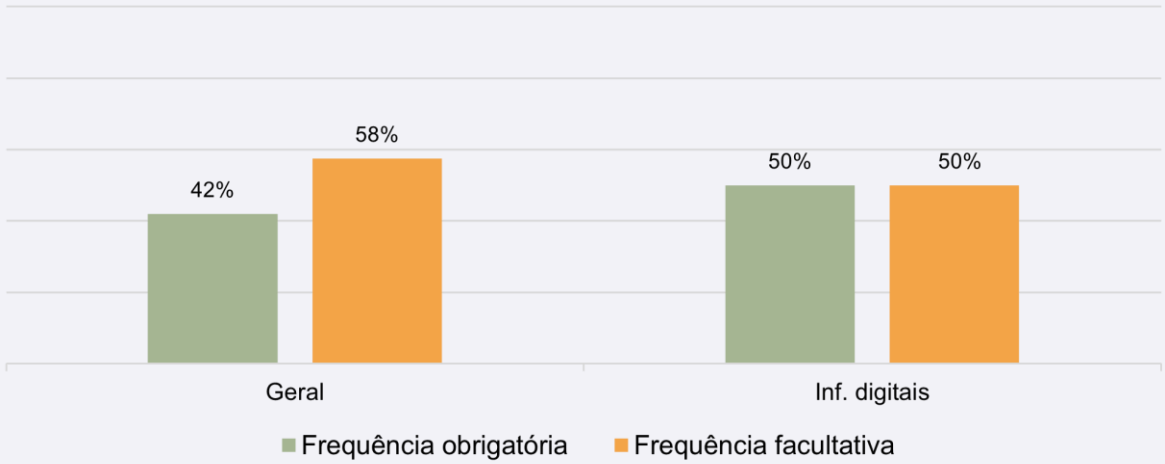


Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSEs nos diversos setores. As exceções a esta realidade verificam-se no setor das infraestruturas digitais, no qual menos de metade dos inquiridos (42%) indica disponibilizar formação aos colaboradores.

Comparando com dados do Inquérito à Utilização das TIC nas Empresas (IUTICE) de 2022, realizado pelo Instituto Nacional de Estatística (INE), 63,3% das empresas em Portugal procuraram consciencializar os seus colaboradores sobre cibersegurança durante o ano de 2021[13]. 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.

[13] 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

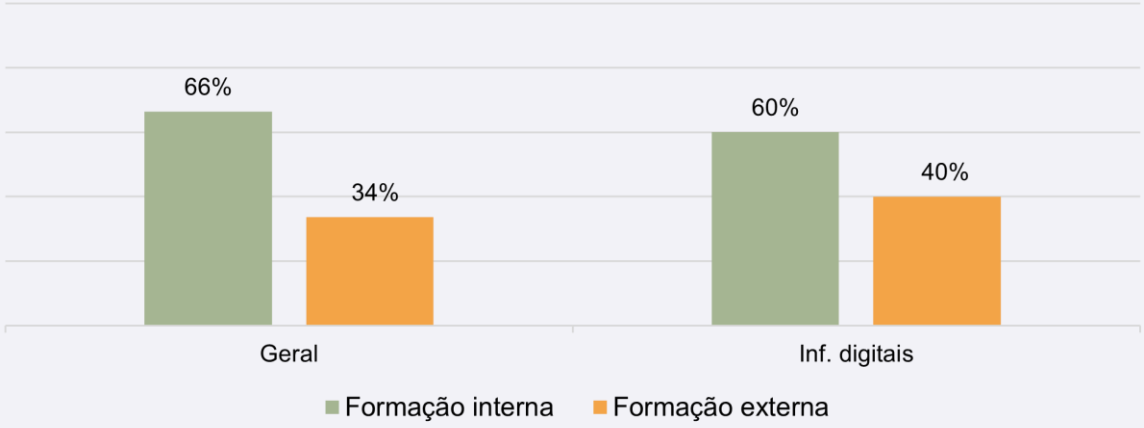
Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



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 setor das infraestruturas digitais, há tantos OSEs onde a formação é obrigatória como onde é facultativa.

Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre OSEs e demais empresas em Portugal. Enquanto em 42% dos OSEs 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 OSEs que disponibilizam formação e em 56,2% das empresas participantes no inquérito[14].

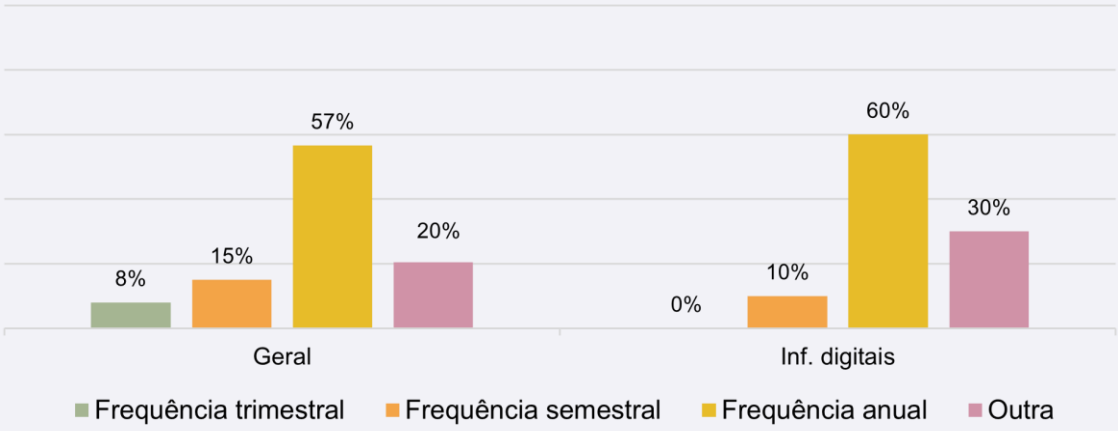
Gráfico 40 - Caráter das formações disponibilizadas - formação interna ou externa



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

Neste gráfico, fica evidenciado o maior recurso à formação interna do que externa entre os OSEs. A maioria dos inquiridos (66%) recorre aos meios internos para fins de formação aos colaboradores. Contudo, cerca de um terço dos OSEs (34%) recorre a entidades externas para formar os seus colaboradores. Um dos setores onde mais se recorre a entidades externas para ministrar formação é o das infraestruturas digitais, com 40% de OSEs a optarem por esse método, embora se continue a registar uma maioria de operadores que recorrem aos meios internos para dar formação.

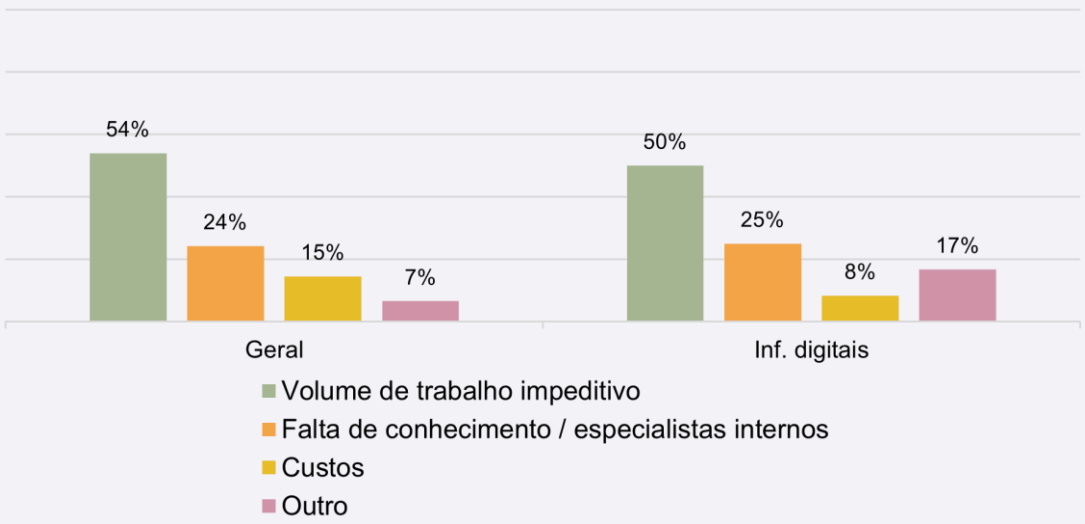
Gráfico 41 - Frequência média dos momentos de formação



Em termos gerais, a maioria dos OSEs que disponibiliza formação (57%) indica que a frequência média dos momentos de formação é anual. No setor das infraestruturas digitais mantem-se a prevalência na frequência anual com 60% dos OSEs, já 10% correspondem a frequência semestral.

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

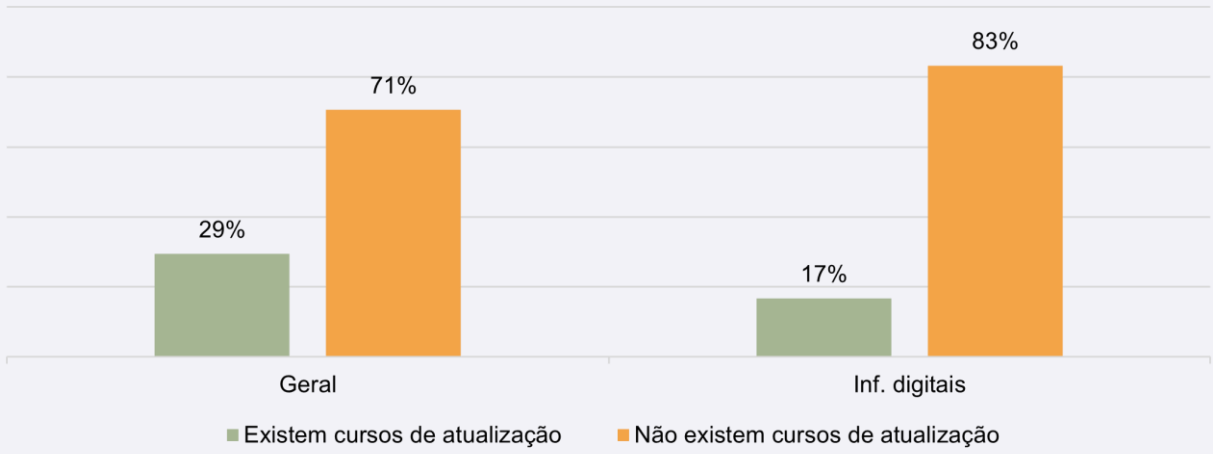
Gráfico 42 - Motivos para a não disponibilização de formação entre os OSEs que não disponibilizam



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 OSEs que afirmaram não disponibilizar formação em cibersegurança aos seus colaboradores.

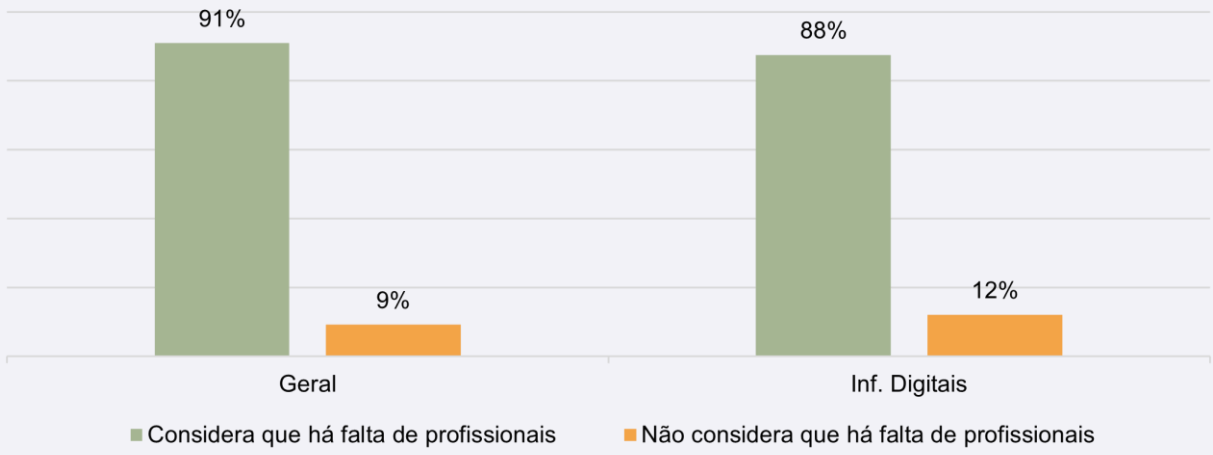
No setor das infraestruturas digitais, o principal motivo indicado continua a ser o volume de trabalho impeditivo, indicado por 50% dos OSEs que não disponibilizam formação, sendo também dos únicos a indicar "Outros" motivos para a falta de formação. Esses outros motivos passam, segundo os OSEs, pela 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 OSEs inquiridos a indicarem a existência destes cursos. O setor das infraestruturas digitais supera a percentagem geral, com mais de 80% dos OSEs a não disponibilizar este tipo de cursos ou formações.

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



A vasta maioria dos OSEs inquiridos (91%) considera haver um cenário de escassez de profissionais de cibersegurança e áreas relacionadas no mercado de trabalho. O setor onde menor percentagem de OSEs considerou haver falta de profissionais de cibersegurança foi o das infraestruturas digitais e, mesmo assim, 88% concordam com a escassez de profissionais na área.

A escassez de profissionais em cibersegurança é um problema que persiste há largos anos, devido à discrepância entre a velocidade a que a tecnologia evolui e o tempo que leva a formar os profissionais. Segundo o Fórum Económico Mundial, a atual escassez global de profissionais em cibersegurança é de cerca de 4 milhões de profissionais[15] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[16]. 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[17]. 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[18] [19].

[15] Banco Mundial, "Strategic Cybersecurity Talent Framework", 5.

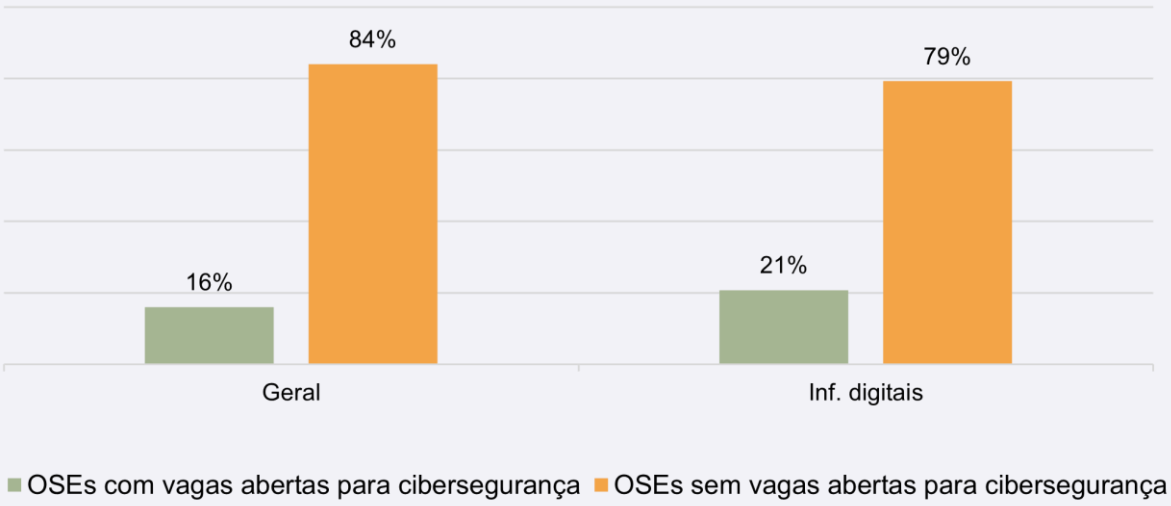
[16] ENISA, "Cybersecurity Skills Conference: Strengthening human capital in the EU", https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.

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

[18] ENISA, "NIS Investments", 2022, 16-17.

[19] Banco Mundial, "Strategic Cybersecurity Talent Framework", 22-25.

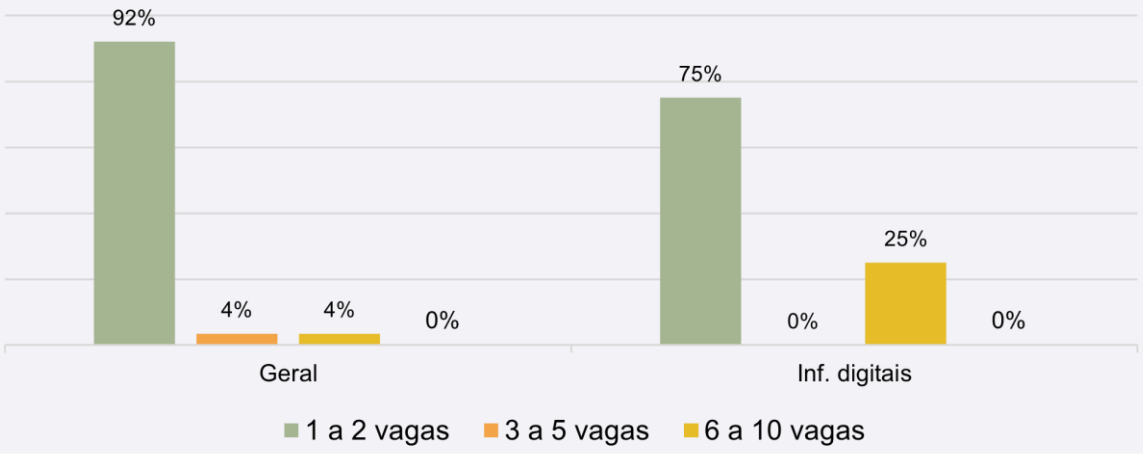
Gráfico 45 - Vagas abertas para a área de cibersegurança



À data da realização do questionário, apenas 16% dos OSEs inquiridos tinham vagas abertas para cibersegurança. Sectorialmente, nas infraestruturas digitais, existe mais 5p.p com vagas abertas do que a generalidade.

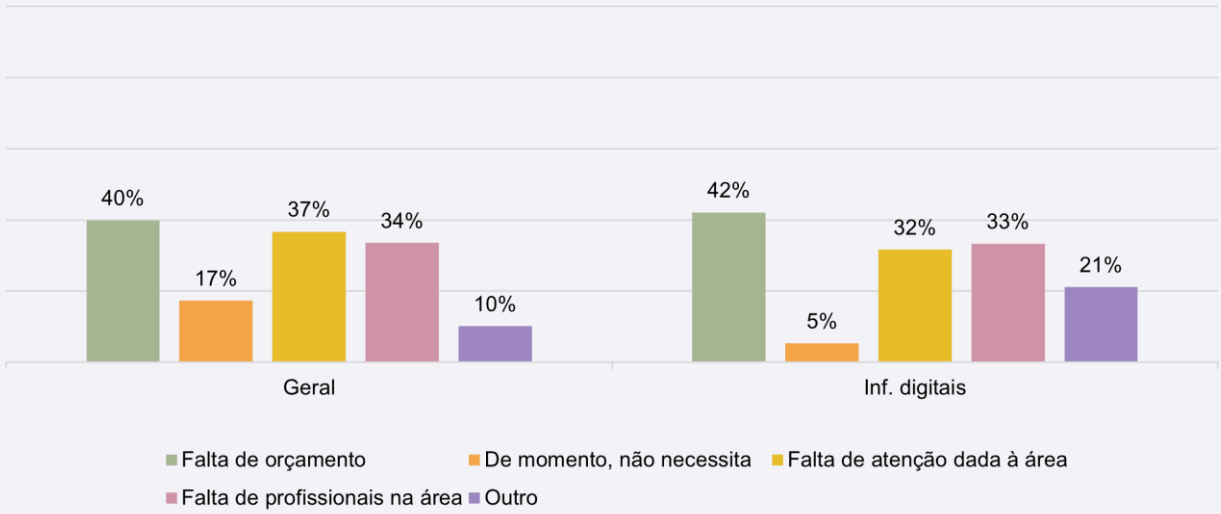
Embora não se possa fazer uma associação direta entre vagas para cibersegurança e para pessoal especialista em TIC, os dados do IUTICE de 2022 mostram que, nesse ano, apenas 6,2% das empresas portuguesas tentaram recrutar pessoal especialista em TIC.

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



Entre os 16% de OSEs que tinham vagas abertas na área de cibersegurança, a maioria destes (92%) tinha 1 a 2 vagas por preencher. Apenas no setor das infraestruturas digitais houve indicação de haver entre 6 a 10 vagas em aberto, correspondendo a 25% das vagas do setor.

Gráfico 47 - Motivos para a não abertura de vagas entre os OSEs 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 OSEs não teriam tais vagas disponíveis.

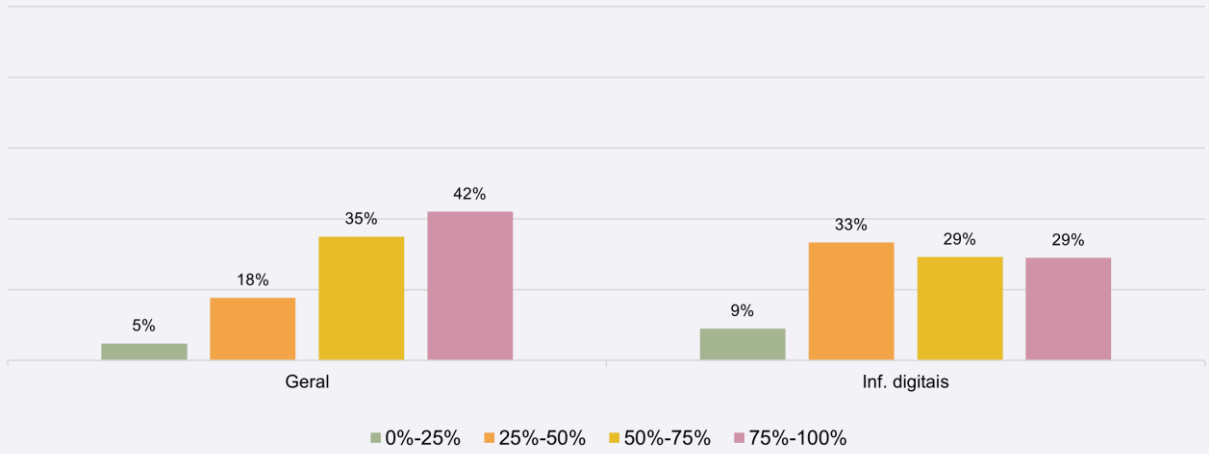
A resposta mais comum foi a falta de orçamento, indicada por 40% dos OSEs sem vagas em aberto, seguida da falta de atenção dada à área (37%) e da falta de profissionais de cibersegurança (34%). Apenas em 17% dos casos foi indicado que não havia vagas em aberto por se considerar que de momento não eram necessários mais profissionais. Os 10% de OSEs 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.

Sectorialmente, o setor das infraestruturas digitais, segue a tendência geral, mencionando apenas que a falta de profissionais na área é um motivo maior que a falta de atenção dada à área.

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.

Voltando aos dados obtidos através do questionário realizado, a "falta de atenção dada à área" indicada por 37% dos OSEs 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"[20], objetivo esse que não pode ser cumprido quando há falta de atenção dada à área. Tratando-se de Operadores de Serviços Essenciais, esta lacuna torna-se ainda mais grave. Recorda-se, também, que é uma boa prática constante de normativos internacionais, como a ISO/IEC 27001, que a direção/administração das organizações demonstre o seu compromisso para com segurança da informação e que esta assegure a alocação dos recursos necessários para cumprir esse desígnio[21].

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



Apesar de predominar entre os OSEs o intervalo 75%-100% de colaboradores com acesso a equipamentos digitais (indicado por 42% dos OSEs), é visível que, com exceção dois setores, há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos.

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

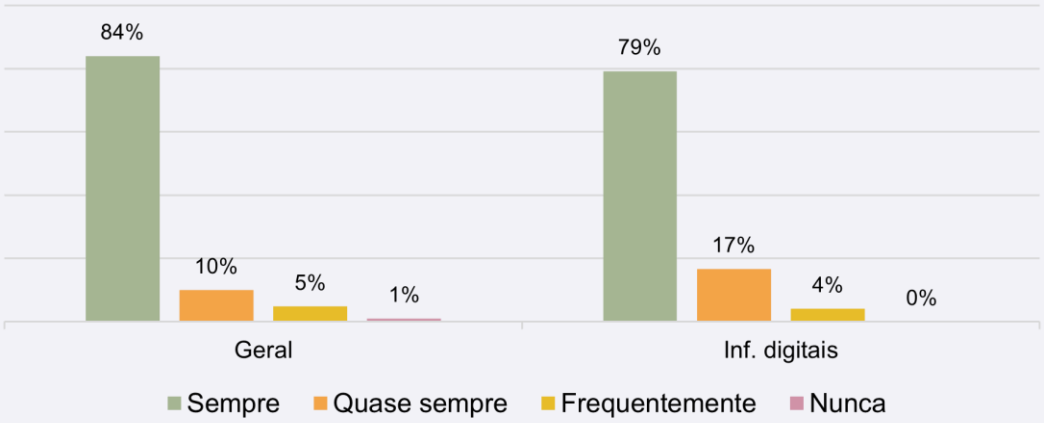
Segundo dados do IUTICE de 2022, em 2021, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais (+17,2 p.p. face a 2021), abrangendo 28,1% do pessoal ao serviço (+4,2 p.p. que em 2021). Neste ano, 74,7% das empresas tinham pessoal ao serviço com acesso remoto ao sistema de correio eletrónico da empresa[22].

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

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

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

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

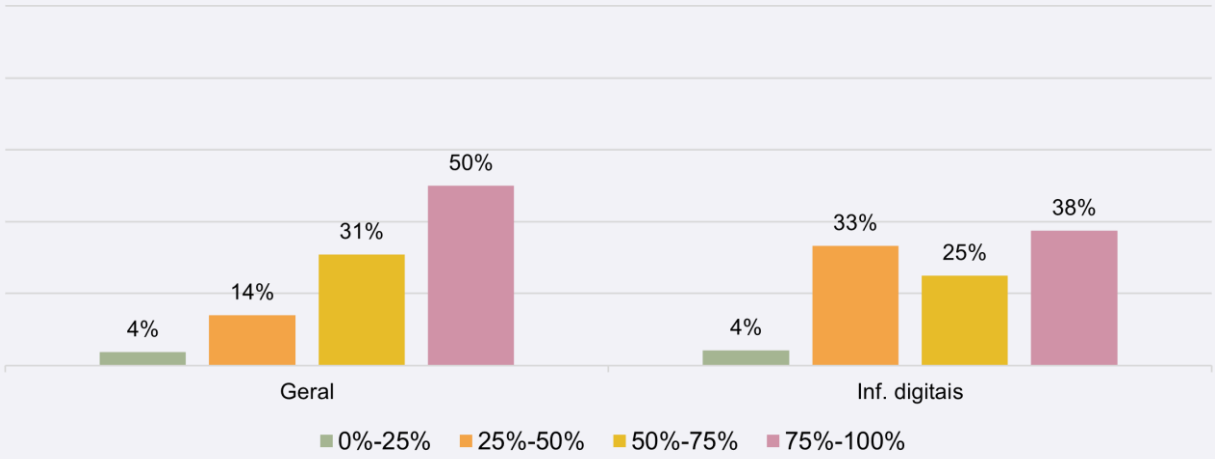


Os OSEs dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. No setor das infraestruturas digitais, registam-se alguns OSEs onde nem sempre o fornecimento dos equipamentos necessários é feito pelo OSE em questão, houve 79% de OSEs a indicar que eram sempre responsáveis pelo fornecimento dos equipamentos. Ressalva-se ainda que não se registaram situações em que os operadores nunca fornecem os equipamentos, impondo esse encargo aos colaboradores.

Novamente, sublinha-se que segundo o IUTICE de 2022, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais, abrangendo 28,1% do pessoal ao serviço[23].

[23] 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

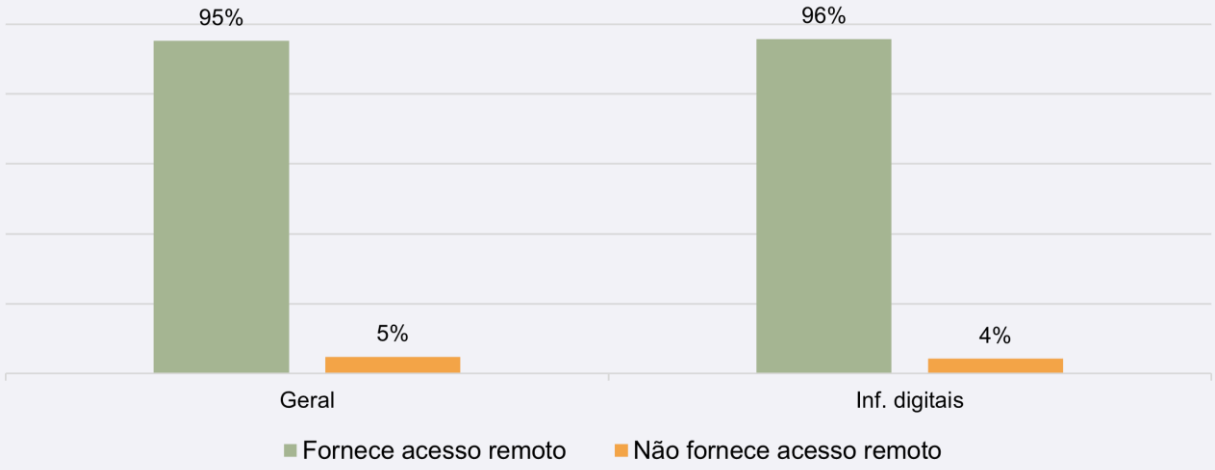


A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.
No setor das infraestruturas digitais a faixa predominante continua a ser aquela em que 75%-100% dos colaboradores tem acesso à Internet no desempenho das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

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 OSEs do que das várias empresas portuguesas. Juntando os dois intervalos onde mais de 50% dos colaboradores têm acesso à Internet, obtém-se 81% de OSEs onde 50% dos colaboradores acedem à Internet no desempenho das suas funções. No contexto empresarial português, apenas 48,9% dos colaboradores têm acesso à Internet para fins de trabalho. Mesmo comparando sectorialmente onde possível, como nos setores da energia e dos transportes, os OSEs 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 OSEs 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 OSEs 88% indicam haver 50% ou mais colaboradores com acesso à Internet para fins de trabalho[24].

[24] 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 OSEs aos colaboradores

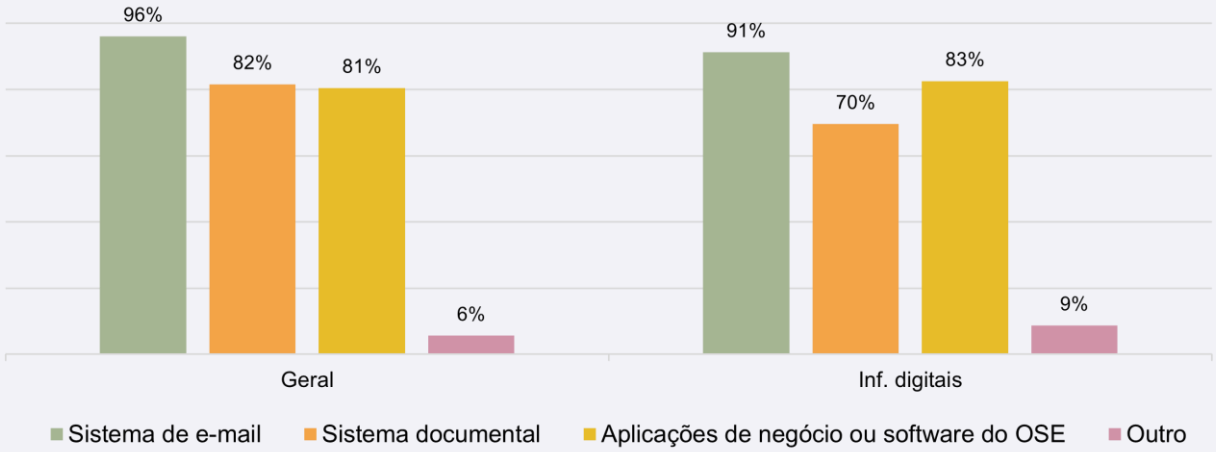


O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSEs aos colaboradores é uma realidade em praticamente todos os OSEs inquiridos (95%). O setor das infraestruturas digitais é um dos poucos onde se registaram exceções. Ainda assim, pelo menos 96% dos operadores neste setor fornecem acesso remoto a esses sistemas aos seus colaboradores.

Voltando a comparar com os dados do IUTICE de 2022, há uma maior percentagem de Operadores de Serviços Essenciais a fornecer acesso remoto ao sistema de e-mail do que na generalidade das empresas em Portugal. Enquanto 95% dos OSEs indicaram dar esse acesso remoto, no contexto empresarial geral apenas 74,7% das empresas fornecem acesso remoto ao sistema de e-mail[25].

[25] 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



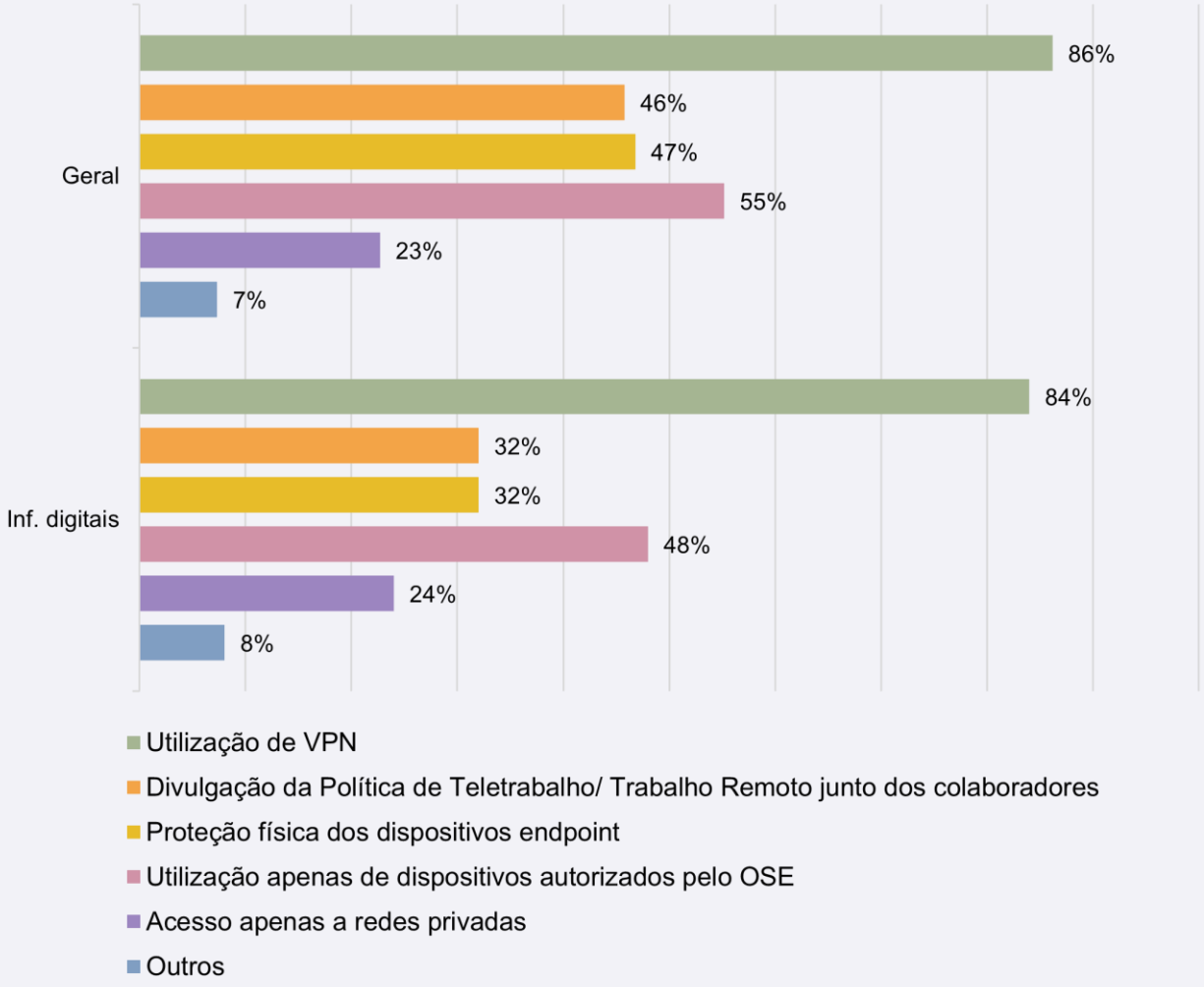
Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSEs a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no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

No setor das infraestruturas digitais, os sistemas de e-mail podem ser acedidos por 91%, documentais por 70% e aplicações de negócio 83% podem ser acedidos remotamente por todos os colaboradores.

Comparando novamente com dados do IUTICE de 2022, os OSEs 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 OSEs (95% a disponibilizar) e empresas (74,7% a disponibilizar). Revisitando essa comparação entre cada sistema, é visível que há mais OSEs a dar acesso remoto aos documentos da organização do que empresas em geral (82% de OSEs contra 65% de empresas) e também mais OSEs a dar acesso remoto a aplicações ou *software* de negócio (81%) do que empresas (63,9%)[26].

[26] 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 OSEs



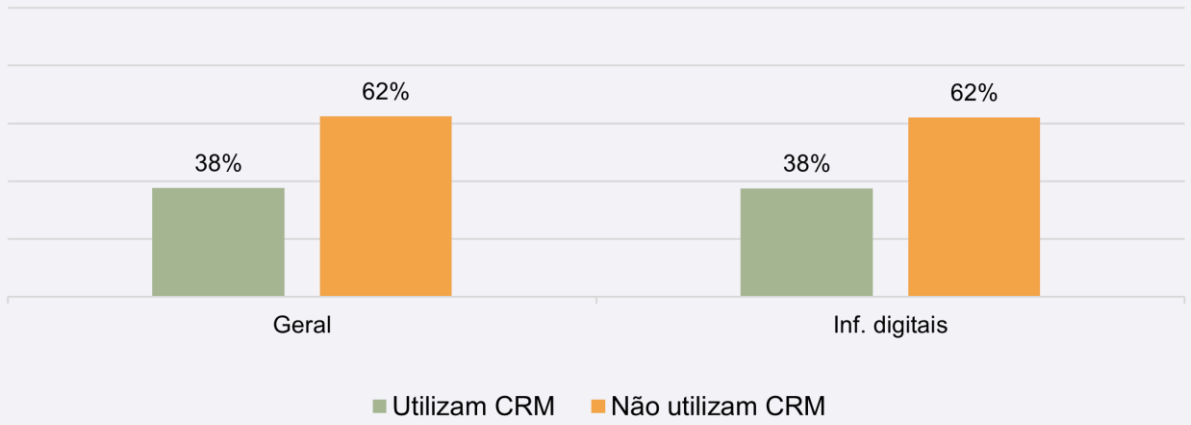
No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança para acesso remoto menos utilizada pelos OSEs. 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 OSEs, 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 setor das infraestuturas digitais mantem a tendência dos restantes setores.

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 OSEs que recorrem a esta medida.

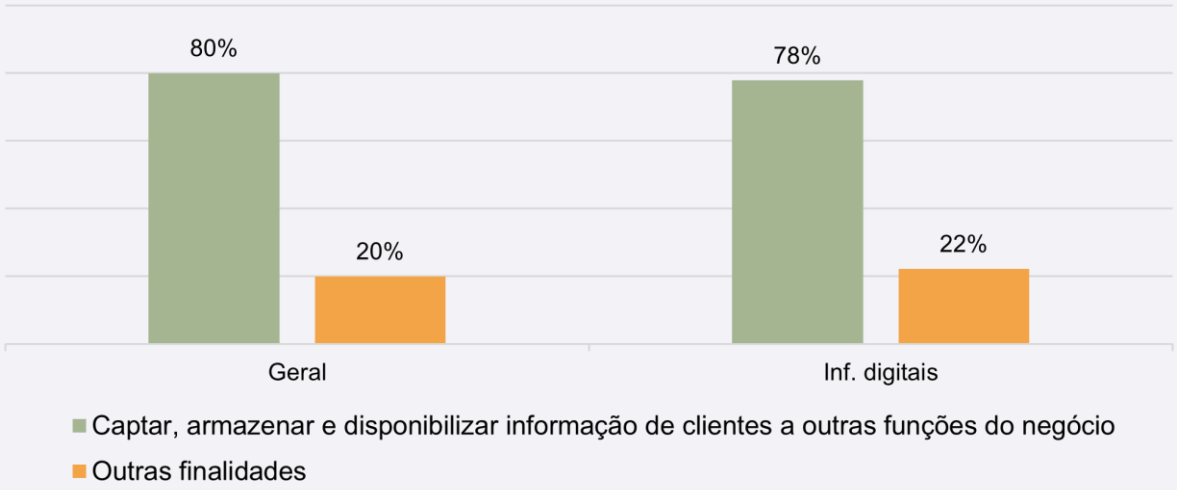
Gráfico 54 - OSEs que utilizam Customer Relationship Management software (CRM)



São mais os operadores que não utilizam *software* de *Customer Relationship Management* (CRM)[27] - 62% - do que aqueles que utilizam - 38%. Curiosamente, o setor das infraestuturas digitais apresenta os mesmos valores que a generalidade.

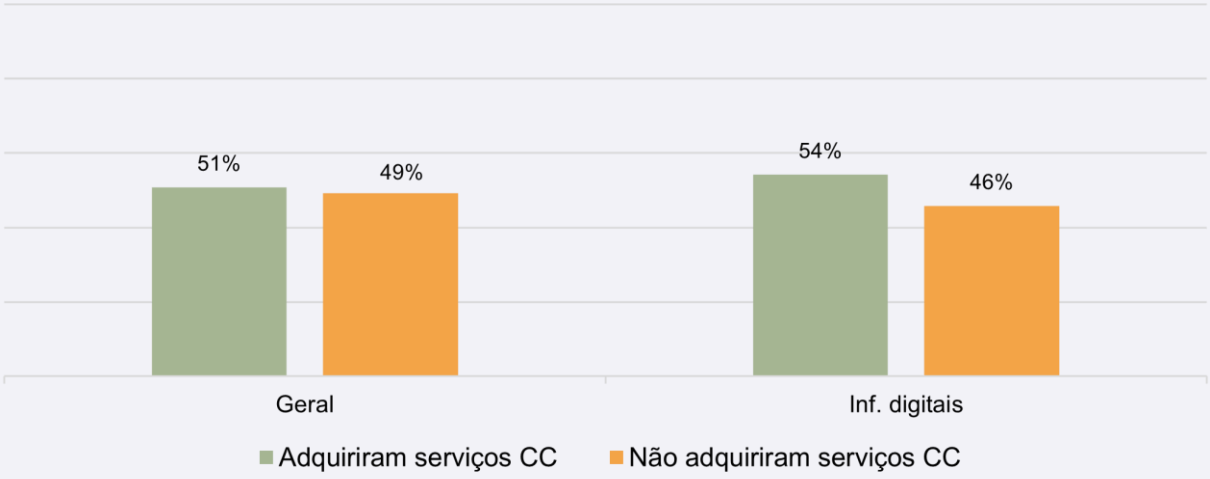
[27] *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos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

Gráfico 55 - OSEs 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. No setor das infraestruturas digitais a utilização de CRM para captar, armazenar e disponibilizar informações é apenas 2% inferior à generalidade.

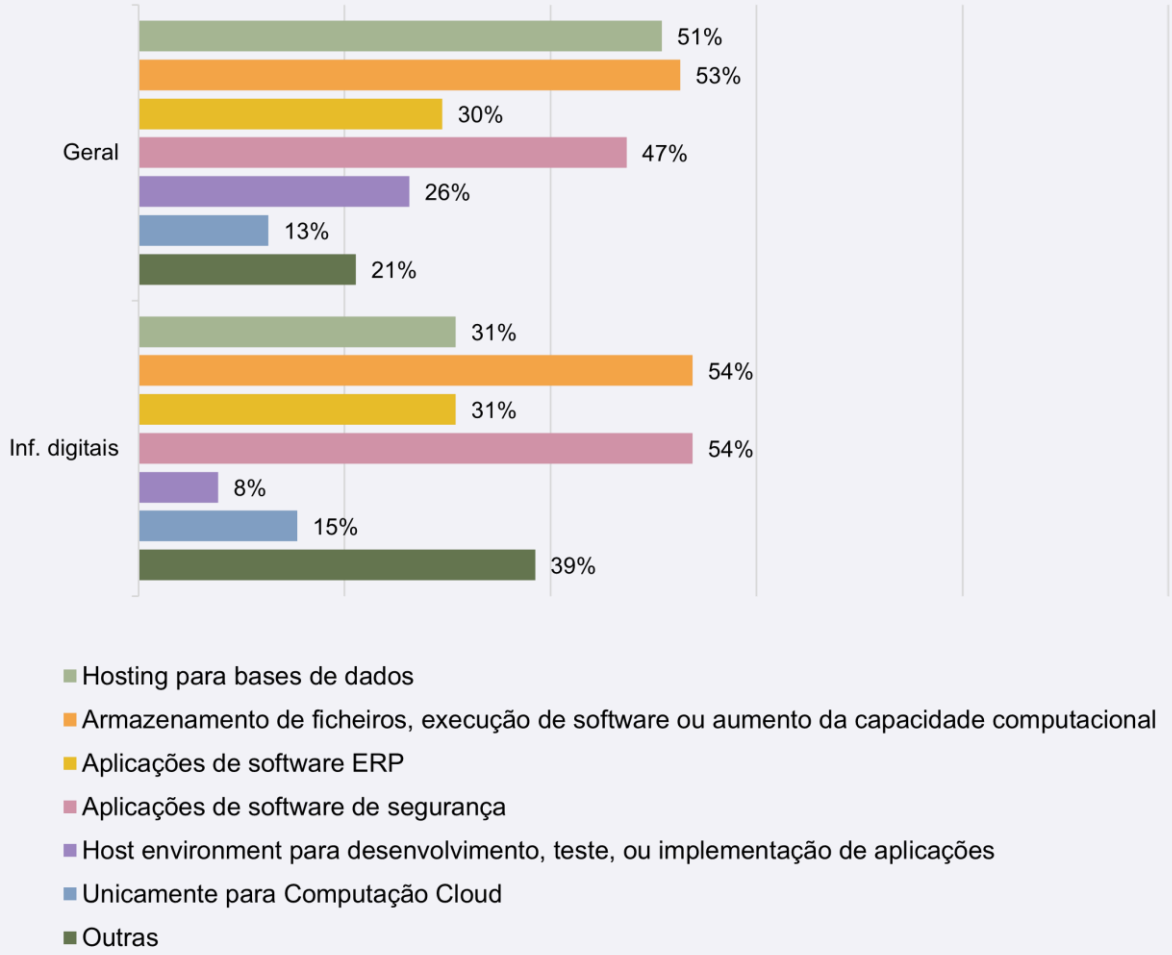
Gráfico 56 - OSEs que adquiriram serviços de Computação *Cloud* (CC)



À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização.
Nas infraestruturas digitais, apenas 54% dos OSEs adquiriram serviços CC.

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 OSEs colocaram o investimento em serviços *cloud* como um dos principais objetivos de 2021[28]. Em 2023, este tipo de serviços continuou a ser uma das áreas onde os OSEs mais aumentaram o seu investimento (49% dos OSEs inquiridos pela ENISA em 2023 indicaram ter aumentado os seus investimentos em plataformas *cloud*)[29]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[30].

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[31] aplicações de *software* de segurança;

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

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

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

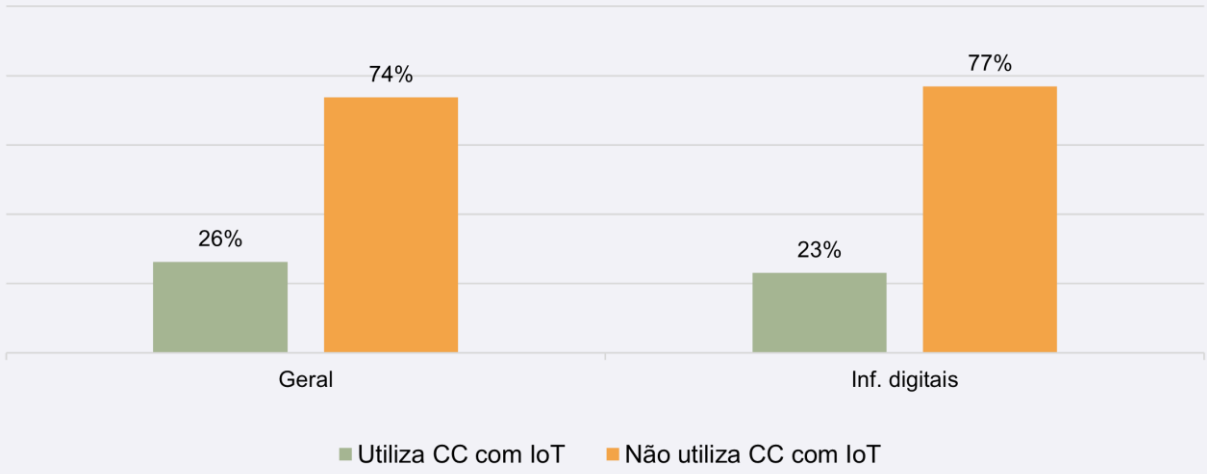
[31] *ERP (Enterprise Resource Planning)* refere-se a um tipo de *software* que as organizações utilizam para gerir os seus recursos e atividades do dia-a-dia, passando pela gestão de projetos, de recursos humanos e logística, entre outras áreas fundamentais para o funcionamento de uma organização. Uma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

host environment para desenvolvimento, teste ou implementação de aplicações; e, por fim, exclusivamente para Computação *Cloud*.
De forma geral, é mais comum os operadores terem como finalidade *hosting* para bases de dados, armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional e aplicações de *software* de segurança.

No setor das infraestruturas digitais, menos finalidades foram indicadas por uma maioria significativa dos OSEs. Neste setor, as duas finalidades indicadas (armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional e utilização de *software* ou de aplicações de segurança) apenas no setor das infraestruturas digitais foram indicadas por mais de 50% dos inquiridos (54%). As restantes finalidades foram indicadas neste setor por cerca de 30% ou menos dos OSEs inquiridos.

Comparando com dados do IUTICE de 2023, os serviços de *cloud computing* foram adquiridos pelas empresas em Portugal tendo em vista o funcionamento do serviço de correio eletrónico (91,1%), o armazenamento de ficheiros (73,7%), o funcionamento de *software* de aplicações de segurança (67,2%) e *software* de escritório (66,1%)[32].

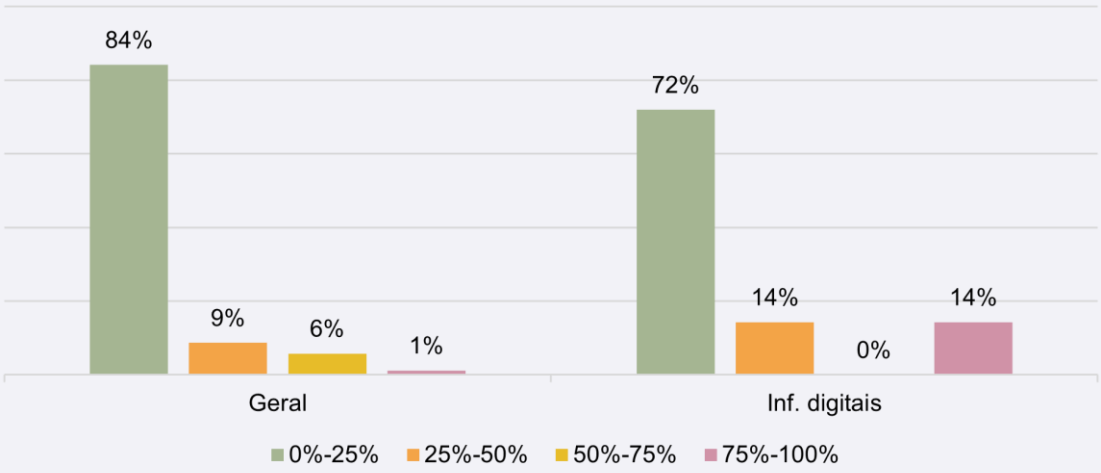
Gráfico 58 - Utilização de serviços de CC em conjunto com *Internet of Things* (IoT)



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%).
O setor das infraestruturas digitais é um dos setores em estudo onde os operadores mais utilizam os serviços CC em conjunto com *Internet of Things*, ultrapassando os 23% de utilização.

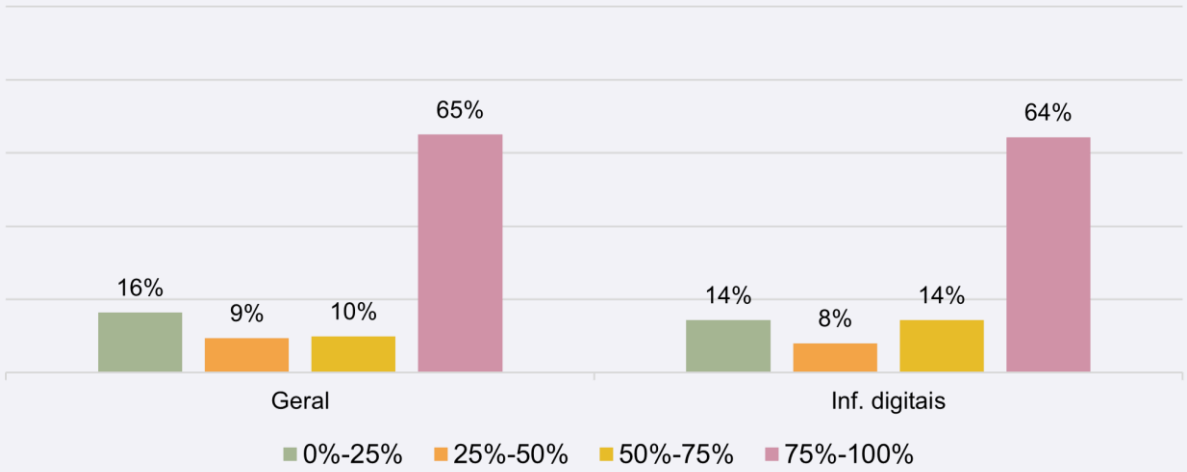
[32] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 59 - Percentagem de sistemas core em *cloud*



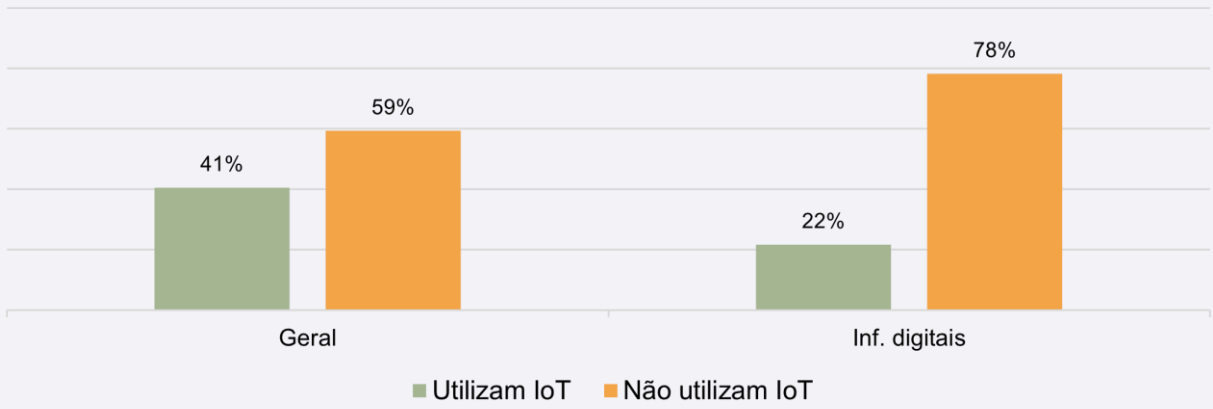
Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos. O setor das infraestruturas digitais não apresenta valores na percentagem de 50%-75%.

Gráfico 60 - Percentagem de sistemas core on-perm



Contrastando com o gráfico anterior, aqui se mostra a tendência dos operadores em manter os seus sistemas core no próprio ambiente da organização (on-prem) e não na cloud. De um modo geral, cerca de 60% dos operadores inquiridos referem que mantêm entre 75% a 100% de sistemas principais dentro do ambiente de TI da sua organização. Nas infraestruturas digitais a maioria dos operadores tem entre 0 a 25% de sistemas principais.

Gráfico 61 - Utilização de IoT pelos OSEs

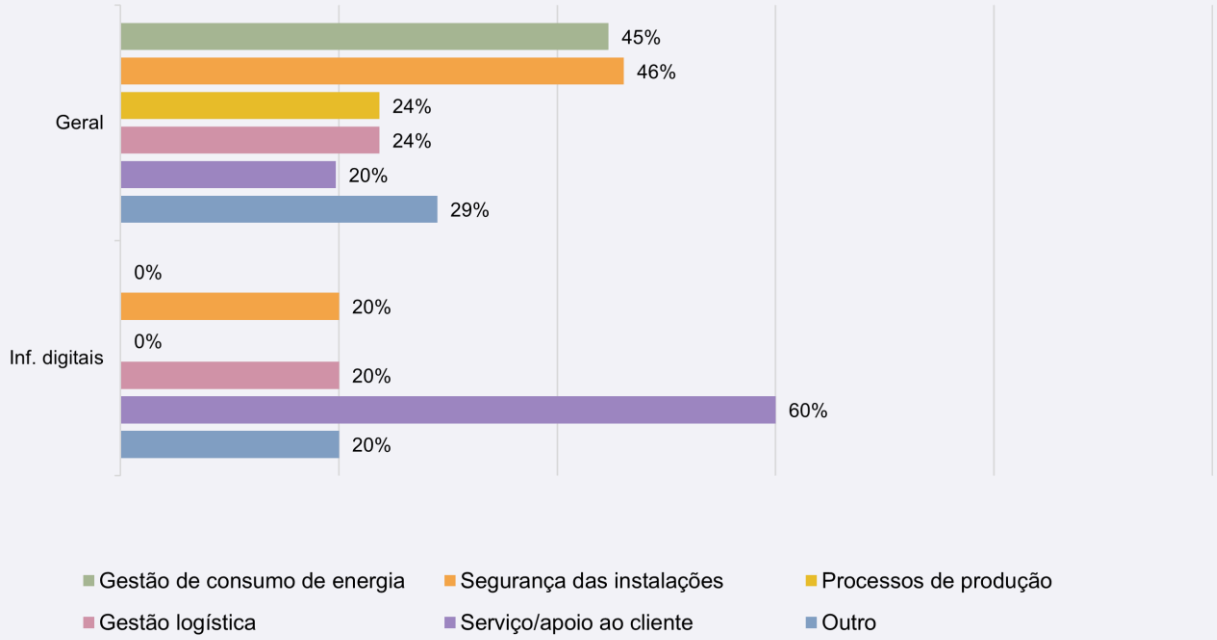


A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT.
No setor das infraestruturas digitais prevalece a não utilização de IoT, nomeadamente 78% dos OSEs não utiliza.

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%[33].

[33] 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

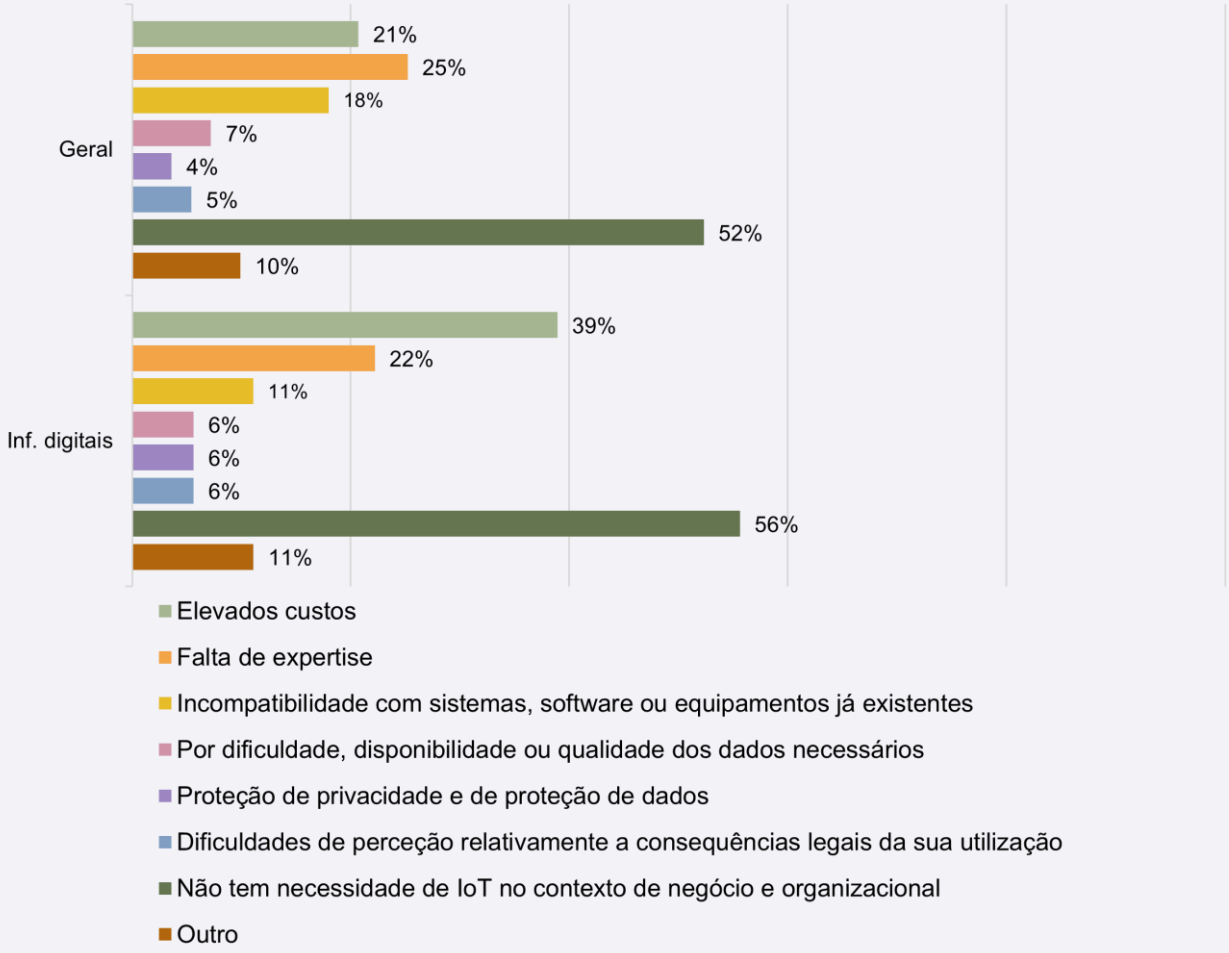


De maneira geral, a utilização de IoT é mais comum nos contextos de gestão do consumo de energia e de segurança das instalações, respondido por cerca de 45% dos inquiridos, ao contrário da utilização de IoT para serviço/apoio ao cliente, que tem menos expressividade, cerca de 20%. No setor das infraestruturas digitais, a utilização de IoT foi para a segurança das instalações (20%), gestão logística (20%), serviço/apoio ao cliente 60% e outras finalidades (20%). Não foi mencionada a utilização para gestão de consumo de energia ou 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%)"[34].

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

Gráfico 63 - Motivos pelos quais não utilizam IoT

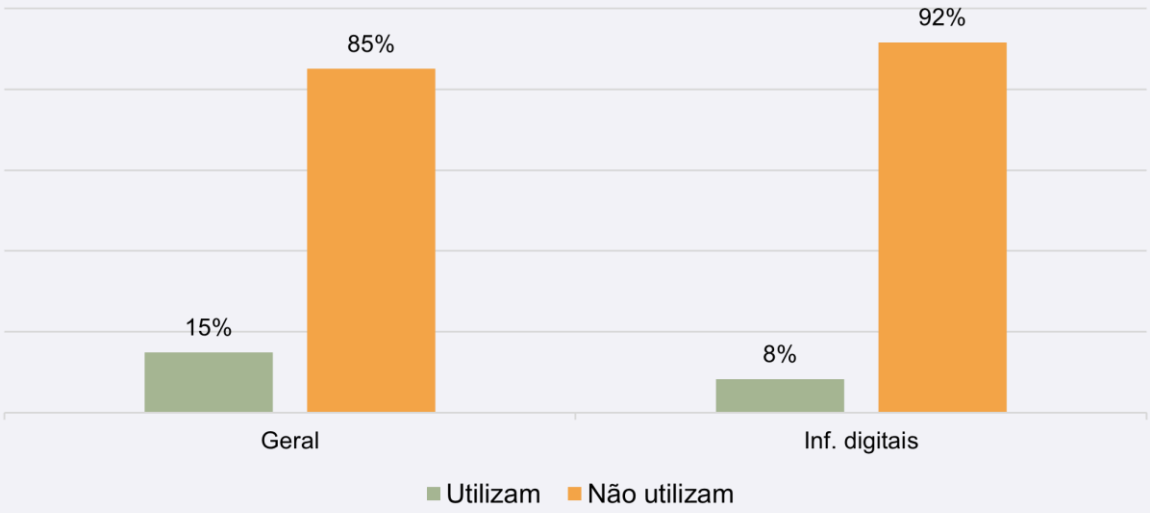


São vários os motivos que fazem com que os operadores não utilizem IoT, desde os custos associados à incompatibilidade com sistemas em utilização, passando por vários outros. No entanto, o motivo mais evidente para a não utilização de IoT é não haver necessidade para tal no contexto de negócio ou organizacional (52%).

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

O setor das infraestruturas digitais menciona que os principais motivos para a não utilização de IoT são a não necessidade de IoT no contexto de negócio e organizacional bem como os elevados custos.

Gráfico 64 - OSEs que utilizam processos que recorrem a IA



A utilização ou o recurso à IA é ainda reduzido entre os OSEs. 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. Apenas 8% dos OSEs do setor das infraestruturas digitais mencionam utilizar processos que recorrem a 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 OSEs 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%)[35], quando no questionário do CNCS o setor da energia surge como aquele onde mais OSEs 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%[36].

[35] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2023, 16-17.
[36] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2023, 16-17.

Gráfico 65 - Funções para as quais utilizam IA

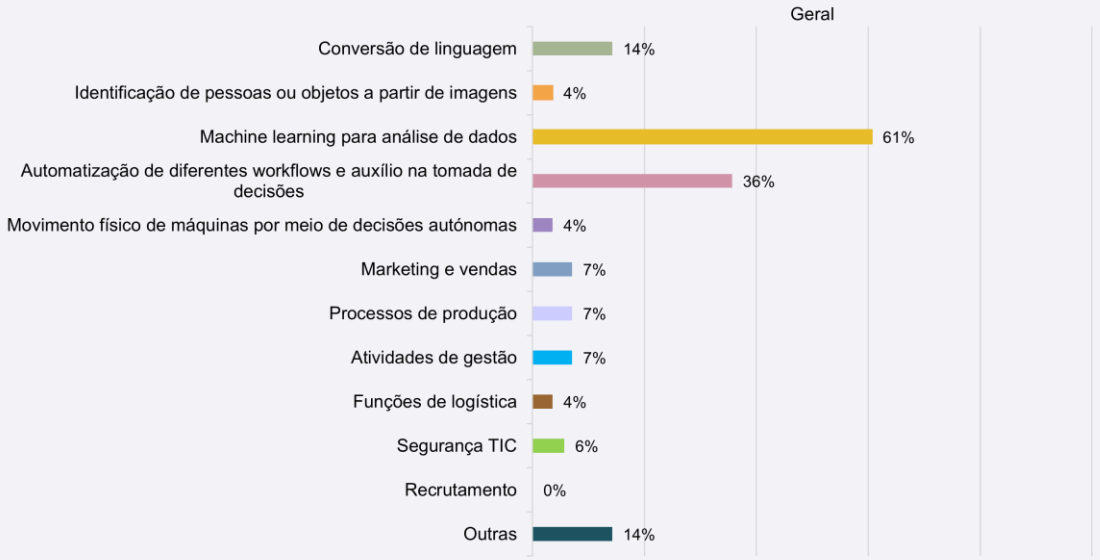
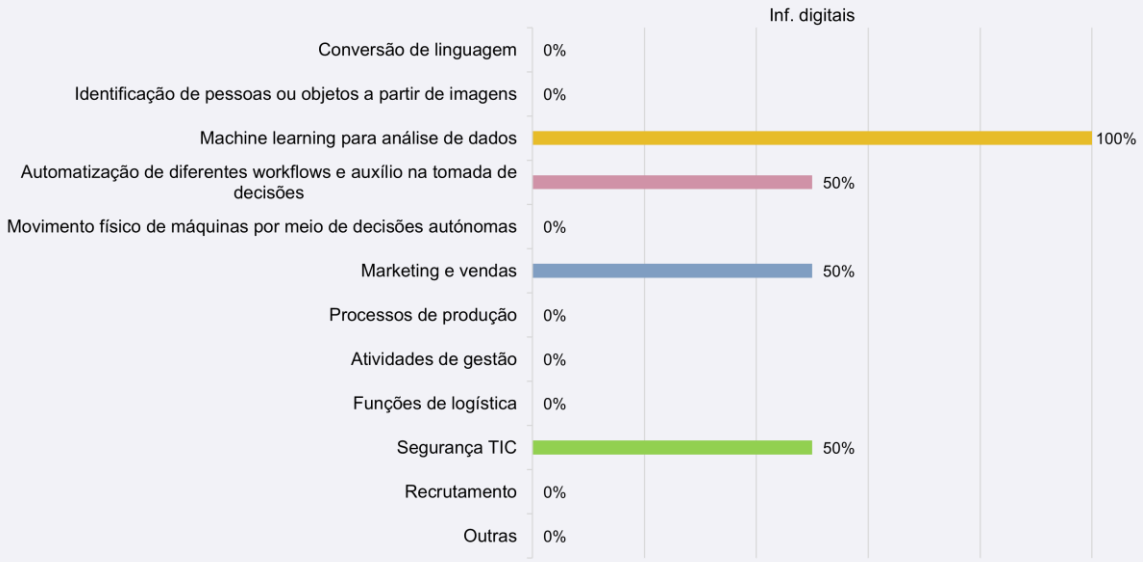


Gráfico 65.1 - Funções para as quais utilizam IA (Infraestruturas Digitais)



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

As restantes funções surgem de forma mais residual, sendo indicadas por apenas 15% ou menos dos OSE que já recorrem a IA. Curiosamente, não se registou o recurso a Inteligência Artificial em processos de recrutamento entre os OSE inquiridos.
No setor das infraestruturas digitais, os OSEs mencionam utilizar IA em *machine lerning* para analise de dados, automatização de fluxos de trabalho e auxílio na tomada de decisões, marketing e vendas bem como em segurança TIC.

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[37].

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”[38]. 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%[39].

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

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança

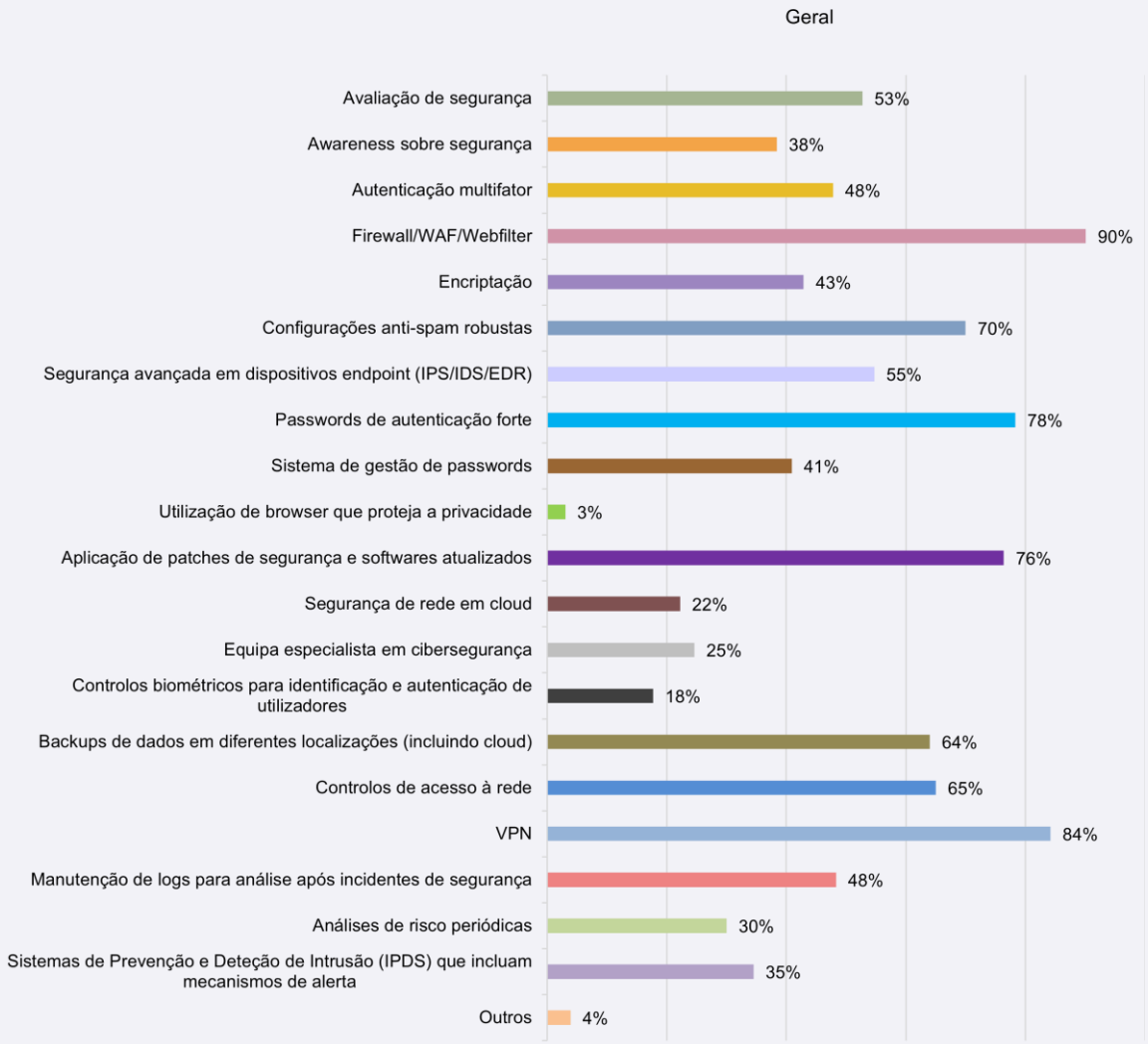


Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança

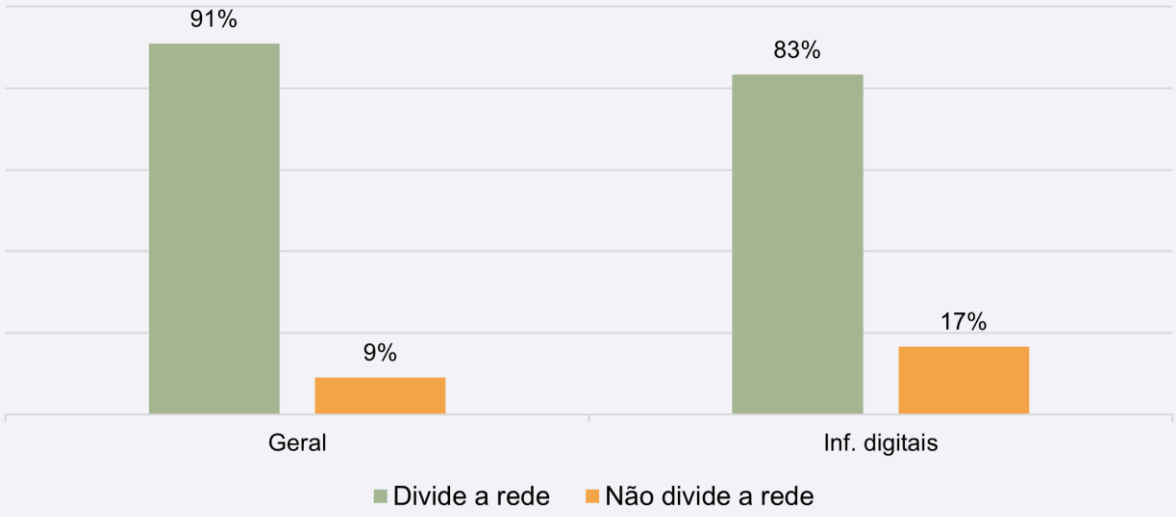
Na análise geral das medidas de segurança utilizadas pelos operadores, é possível verificar que medidas técnicas como a utilização de Firewall/WAF/Webfilter, utilização de VPN, palavras-passe de autenticação forte, aplicação de patches de segurança, a atualização dos softwares e backups de dados em diferentes 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%[40].

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 multi-fator (37%) e criptografia de dados, para proteger os ativos da empresa (36%)[41].

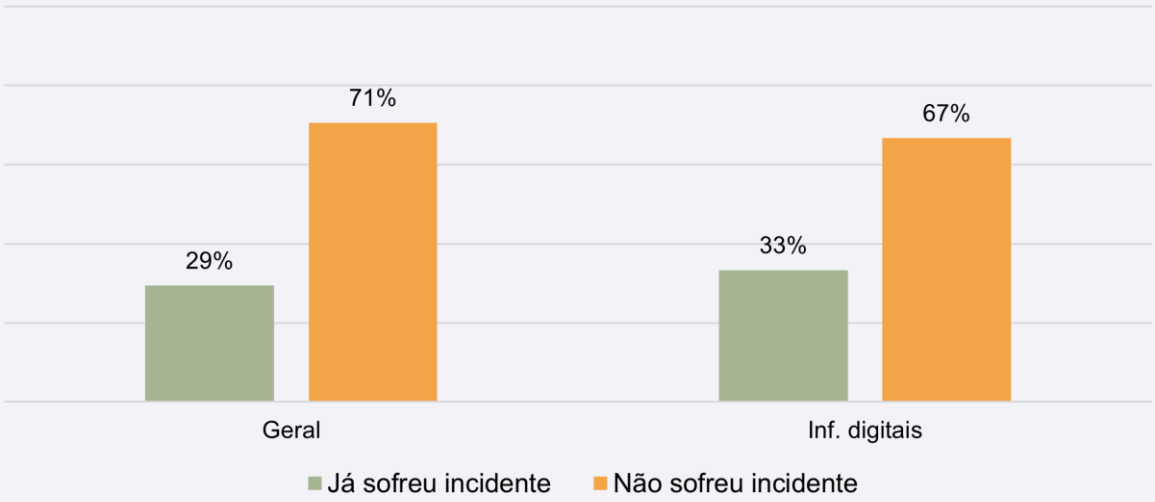
Gráfico 67 - Divisão entre rede dos colaboradores e rede para *guests*



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%. No setor das infraestruturas digitais apenas 17% não divide a rede.

[40] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 18.
[41] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 7.

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



Em contexto TIC, pelo observado no gráfico, conclui-se que a maioria dos OSEs inquiridos (71%) não sofreu incidentes neste contexto. Quanto ao setor inquirido das infraestruturas digitais, 33% dos OSEs mencionaram já ter sofrido incidentes.

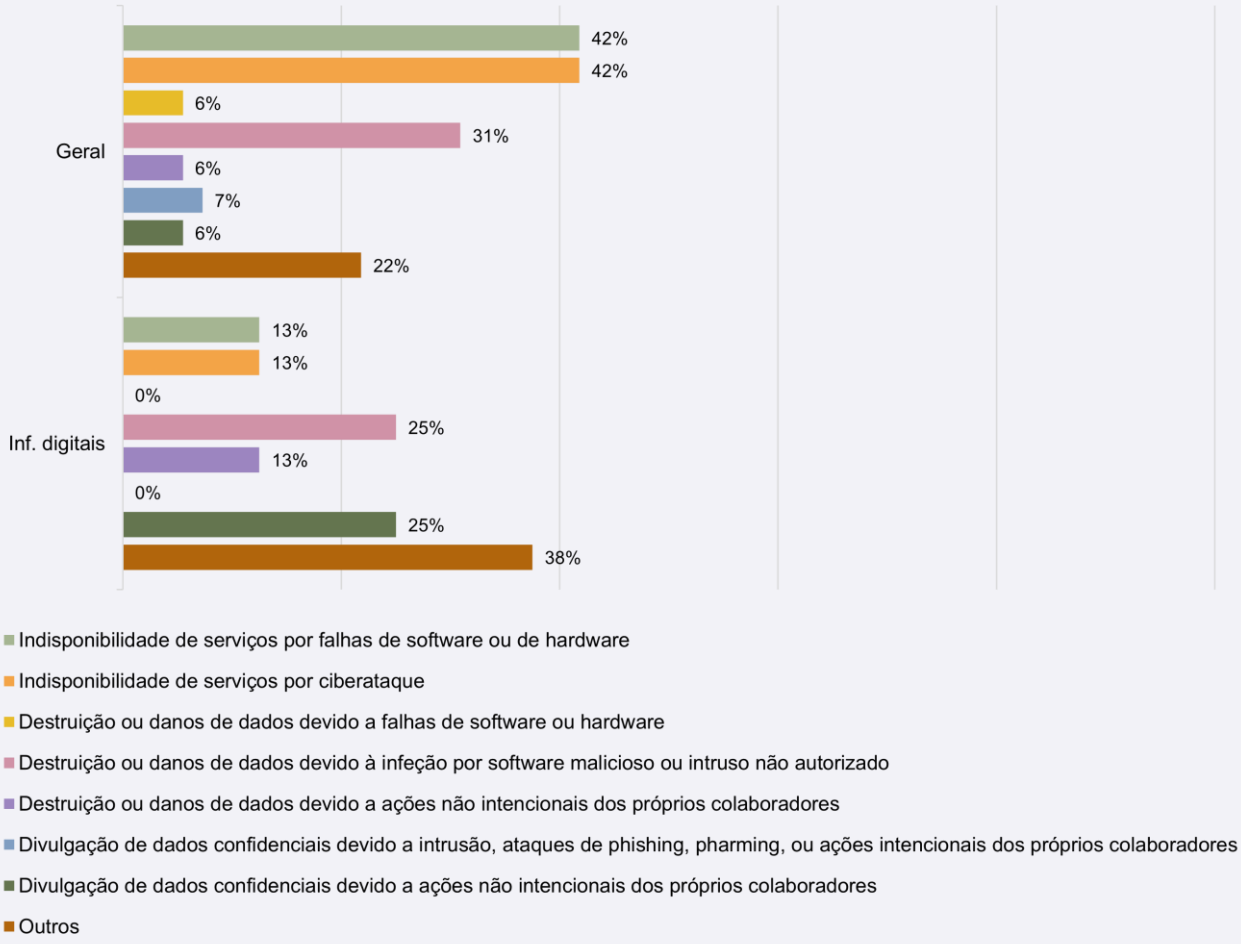
Sendo o IUTICE de 2022, Portugal registou a segunda menor proporção de empresas com incidentes de segurança das TIC na União Europeia (UE). Em 2021, 89,7% das empresas em Portugal, e 91,8% no total da UE, utilizaram pelo menos uma medida para garantir a integridade, a disponibilidade e a confidencialidade dos seus dados e sistemas de Tecnologias de Informação e Comunicação (TIC)[42].

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[43].

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

[43] 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



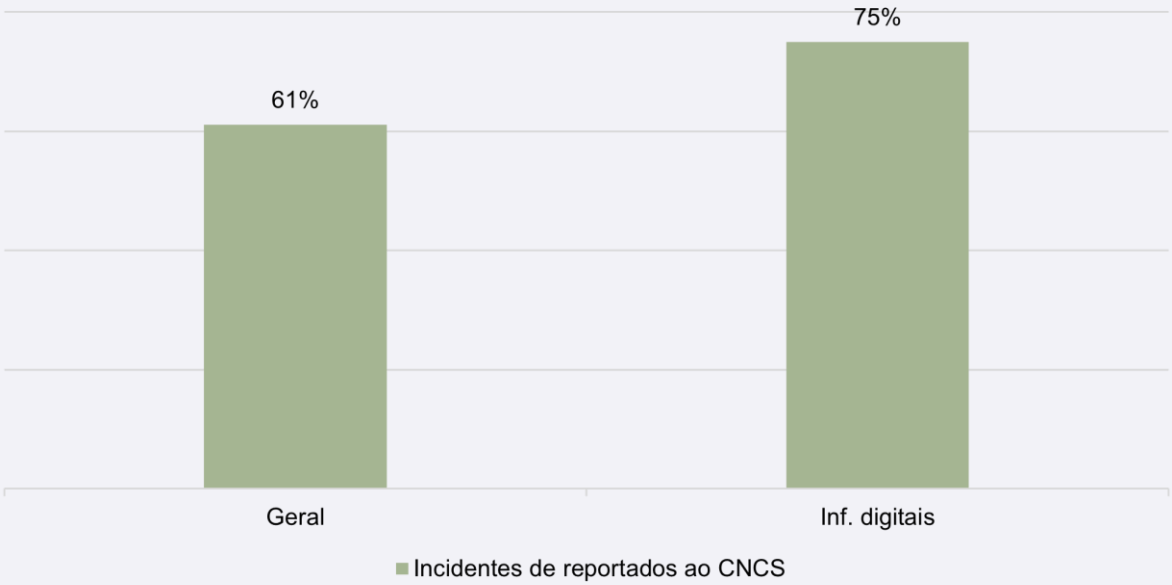
A grande maioria dos incidentes ocorridos afetou a disponibilidade dos serviços, quer por falha de *software* ou de *hardware*, quer por ciberataque. Depois destes, seguem-se os incidentes que resultaram na destruição de dados devido à infeção por *malware* ou devido a intrusão. Os operadores que referiram 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 das infraestruturas digitais os efeitos dos incidentes dividem-se entre a indisponibilidade de serviços por falha de *software* ou *hardware* e indisponibilidade de serviços por ciberataque.

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)[44].

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[45].

Gráfico 70 - Incidentes de cibersegurança reportados pelos OSEs ao CNCS



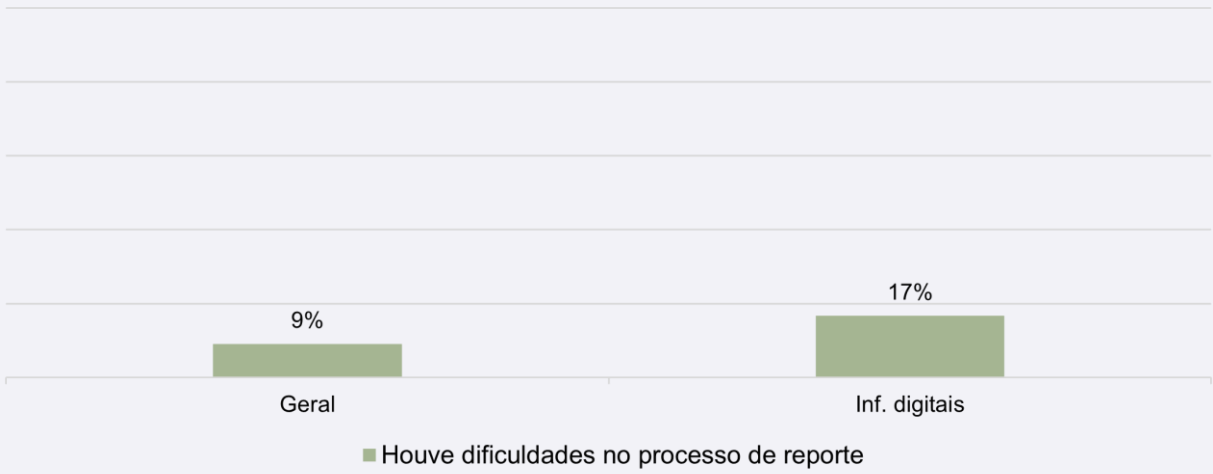
De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSEs, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n. º1 do artigo 16.º da lei n. º46/2018, de 13 de agosto, os OSEs estão apenas 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**.

[44] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 20.
[45] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 6.

No setor das infraestruturas digitais, observa-se a mesma tendência que na generalidade, onde a maior parte dos operadores notificaram o CNCS. No entanto, como podemos verificar no **Gráfico 75,** em todos os casos onde o incidente não foi notificado, o impacto não foi relevante para a continuidade dos serviços.

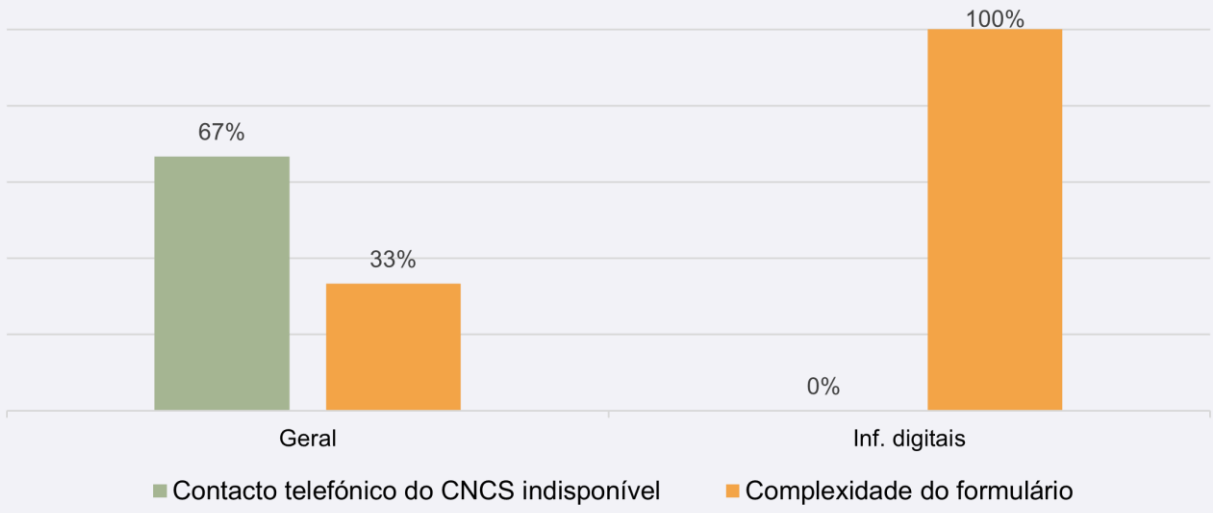
No entanto, como podemos verificar no **Gráfico 75,** em todos os casos onde o incidente não foi notificado, o impacto não foi relevante para a continuidade dos serviços.

Gráfico 71 - Dificuldades no processo de notificação ao CNCS



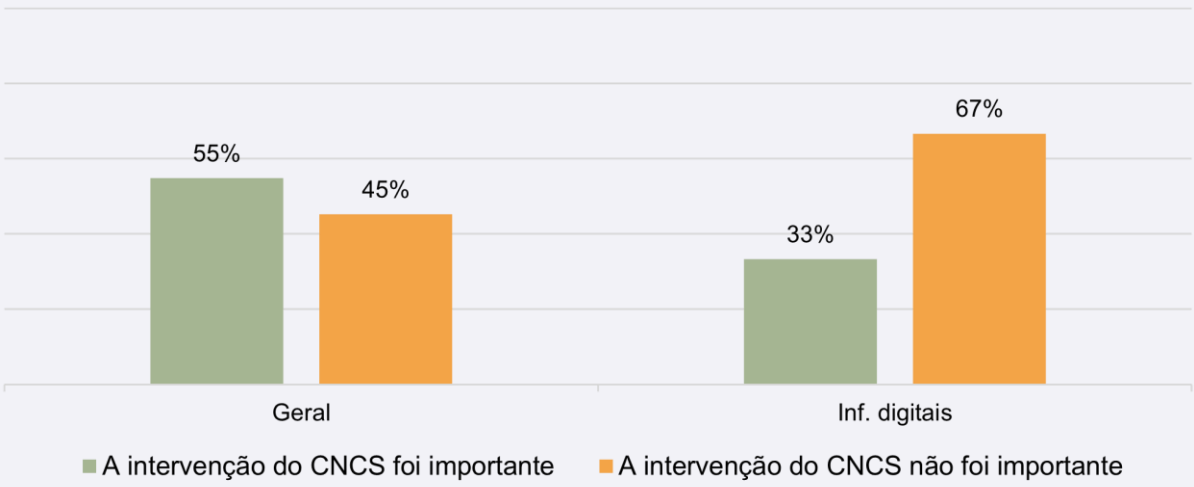
De modo geral, os operadores não tiveram dificuldades no processo de notificação de incidentes ao CNCS. No entanto, a nível geral, houve ainda cerca de 9% dos operadores a indicarem dificuldades na notificação. O setor das infraestruturas digitais destaca-se superando a generalidade, onde 17% mencionou dificuldades no processo de reporte.

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



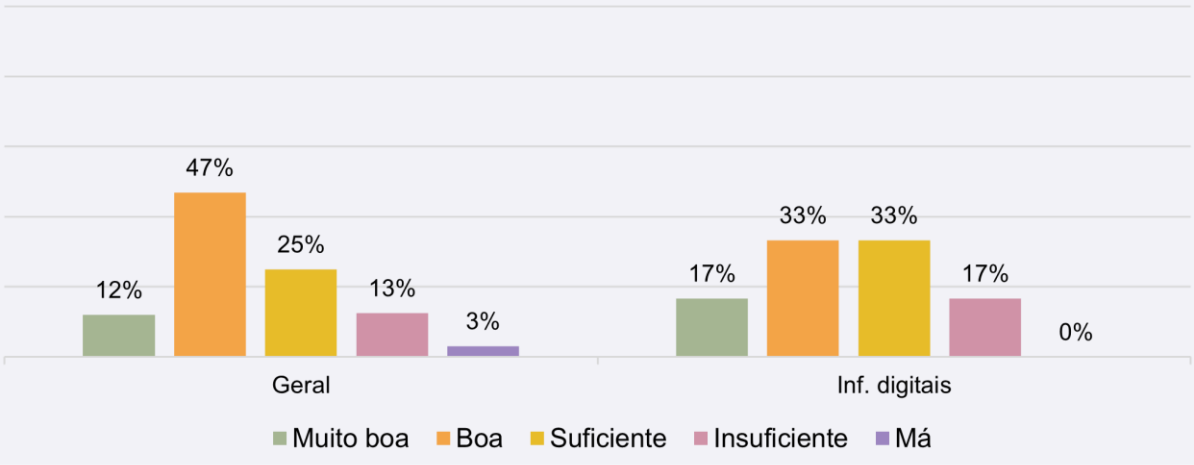
Entre os setores que identificaram dificuldades na notificação de incidentes ao CNCS, dois referiram que a principal dificuldade durante o processo de notificação foi a indisponibilidade do contacto telefónico e um (infraestruturas digitais) atribuiu a principal dificuldade à complexidade do formulário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

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%).
No setor das infraestruturas digitais, predomina a opinião de que a intervenção do CNCS não foi relevante para a resolução do incidente notificado, referido por dois terços dos inquiridos.

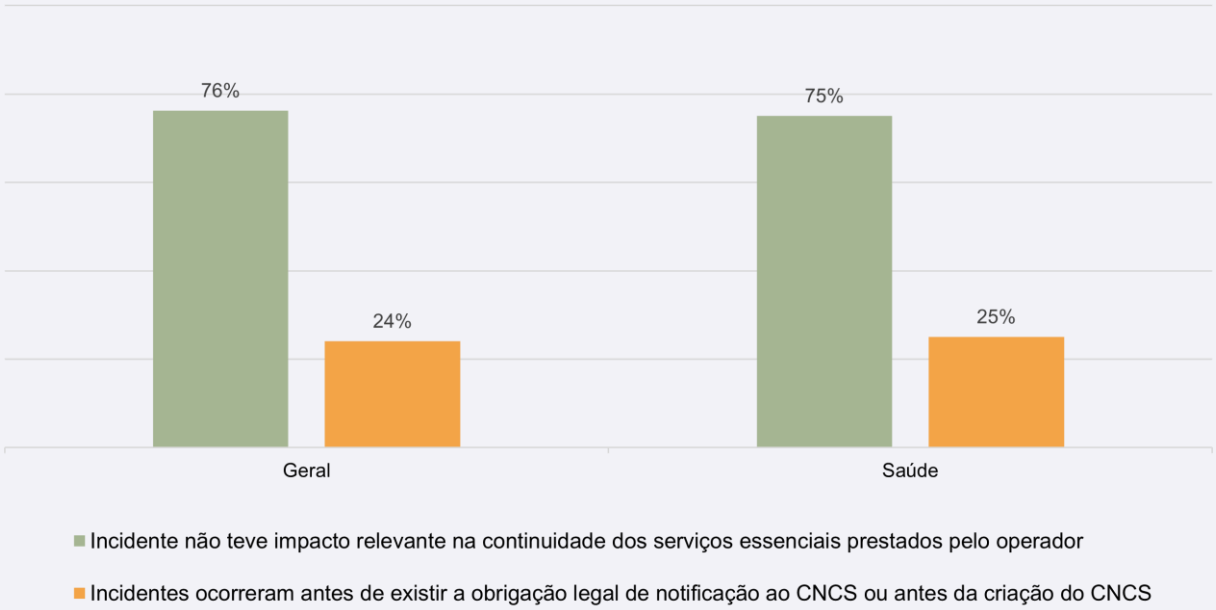
Gráfico 74 - Avaliação da resposta dada pelo CNCS



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%).

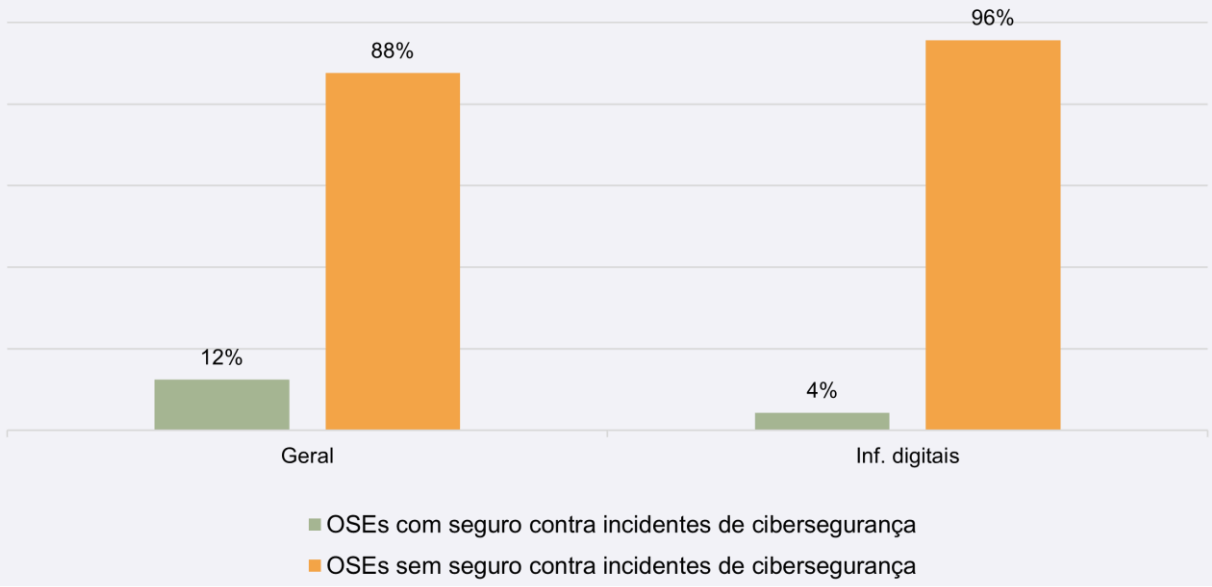
No setor das infraestruturas digitais existem algumas discrepâncias nas perspetivas dos diferentes operadores. Em geral, a opinião foi positiva, no entanto, mais de 15% classificou a resposta do CNCS como insuficiente.

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 OSEs, 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 das infraestruturas digitais mencionou que o incidente não teve impacto relevante na continuidade dos serviços essenciais.

Gráfico 76 - Seguro contra incidentes de cibersegurança



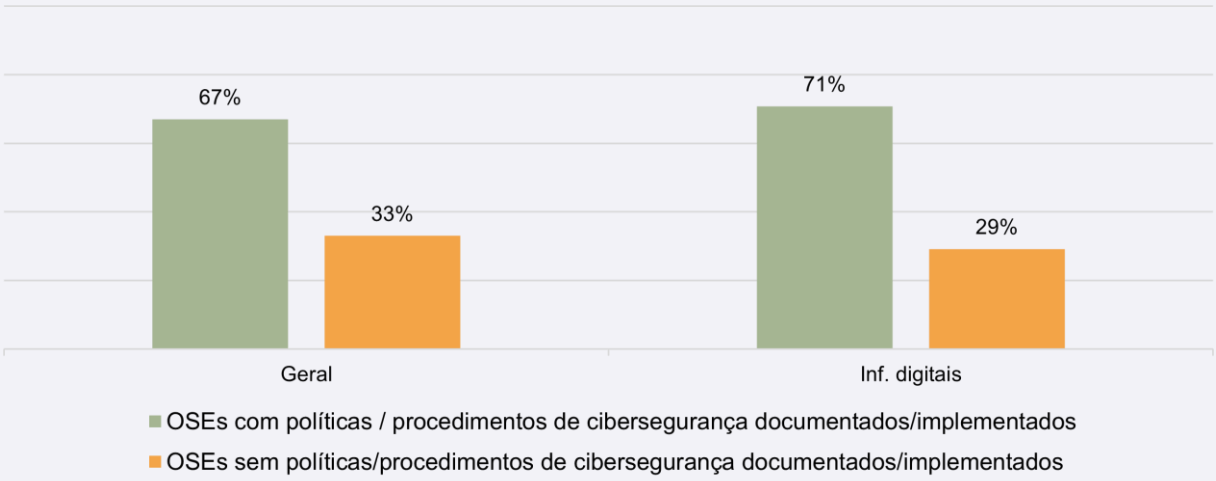
Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. A lógica geral mantém-se no setor das infraestruturas digitais, com a maior parte dos inquiridos a não possuírem este tipo de seguro (96%).

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[46].

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[47].

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

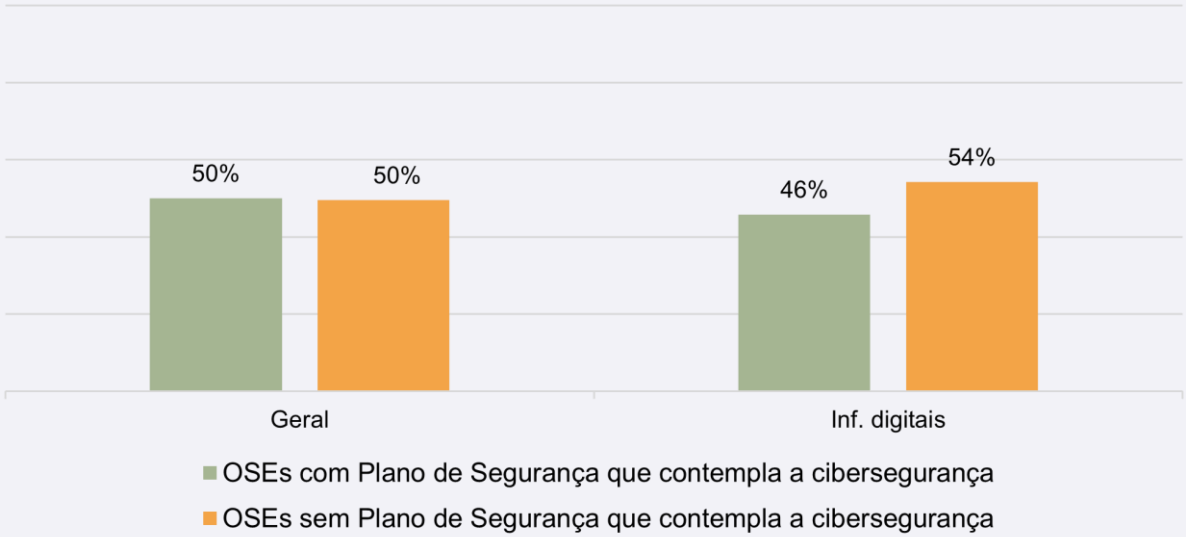
Gráfico 77 - Documentação/implementação de políticas e procedimentos de cibersegurança



Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados. No setor das infraestruturas digitais, 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[48].

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



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

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 das infraestruturas digitais a pergentagem de OSEs com plano de segurança é 4 p.p inferior à generalidade.

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[49].

Gráfico 79 - Políticas incluídas no Plano de Segurança

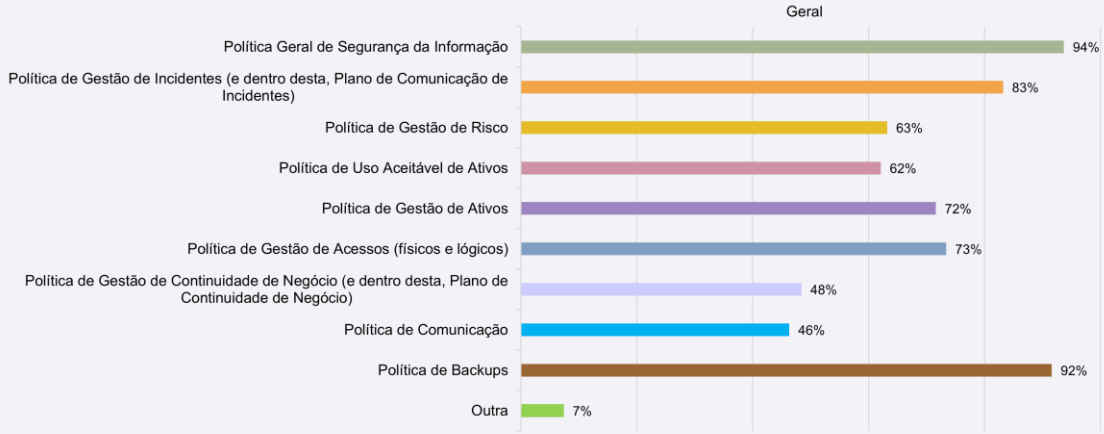
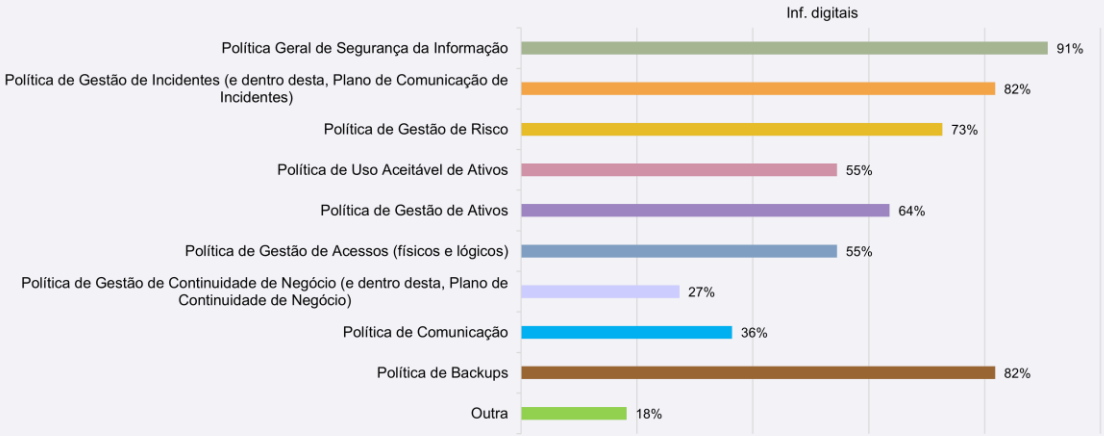


Gráfico 79.1 - Políticas incluídas no Plano de Segurança

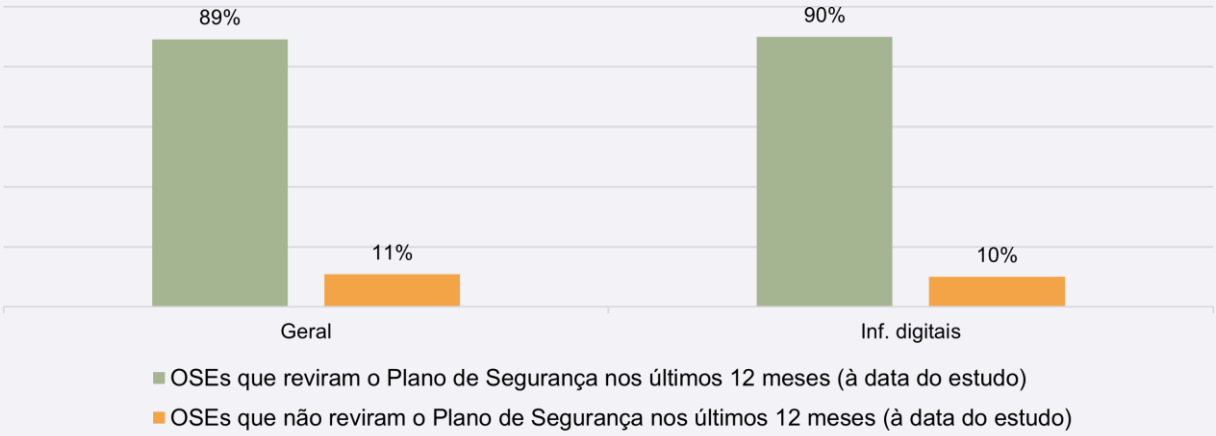


Os gráficos acima representam a percentagem de operadores com plano de segurança que tem as diversas políticas elencadas elaboradas no âmbito desse mesmo plano.
As políticas mais comuns são a Política de Geral de SI (94%), a Política de Backups (92%), a Política de Gestão de Incidentes (83%), a Política de Gestão de Acessos (73%), a Política de

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

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 das infraestruturas digitais, a grande maioria dos operadores com plano de segurança realizou a revisão do mesmo. apenas 10%, respetivamente, dos operadores refere não realizar o plano de segurança nos últimos 12 meses (à data do estudo).

Segundo dados do IUTICE 2022, a maioria (61,7%) das empresas definiu ou fez uma revisão aos documentos sobre medidas, práticas ou procedimentos de segurança nos últimos 12 meses[50].

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

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

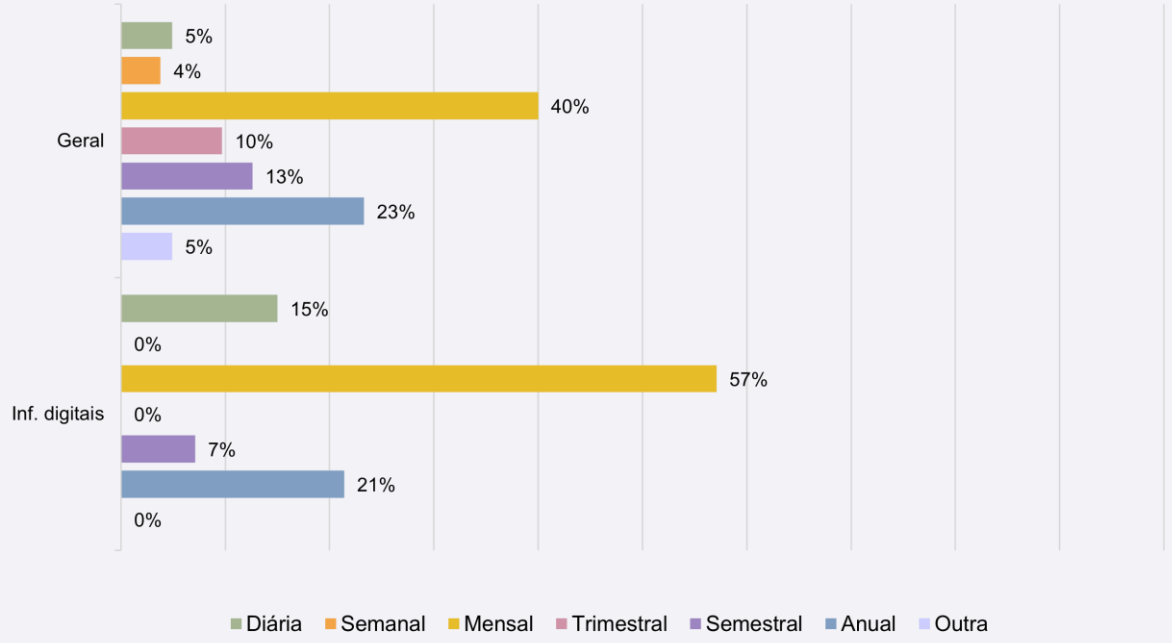
Mais de 60% dos operadores inquiridos dos diferentes setores referem realizar procedimentos de deteção e gestão de vulnerabilidades. 67% dos OSEs inquiridos do setor das infraestruturas digitais realiza os procedimentos.

Gráfico 82 - OSEs 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.

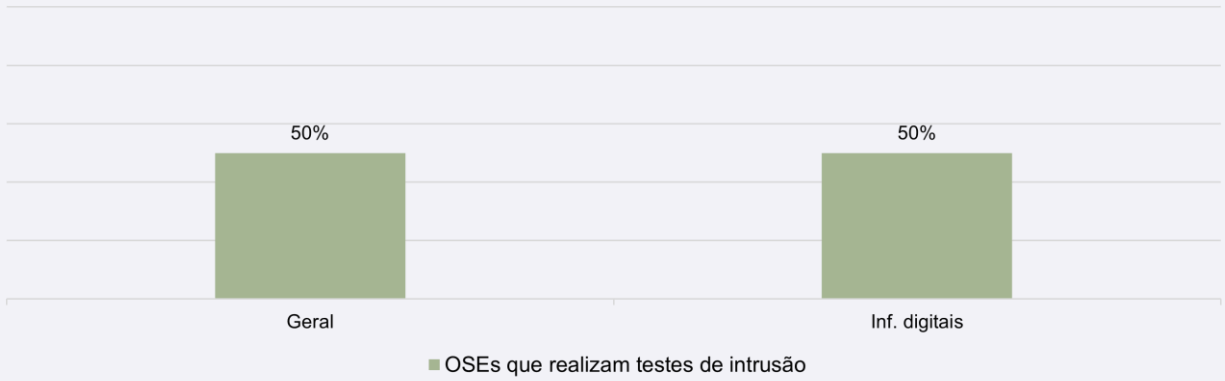
No setor das infraestruturas digitais, embora a análise de vulnerabilidades não seja realizada por todos os operadores de cada setor, esta é realizada por pelo menos 88% dos operadores inquiridos.

Gráfico 83 - Frequência da análise de vulnerabilidades



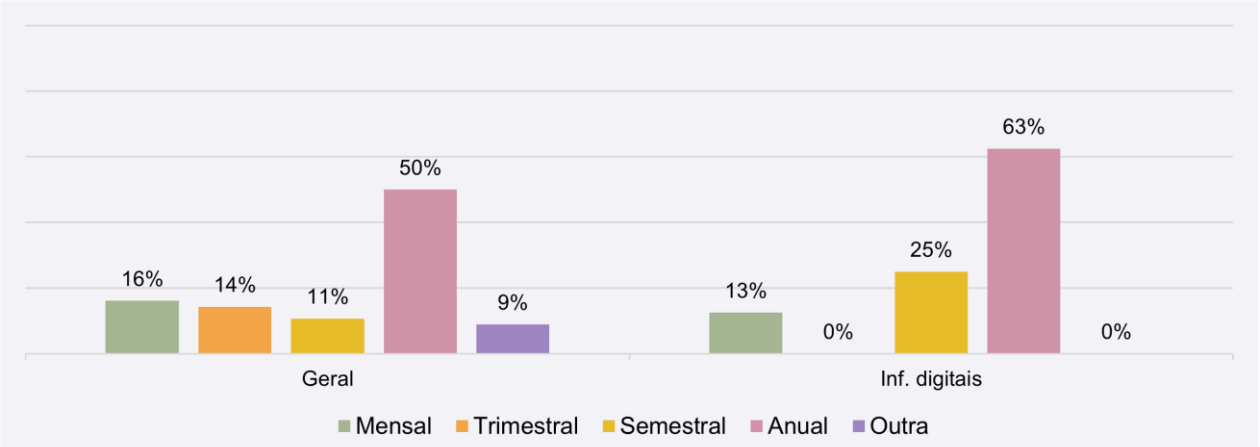
A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.
A frequência semanal e trimestral não foi mencionada por nenhum dos OSEs inquiridos do setor das infraestruturas digitais.

Gráfico 84 - Realização de testes de intrusão



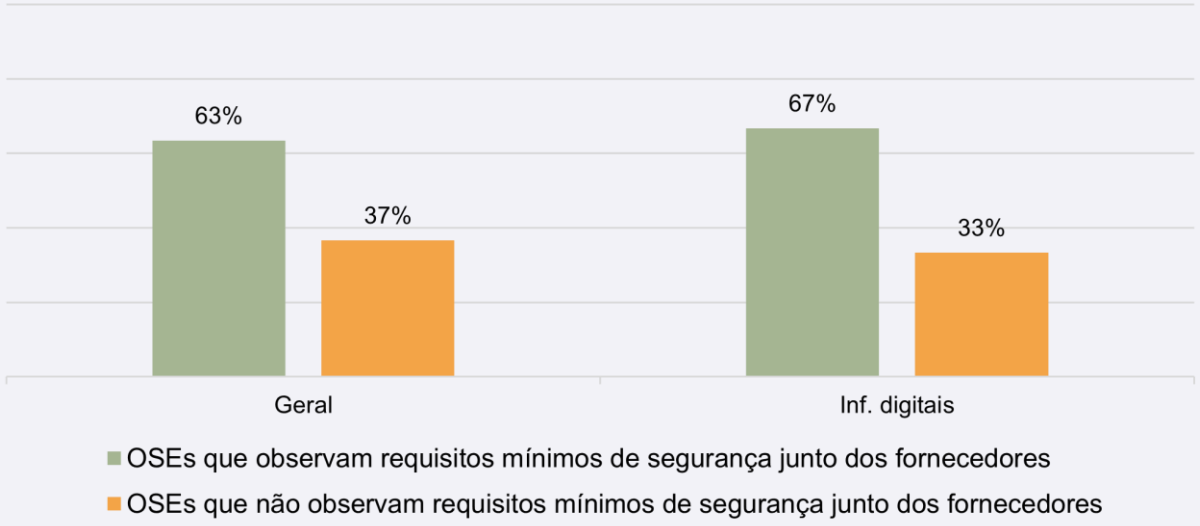
Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).
No setor das infraestruturas digitais, há 50% dos inquiridos a realizar testes de intrusão.

Gráfico 85 - Frequência de testes de intrusão



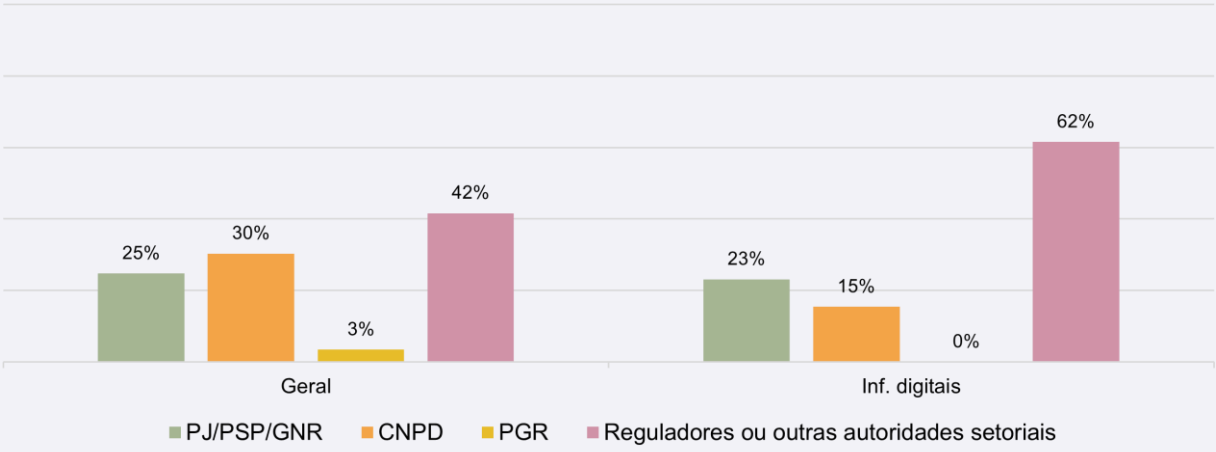
Com exceção dos operadores de dois setores, os operadores dos setores tendem a realizar testes de intrusão anualmente.
O setor das infraestruturas digitais não realiza testes de intrusão trimestrais, prevalece ainda a frequência anual.

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. No setor das infraestruturas digitais, os requisitos a são cumpridos por menor percentagem de operadores, mas atingindo a maioria.

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



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.

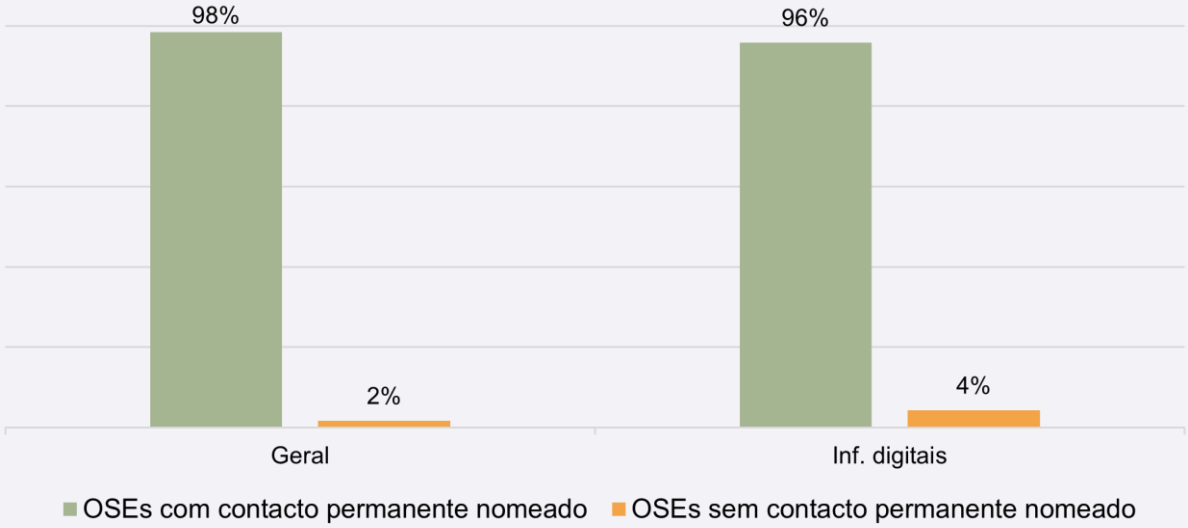
Apenas uma quantidade muito reduzida dos operadores tem previsto fazer qualquer tipo de notificação à Procuradoria-Geral da República (PGR).

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 OSEs 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.

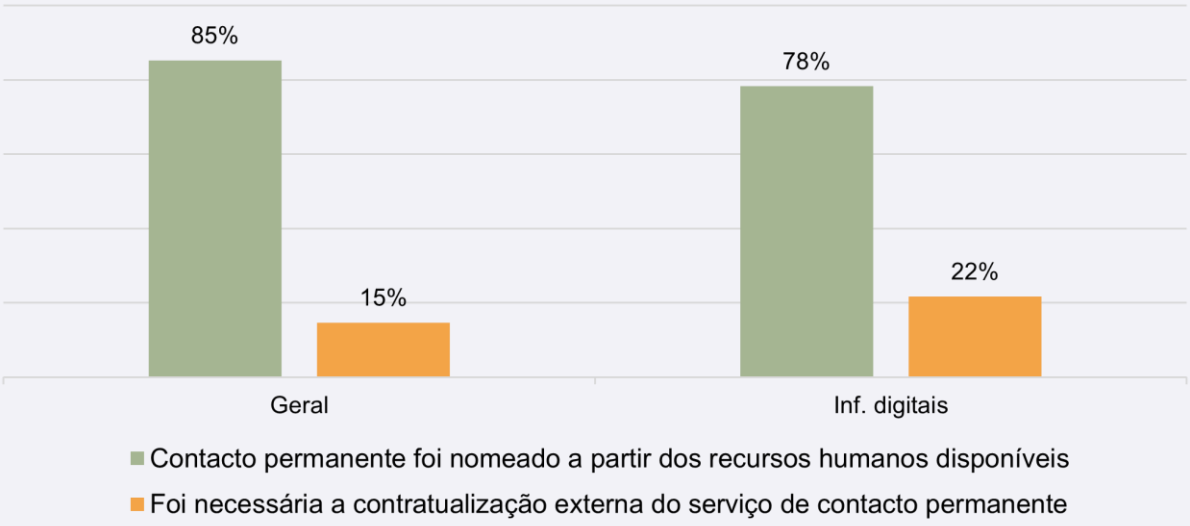
O setor das infraestruturas digitais opta por não notificar a PGR.

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



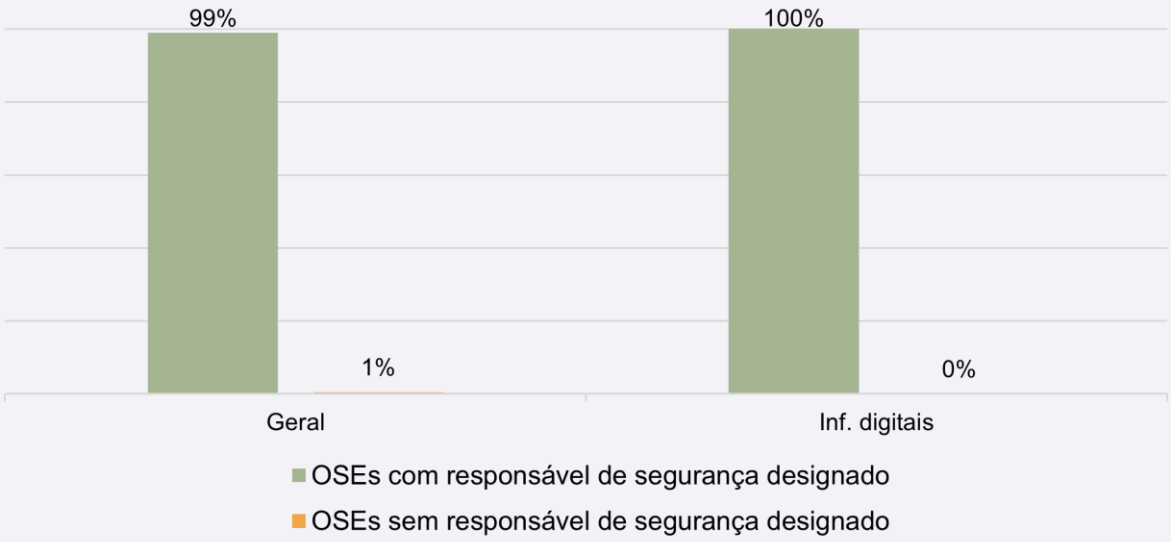
98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado. Verificam-se exceções no setor das infraestruturas digitais. Neste setor houve uma entidade inquirida que ainda não tinha nomeado o contacto permanente.

Gráfico 89 - Designação do contacto permanente



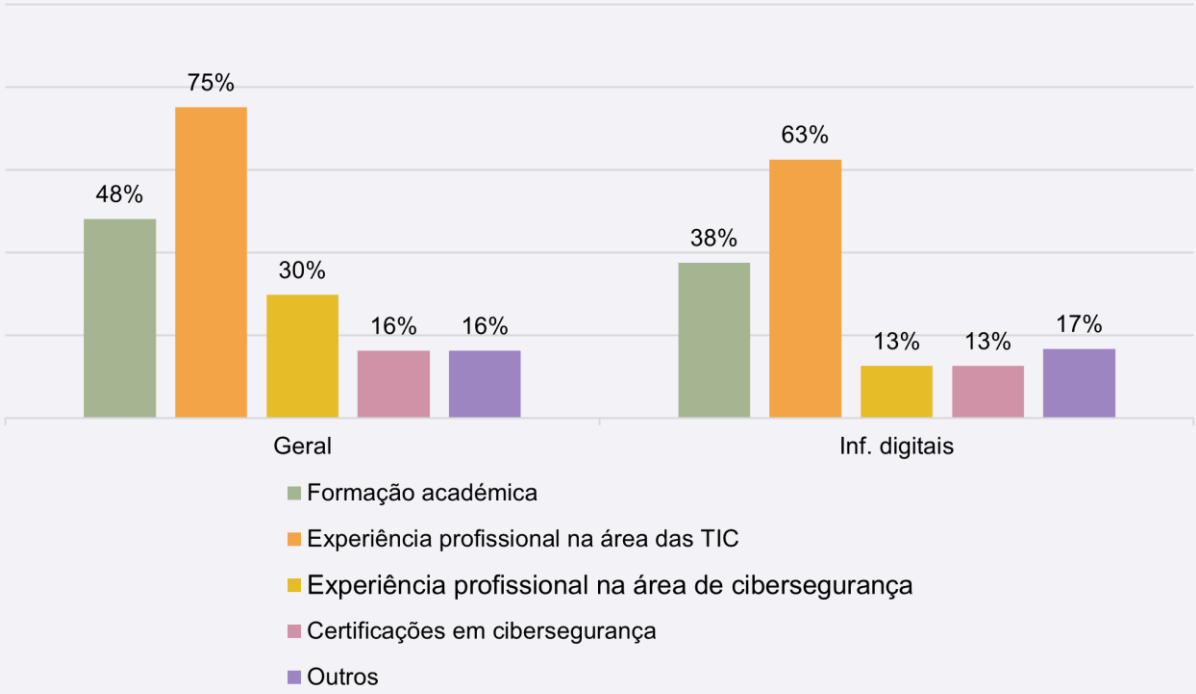
A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No entanto, houve ainda alguns operadores que tiveram de recorrer à contratualização externa do serviço de contacto permanente, com particular destaque para alguns setores, incluído o das infraestruturas digitais, nos quais a percentagem de operadores que necessitou de contratualizar o serviço foi acima de 17%.

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. Os OSEs inquiridos do setor das infraestruturas digitais encontram-se em conformidade com a exigência do decreto-lei n.º 65/2021.

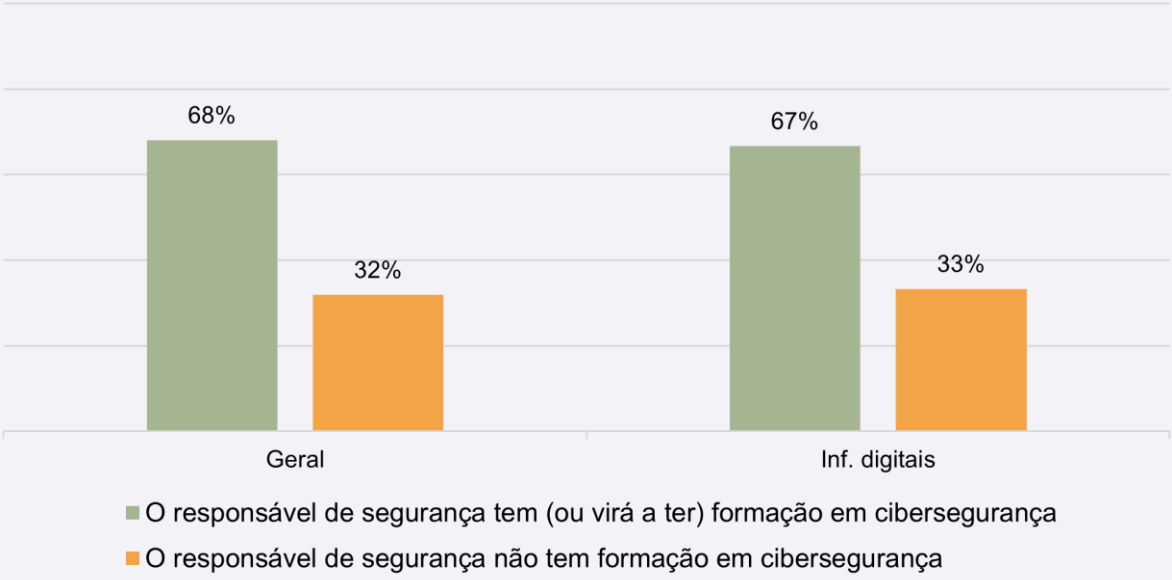
Gráfico 91 - Critérios utilizados para a designação do responsável de segurança



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.

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

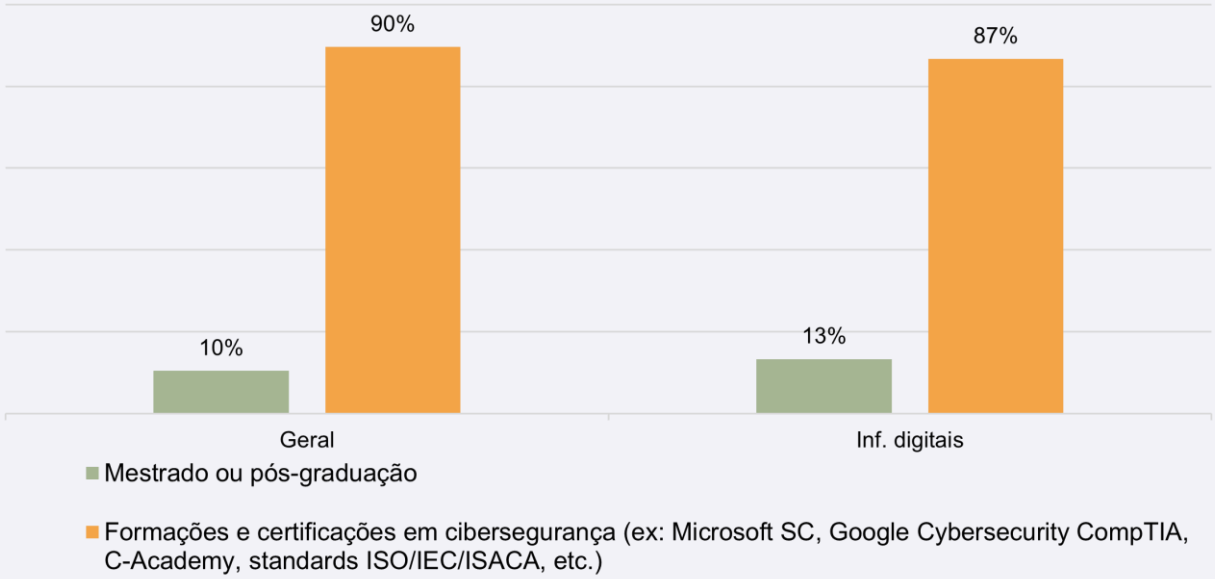
Gráfico 92 - Formação específica de cibersegurança do responsável de segurança



Em cerca de 70% dos casos, o responsável de segurança tem ou virá a ter formação específica em cibersegurança.

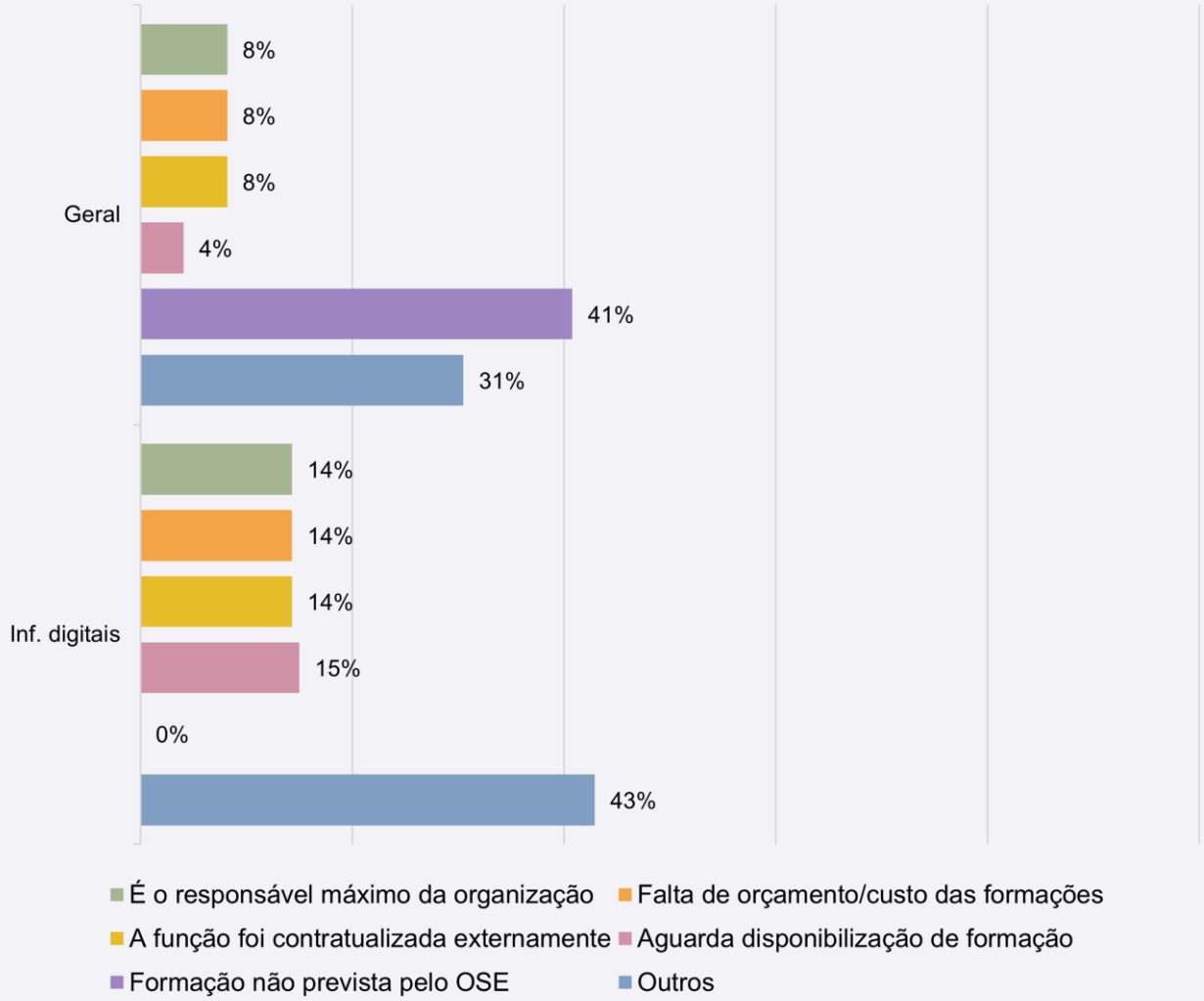
Um dos setores onde mais se verificam operadores cujo responsável de segurança não tem formação em cibersegurança são os setores da saúde é o das infraestruturas digitais, no qual 33% dos responsáveis de segurança não têm formação em cibersegurança, nem está planeado que venham a ter proximamente.

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 das infraestruturas digitais o valor é de 87% de responsáveis com esse tipo de formações.

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



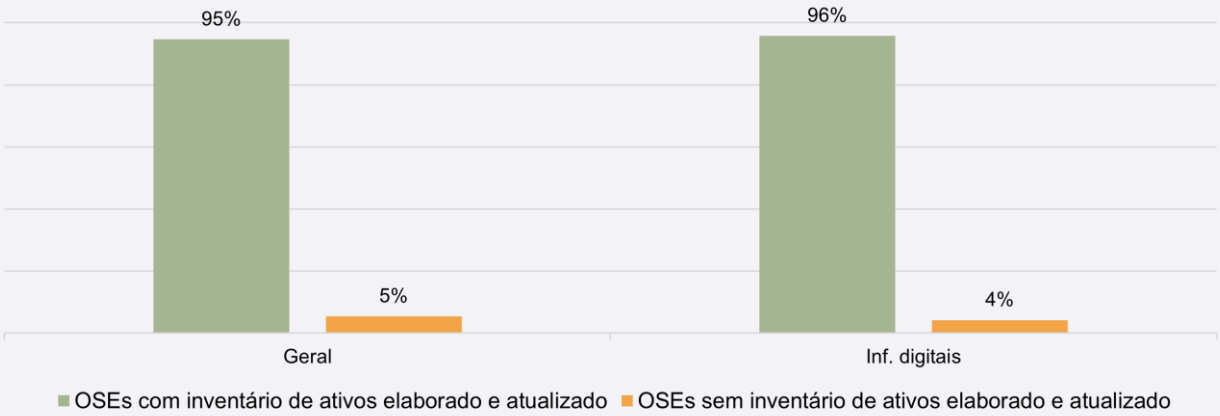
Os motivos pelos quais um responsável de segurança de um operador não tem formação específica em cibersegurança são diversificados. Na generalidade, o motivo mais vezes observado, em cerca de 40% dos operadores onde o responsável não tem formação na área, é o facto de essa formação não estar prevista 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 das infraestruturas digitais as motivações para que o responsável de segurança não tenha formação específica em cibersegurança estão bastante divididas. Essas motivações incluem o facto de o responsável de segurança ser o responsável máximo da organização ou a falta de orçamento/custo.

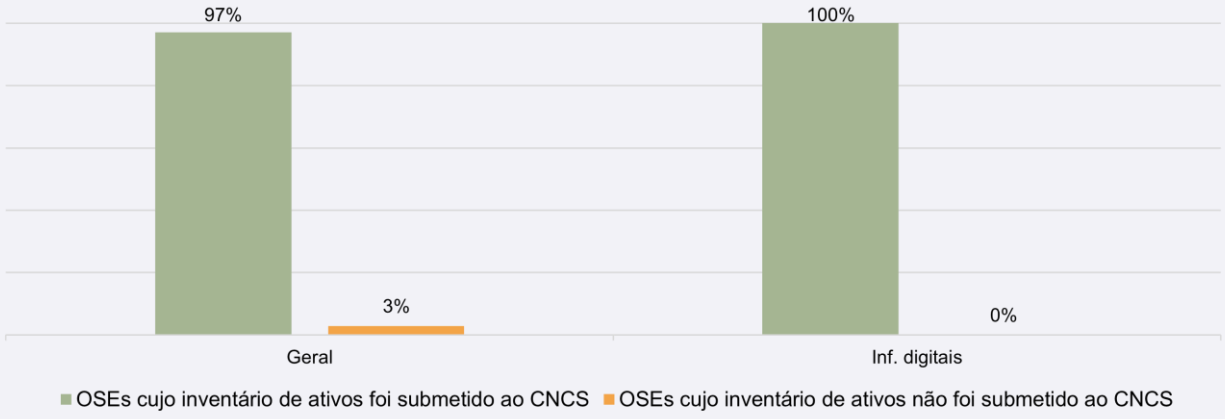
Tal como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado “Compromisso C-Academy” que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança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

Gráfico 95 - Inventário de ativos essenciais elaborado e atualizado



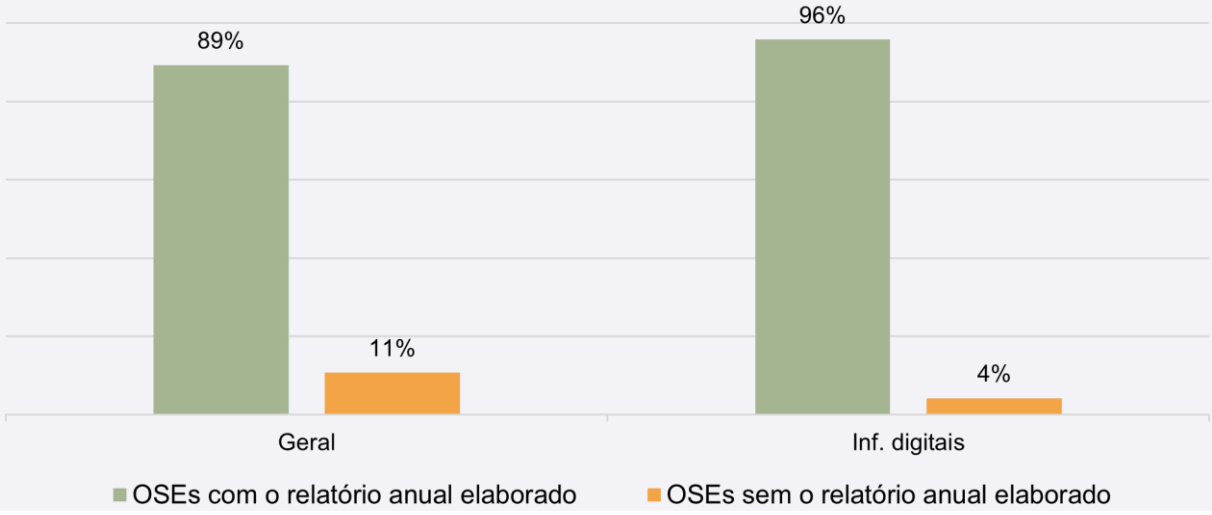
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. No setor das infraestruturas digitais, a percentagem de operadores cujo inventário de ativos essenciais não está elaborado e atualizado é de 4%.

Gráfico 96 - Submissão do inventário de ativos ao CNCS



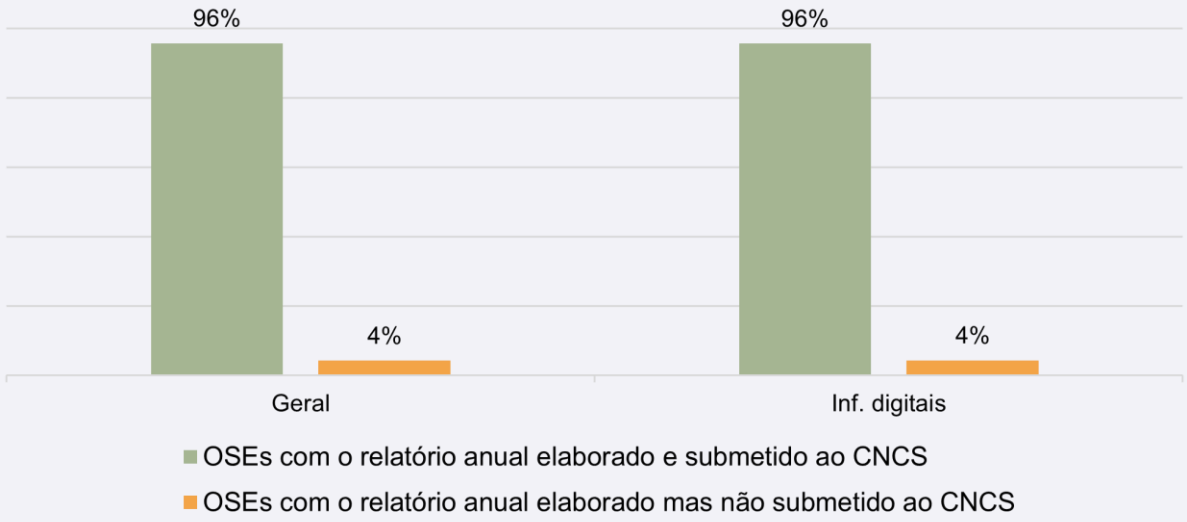
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. Destaca-se o setor das infraestruturas digitais, no qual 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



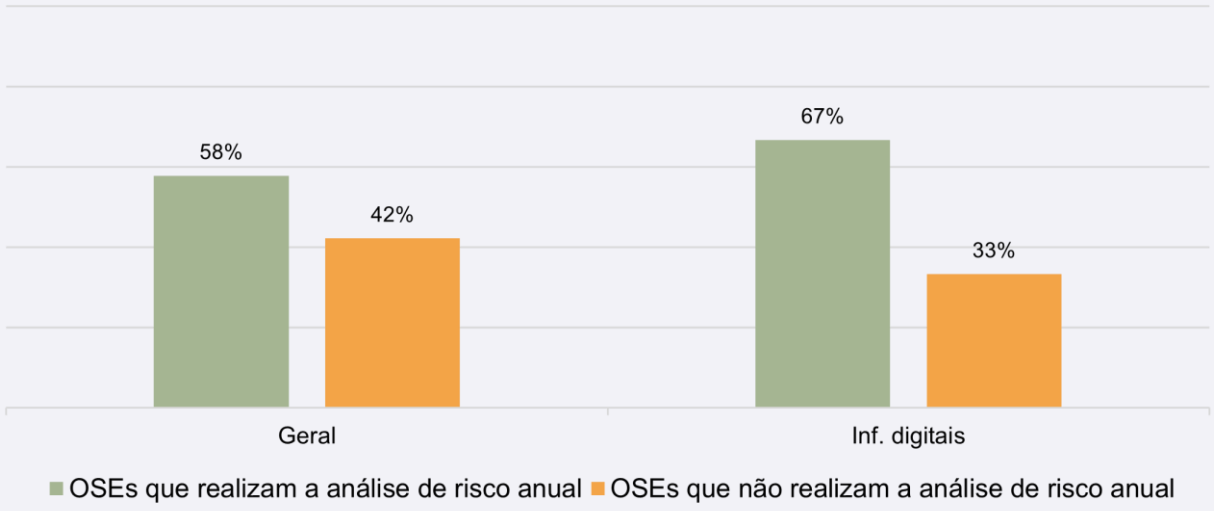
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. No setor das infraestruturas digitais essa percentagem é de 96%.

Gráfico 98 - Submissão do relatório anual ao CNCS



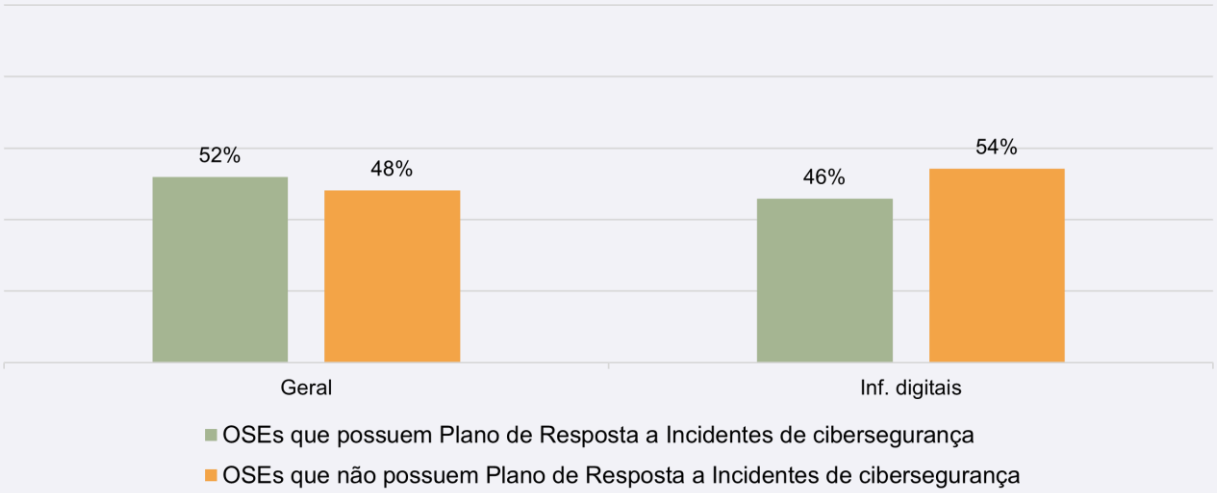
Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 96% submeteram-no ao CNCS. O setor das infraestruturas digitais é um dos casos em que tal não se verificou na totalidade a sua submissão, ou seja, em que o relatório foi elaborado, mas não submetido foi de 4%.

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



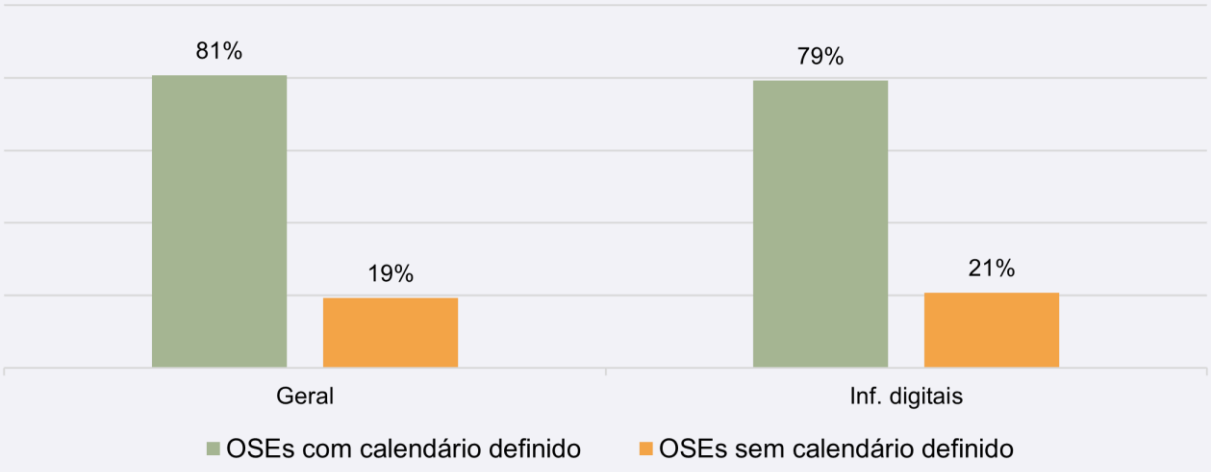
A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. O setor das infraestruturas digitais é um dos setores nos quais supera o valor geral onde 67% realiza esta análise.

Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança



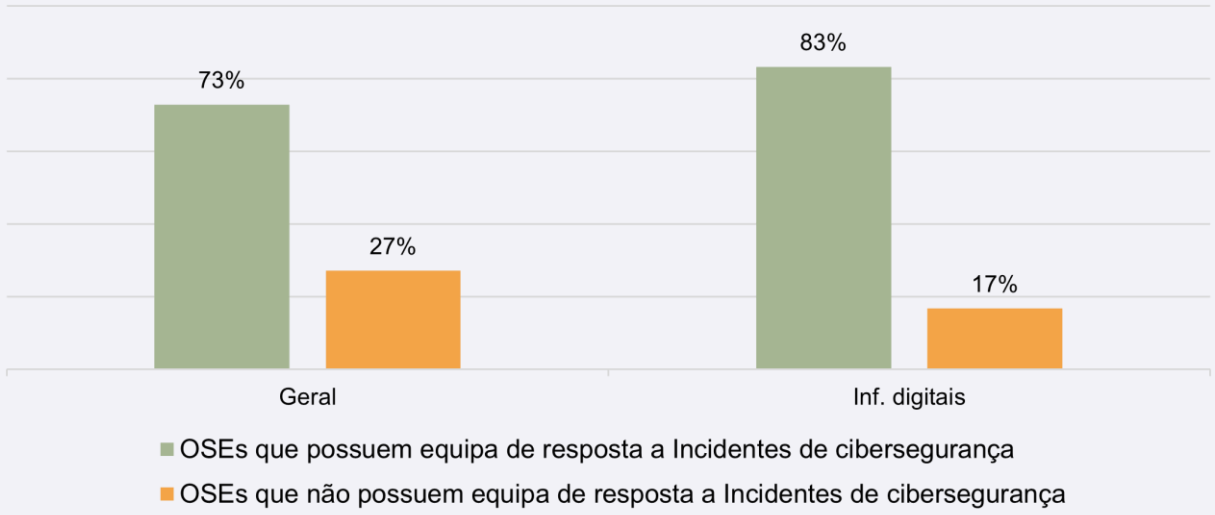
Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. No setor das infraestruturas digitais, os operadores sem plano de resposta a incidentes superam os operadores com plano, havendo apenas 46% de operadores com plano.

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



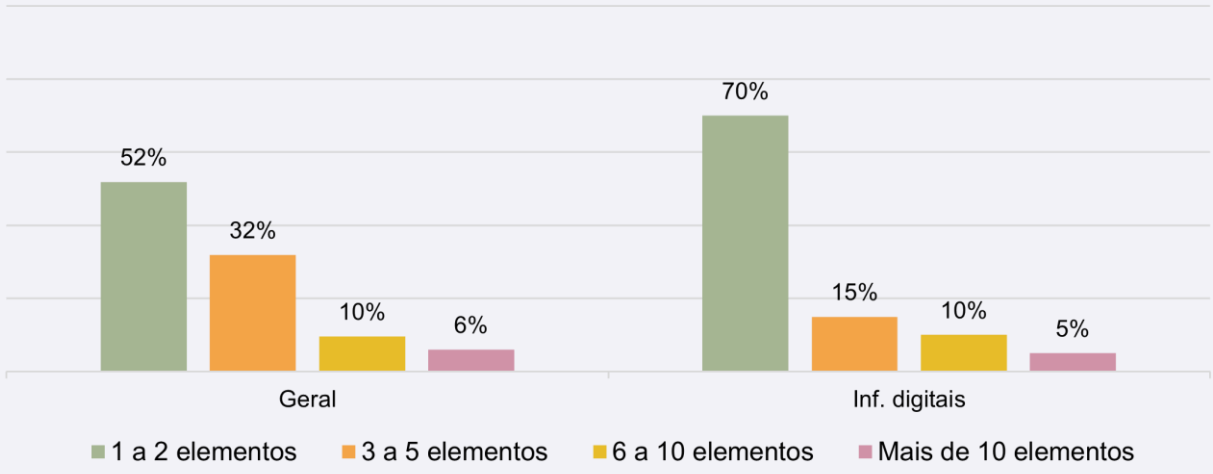
A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. No setor das infraestruturas digitais 21% não define esse calendário. Há que salientar ainda que, tal como revelam os gráficos anteriores, mesmo com 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



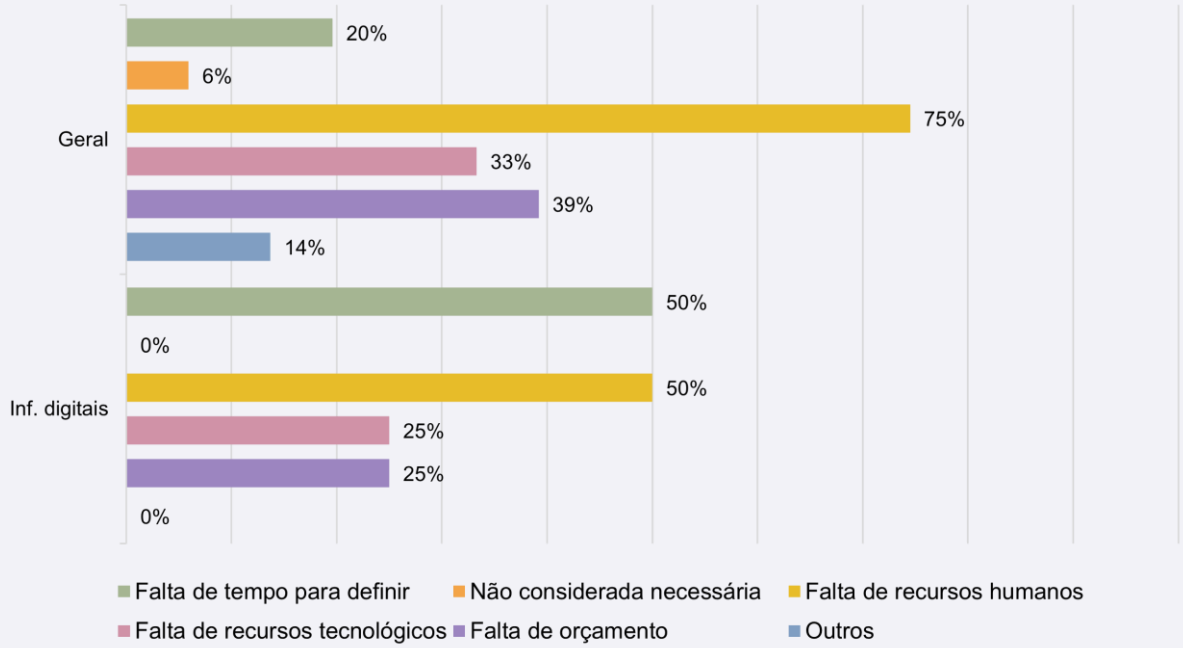
A nível geral, 73% dos operadores possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de operadores que possui tal equipa é sempre superior a 60%. O setor das infraestruturas digitais apresenta elevadas percentagens de operadores com equipas de resposta a incidentes, nomeadamente 83%.

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



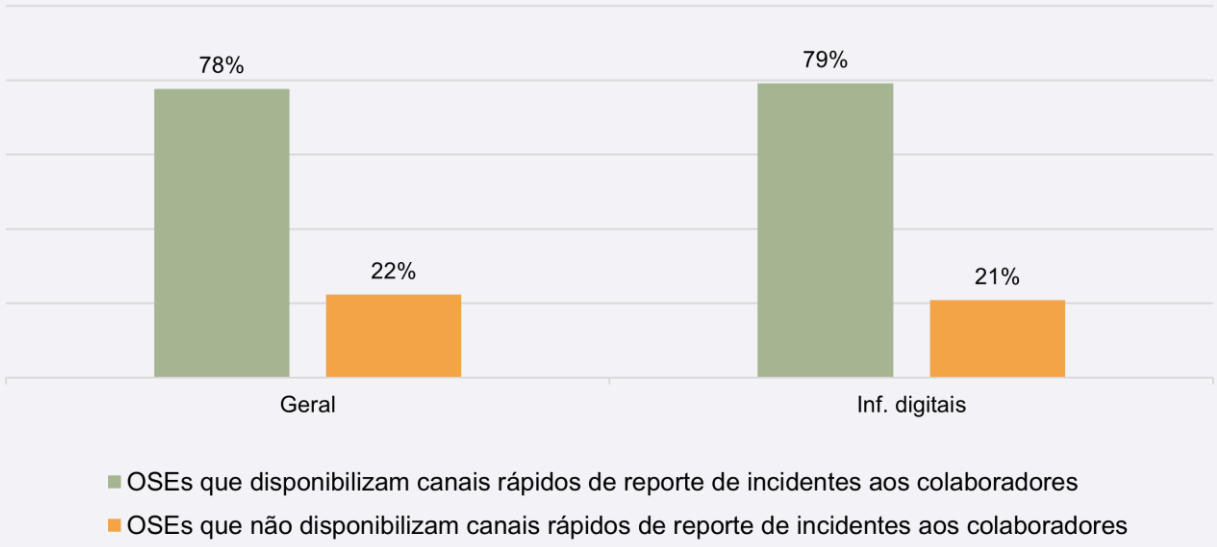
Na visão geral, 55% dos operadores com equipa de resposta a incidentes de cibersegurança conta com equipas compostas por 1 a 2 elementos. A nível setorial, a prevalência de equipas de resposta a incidentes com 1 a 2 elementos repete-se nos setores das infraestruturas digitais (70%), equipas com 3 a 5 elementos (15%), equipas com 6 a 10 elementos (10%) e equipas com mais de 10 elementos (5%).
Em resumo, a composição das equipas de resposta a incidentes de cibersegurança tende a ser maioritariamente pequena, especialmente em setores como das Infraestruturas Digitais, com uma proporção maior de equipas muito pequenas.

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



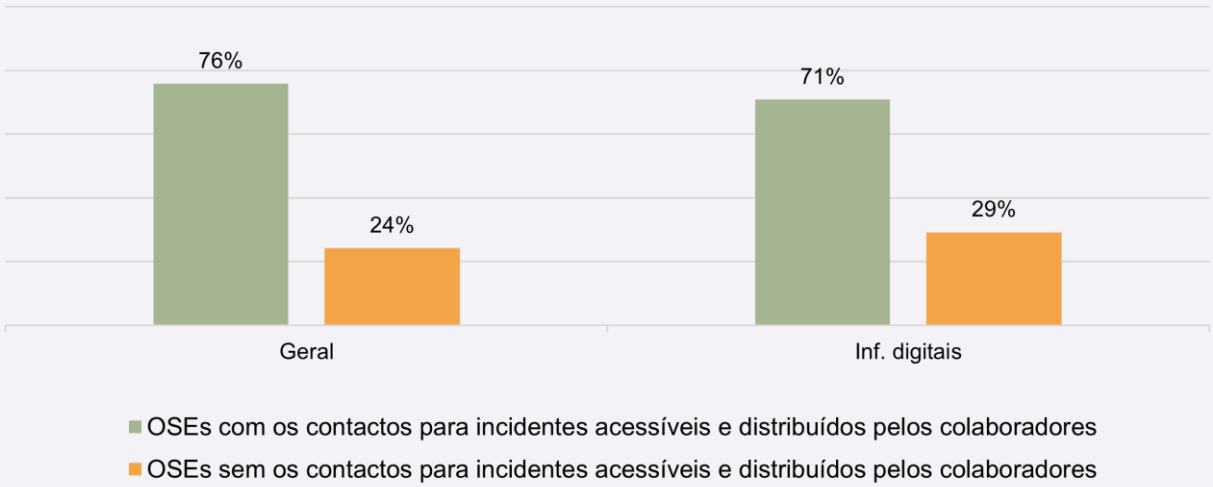
O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. No caso dos operadores do setor da energia, esse é mesmo o único motivo indicado. O único setor onde a escassez de recursos humanos não é o motivo mais apontado entre os restantes é o das infraestruturas digitais, no qual houve tantos operadores a indicar como motivo a escassez de recursos humanos, bem como a indicar a falta de tempo para definir a equipa de resposta a incidentes. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. 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%. 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



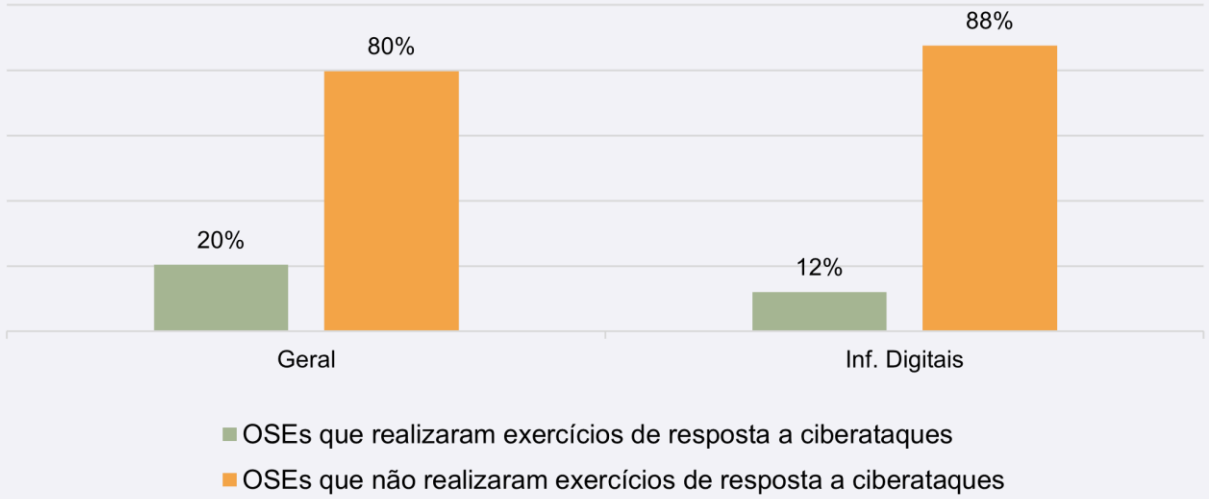
No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. No setor das infraestruturas digitais, a percentagem de operadores que disponibiliza estes canais rápidos fixa-se nos 79%.

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



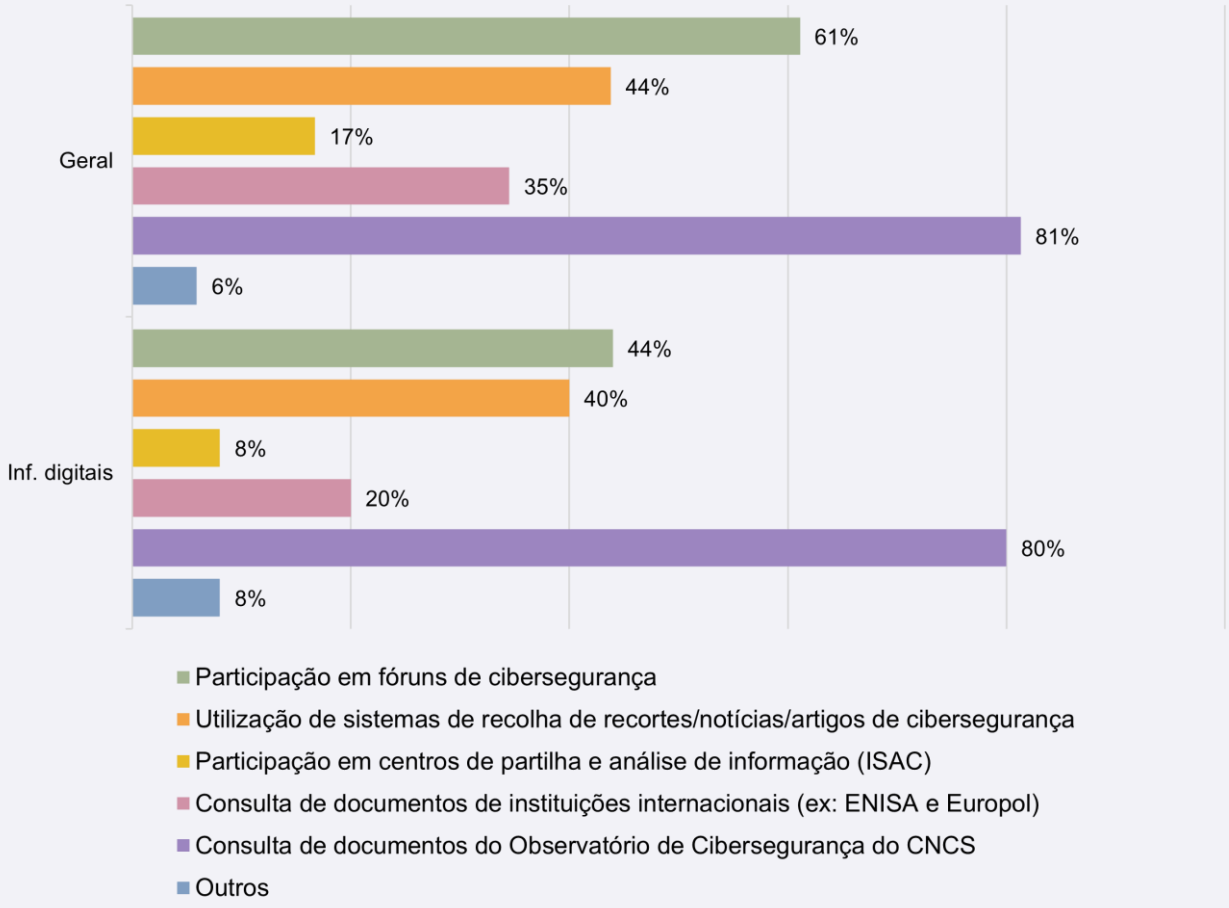
Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. Seguem-se os setores da saúde, onde 80% dos operadores têm estes contactos distribuídos e acessíveis por todos os colaboradores, 71% dos OSEs do setor das infraestruturas digitais dispõem dos contactos para incidentes acessíveis e distribuídos pelos colaboradores.

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. O setor das infraestruturas digitais, é um dos que menos realiza exercícios de resposta a ciberataques, onde a percentagem de operadores que realizam estes exercícios é de 12%.

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



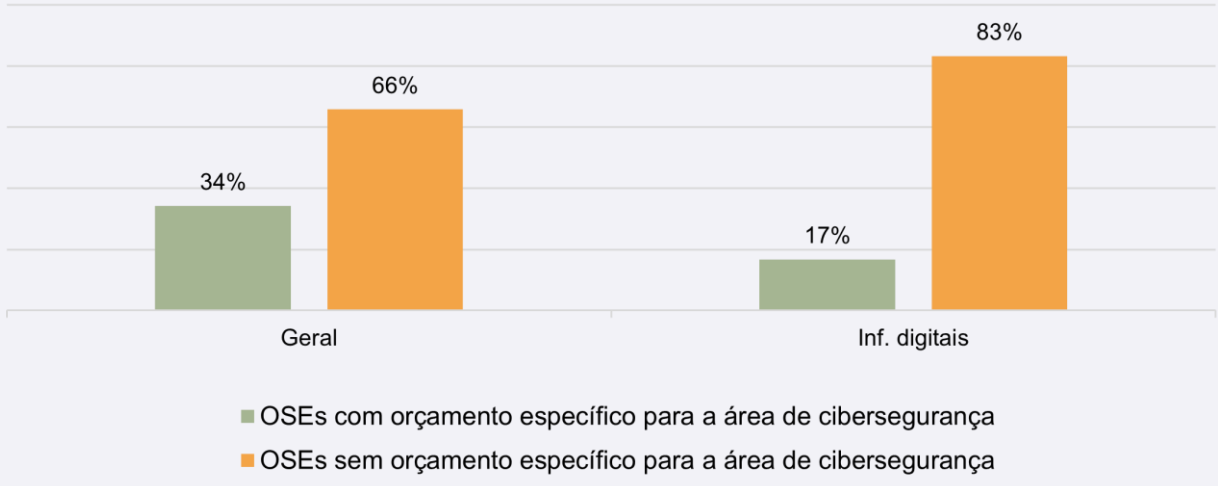
Independentemente dos métodos utilizados ou das fontes escolhidas para recolher informação sobre boas práticas relativas a riscos e incidentes de cibersegurança, verifica-se que a totalidade dos operadores inquiridos faz essa recolha. Os dois métodos mais comummente utilizados pelos operadores são a 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 OSEs em Portugal a participarem em ISACs[51].

[51] ENISA, "NIS Investments 2023", 59-61.

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"[52]. 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[53].

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[54]. 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*)[55]. 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[56].

Gráfico 109 - Orçamento específico para a área de cibersegurança



[52] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.
[53] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.
[54] Empowering EU ISACs, "European ISACs", https://www.isacs.eu/european-isacs.
[55] Exemplos retirados do European Energy Information Sharing & Analysis Centre (EE-ISAC), "Impact", https://www.ee-isac.eu/impact/#.
[56] Exemplo retirado do EE-ISAC, "Impact".

Praticamente dois terços dos operadores inquiridos (66%) não possuem orçamento específico para a área de cibersegurança. No setor das infraestruturas digitais, a percentagem de OSEs com orçamento específico para a área de cibersegurança não ultrapassa os 17%. O setor das infraestruturas do mercado financeiro foi o único onde nenhum dos inquiridos indicou ter orçamento específico para a área de cibersegurança.

O Relatório *NIS Investments* de 2021 foi o último relatório da série da ENISA a analisar a questão de um orçamento específico para a cibersegurança, tendo os últimos dois relatórios, de 2022 e 2023, orientado o seu foco para orçamentos dedicados a riscos terceiros (*third-party risk*) e à formação em cibersegurança, respetivamente. No relatório de 2021, os resultados verificados ao nível da UE são próximos dos obtidos a nível nacional no questionário realizado pelo CNCS: na UE, apenas cerca de 38% dos OSEs inquiridos tinham orçamentos dedicados à cibersegurança[57], próximo dos 33% registados pelo CNCS. O mesmo relatório indica que a maioria dos OSEs aloca fundos à cibersegurança a partir do orçamento dedicado à parte informática.

Importa também referir que a Diretiva NIS (RJSC) não obriga os OSEs 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[58]. 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[59]. 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[60].

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

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

[59] 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.

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

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

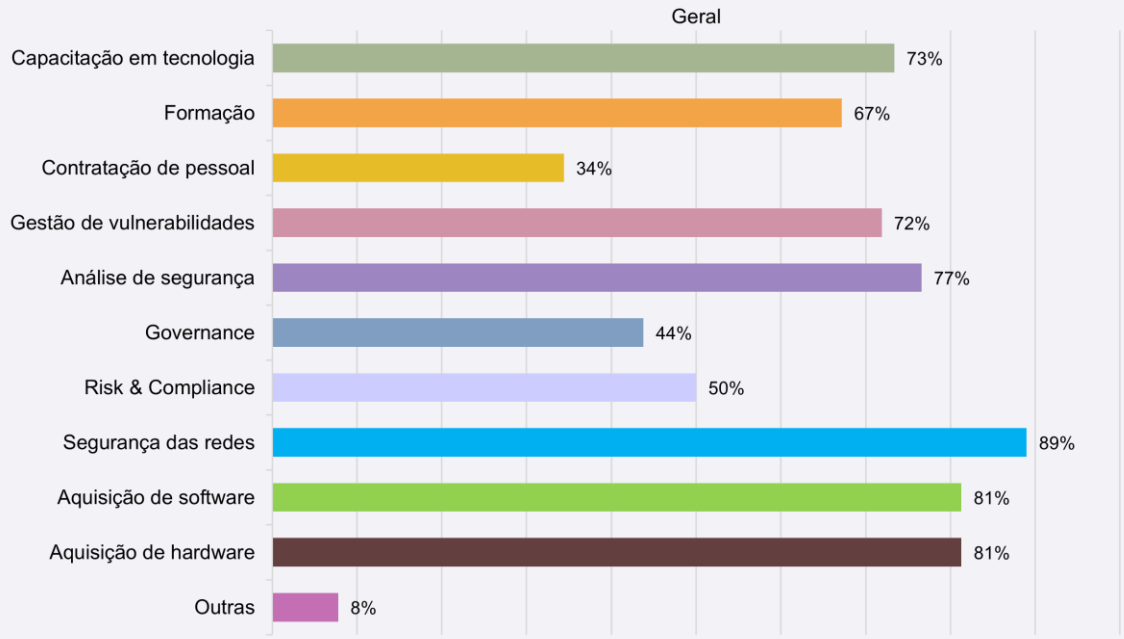
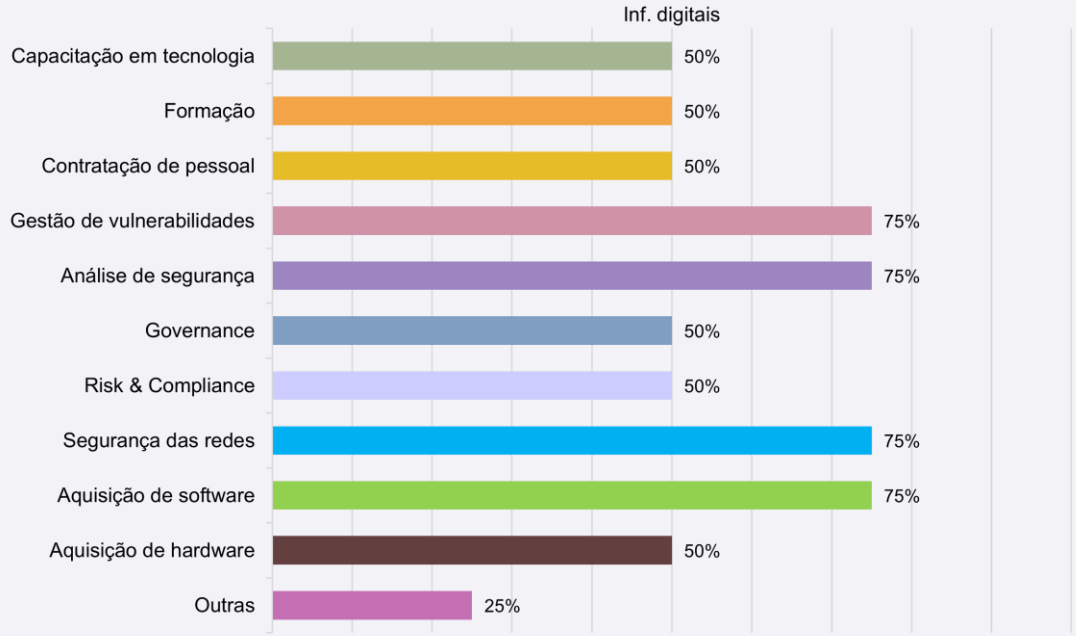


Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança

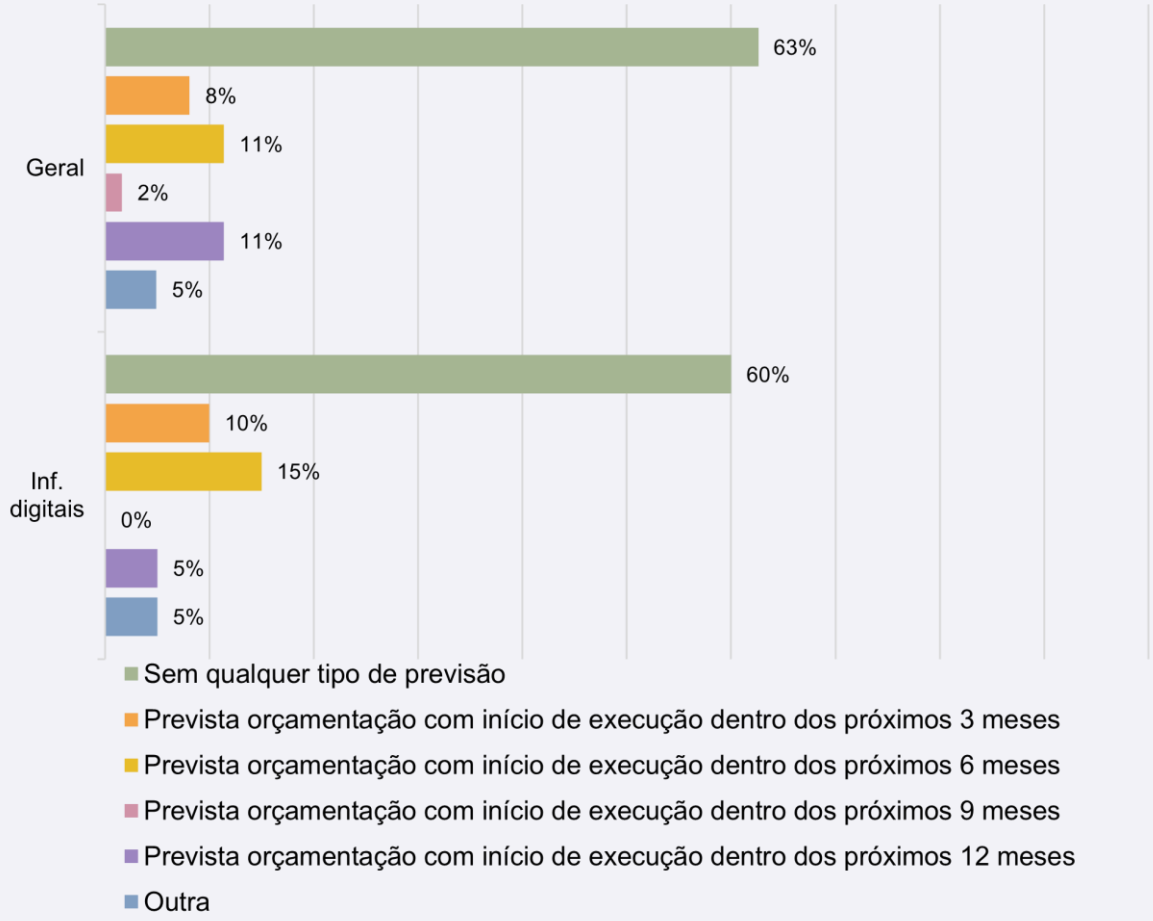


Entre os operadores que possuem orçamento específico para a cibersegurança, as áreas onde estes são mais comumente aplicados são a capacitação em tecnologia (73%), a formação dos colaboradores (67%), a gestão de vulnerabilidades (72%), análises de segurança (77%), *Risk & Compliance* (50%), segurança 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*.

A ENISA realizou um inquérito a 251 organizações OSEs 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[61]. 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[62].

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



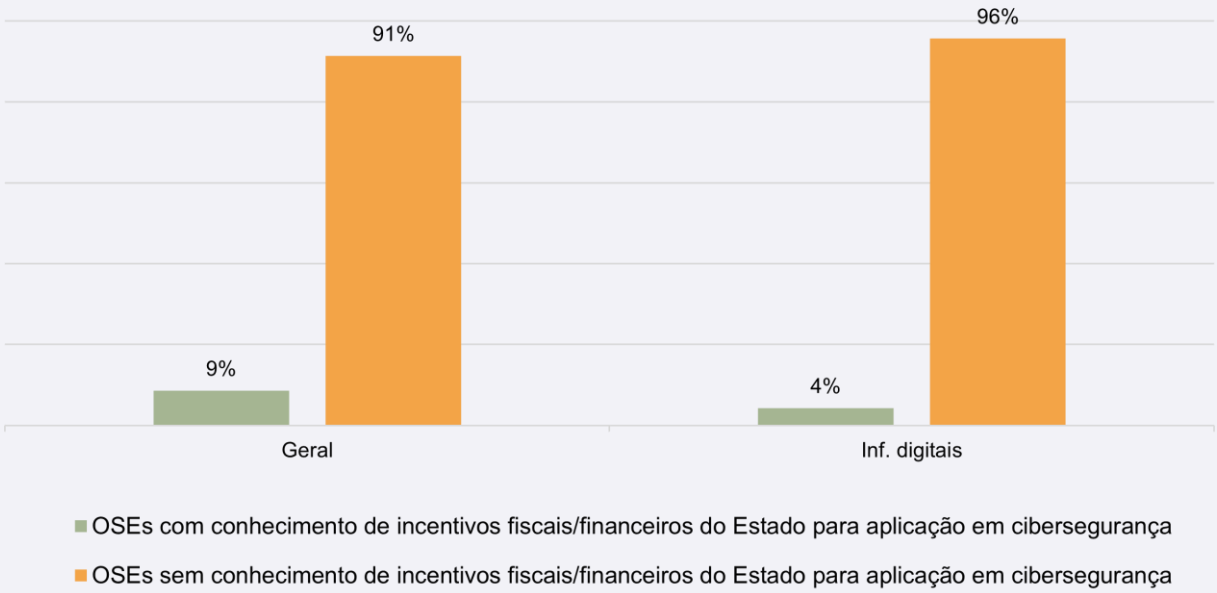
Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024.

[61] 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.

[62] ENISA, "NIS Investments", 2023

63% destes não têm qualquer previsão de vir a ter tal orçamento. No setor das infraestruturas digitais 60% não tem qualquer previsão de vir a iniciar a execução de um orçamento específico para cibersegurança. 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

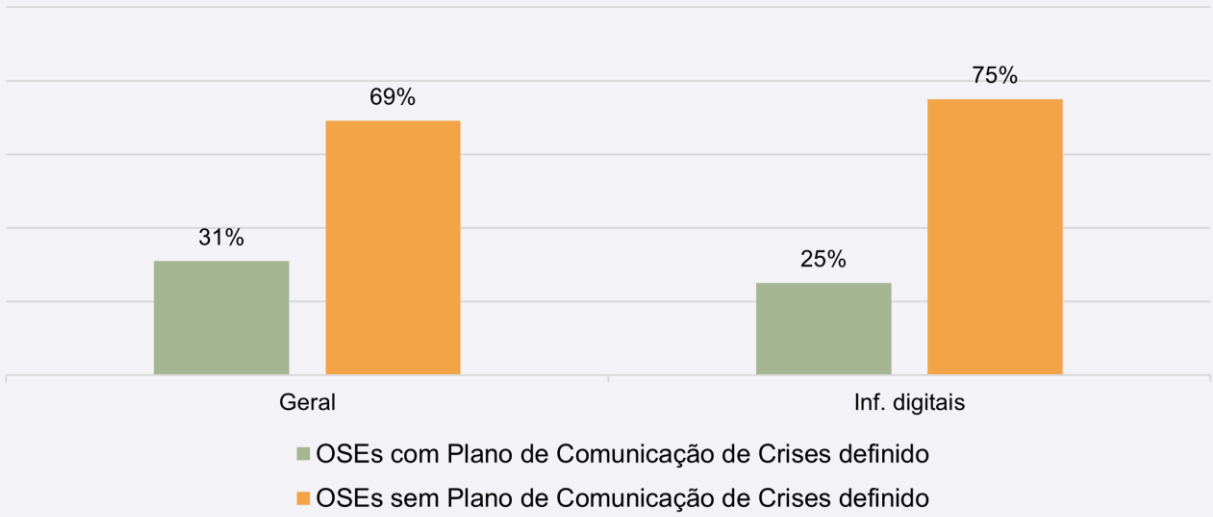


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No setor das infraestruturas digitais apenas 4% dos OSEs tinha conhecimento de tais incentivos.

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[63].

[63] 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. No setor das infraestruturas digitais, a percentagem de operadores com plano de comunicação de crises é de 25%.

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises

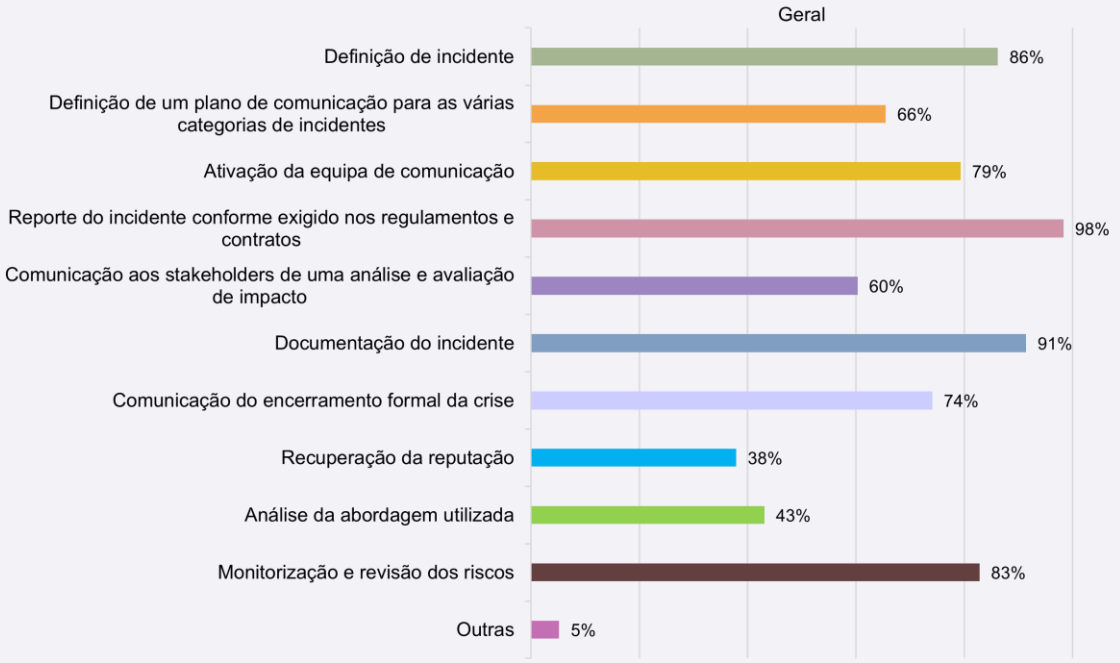
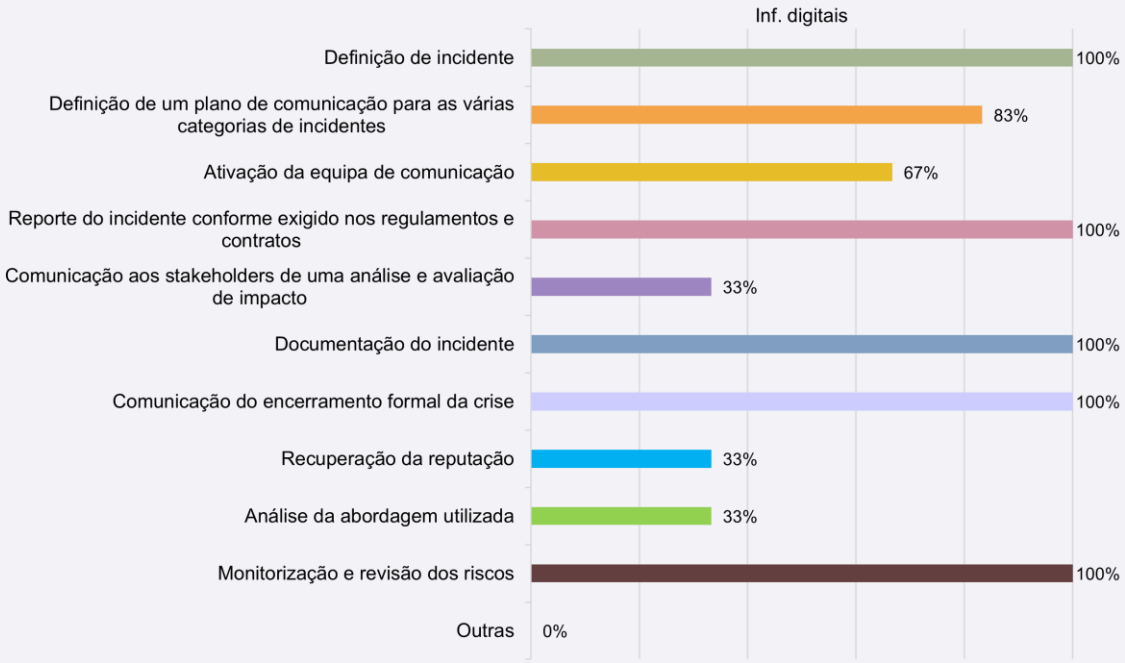


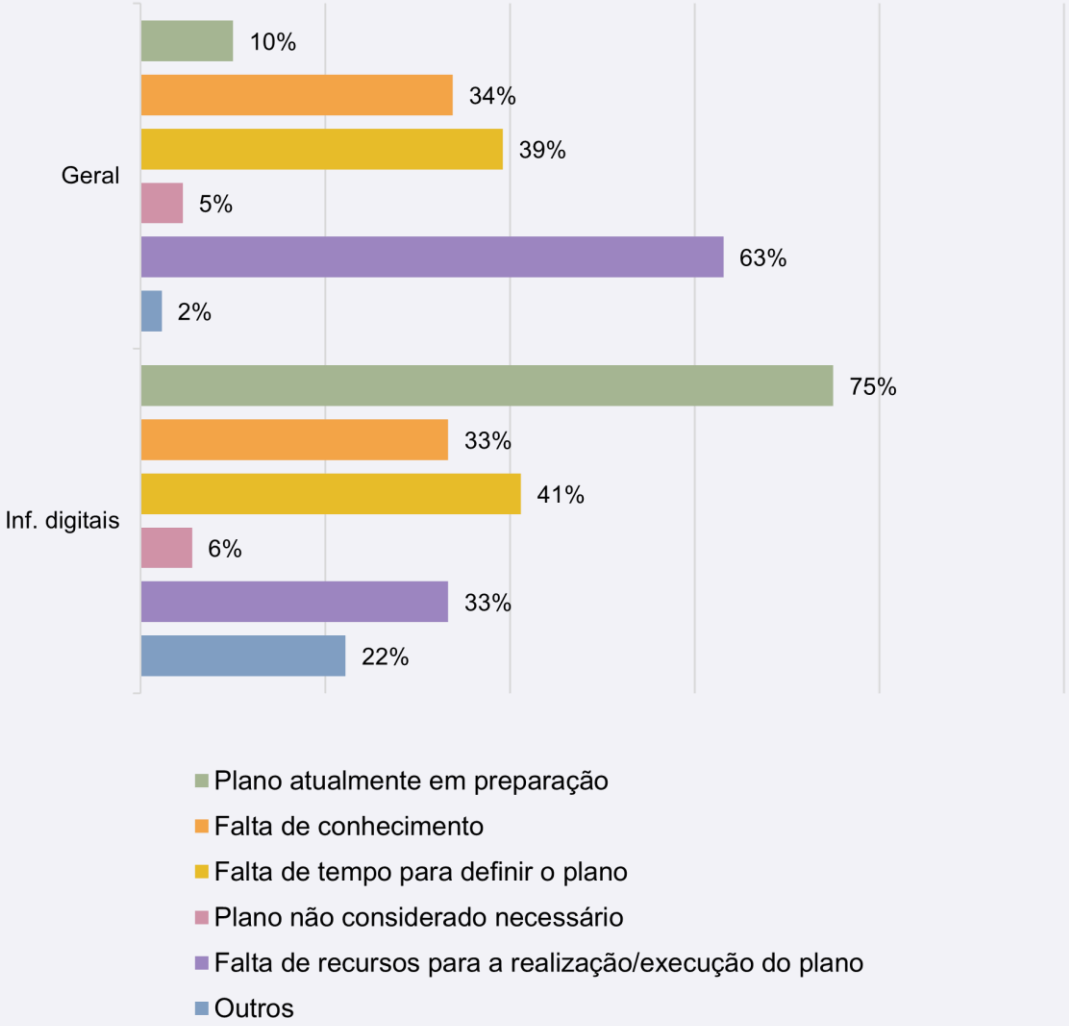
Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises



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.

Para 75% dos OSEs do setor das infraestruturas digitais, o motivo com maior peso para a não definição do plano de Comunicação de Crises é o mesmo estar atualmente em preparação.

Análise Setorial

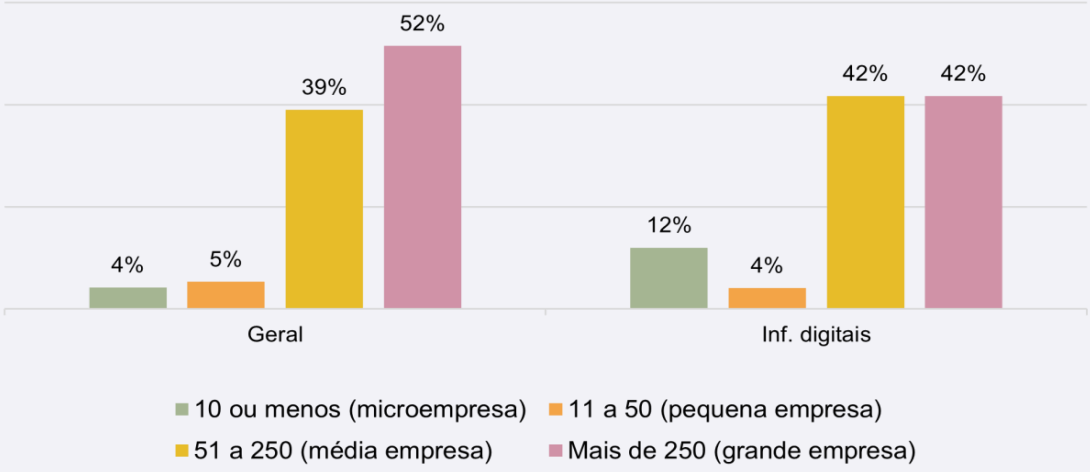
1. Infraestruturas digitais

1.1. Contextualização setorial

O setor das infraestruturas digitais refere-se às entidades e aos serviços que são essenciais para o funcionamento das redes e sistemas de informação na União Europeia. No âmbito do Regime Jurídico de Segurança do Ciberespaço (RJSC) e da Diretiva 2016/1148 (NIS), este setor compreende três tipos de entidades: pontos de troca de tráfego (Internet Exchange Points: IXP), fornecedores de serviços de DNS e registos de nomes de domínio de topo[64]. O desenvolvimento deste setor em Portugal tem-se devido sobretudo à ação de duas entidades: a Fundação para a Computação Científica Nacional (FCCN) e a associação DNS.PT.

Segundo o questionário realizado, foi possível aferir que este setor é sobretudo composto por grandes e médias empresas, representando estas 84% dos operadores do setor, com as pequenas e microempresas a constituírem a restante minoria (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



[64] Diretiva (UE) 2016/1148, Anexo II: Tipos de entidades para efeitos do artigo 4.º, ponto 4, *Jornal Oficial da União Europeia*, 19 de julho de 2016, 29, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L1148

Também segundo os dados obtidos através do questionário, foi possível verificar que o regulador do setor considera que a maturidade deste em cibersegurança é média, uma perceção que pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores. Este é o setor que menos operadores tem a disponibilizar formação (42%), abaixo da média dos setores (65%). As medidas menos adotadas pelo setor foram: Ter uma equipa especialista em cibersegurança (16% dos inquiridos), utilização de controlos biométricos para a identificação e autenticação dos utilizadores (também 16%), operadores que apostam nas formações de sensibilização em cibersegurança (28%). Apenas uma pequena minoria dos operadores dedicam orçamentos específicos à área de cibersegurança (17% contra 34% no geral dos setores). É também um setor que, por enquanto, se mantém com uma taxa de incidentes cibersegurança abaixo dos 50%, com 33% dos inquiridos a já terem sofrido um incidente.

Pontos de Troca de Tráfego

De acordo com o disposto na Diretiva NIS, "a função de um ponto de troca de tráfego consiste em interligar redes. Os pontos de troca de tráfego não proporcionam o acesso às redes nem atuam como prestadores ou operadores de tráfego. Os pontos de troca de tráfego também não prestam outros serviços não relacionados com interligação, embora isso não impeça o operador de um ponto de troca de tráfego de prestar também serviços não conexos. Os pontos de troca de tráfego existem para interligar redes que estejam separadas em termos técnicos e organizativos"[65]. Por outras palavras, pontos de troca de tráfego são "terrenos comuns" de rede Internet Protocol (IP), onde ocorre troca de tráfego entre diferentes organizações, permitindo que os fornecedores de serviços de Internet neles incluídos troquem dados destinados às suas respetivas redes e que essas redes se possam interligar da forma mais eficiente[66].

O primeiro operador destes pontos de troca de tráfego em Portugal foi a GigaPIX, estabelecida em outubro de 1995 pela FCCN. A GigaPIX nasceu com a implementação de portas Gigabit no Portuguese Internet eXchange (PIX). Atualmente, a GigaPIX conecta dezenas de redes nas suas instalações em Lisboa e no Porto, oferecendo velocidades que variam de 10Gbps a 100Mbps[67]. Outras duas entidades que se dedicam principalmente à gestão de pontos de troca de tráfego são a LIS-IX e a Equinix. A LIS-IX foi criada em 2023 e tem como grande objetivo agitar as trocas de tráfego em Portugal. Para isso, a LIS-IX reduz a distância que os dados necessitam de efetuar e oferece uma rede estratégica devido às parcerias com entidades chave da internet e telecomunicações[68]. A Equinix é outra entidade que também está localizada em Lisboa e é uma empresa global de *datacenters* e serviços de troca de tráfego[69].

[65] Diretiva (UE) 2016/1148, 4.

[66] "QUE FAZ O GIGAPIX ?", GigaPIX, https://gigapix.pt/pt/home/.

[67] "Sobre nós", *GigaPIX*, https://gigapix.pt/pt/sobre-nos/.

[68] "What is LIS-IX?", *LIS-IX*, https://lis-ix.pt/#what-is.

[69] "LS1", Equinix, https://www.equinix.com/data-centers/europe-colocation/portugal-colocation/lisbon-data-centers/ls1.

Os principais objetivos de entidades como estas são melhorar e aumentar a qualidade da rede IP em Portugal, o que é feito evitando o uso de ligações internacionais para comunicações locais, o que também ajuda a reduzir os custos dessas operações. Estas entidades visam também diminuir a latência dos serviços e proporcionar uma melhor experiência aos utilizadores. Os principais pontos de troca de tráfego em Portugal estão distribuídos pelas cidades de Lisboa e do Porto. As organizações comumente conhecidas como "operadoras", que fornecem os tradicionais serviços de telefone, internet e televisão, também costumam operar pontos de troca de tráfego. Por exemplo, através da rede MEO, o serviço de interligação "Trânsito Nacional PT" permite fazer a ligação para troca de tráfego entre dois outros operadores, sem que estes se tenham de interligar diretamente. Este tipo de serviço de pontos de troca de tráfego permite que a rede transporte uma chamada que tenha origem na rede de um operador cujo destino é o ponto terminal da rede ou o serviço de um terceiro operador, através de um acordo entre os operadores de origem/destino. As vantagens deste serviço são o valor económico, por não ser necessário estabelecer ligações entre operadores, a eficiência, a transparência, a flexibilidade de acesso, segurança e elevado grau de disponibilidade e a supervisão[70].

Prestadores de serviços de DNS

Os DNS (*Domain Name Systems*) são responsáveis pela tradução dos nomes de domínio normalmente usados para referir *websites* nos seus endereços IP, de modo a serem compreendidos pelos computadores. A título ilustrativo, DNS é o que traduz o que é conhecido normalmente como "exemplo.com" no seu endereço IP real, como "192.0.2.1".

A FCCN foi a primeira entidade responsável pela gestão dos DNS em Portugal, tendo sido nomeada pela Internet Assigned Numbers Authority (IANA) para tal em 1988[71].

Atualmente, existem em Portugal diversos prestadores deste tipo de serviços, abrangendo tanto opções locais como internacionais, com diferentes características e níveis de serviço. Os principais fornecedores locais incluem grandes operadoras de telecomunicações como a MEO, NOS, Vodafone Portugal e NOWO. Todas estas operadoras fornecem um serviço de *DNS* integrado com os seus serviços de Internet[72].

Além dos fornecedores locais, existem vários fornecedores internacionais que também têm uma presença significativa em Portugal. Por exemplo, a Google Public DNS[73] utiliza os endereços 8.8.8.8 e 8.8.4.4. Já o OpenDNS[74] oferece filtros de conteúdo e proteção contra *phishing* e opera com os endereços 208.67.222.222 e 208.67.220.220. Estes fornecedores oferecem diferentes opções para as diferentes necessidades e preferências, desde serviços básicos até soluções mais avançadas com foco na segurança e privacidade.

[70] "Interligação e Serviço Universal", ANACOM, 23 de fevereiro de 2006, https://www.anacom.pt/render.jsp?categoryId=183071&languageId=0

[71] Pedro Fonseca, Paul McCarthy e Marian-Andrei Rizoiu, *Registentes: Os primeiros domínios .pt* (Loures: Conclusão das Letras, julho de 2021), 13, https://tictank.pt/wp-content/uploads/2021/08/2107-registentes_livro.pdf.

[72] "DNS servers in Portugal", Public DNS,https://public-dns.info/nameserver/pt.html.

[73] "Google Public DNS", Google, https://dns.google/.

[74] "About Us", OpenDNS, https://www.opendns.com/about/.

Registo de nomes de domínio de topo

Os nomes de domínio de topo (*top-level domains* - TLD) são a parte de um endereço *web* depois do seu nome de domínio. Ou seja, em "exemplo.com", ".com" é o TLD em questão. Existem diversos TLDs, sendo alguns dos mais comuns o ".com" e ".org", havendo também os TLDs relativos a diferentes países, como ".us", dos EUA, ".es", de Espanha, ".fr", de França e, no caso de Portugal, ".pt". Em 1988, a par da sua nomeação para gestão dos DNS, a FCCN foi designada como a responsável pelos registos de domínios ".pt"[75]. Seria depois constituída, em 2013, a Associação DNS.PT, associação sem fins lucrativos que é composta por membros como a Fundação para a Ciência e Tecnologia, IP (FCT), a Associação de Economia Digital (ACEPI) e a Associação Portuguesa para a Defesa do Consumidor (DECO), sucedendo à FCCN nos direitos e obrigações na gestão, registo e manutenção dos domínios ".pt". A missão da DNS.PT é a de fortalecer o ecossistema digital em Portugal, em conformidade com a Europa e o Mundo, respondendo às necessidades do público consumidor, parceiro e colaborador. O principal objetivo é o de oferecer elevados níveis de qualidade, fiabilidade e segurança no registo de nomes de domínio ".pt", assim como assegurar o correto funcionamento e manutenção do mesmo[76].

1.1.1. Impacto socioeconómico

Segundo o documento final de "Avaliação do Potencial Económico da Transição Digital em Portugal" de 2023, conclui-se que o impacto das infraestruturas digitais se verifica em três vertentes:

- Impacto das infraestruturas e conectividade:
  - **Acesso**: A disponibilidade de infraestruturas digitais de qualidade amplia o acesso a tecnologias avançadas, permitindo que empresas e indivíduos aproveitem os benefícios da economia digital;
  - **Cobertura**: A ampla cobertura de redes digitais assegura que uma maior parte da população e das empresas tenha acesso a serviços de alta velocidade, facilitando a inclusão digital;
  - **Funcionalidades de Rede**: A capacidade das redes de suportar diferentes funcionalidades é crucial para impulsionar a inovação, a eficiência e a produtividade em diversos setores económicos[77].

Estas variáveis - acesso, cobertura e funcionalidades de rede - são fundamentais para explicar o aumento do valor acrescentado bruto (VAB) e a melhoria da produtividade, que são indicadores importantes do impacto positivo das infraestruturas digitais na economia nacional.

[75] "História", .PT, https://www.pt.pt/pt/historia/.

[76] "Quem somos", .PT, https://www.pt.pt/pt/pt/quem-somos/.

[77] Deloitte e Universidade de Coimbra,"Avaliação do Potencial Económico da Transição Digital em Portugal", 2023, 89, https://portugaldigital.gov.pt/wp-content/uploads/2023/05/Portugal-Digital_Avaliacao-Transicao-Digital_Documento-Final_v20230330_VF.pdf.

Segundo o Índice de Digitalidade da Economia e da Sociedade (IDES), publicado no último trimestre de 2023, Portugal melhorou o seu desempenho nas redes fixas de alta capacidade (VHCN) e na cobertura de fibra (91% de cobertura de instalações) e na oferta de banda larga fixa com, no mínimo, 100 Mbps (77%)[78]. Embora na dimensão do 5G, o contexto nacional esteja mais atrasado, a melhoria destas infraestruturas faz com que as empresas estejam mais capazes de adotar meios digitais mais avançados como computação *cloud*, *big data* ou IA. Uma condição essencial às empresas para que possam ter acesso a tecnologias mais complexas que impulsionem os seus serviços, como as referidas anteriormente, é o acesso à internet de alta velocidade. A análise da amostra do Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas (IUTICE) e do Sistema de Contas Integrado das Empresas (SCIE) revela um crescimento significativo no acesso rápido à internet entre as empresas em Portugal. Esse crescimento é refletido no gráfico e no relatório correspondente.

- Crescimento do Acesso Rápido à Internet:
  1. **Evolução do Acesso:**
     - Em 2020, 29% do valor acrescentado bruto (VAB) era gerado por empresas com acesso rápido à internet[79].
     - Em 2022, o número de empresas com acesso a velocidades de internet iguais ou superiores a 1 Gb/s aumentou para cerca de 23%, representando um crescimento de 3% em relação a 2021[80].
  2. **Significado do Crescimento**:
     - **Produtividade e Competitividade**: O aumento da velocidade de internet nas empresas contribui diretamente para a produtividade e competitividade. Acesso a internet de alta velocidade permite operações mais eficientes, maior capacidade de processamento de dados e melhor comunicação interna e externa[81].
     - **Inovação e Transformação Digital**: Empresas com acesso rápido à internet estão mais bem posicionadas para adotar novas tecnologias, como inteligência artificial, *big data* e internet das coisas (IoT), impulsionando a inovação e a transformação digital.
     - **Inclusão Digital**: A expansão do acesso rápido à internet ajuda a reduzir a desigualdade digital, permitindo que mais empresas, independentemente do seu tamanho ou localização, acessem as mesmas oportunidades e ferramentas digitais[82].

[78] Manuel Dias, "Estará no plano do próximo Governo colocar Portugal na vanguarda da Europa digital?", *Observador*, 3 de janeiro de 2024, https://observador.pt/opiniao/estara-no-plano-do-proximo-governo-colocar-portugal-na-vanguarda-da-europa-digital/.

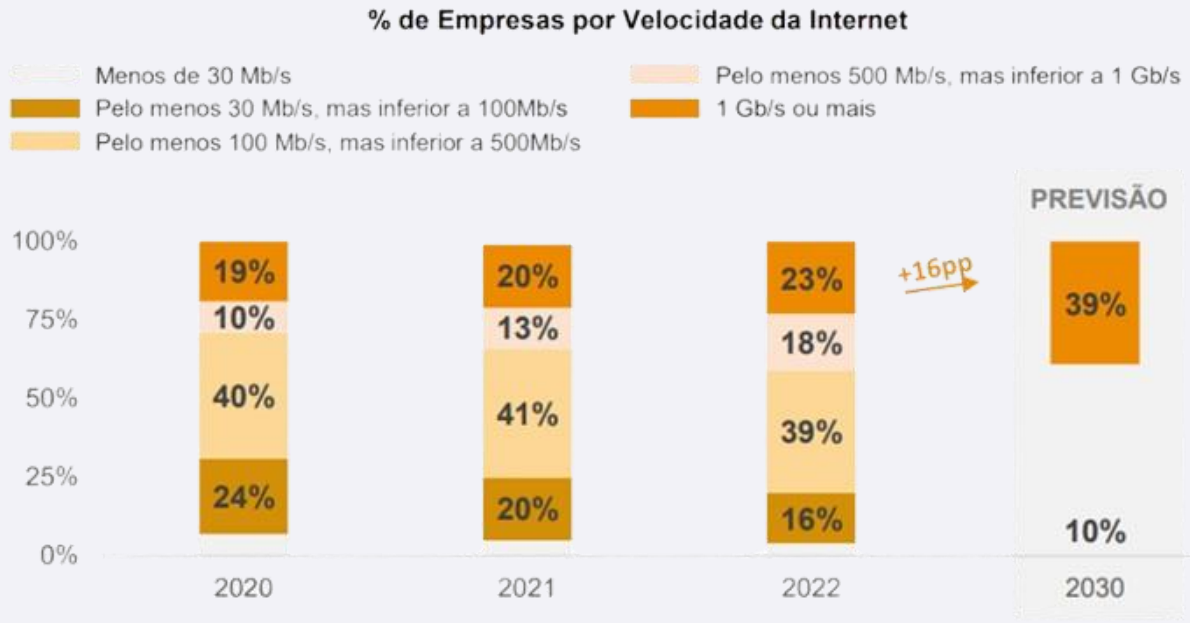
[79] Deloitte e Universidade de Coimbra,"Avaliação do Potencial Económico", 89.

[80] Deloitte e Universidade de Coimbra,"Avaliação do Potencial Económico", 89.

[81] Deloitte e Universidade de Coimbra,"Avaliação do Potencial Económico", 91.

[82] "Inquérito à utilização de tecnologias da informação e da comunicação nas empresas", *INE*, 21 de novembro de 2023, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637881953&att_display=n&att_download=y.

Figura 1 - Velocidade de Internet



(Fonte: Deloitte e Universidade de Coimbra, "Avaliação do Potencial Económico da Transição Digital em Portugal", 2023, 89)

- Cobertura de internet de alta velocidade:
  - Um estudo comparativo entre os preços dos pacotes de acesso a banda larga, voz e dados móveis, concluiu que os preços nacionais aparentam estar acima da média europeia. Através da análise aos preços dos cabazes das 3 vertentes - internet fixa, dados móveis e convergente - verificou-se que Portugal se insere nos *clusters* de países com os preços mais elevados da UE;
  - Para o ano de 2021, Portugal apresentou o indicador relativo à cobertura 5G com valores nulos nas estatísticas do Eurostat de 2021 - o que representava um atraso significativo em comparação com os valores da UE nesse mesmo ano (65,8% de cobertura 5G).
  - Portugal encontra-se na sétima posição no que diz respeito à cobertura de internet de alta velocidade, segundo a Eurostat, com Malta, Luxemburgo e Dinamarca a liderar. Países como a Grécia, Chipre e Itália são os Estados-Membros que ocupam as posições finais da tabela, com valores mínimos de 44% de cobertura[83].
  - No entanto, a ANACOM revelou que no ano de 2022, 98% dos concelhos e 49% das freguesias estavam já cobertos por 5G. Este aumento é justificado pela estratégia para a quinta geração de comunicações móveis (5G) e pelo Leilão 5G[84].

[83] "Broadband Coverage in Europe 2021", Comissão Europeia, agosto de 2022, https://ec.europa.eu/newsroom/dae/redirection/document/88314 .
[84] Deloitte e Universidade de Coimbra, "Avaliação do Potencial Económico da Transição Digital", 85.

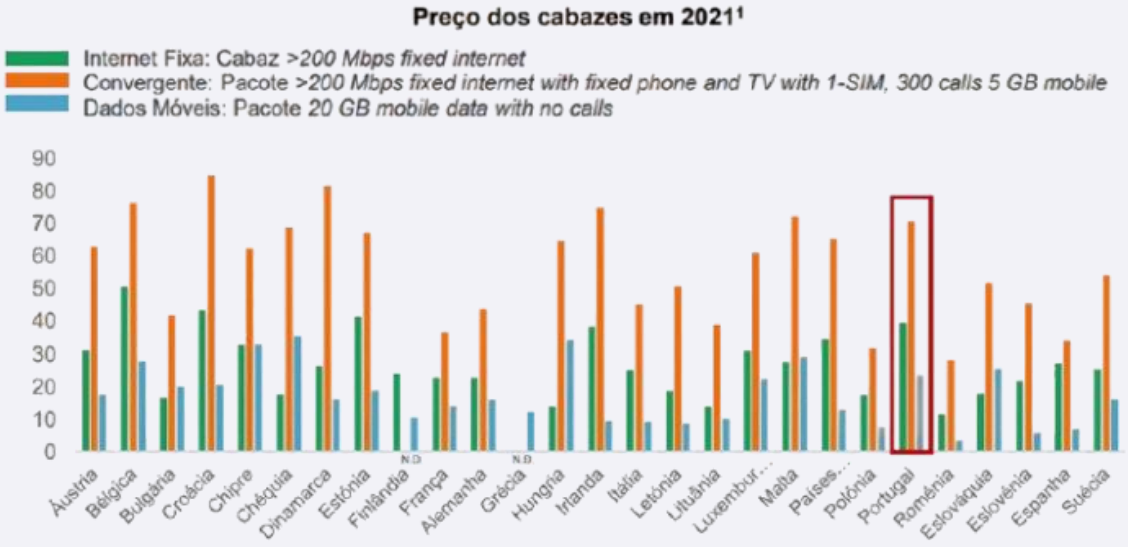
Tabela 5 - Velocidade de Internet

	Cobertura por rede gigabit (%)	Cobertura 5G (%)
Target	100	100
EU 2021	70,2	65,8
PT 2021	90,5	0
PT 2022	-	Concelhos - 98
		Freguesias - 49

(Fonte: Deloitte e Universidade de Coimbra, "Avaliação do Potencial Económico da Transição Digital em Portugal", 2023, 85)

Uma nota importante relativamente a estes dados é a forma como a recolha dos valores dos indicadores é feita pela ANACOM em Portugal e pela UE. Até à data deste relatório, não há forma de identificar e validar que a recolha é feita da mesma forma por ambas as entidades. Neste sentido, não se pode concluir se o atraso significativo verificado em 2021 foi ou não recuperado em 2022. Esta validação só se poderá confirmar na próxima atualização anual dos dados por parte do Eurostat, através de comparação direta.

Figura 2 - Preço dos Cabazes



(Fonte: Deloitte e Universidade de Coimbra", Avaliação do Potencial Económico da Transição Digital em Portugal", 2023, 87)

Ainda no contexto da cobertura 5G em Portugal, em 2019 a Ericsson conduziu a um estudo relativo ao Impacto da quinta geração (5G) em Portugal - Relatório de Mobilidade da Ericsson[85]. As conclusões da Ericsson avançam que, até ao fim de 2025, o 5G deverá cobrir 65% da população mundial e será responsável por 45% do tráfego global de dados móveis. No contexto nacional, o Relatório de Mobilidade da Ericsson relata que o lançamento de cobertura de 5G terá um impacto de cerca de 3,6 mil milhões de euros na economia portuguesa até 2030. Segundo as estimativas da empresa, haverá um consumo global de 24 Gigabyte (GB) por mês, em média, por parte dos utilizadores de *smartphones*. Até 2019, a utilização era de 7,2 GB.

O impacto e papel que as infraestruturas digitais trazem para o contexto económico nacional, o investimento feito na área, a adaptação de ações a contextos europeus e a crescente colaboração entre países europeus atuam também, consequentemente, como forte impulsionador a empresas, indivíduos, serviços e contextos que dependem, direta ou indiretamente, de infraestruturas digitais.

No seguimento do papel da GigaPIX na qualidade de rede IP em Portugal, é de notar o forte impacto que é promovido através da redução de latência de serviço (e, consequente, melhoria das ligações de rede IP), aumento da velocidade e diminuição dos custos de serviço - aumentando o acesso a mais entidades coletivas e individuais.

Dados divulgados pela Associação .PT - DNS.PT, mostram que o aumento do domínio .pt cresceu 11% no ano de 2021, em relação ao ano de 2019, batendo recorde e tornando-se o .pt um dos domínios de topo que mais cresceu no espaço europeu[86].

Foi também criado o projeto Empresa na Hora, enquadrado na iniciativa 3em1[87] que permite atribuir, a alguém que crie uma empresa, um pacote de serviços gratuitos com domínio registado em .pt, ferramenta de desenvolvimento de site, alojamento técnico e caixas de correio eletrónico. Esta é uma ação que permite às "empresas, em particular, perceberem que têm de continuar a fazer esta transformação e a investir numa presença *online* para impulsionar os seus negócios"[88].

A pandemia de covid-19 veio trazer uma mudança significativa no setor das infraestruturas digitais, sendo a mais importante a adoção do teletrabalho. Inicialmente, as infraestruturas de TI da maior parte das empresas não estavam preparadas para suportar um volume tão alto de acessos remotos e, de forma a mitigar estes problemas, as empresas tiveram de investir na segurança, melhorar as capacidades de rede e implementar soluções como *VPNs* e ferramentas de monitorização e gestão de forma remota. A medida "TD-C16-i05" surgiu como uma das iniciativas do Plano de Recuperação e Resiliência de Portugal, conhecida como Plano Renova Portugal. Este plano foi desenvolvido em resposta à crise económica e social provocada pela pandemia COVID-19, com o objetivo de promover a recuperação e fortalecer a resiliência da economia portuguesa[89].

---

85 Juliana Guerra, "Impacto do 5G em Portugal pode chegar aos 3,6 mil milhões de euros", *Ericsson*, 11 de junho de 2019, https://www.ericsson.com/pt/press-releases/2019/6/ericsson-mobility-report-a-adocao-da-tecnologia-5g-e-ainda-mais-rapida-do-que-esperada.

86 "Domínio .pt cresceu 11% em 2021", Comunicados, República Portuguesa, 25 de janeiro de 2022, https://www.portugal.gov.pt/pt/gc22/comunicacao/comunicado?i=dominio-pt-cresceu-11-em-2021.

87 "Sobre", Três Em Um, https://3em1.pt/.

88 Fátima Caçador, "Registo de domínios .pt com novo recorde em 2022. Foram registados mais de 150 mil", *Sapo TEK*.

89 "TD-C16-i05 CAPACITAÇÃO E TRANSFORMAÇÃO DIGITAL DAS EMPRESAS DOS AÇORES", Recuperar Portugal, https://recuperarportugal.gov.pt/transicao-digital/empresas-4-0/td-c16-i05-capacitacao-e-transformacao-digital-das-empresas-dos-acores/.

De forma a suportar todo este acréscimo de utilização, o setor das infraestruturas digitais teve avanços significativos, houve um aumento da capacidade de processamento dos centros de dados, assim como de armazenamento. Portugal está no sexto lugar de melhor país para trabalho remoto, segundo a *NordLayer* (empresa que criou o Índice Global de Trabalho Remoto[90]). Este índice leva em conta 4 dimensões: cibersegurança, economia, infraestrutura física e digital e a segurança no país.

Atualmente, segundo as estatísticas do emprego realizadas pelo INE, no primeiro trimestre do ano de 2024, mais de 19% da população empregada trabalhou a partir de casa. O regime misto é o mais adotado pelas empresas, sendo que mais de 73% das pessoas que indicaram trabalhar regularmente a partir de casa referiu que está neste regime[91].

1.1.2. Especificidades tecnológicas

A fibra ótica e a tecnologia 5G são componentes essenciais para o avanço do setor das infraestruturas digitais. A fibra ótica tem a capacidade de transmitir grandes volumes de dados a uma velocidade extremamente alta com uma perda de sinal mínima, e permite suportar os crescentes pedidos pela largura de banda devido ao aumento de consumo de conteúdos digitais, como serviços de *streaming*. Já a tecnologia 5G trouxe a disponibilização de conetividade sem fios, com velocidades de *download* e *upload* significativamente mais altas do que a tecnologia 4G (geração anterior). O aumento da capacidade de dispositivos ligados e a redução da latência são outras duas características importantes da tecnologia. A primeira permite o desenvolvimento da Internet das Coisas (IoT) e a segunda permite várias aplicações como cirurgias remotas, carros autónomos e até a realidade aumentada.

Em 2023, foi aberto um concurso público internacional com o objetivo de dar cobertura de fibra a zonas sem acesso. A data prevista de finalização é entre 2026 e 2027 e, caso seja implementado com sucesso, Portugal poderá ser um dos primeiros países da União Europeia a ter uma cobertura com redes fixas de capacidade muito elevada em todo o seu território. É importante realçar que, com este projeto, também haverá um reforço significativo na cobertura de rede móvel, nomeadamente, a rede 5G[92]. O investimento em causa será de 425 milhões de euros, sendo cerca de 150 milhões comparticipados pelos Programas Regionais do Portugal 2030[93]. De forma a perceber que zonas não têm cobertura de redes fixas de capacidade muito elevada, a ANACOM procedeu a um levantamento geográfico onde foram identificados cerca de 417 mil edifícios residenciais e não residenciais sem cobertura[94].

[90] "Which countries score the highest?", *Nordlayer*, última atualização em 22 de agosto de 2024, https://nordlayer.com/global-remote-work-index/#countries-score-table.
[91] "Estatísticas do emprego", *INE*, 8 de maio de 2024, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=665513779&att_display=n&att_download=y .
[92] "Telecomunicações e acesso à Internet de qualidade finalmente uma realidade em todo o País", Anacom, 6 de dezembro de 2023, https://www.anacom.pt/render.jsp?contentId=1769445.
[93] "Fibra ótica vai chegar a todo o país até 2027", Portugal.gov.pt, 12 de dezembro de 2023, https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=esta-aberto-o-concurso-para-levar-a-fibra-otica-a-todo-o-pais.
[94] "Telecomunicações e acesso à Internet de qualidade finalmente uma realidade em todo o País", Anacom, 6 de dezembro de 2023.

De acordo com o relatório de tecnologias emergentes, elaborado pelo CNCS em maio de 2023, a tecnologia 5G já tem um fim previsto. A próxima tecnologia (6G) já está a ser preparada, estando previsto para 2027 as discussões finais sobre a alocação do espectro a ser utilizado e a especificação final deverá sair em 2030[95].

Portugal tem uma localização estratégica pois liga três continentes (Europeu, Americano e Africano), tendo sido este um fator importante para atrair investimentos nesta área. Devido ao crescente número de pedidos pelos serviços digitais, necessidade de armazenamento e processamento de dados, espera-se um crescimento ainda maior de centros de dados em Portugal[96].

A maioria das tecnologias digitais têm sistemas de segurança, nomeadamente do tipo criptográfico. Por exemplo, os dados enviados e recebidos por um ponto de troca de tráfego são sempre cifrados. Atualmente, a forma de cifragem mais utilizada é a cifragem de chave pública, onde existe uma chave pública que, como o nome indica, é do conhecimento público e tem como propósito cifrar os dados. Existe, também, uma chave privada de acesso restrito que pode desencriptar os mesmos. Como este processo de cifragem é baseado no poder computacional disponível e não em provas matemáticas, não é possível garantir a segurança e/ou privacidade dos dados num período razoável. Uma das soluções atuais é cifrar os dados com chaves cada vez mais longas. No futuro, com o surgimento da computação quântica, será possível decifrar estes dados numa questão de minutos. Ainda de acordo com o relatório do CNCS: "É previsível o aparecimento na próxima década de um computador quântico plenamente funcional" e deverá ser criada uma tecnologia criptográfica[97].

Devido ao grande volume de dados processados nos pontos de troca de tráfego (por exemplo, o GigaPix, de setembro de 2023 a agosto de 2024 processou, em média, cerca de 193.49GB por segundo[98]), estes têm recorrido aos serviços *cloud* para aumentar a sua capacidade de armazenamento e processamento de dados. A IA (Inteligência Artificial) também está a ser amplamente difundida via *cloud* pois as utilizações de ferramentas de IA necessitam de um elevado poder computacional, assim como de recursos humanos especializados e, utilizando as soluções de *cloud*, este problema consegue ser evitado[99].

[95] "Tecnologias Emergentes", Centro Nacional de Cibersegurança, maio de 2023, 73, https://www.cncs.gov.pt/docs/rel-tecemer2023-observ-cncs.pdf.

[96] "A economia dos Data Centers em Portugal: o que esperar para os próximos anos?", *DatacenterDynamics*, 26 de abril de 2023, https://www.datacenterdynamics.com/br/an%C3%A1lises/a-economia-dos-data-centers-em-portugal-o-que-esperar-para-os-proximos-anos-/.

[97] "Tecnologias Emergentes", Centro Nacional de Cibersegurança, 87,88 e 89.

[98] https://gigapix.pt/en/technical/traffic-stats/ (dados de tráfego são apresentados em contínuo e não é possível definir um período para a consulta do tráfego)

[99] "Tecnologias Emergentes", Centro Nacional de Cibersegurança, 21 e 22.

Segundo a IDC, a área de *cloud computing* vai atingir um investimento de mil milhões de euros em 2026 onde o destaque vai para a área de *Software as a Service* (*SaaS*) que representa 70% do mercado e tem uma previsão de subir 685 milhões de euros até 2026. Prevê-se um crescimento de 30% até 2026 para o modelo *Platform as a service* (*PaaS*), atingindo 223,4 milhões de euros. Já o modelo *Infrastructure as a service* (*IaaS*) deverá ter um crescimento de 25% e 264 milhões de euros de investimento até ao mesmo ano[100].

[100] Dave McCarthy et al, "IDC FutureScape: Worldwide Cloud 2023 Predictions", *IDC*, outubro de 2022, https://www.idc.com/getdoc.jsp?containerId=US48602322.

1.2. Ameaças

As principais ameaças de cibersegurança neste setor prendem-se com os serviços por este prestados, ou seja, são sobretudo as ameaças e os ataques relativos aos DNS, como *DNS amplification*, *spoofing/cache poisoning*, *tunneling*, ataques aos pontos de troca de tráfego, tais como ataques de interseção (*Man-in-the-Middle*) ou de *rerouting*, e ataques aos registos de domínios de topo, tais como ataques de *domain hijacking*.

Segundo o relatório da Enisa "*DNS Identity*", elaborado em 2023, as credenciais são uma parte essencial do registo dos domínios e, como tal, os ataques a estas credenciais resultam em alguns problemas, tais como interceção de tráfego, ataques de engenharia social, ataques ao domínio, entre outros. O relatório refere alguns exemplos, como o ataque ao domínio de cripto *Coin Check* e ao domínio da Lenovo[101].

O primeiro ataque ocorreu em junho de 2020 e, como resultado, a *Coin Check* sofreu uma violação de dados após um terceiro, não autorizado, aceder à conta de registo de domínio da empresa. O atacante utilizou o domínio ".jp" para enviar e-mails fraudulentos, resultando na exposição de dados de cerca de 200 clientes[102]. No segundo ataque, ocorrido em fevereiro de 2015, os domínios da Lenovo e da Google no Vietname foram sequestrados pelo grupo Lizard Squad, que explorou uma vulnerabilidade na Webnic (empresa de registo de domínios). Através do controlo do *DNS*, os atacantes redirecionaram o tráfego para servidores controlados pelo grupo ficando assim com acesso a toda a informação[103].

De acordo com a *OWASP* (*Open Web Application Security Project*), existem três ataques típicos que podem afetar tanto os registos como os sistemas de gestão de identidade que os mesmos utilizam:

1. Utilizar listas de palavras-passe conhecidas e utilizar essa informação numa aplicação que não contenha qualquer tipo de proteção contra ataques de *credential stuffing*;
2. Elaborar ataques de autenticação contra aplicações sem requisitos de complexidade ou rotação de palavras-passe, ou até mesmo sem *MFA* (autenticação multifator) implementada;
3. A aplicação não tem os tempos das sessões implementadas corretamente ou o utilizador usa um computador público para aceder a uma aplicação e, quando sai, não termina a sessão. Com isto, um atacante consegue aceder à sua conta no mesmo *browser*, passado uma ou duas horas[104].

[101] "DNS IDENTITY Verification and Authentication of Domain Name Owners", *ENISA*, maio de 2023, 18, https://www.enisa.europa.eu/publications/dns-identity.
[102] Paddy Baker, "Coincheck Customers Fall Victim to Data Breach After Domain Account Error", Coincheck, 3 de junho de 2020, https://www.coindesk.com/markets/2020/06/03/coincheck-customers-fall-victim-to-data-breach-after-domain-account-error/.
[103] "Webnic Registrar Blamed for Hijack of Lenovo, Google Domains", KrebsonSecurity, 26 de fevereiro de 2015, https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/.
[104] ENISA, "DNS IDENTITY Verification and Authentication of Domain Name Owners", 19.

Existem outros tipos de ataques, todos com o mesmo objetivo: obter de forma ilegítima as credenciais do registo de domínios. Estes ataques podem ser de engenharia social levando a que um utilizador coloque as credenciais num *website* falso (*Phishing*). Também existem ataques de *brute-force* que consistem no uso de ferramentas automatizadas que geram milhares de milhões de possíveis palavras-passe e ocorrem outras tantas tentativas até ser descoberto a combinação correta. Este tipo de ataque é facilmente evitado limitando o número de tentativas falhadas na aplicação[105].

Conforme já referido anteriormente, o sistema de nomes de domínio é uma parte crucial da infraestrutura da Internet e é essencial para a tradução de nomes de domínio legíveis para endereços de *IP* e vice-versa. Devido a esta importância, o *DNS* é um alvo sistemático de ataques de cibersegurança. Um dos ataques mais frequentes é o ataque de negação de serviço onde é enviado um grande número de requisições *DNS* para sobrecarregar o servidor em questão, tornando assim o servidor lento e sem capacidade de resposta. Outro ataque passa pela modificação dos dados, mais conhecido por ataque *man-in-the-middle*, onde existe um atacante entre o recetor e o emissor dos dados, conseguindo assim romper a cadeia de confiança e modificar os dados enviados. Ainda dentro dos ataques de *DNS*, temos o ataque *DNS ID hacking* onde um atacante faz-se passar por um servidor de *DNS* fidedigno e, por fim, temos o ataque por envenenamento de cache que consiste num atacante a injetar dados maliciosos de *DNS* nos servidores de *DNS* utilizados pelos *ISPs*[106].

Existem outros tipos de ataques denominados por ataques de amplificação. Estes ataques aumentam o volume do tráfego enviado a um alvo, utilizando respostas de *DNS* amplificadas. Estas são caracterizadas por enviar uma consulta a um servidor de *DNS* que replica com uma resposta muito maior, aumentando assim o tráfego. Fora deste tipo de ataques, temos o *DNS Hijacking* que tem como objetivo subverter a resolução de consultas *DNS*. Pode ser realizado por um *malware* que modifica as configurações *TCP/IP* de um computador de forma a colocar o mesmo a apontar para um servidor *DNS* controlado por um atacante ou pela modificação de um servidor *DNS* confiável. Este tipo de ataque pode servir como porta de entrada para ataques de *Phishing*, pois o atacante pode redirecionar as vítimas para um site falso, pedindo às mesmas para introduzirem as credenciais de *login* ou até mesmo informações bancárias confidenciais[107].

[105] ENISA, “DNS IDENTITY Verification and Authentication of Domain Name Owners”, 19 e 20.

[106] “DNS Advanced Attacks and Analysis”, Adam Ali.Zare Hudaib e Esra'a Ali Zare Hudaib, 2014, 65, https://www.academia.edu/download/35520765/DNS_Advanced_Attacks_and_Analysis.pdf.

[107] Adam Ali.Zare Hudaib e Esra'a Ali Zare Hudaib, “DNS Advanced Attacks and Analysis”, 67 e 68.

Dados apresentados no Relatório de Atividades e Contas de 2022[108] da .PT, sugerem que se manteve, em 2022, um crescimento da deteção e/ou reporte de eventos e incidentes nos canais internos e externos da .PT. Este crescimento deveu-se, não só ao crescimento de atividade maliciosa no contexto de atuação do .PT como também à capacidade interna na identificação e reporte de qualquer atividade maliciosa. O relatório espelha ainda que, comparativamente com o mesmo período do ano de 2021, foram registados mais de 600 eventos de cibersegurança - representando um aumento de 69,4%. Destes eventos de cibersegurança, 2 foram classificados como incidentes de segurança, embora mitigados de forma que não causassem um impacto significativo nas operações do .PT. Foi criada uma maior segurança e confiança no domínio .pt, através da monitorização e gestão de atividades de *DNS Abuse* e através da identificação proativa de domínios registados sob .PT usados para desenvolver atividade maliciosa, como a disseminação de *malware* ou de *phishing* e na colaboração para a sua rápida mitigação, através da cooperação com parceiros e autoridades competentes, quando necessário. Em 2022, foram identificados 130 casos de *DNS Abuse*. Do total, 96 dos casos tinham o objetivo de desenvolver atividade de *phishing*, 28 distribuiam *malware* e 6 estavam a ser utilizados para *spam*. Estes valores representam um aumento de 36% desta atividade quando comparado com 2021.

De acordo com o relatório anual de 2023 elaborado pelo SOCPT, existiram 164 eventos reportados, cerca de 330 mil e-mails maliciosos recebidos, 647 casos identificados de abuso de DNS e 130 reportados, 89% destes casos tratava-se de *phishing* e 82% foram resolvidos em menos de 8 dias. Em relação a *standards* de segurança implementados nos registadores, cerca de 94% têm *HTTPS* e um certificado digital válido, 22% têm DNSSEC e 35% têm *HSTS*[109]. Relativamente à formação e sensibilização, em 2023, houve 5 cursos de cibersegurança onde participaram mais de 3 mil pessoas, houve sete publicações da PTSOC {Digest} e 4 edições da {News} e ocorreram 16 *workshops* onde participaram mais de 650 pessoas[110].

[108] .pt, "Relatório de Atividades e Contas 2022", 33, https://www.pt.pt/fotos/editor2/relatorios/relatorio_atividades_contas_2022.pdf.

[109] "Annual Report PTSOC 2023", *PTSoc*, 12-13, https://ptsoc.pt.pt/en/relatorio-anual-ptsoc-2023/.

[110] "Annual Report PTSOC 2023", *PTSoc*, 16.

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos[111], 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[112].
- **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[113].
- ***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[114].
- **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[115]. No caso, consideraram-se os colaboradores internos maliciosos.

[111] CNCS, "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança, https://www.cncs.gov.pt/pt/observatorio/#relatorios.
[112] CNCS, "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021", maio de 2021, 74, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf.
[113] CNCS, "Relatório Riscos & Conflitos 2021", 75.
[114] CNCS, "Relatório Riscos & Conflitos 2021", 75-76.
[115] CNCS, "Relatório Riscos & Conflitos 2021", 76-77.

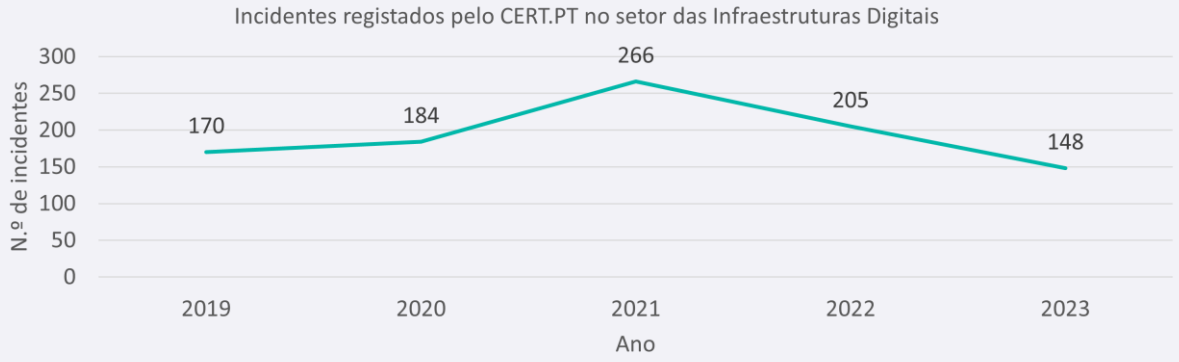
Tabela 6- Agentes de ameaça mais prováveis (Infraestruturas Digitais)

Tipo de ameaça	Cibercriminosos	Agentes estatais	*Hacktivistas*	Colaboradores internos
Ransomware	■	■	■	■
DDoS	■	■	■	
Ataques *DNS*	■	■	■	
Vulnerabilidades	■	■	■	■
Phishing, Spear Phishing e *Smishing*	■	■	■	
Manipulação de Sistemas (TI)	■	■		■

Legenda:
■ - Agente de ameaça provável

A atratividade do setor das infraestruturas digitais para ciberataques é comprovada pelo número de ataques que o setor tem sofrido em Portugal. Segundo dados do CERT.PT, registaram-se 825 ataques entre 2019 e 2022, tornando este setor o setor que sofreu mais ataques. Este registo ficou apenas atrás do setor bancário[116].

Figura 3 - Número de incidentes no setor das Infraestruturas Digitais anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, https://www.cncs.gov.pt/pt/estatistica/)

[116] CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, https://www.cncs.gov.pt/pt/estatistica/.

1.3. Capacitação

Capacitação Digital em Portugal

O Relatório de atividades e contas de 2022 da .PT permite fazer um resumo geral da estratégia presente (2022) e futura[117]:

1. **Desenvolvimento de competências**
   - 1.1. Programas de Formação e Workshops
     - 1.1.1. Organização de *workshops* com o objetivo de fortalecer as competências técnicas dos *registrars* em *DNSSEC*;
     - 1.1.2. Adoção do programa *Cisco Networking Academy*® (*NetAcad*) pelo .PT no âmbito das atividades do seu Centro de Formação.
   - 1.2. Sensibilização e Educação
     - 1.2.1. Disponibilização de materiais educativos sobre segurança, como campanhas sobre o Registry Lock Service;
     - 1.2.2. Realização de exercícios internos de phishing para aumentar a sensibilização sobre cibersegurança da organização e entre os registrars.
   - 1.3. Formação Especializada
     - 1.3.1. Desenvolvimento de formações específicas para a equipa do PTSOC, com o objetivo de melhorar as competências na monitorização e resposta a incidentes de segurança.

2. **Cibersegurança**
   - 2.1. Monitorização
     - 2.1.1. Implementação da monitorização contínua das ameaças e manutenção da plataforma SIEM;
     - 2.1.2. Revisão dos procedimentos e destacamento da importância da proteção dos domínios contra acessos não autorizados.
   - 2.2. Auditorias e Certificações
     - 2.2.1. Realização periódica de auditorias para garantir a conformidade com os padrões de segurança;
     - 2.2.2. Alcançar novos níveis de certificação, de forma a reforçar a credibilidade e segurança dos serviços prestados.

3. **Parcerias estratégicas**
   - 3.1. Colaboração com entidades de segurança
     - 3.1.1. Participação ativa nas iniciativas da rede nacional CSIRT;
     - 3.1.2. Desenvolvimento de uma plataforma em colaboração com o CNCS, com capacidade de deteção e mitigação de vulnerabilidades em websites.

4. **Promoção da segurança digital**
   - 4.1. Conscientização e adesão
     - 4.1.1. Elaborar iniciativas colaborativas com os registrars para promover a adoção de medidas de segurança;
     - 4.1.2. Publicação de um relatório sobre os padrões de segurança nos registrars por parte da equipa PTSOC, com o objetivo de melhorar a transparência.

[117] .pt, “Relatório de Atividades e Contas 2022”, 18-19 e 30-36.

Portugal tem feito uma aposta significativa em tecnologias e infraestruturas digitais, como o Plano de Ação para a Transição Digital. O desafio reside, em grande parte, na adoção e integração destas tecnologias pelas empresas e na formação dos seus trabalhadores para utilizar eficazmente as novas ferramentas digitais. A resistência à mudança e a falta de competências digitais entre os trabalhadores são barreiras que precisam de ser superadas para que o país possa aproveitar plenamente os benefícios da economia digital[118].

A iniciativa Plano de Ação para a Transição Digital tem como grande objetivo acelerar a transformação digital de Portugal (estado, empresas e pessoas), tornando o país mais competitivo a nível internacional, conforme é definido pela Diretiva NIS. Os três principais pilares de atuação deste plano são: "Capacitação e inclusão digital", "Transformação digital empresarial" e "Digitalização do Estado"[119].

O primeiro pilar, "Capacitação e inclusão digital", tem como foco três subpilares: "Educação digital", "Requalificação e formação digital", e "Literacia digital"[120]. O primeiro subpilar propõe-se a ser cumprido com a implementação de um programa para transformar digitalmente as escolas, colocar a disciplina de TIC no ensino básico, fazer uma promoção da programação e robótica na escola e criar uma iniciativa denominada por "Engenheiras por 1 Dia", onde incentiva a participação de pessoas do género feminino nas áreas de tecnologias[121]. No subpilar "Requalificação e formação digital" propõe-se a ser criado um programa "UpSkill" que irá formar intensivamente cerca de 3000 profissionais na área digital, haverá formações nas áreas digitais para desempregados, professores e formadores, e irão ser aplicadas metodologias inovadoras em cursos profissionais. Por fim, no subpilar "Literacia digital", propõe-se a ser criado um programa de inclusão digital com o objetivo de oferecer competências digitais básicas a cerca de um milhão de adultos, irá também ser criada uma tarifa social para garantir o acesso a serviços de Internet a preços mais reduzidos e irão ser desenvolvidas comunidades criativas para promover a inclusão digital[122]. O principal objetivo deste pilar é melhorar a qualidade do ensino, dotar os alunos de competências digitais, promover a igualdade de oportunidades, alargar a oferta formativa das instituições de ensino superior, aproximando-as das necessidades do mercado laboral e requalificar trabalhadores para minimizar o impacto da automatização que já está a decorrer no mercado de trabalho[123]. A Diretiva NIS exige que as infraestruturas essenciais, como saúde, energia, telecomunicações e transportes, estejam protegidas contra incidentes de cibersegurança. Devido a isto, é vital assegurar que as pessoas que operam ou interagem com estas infraestruturas tenham o conhecimento necessário e estejam aptas para manter a segurança e a integridade dos sistemas[124].

[118] Miguel Abecasis et al.,, "O impacto do digital na economia portuguesa", https://web-assets.bcg.com/img-src/O-impacto-do-Digital-na-economia-portuguesa_tcm9-214461.pdf.

[119] "Sobre nós", Portugal Digital, https://portugaldigital.gov.pt/sobre-nos/.

[120] "Plano de Ação para a Transição Digital de Portugal", Portugal Digital, 5 de março de 2020, 16, https://portugaldigital.gov.pt/wp-content/uploads/2022/01/Plano_Acao_Transicao_Digital.pdf.

[121] Portugal Digital, "Plano de Ação para a Transição Digital de Portugal", 17.

[122] Portugal Digital, "Plano de Ação para a Transição Digital de Portugal", 18.

[123] Portugal Digital, "Plano de Ação para a Transição Digital de Portugal", 22,23 e 25.

[124] Diretiva 2016/1148, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.

O segundo pilar denominado por “Transformação digital empresarial” é constituído por três subpilares: "Empreendedorismo e atração de investimento", "Tecido empresarial, com foco nas PME" e "Transferência de conhecimento científico e tecnológico para a economia"[125]. No primeiro subpilar está planeada a criação do programa "e-Residency", e tem como objetivo criar um sistema de identidade digital de forma a facilitar a relação das empresas estrangeiras com Portugal. Este subpilar conta com mais iniciativas, nomeadamente: A criação de um programa de capacitação digital de Pequenas e Médias empresas (PMEs) localizadas no interior do país, financiamento e apoio a investimento feito em iniciativas digitais e a criação do programa *Experience i4.0* que tem como objetivo fornecer ferramentas para medir a maturidade digital das empresas. O objetivo do segundo subpilar é conectar as PMEs com grandes empresas, desenvolver ferramentas para apoiar as PMEs no registo de patentes e financiar o aumento da presença digital das PMEs. Por fim, no último subpilar a principal medida é a promoção das zonas livres tecnológicas (ZLT), estas ZLT têm como grande objetivo incentivar a inovação e a criação de parcerias com universidades. Este pilar tem como grande objetivo tornar o tecido empresarial das PMEs mais digital[126]. De acordo com a Diretiva NIS, a adoção de novas tecnologias e a digitalização dos processos empresariais aumentam a exposição a riscos de cibersegurança, devido a isto, é importante garantir que esta inovação tecnológica não compromete a segurança e a continuidade operacional nos setores essenciais para a economia e segurança nacional[127].

Por fim, o terceiro pilar “Digitalização do Estado” tem, também, três subpilares e o principal objetivo deste pilar é digitalizar os serviços do estado. O primeiro subpilar "Serviços Públicos Digitais" apresenta medidas como a digitalização dos serviços públicos mais utilizados pelos cidadãos e empresas, e aumentar a oferta de serviços digitais no portal ePortugal. O segundo subpilar "Administração central ágil e aberta" tem como principais medidas: tramitação eletrónica de processos de contraordenação, desenvolvimento de uma estratégia *cloud* para a administração pública e uma promoção ativa do teletrabalho. Por fim, o subpilar "Administração regional e local conectada e aberta" tem como medidas a implementação da estratégia nacional de Cidades Inteligentes e a coordenação do território através do Balcão Único do Prédio[128].

Esta iniciativa é considerada um documento "vivo", pois está sujeito à inclusão de novas medidas ou atualização das já existentes. A iniciativa deverá refletir o dinamismo das prioridades e preocupações da economia e da sociedade e, também, deve respeitar a estrutura estabelecida[129]. Conforme o contexto da Diretiva NIS, a transição digital das infraestruturas digitais é fundamental no setor. É importante assegurar que esta transformação ocorre de maneira segura, protegendo sempre as infraestruturas críticas de forma a garantir a segurança nacional num cenário digital global.

[125] Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 27.
[126] Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 27-37.
[127] Diretiva 2016/1148.
[128] Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 39-46.
[129] Portugal Digital, “Plano de Ação para a Transição Digital de Portugal”, 65 e 66.

1.4. Investimento em cibersegurança

Segundo o documento final "Avaliação do potencial económico da transição digital em Portugal" de 2023, existem dois principais "Apoios públicos no âmbito de Infraestruturas e Conectividade"[130]:

- Apoios públicos no âmbito de intervenções em infraestruturas digitais e conectividade a nível nacional:
- intervenções enquadradas no objetivo específico "RSO1.5. Reforçar a conectividade digital" integrado no **Portugal 2030.**
- Apoios públicos, iniciativas, planos e programas europeus no âmbito da promoção das infraestruturas digitais e conectividade na **UE**:
    - UE dispõe de um conjunto de instrumentos, iniciativas, planos e programas destinados a promover as infraestruturas digitais e a conectividade a nível europeu, em alinhamento com os objetivos definidos no programa Década Digital[131];
    - No caso da produção de semicondutores, existe a Aliança para Tecnologias de Processadores e Semicondutores[132].
    - No caso do aumento da implantação de nós periféricos, destacam-se a Aliança Europeia para os Dados Industriais, *Edge* e Nuvem[133], que resultará potencialmente em sinergias de investimento, e o Programa Europa Digital[134], que tem como objetivo financiar, entre outros temas, a criação de nós periféricos.
    - Sobre a criação do primeiro computador com aceleração quântica, destaca-se a iniciativa *Quantum Technologies Flagship*[135].

[130] Portugal Digital, "Plano de Ação para a Transição Digital de Portugal", 95.

[131] Comissão Europeia, "Década Digital da Europa: metas digitais para 2030", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt.

[132] Comissão Europeia, "Aliança sobre processadores e tecnologias de semicondutores", Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/pt/policies/alliance-processors-and-semiconductor-technologies .

[133] Comissão Europeia, "Aliança Europeia para os Dados Industriais, a Edge e a Nuvem", Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/pt/policies/cloud-alliance.

[134] Comissão Europeia, "Programa Europa Digital", Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/pt/activities/digital-programme.

[135] Comissão Europeia, "Quantum Technologies Flagship", Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.

No contexto dos apoios públicos no âmbito de intervenções em infraestruturas digitais e conectividade a nível nacional, estão definidas ações enquadradas no objetivo específico "RSO1.5. Reforçar a conectividade digital" integrado no **Portugal 2030,** a aplicar a diferentes regiões:

Tabela 7 - Intervenções em Infraestruturas Digitais

Região	Prioridade	Ações
PT - Programa Regional de Lisboa[136]	Não estão definidas ações no contexto de reforço de conectividade digital na região de Lisboa.	
PT - Programa Regional do Centro 2021-2027[137]	Conectividade Digital	Instalação de redes de banda larga
PT - Programa Regional do Norte 2021-2027 [138]	Norte mais Competitivo e Conectividade Digital	Instalação, gestão, exploração e manutenção de redes de comunicações eletrónicas de capacidade muito elevada (Gigabit)
PT - Programa Regional do Alentejo 2021-2027[139]	Alentejo mais digital	Instalação, gestão, exploração e manutenção de redes de comunicações eletrónicas de capacidade muito elevada (banda larga) - Instalação, gestão, exploração e manutenção de redes de comunicações eletrónicas de capacidade muito elevada: Infraestruturas digitais de banda larga (fixa e móvel) seguras, eficientes e sustentáveis prioritariamente em espaços de baixa densidade populacional ou do interior, instalando redes de comunicações eletrónicas de elevada capacidade nos territórios não cobertos pelo mercado de telecomunicações (e.g. zonas brancas), onde estas operações comerciais não são rentáveis, procurando, assim, suprir através de investimento público, nas componentes grossista e (parte) retalhista, a oferta de serviços não coberta pelas obrigações decorrentes do leilão 5G.
PT - Programa Regional do Algarve 2021-2027[140]	Conectividade Digital	Instalação e gestão de redes de comunicações eletrónicas de capacidade muito elevada (banda larga)

[136] "PT - Programa Regional de Lisboa 2021-2027", *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_lisboa.pdf.
[137] "PT - Programa Regional do Centro 2021-2027", *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_centro.pdf.
[138] Alina Silva et al., "Estratégia de Desenvolvimento do Norte para Período de Programação 2021-27 das Políticas da União Europeia", PT - Programa Regional do Norte 2021-2027, Portugal 2030, https://www.ccdr-n.pt/storage/app/media/2021/CCDRN%202030-compactado.pdf.
[139] "PT - Programa Regional do Alentejo 2021-2027", *Portugal 2030*, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_alentejo.pdf.
[140] "PT - Programa Regional do Algarve 2021-2027", Portugal 2030, https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_algarve.pdf.

Lançada em julho de 2021 pela Comissão Europeia, a **Aliança sobre processadores e tecnologias de semicondutores** tem como objetivo reunir *stakeholders* essenciais que contribuam para a projeção e produção de *microchips*. O objetivo final destes *stakeholders* é o de dotar a UE das capacidades necessárias em tecnologias de semicondutores para alimentar as suas infraestruturas digitais críticas e redes de comunicação. As principais ações são as seguintes[141]:

1. O reforço do ecossistema europeu de conceção eletrónica, incluindo nós finais e soluções de *hardware* de código aberto.
2. O estabelecimento da capacidade de fabrico necessária, incluindo testes de montagem para produção de processadores fiáveis, componentes eletrónicos e tecnologias. Semicondutores mais avançados permitirão o aumento de desempenho e a redução da energia utilizada por *data centers* ou *endpoints*.

Da mesma maneira, a **Aliança Europeia para os Dados Industriais, a *Edge* e a Nuvem** pretendem reunir representantes que tenham um papel determinante no reforço da posição da UE no que diz respeito a tecnologias de computação em nuvem e periféricas (IA, IoT e tecnologia 5G). As suas ações são as seguintes[142]:

- reunir os intervenientes relevantes para preparar e atualizar roteiros de investimento horizontais e tecnológicos específicos em matéria de computação em nuvem e de vanguarda;
- formular recomendações para assegurar a integração coerente dos investimentos para a instalação de espaços comuns europeus de dados em domínios relevantes;
- aconselhar a Comissão sobre os requisitos e normas aplicáveis aos serviços de computação em nuvem, incluindo os contratos públicos.

O **Programa Europa Digital** consiste num programa de financiamento da UE centrado na integração da tecnologia digital nas empresas, cidadãos e administrações públicas. Neste sentido, e com foco nas PMEs, o orçamento previsto de 7,5 mil milhões de euros pretende apoiar projetos em cinco principais domínios de capacidade: supercomputação, IA, cibersegurança, competências digitais avançadas e garantia de uma ampla utilização das tecnologias digitais em toda a economia e na sociedade, nomeadamente através de polos de inovação digital[143].

Com um orçamento previsto de mil milhões de euros da UE, a iniciativa ***Quantum Technologies Flagship*** pretende apoiar o trabalho de centenas de investigadores quânticos num período de 10 anos. O principal objetivo deste projeto é o de apoiar diferentes ramos da investigação em domínio europeu, tais como: computação quântica, simulação quântica, comunicação quântica e deteção quântica[144].

[141] Comissão Europeia, "Aliança sobre processadores e tecnologias de semicondutores", *Shaping Europe's digital future*.

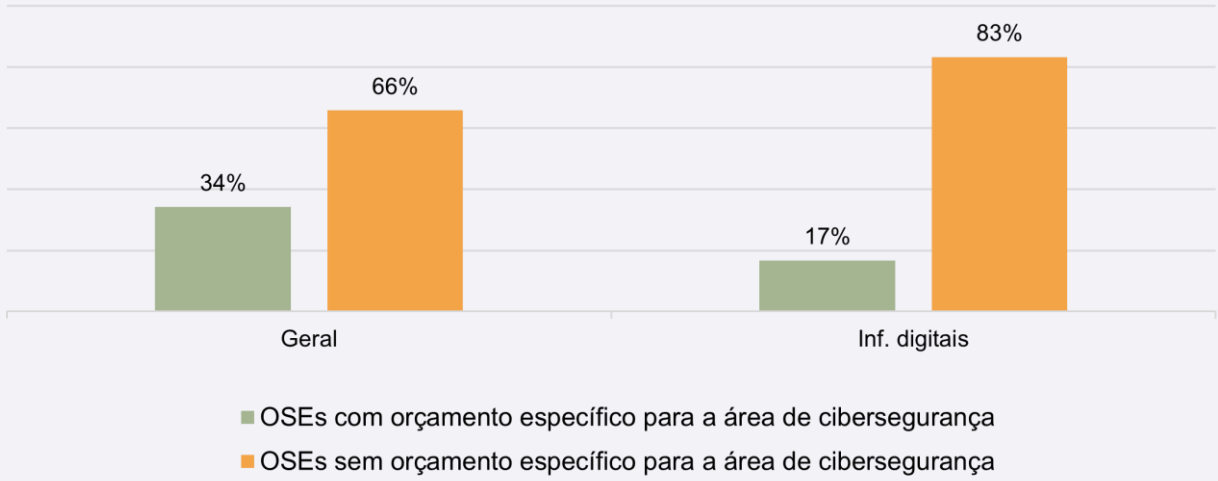
[142] Comissão Europeia, "Aliança Europeia para os Dados Industriais, a Edge e a Nuvem apresenta os seus primeiros resultados", *Shaping Europe's digital future*.

[143] Comissão Europeia, "Programa Europa Digital", *Shaping Europe's digital future*.

[144] Comissão Europeia, "Quantum Technologies Flagship", *Shaping Europe's digital future*.

Deste setor, cerca de 17% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Relativamente às áreas de aplicação do orçamento de cibersegurança, a maior parte das áreas de aplicação têm um valor de 50%, exceção para a gestão de vulnerabilidades, análise de segurança, segurança das redes e aquisição de *software* com 75%. Relativamente ao contexto geral, este setor tem uma percentagem maior na contratação de pessoal, gestão de vulnerabilidades e *governance* (**Gráfico 110 e 110.6**).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

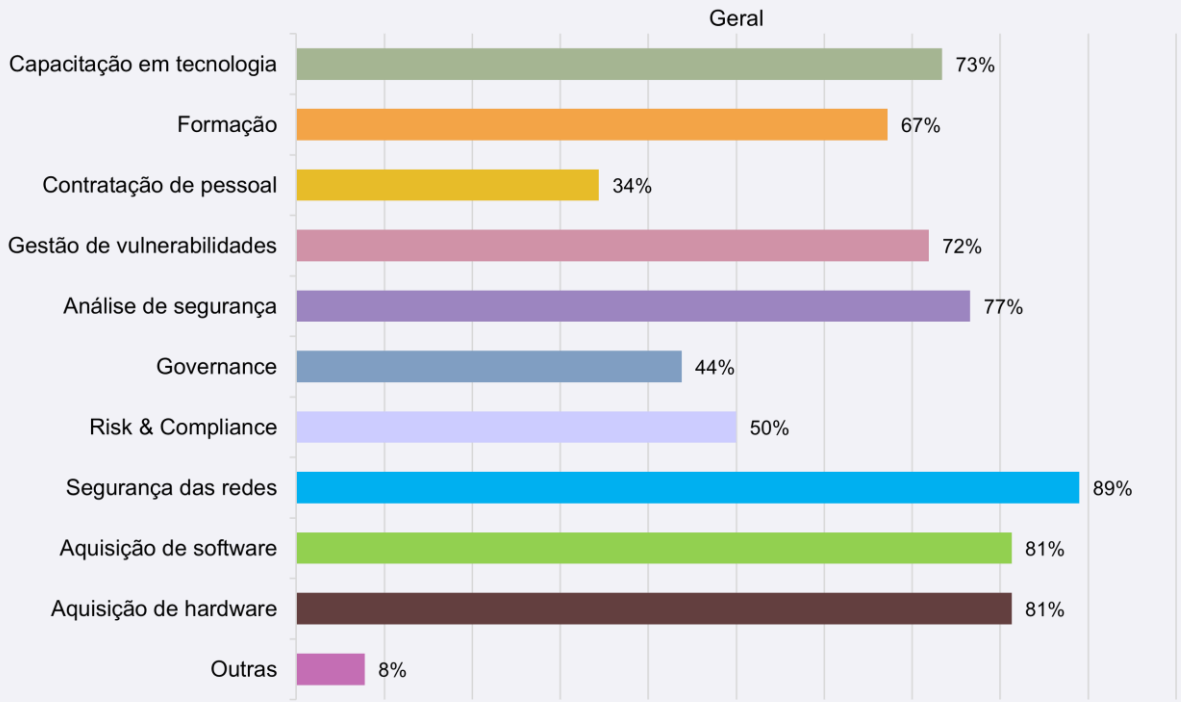
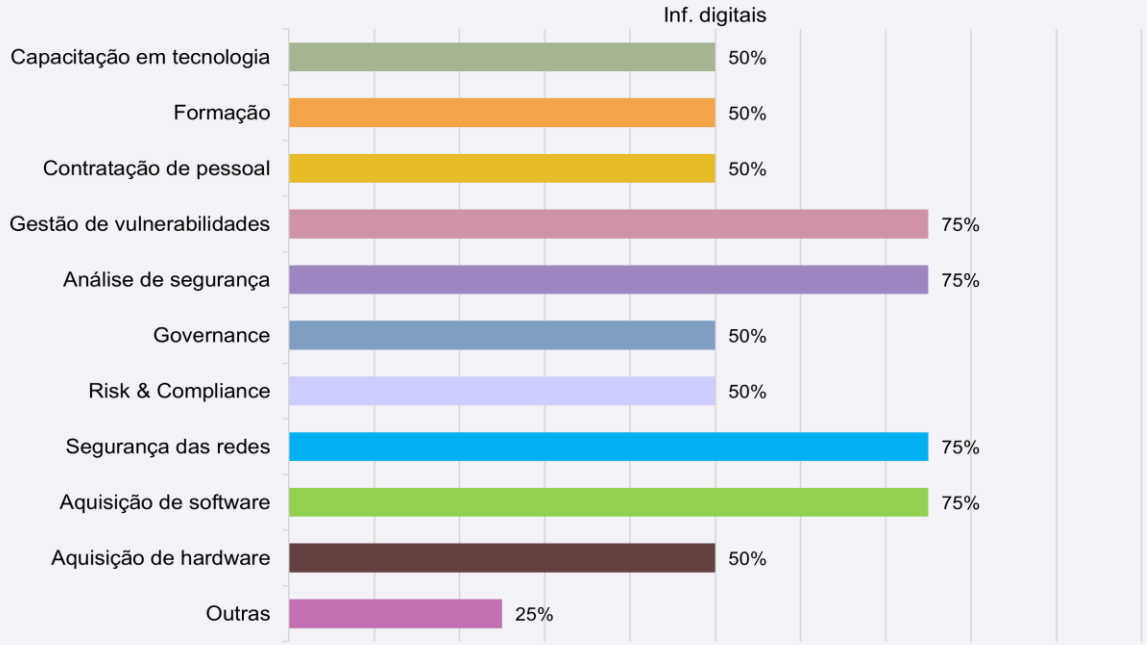
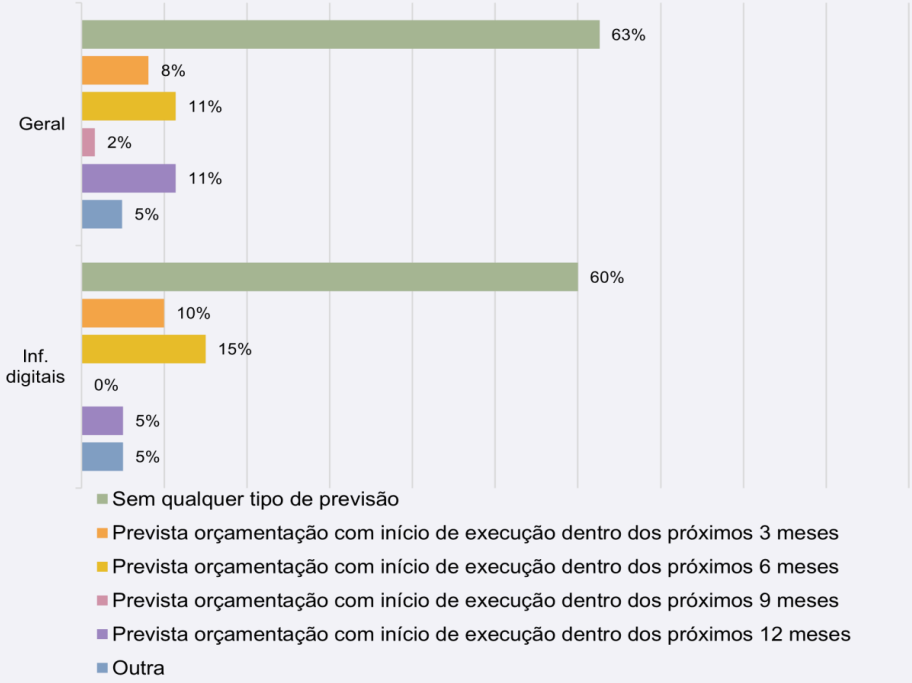


Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 60% não tem qualquer previsão para a orçamentação, 10% tem previsto a orçamentação dentro dos próximos 3 meses, 15% tem previsto a orçamentação para os próximos 6 meses e 5% para os próximos 12 meses. A maior diferença em relação à média geral está na orçamentação com início de execução dentro dos próximos 6 meses, onde este setor tem 15% e a média geral é de 11% (**Gráfico 111**).

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



Atualmente, os centros de dados são peças fundamentais para o funcionamento das empresas. Há cada vez mais centros de dados em Portugal, o que leva a um crescimento da economia e à formação de novos empregos. Ainda relativamente à transição digital, existem outros conjuntos de iniciativas e medidas:

- **Indústria 4.0**: É uma iniciativa que está integrada na Estratégia Nacional para a Digitalização da Economia, com o objetivo de criar condições favoráveis para o desenvolvimento da indústria nacional;
- **Open Days i4.0**: Integra a iniciativa da Indústria 4.0 e tem como grande objetivo demonstrar e partilhar as boas práticas das empresas nacionais;
- **Capacitar i4.0**: Também integra a iniciativa da Indústria 4.0 e tem como objetivo preparar e qualificar pessoas e organizações com competências técnicas para a Indústria 4.0;
- **SHIFT2Future**: O principal objetivo deste projeto é o de acelerar e apoiar a transição para a economia 4.0 e tem como publica alvo as PMEs dos setores de moldes e plásticos, pedra, cerâmica, automóvel, TI, *IoT*, entre outros, nas regiões Norte, Centro e Alentejo;
- **SHIFT to 4.0**: É uma ferramenta de diagnóstico para avaliar a maturidade digital de uma empresa, elaborando um relatório com linhas orientadoras de forma a ser possível melhorar a mesma com base na economia 4.0[145].

[145] "Transição Digital", *IAPMEI*, 23 de novembro de 2023, https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Industria-e-Sustentabilidade/Transformacao-digital.aspx.

1.5. RJSC e legislação setorial

A União Europeia tem sido o principal legislador do setor das infraestruturas digitais ao nível da cibersegurança, através da publicação de regulamentos e diretivas. A nível nacional, a legislação existente decorre principalmente da transposição dos diplomas europeus para o ordenamento jurídico português e da regulamentação feita pela entidade reguladora do setor - a Autoridade Nacional de Comunicações (ANACOM).

Apesar da atual preponderância do direito europeu no setor, é importante referir que este foi primeiro legislado a nível nacional no ano de 2004. A Lei n.º 5/2004, de 10 de fevereiro, também conhecida como Lei das Comunicações Eletrónicas, impunha "às empresas que oferecem redes e serviços de comunicações eletrónicas [condições de] segurança das redes públicas contra o acesso não autorizado (...) [e de] proteção dos dados pessoais e da privacidade no domínio específico das comunicações eletrónicas, em conformidade com a legislação aplicável à proteção de dados pessoais e da privacidade"[146]. Com o tempo, esta lei foi sendo alterada por outras, de modo a acomodar novos requisitos legais face à evolução tecnológica e à legislação europeia que foi sendo produzida. A lei n.º 5/2004 acabaria por ser integralmente revogada com a Lei n.º 16/2022, de 16 de agosto, que transpõe o Código Europeu das Comunicações Eletrónicas (Diretiva (UE) 2018/1972).

Veja-se então que legislação, nacional e europeia, foi surgindo para o setor das infraestruturas digitais até à revogação da Lei n.º 5/2004.

Diretiva n.º 2002/58/CE e Lei n.º 41/2004, de 18 de agosto (transposição): Esta diretiva e lei estabeleciam o regime aplicável ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, colocando obrigações "às empresas que oferecem redes e as empresas que oferecem serviços de comunicações eletrónicas"[147] ao nível da segurança, tal como o dever de "colaborar entre si no sentido da adoção de medidas técnicas e organizacionais eficazes para garantir a segurança dos seus serviços e, se necessário, a segurança da própria rede"[148], bem como de "garantir a inviolabilidade das as comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público"[149].

[146] Lei n.º 5/2004, de 10 de fevereiro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/5-2004-581061.
[147] Lei n.º 41/2004, de 18 de agosto, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/41-2004-480710.
[148] Lei n.º 41/2004.
[149] Lei n.º 41/2004.

Diretivas n.ºs 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/CE, 2009/140/CE e Lei n.º 51/2011, de 13 de setembro (transposição):

Respetivamente, a primeira diretiva era relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos[150], a segunda relativa à autorização de redes e serviços de comunicações eletrónicas[151], a terceira relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas[152], a quarta relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas[153]. A quinta diretiva (2009/140/CE) introduziu alterações às primeiras quatro referidas. A Lei n.º 51/2011, de 13 de setembro, transpôs estas diretivas para o ordenamento jurídico português. Estas diretivas e lei impuseram obrigações de "avaliar a segurança e integridade das redes e serviços no âmbito das políticas de segurança adotadas"[154], de adotar "medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços visando, em especial, impedir ou minimizar o impacte dos incidentes de segurança"[155], bem como de informar as autoridades reguladoras competentes (ENISA) e o público sobre graves violações de segurança[156].

Regulamento (UE) 2015/2120: Este regulamento não introduziu novas obrigações ao nível da cibersegurança, mas alterou a Lei das Comunicações Eletrónicas de modo a fortalecer os direitos dos cidadãos europeus no acesso à Internet aberta e ao tratamento equitativo do tráfego de dados por dos prestadores de serviços de acesso à Internet[157].

---

[150] Diretiva 2002/19/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos (diretiva acesso), *Jornal Oficial das Comunidades Europeias*, 7, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0019.

[151] Diretiva 2002/20/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa à autorização de redes e serviços de comunicações eletrónicas (diretiva autorização), *Jornal Oficial das Comunidades Europeias*, 21, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:PT:PDF

[152] Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), *Jornal Oficial das Comunidades Europeias*, 33, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:pt:PDF.

[153] Diretiva 2002/22/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas (diretiva serviço universal), *Jornal Oficial das Comunidades Europeias*, 51, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0022.

[154] Lei n.º 51/2011, de 13 de setembro, *Procuradoria-Geral Distrital de Lisboa*, https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=1515&pagina=1&ficha=1#.

[155] Lei n.º 51/2011.

[156] Lei n.º 51/2011.

[157] Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta, J*ornal Oficial da União Europeia*, 8, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015R2120.

Diretiva (UE) 2016/1148 (NIS), Lei n.º 46/2018, de 13 de agosto (transposição que estabelece o Regime Jurídico da Segurança do Ciberespaço - RJSC) e Decreto-Lei n.º 65/2021, de 30 de julho (que regulamenta o RJSC): A Diretiva (UE) 2016/1148[158], bem como a Lei n.º 46/2018, de 13 de agosto[159], foram os diplomas que identificaram os operadores deste setor como operadores de serviços essenciais. Embora legislação anterior impusesse já obrigações ao nível da cibersegurança, estes foram os atos legislativos de maior importância dedicados exclusivamente à segurança das redes e sistemas. Foram também estes atos legislativos que impuseram obrigações de reporte de incidentes relevantes ao Centro Nacional de Cibersegurança. Depois, com a publicação do Decreto-Lei n.º 65/2021, de 30 de julho, que veio regulamentar o RJSC, foram impostas obrigações como a designação de um ponto de contacto permanente, um responsável de segurança, a elaboração e manutenção de um inventário de ativos, a elaboração e implementação de um plano de segurança, a elaboração de um relatório anual que inclua as principais atividades desenvolvidas em matéria de cibersegurança e estatísticas análises agregadas dos incidentes relevantes ocorridos, bem como a realização de uma análise de risco anual[160].

Lei n.º 16/2022, de 16 de agosto: Face às diversas alterações que foram sendo introduzidas à primeira Lei das Comunicações Eletrónicas, foi criada em 2022 uma nova Lei das Comunicações Eletrónicas, alinhada com a evolução tecnológica ocorrida desde 2004 e com as exigências legais europeias, revogando a Lei n.º 5/2004. Ao nível da cibersegurança, foram introduzidos novos requisitos, tais como o dever de cooperar com a Autoridade Reguladora Nacional (a ANACOM) no âmbito da segurança do ciberespaço; a utilização de cifragem, quando adequada, para maior proteção das redes e dos serviços, bem como para minimização dos impactos dos incidentes de segurança[161]. A nova lei refere também que, ao adotar medidas técnicas e organizacionais de segurança, devem ser tidos em conta diversos aspetos, como a segurança física e ambiental, a capacidade de deteção e os procedimentos de gestão de incidentes de segurança, a continuidade operacional e de prestação do serviço, bem como auditorias testes exercícios aos planos de contingência, à segurança das redes e à capacidade de prestação de serviços[162]. Ao nível dos incidentes de segurança, esta lei reproduz a necessidade já inscrita no RJSC (Lei n.º 46/2018, de 13 de agosto) de notificar o Centro Nacional de Cibersegurança de qualquer incidente de segurança com impacto significativo no funcionamento das redes ou serviços, mas acrescentando também a necessidade de o comunicar à ANACOM[163].

[158] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, *Jornal Oficial da União Europeia*, 14 e 29, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148.

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

[160] Decreto-Lei n.º 65/2021, de 30 de julho, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.

[161] Lei n.º 16/2022, de 16 de agosto, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298.

[162] Lei n.º 16/2022.

[163] Lei n.º 16/2022.

Diretiva (UE) 2022/2555[164] (NIS 2): Seis anos depois da publicação da Diretiva NIS, as instituições europeias publicaram uma nova Diretiva que veio atualizar a anterior. A Diretiva NIS 2 classifica dois tipos de setores: "setores de importância crítica"[165] e "outros setores críticos"[166]. Os setores já visados pela Diretiva NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

O setor das infraestruturas digitais é um dos setores que passa por uma maior transformação. Enquanto na Diretiva NIS 1 o setor era composto por apenas três tipos de entidades (IXPs, prestadores de serviços de DNS, e registos de domínios de topo), na Diretiva NIS 2 o setor passa abranger seis novos tipos de entidades. São eles: prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados (*data centres*), fornecedores de redes de distribuição de conteúdos, prestadores de serviços de confiança, fornecedores de redes públicas de comunicações eletrónicas e prestadores de serviços de comunicações eletrónicas acessíveis ao público[167].

Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos[168]. 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[169].

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como "ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques"[170].

[164] 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

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

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

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

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

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

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

1.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor de Infraestruturas Digitais, segundo o relatório "*Mapping of OES Security Requirements to Specific sectors*" da ENISA.

Tabela 8 - Standards e Boas Práticas

Standards	Boas práticas
• ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 • NIST Cybersecurity Framework • TIA-942 • ISO/IEC 20000 • ISO/IEC 17788	• Technical guidance on the security measures for Telcos in Article 13a, ENISA • Best Practices – IX-F • ITIL - Information Technology Infrastructure Library

De seguida, apresenta-se um breve sumário de cada um dos *standards* e boas práticas:

- ***ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002***: Estabelece um quadro de políticas e processos para gerir a segurança da informação de forma sistemática para organizações de telecomunicações, garantindo assim a confidencialidade e a integridade de informações sensíveis[171];
- ***NIST Cybersecurity Framework***: Utilizado para ajudar as organizações a entender e gerir os riscos de cibersegurança. Está organizado em cinco funções principais: Identificar, Proteger, Detetar, Responder e Recuperar[172];
- ***TIA-942***: Estabelece requisitos para a infraestrutura de centro de dados, incluindo para a arquitetura, energia e segurança[173];
- ***ISO/IEC 20000***: Norma para a gestão de serviços de TI, baseada em *ITIL*[174];
- ***ISO/IEC 17788***: Define os conceitos e terminologia a utilizar nos serviços de *cloud*[175];

[171] ISO, "Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002", 2008, https://www.iso.org/standard/43751.html.
[172] NIST. "NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral", fevereiro de 2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf.
[173] Telecommunications Industry Association, "ANSI/TIA-942 Standard", https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/.
[174] ISO, "Part 1: Service management system requirements", 2018, https://www.iso.org/standard/70636.html.
[175] ISO, "Information technology — Cloud computing — Overview and vocabulary", 2014, https://www.iso.org/standard/60544.html.

- ***Technical guidance on the security measures for Telcos in Article 13a, ENISA***: O artigo 13 da ENISA detalha os requisitos de proteção contra ameaças de cibersegurança. Fornece também diretrizes específicas para garantir a resiliência e segurança dos serviços de telecomunicações[176];
- ***Best Practices – IX-F***: Fornece diretrizes para uma operação eficiente e com segurança de *IXPs* (*Internet Exchange Points*). É abordado, também, a gestão de tráfego, segurança e infraestrutura[177];
- ***ITIL - Information Technology Infrastructure Library***: Conjunto de práticas para a gestão de serviços de TI[178].

[176] ENISA, "Technical Guideline on Security Measures", https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures.
[177] Euro-IX, "IX-F – Best Practices", agosto de 2015, https://www.af-ix.net/sites/default/files/08%20-%20Bijal%20Sanghani%20-%20IX-F%20Best%20Practices.pdf.
[178] CIO, "What is ITIL? Your guide to the IT Infrastructure Library", 16 de maio de 2022, https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html.

1.7. Desafios

No contexto da área de Infraestruturas e Conectividade analisado no documento "Avaliação do Potencial Económico da Transição Digital em Portugal" de 2023, encontram-se identificados alguns desafios e obstáculos resultado de exercícios de auscultação aos principais *stakeholders* (entre empresas e entidades institucionais/ públicas) no âmbito da transição digital. Cerca de 3% destes *stakeholders* (13% PME) dizem haver uma inadequada/reduzida infraestrutura digital em Portugal. As limitações levantadas são as seguintes[179]:

- desequilíbrio da presença de infraestruturas de suporte digital (3G, 4G e 5G) no território nacional (urbano vs rural), que provoca uma escassa presença de infraestruturas que suportem a Transição Digital no setor agrícola na totalidade do território, revelando-se fundamental a comparticipação das câmaras municipais na mitigação desta situação;
- a escassez de redes de suporte desenvolvidas a nível nacional;
- falta de disponibilidade e qualidade da infraestrutura digital disponível, limitando a rentabilidade de certas zonas do país por escassez de infraestruturas;
- a escassez de infraestruturas de conectividade e computação a preços competitivos;
- elevado valor dos equipamentos/manutenção para as empresas mais pequenas, resultando em *outsourcing;*
- equipamentos obsoletos que não suportam a Transição Digital;
- dificuldades de licenciamento para *setup* e expansão da atividade.

De acordo com o artigo "O desafio digital" elaborado em junho de 2022, existem vários desafios neste setor, nomeadamente o aumento das desigualdades sociais e tensões sociais se não forem tomadas medidas adequadas na educação e formação, pois existe uma divisão crescente entre as pessoas que têm acesso às competências digitais e os que não têm e, esta desigualdade pode resultar em disparidades de bem-estar e possíveis exclusões no mercado de trabalho. A criação de nova tecnologia também traz alguns dilemas éticos com a crescente facilidade de vigilância personalizada e maciça, assim como o uso de dados pessoais sem autorização dos proprietários dos mesmos[180].

Este setor tem como principais tecnologias, para a conectividade, a fibra ótica e a rede 5G. Estas tecnologias oferecem diversas vantagens, já referidas anteriormente, mas encerram também algumas desvantagens, passíveis de colocar desafios ao setor, sobretudo a nível de custos. A fibra ótica tem um grande custo de instalação, e as interfaces e os conectores apresentam também custos elevados. O processo de reparar e manter os sistemas de fibra é, também este, elevado[181]. Relativamente à tecnologia 5G, o grande desafio estará sempre na sua infraestrutura e no custo da mesma. Esta tecnologia requer a instalação de mais torres e antenas do que a tecnologia 4G, o que irá aumentar exponencialmente os seus custos, tanto de instalação como de manutenção e reparação[182].

---

[179] "Avaliação do Potencial Económico da Transição Digital em Portugal", Deloitte Business Consulting S.A e Universidade de Coimbra, 2023.

[180] Pedro Duarte, "O DESAFIO DIGITAL", *Janus*, junho de 2022, https://repositorio.ual.pt/server/api/core/bitstreams/350ce9d5-f3e3-45e2-aa85-8c76378eb077/content.

[181] Kareem et al., "A Survey of Optical Fiber Communications: Challenges and Processing Time Influences", abril de 2021, 51,https://www.researchgate.net/profile/Subhi-Zeebaree/publication/351005349_A_Survey_of_Optical_Fiber_Communications_Challenges_and_Processing_Time_Influences/links/607ed8d48ea909241e10b11a/A-Survey-of-Optical-Fiber-Communications-Challenges-and-Processing-Time-Influences.pdf.

[182] Ahmed A. Thabit, Bassam H. Abd e Ahmed Alkhayyat, "Challenges and Solutions of 5G Technology", 2021, 55, https://ieeexplore.ieee.org/abstract/document/9717458.

Outro futuro desafio neste setor será a implementação da criptografia quântica. A criptografia quântica é mais complexa de implementar, uma vez que é baseada em algoritmos matemáticos altamente complexos. O maior desafio será implementar esta criptografia em certos dispositivos como por exemplo os de *IoT*. Estes dispositivos têm recursos muito limitados para correr algoritmos complexos o que torna a implementação difícil e pouco prática[183].

Por fim, o setor enfrenta um desafio crescente no âmbito do processamento de dados. Todos os dias existem novos dispositivo ligados à Internet, gerando assim um aumento da circulação de novos dados. Tal implica um aumento nos custos de armazenamento, bem como um grande aumento no esforço de gestão dos dados guardados e espaço de armazenamento disponível.

[183] David Ott et al., "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility", setembro de 2019, 7, https://arxiv.org/pdf/1909.07353.

1.8. Recomendações

Segundo o documento de "Avaliação do Potencial Económico de Transição Digital em Portugal", e fruto dos exercícios de auscultação aos *stakeholders* identificados no âmbito da transição digital, foram levantadas várias recomendações a aplicar a esta área no futuro, como consequência da necessidade em assegurar uma adequada Infraestrutura Digital[184]:

- Fomento de lógicas de *public computing;*
- Dinamização e apoio às infraestruturas tecnológicas (e.g.: 5G), nomeadamente, para a criação de *test beds;*
- Desenvolvimento de *clusters* de computação de fácil acesso;
- Reforço da conectividade;
- Desenvolvimento/ implementação de infraestruturas de conectividade e computação avançada, com modelos de disponibilização, preferencialmente abertas ou a preços competitivos;
- Implementação de incentivos à renovação da infraestrutura existente.
- No mesmo documento, são levantadas 3 grandes áreas de oportunidade de trabalho para o futuro do digital[185]:
- **Acesso a Internet de Alta Velocidade e Desempenho** através da promoção do desenvolvimento da cobertura e utilização de internet fixa e móvel de alta velocidade e desempenho, com foco na cobertura da rede de internet fixa de alta velocidade e aumento dos níveis de utilização deste tipo de serviço e na maximização da cobertura da rede 5G e participação ativa no desenvolvimento da rede 6G. As iniciativas levantadas e responsáveis por promover a melhoria desta área são as seguintes:
    - **Criação de incentivos e/ou mecanismos regulatórios e contratuais** que garantam a cobertura da rede de internet fixa de alta velocidade nos pontos onde não exista;
    - Desenvolvimento de mecanismos de suporte e estímulo à adoção de serviços de internet fixa de alta velocidade;
    - Normalização dos preços das comunicações tendo em consideração as práticas da UE, nomeadamente nos pacotes mais usados pelas empresas;
    - Investimento na cobertura total do território com rede de internet móvel 5G;
    - Diagnóstico e reflexão às melhores práticas e áreas de melhoria na implementação do 5G, como forma de participar no desenvolvimento ativo e apostar na posterior rápida instalação do 6G;
    - Desenho de regulamentação e legislação que favoreça e facilite a adoção e o desenvolvimento da tecnologia 6G;
    - Promoção da alocação e participação de especialistas em fóruns internacionais relativamente à rede 6G.
- Aposta na instalação de ***Data Centres***;
- **Cooperação Internacional** para o Desenvolvimento das Infraestruturas Digitais: Dinamização da participação de Portugal nos instrumentos/ planos da UE, para promoção do desenvolvimento de ações em conjunto e criação de parcerias.

[184] Portugal Digital, "Plano de Ação para a Transição Digital de Portugal", 95.
[185] Portugal Digital, "Plano de Ação para a Transição Digital de Portugal", 95.

De acordo com o relatório “Riscos & Conflitos” de 2021, publicado pelo CNCS, existem vários cenários de risco neste setor. Tais cenários são indicados na seguinte tabela:

Tabela 9 - Cenários de risco

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (*SQL Injection* ou *Cross-site Scripting*).
FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade,** sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

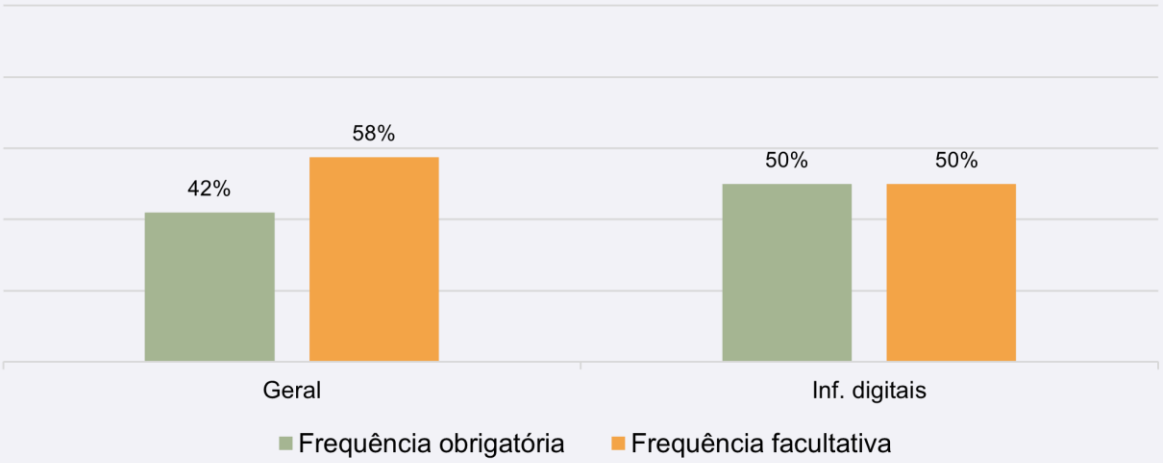
(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 23 de setembro de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf)

Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor, de seguida sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

Os resultados do questionário evidenciam que os OSEs do setor se encontram divididos em partes iguais, onde 50% das formações em cibersegurança são de caráter facultativo e a restante percentagem não é, ressalvando que menos de metade do setor oferece formação. Relativamente ao contexto geral, este setor tem uma percentagem superior de frequência obrigatória com 42% no contexto geral contra 50% neste setor (**Gráfico 39**). Salientando que na maioria das entidades os momentos de formação têm frequência anual, o que, no contexto em questão, poderá ser insuficiente para assegurar a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores. Verifica-se ainda que a existência de cursos de atualização é escassa no setor. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória.

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



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor das infraestruturas digitais, comparativamente com o geral, está abaixo em quase todas as medidas de proteção, com excepção das seguintes: *Firewall*/*WAF*/*Webfilter*, controlos de acesso à rede, manutenção de *logs* para análise após incidentes de segurança e análises de risco periódicas. Das medidas de proteção abaixo da média destacam-se as medidas de *awareness* sobre segurança, encriptação, autenticação multifator, equipa especialista em cibersegurança e *backups* de dados em diferentes localizações onde existe uma diferença entre 10 a 12%. Recomenda-se que estas medidas sejam aplicadas para se manterem com a média geral dos setores (**Gráfico 66.7**).

Gráfico 66.7 - Medidas de proteção contra ameaças de cibersegurança

É recomendado aos OSEs do setor das infraestruturas digitais que:

- Realizem **avaliações de segurança** regularmente, conduzindo, no mínimo, uma avaliação anual, que inclua testes de penetração e auditorias de segurança para identificar e corrigir vulnerabilidades;
- Implementem **programas de sensibilização** em cibersegurança com a realização de sessões de formação semestrais obrigatórias para todos os colaboradores, com foco em boas práticas de cibersegurança, identificação de ameaças e resposta a incidentes;
- Adotem **métodos de cifragem**, utilizando a cifragem para proteger dados sensíveis tanto em trânsito quanto armazenados, assegurando que mesmo em caso de acesso não autorizado, os dados não possam ser lidos ou utilizados indevidamente;
- Implementem **autenticação multifator** (MFA) para todos os sistemas críticos, garantindo uma camada adicional de segurança;
- Realizar uma **monitorização da conformidade legal**, assegurando que a organização está em conformidade com todas as leis e regulamentos aplicáveis em matéria de cibersegurança, realizando auditorias regulares para verificar e manter essa conformidade;
- Façam uma **revisão e atualização de políticas de cibersegurança** de forma periódica (no mínimo, anualmente) para mantê-las alinhadas com a evolução das ameaças e as mudanças organizacionais.

Políticas, procedimentos e planos de cibersegurança

De acordo com os dados obtidos no questionário, mais de dois terços dos OSEs do setor tinham documentado e implementado políticas e procedimentos de cibersegurança, uma percentagem superior à média dos setores. Além disso, apenas 46% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança, o que coloca este setor 4% abaixo da média geral dos outros setores (**Gráficos 77 e 78**).

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

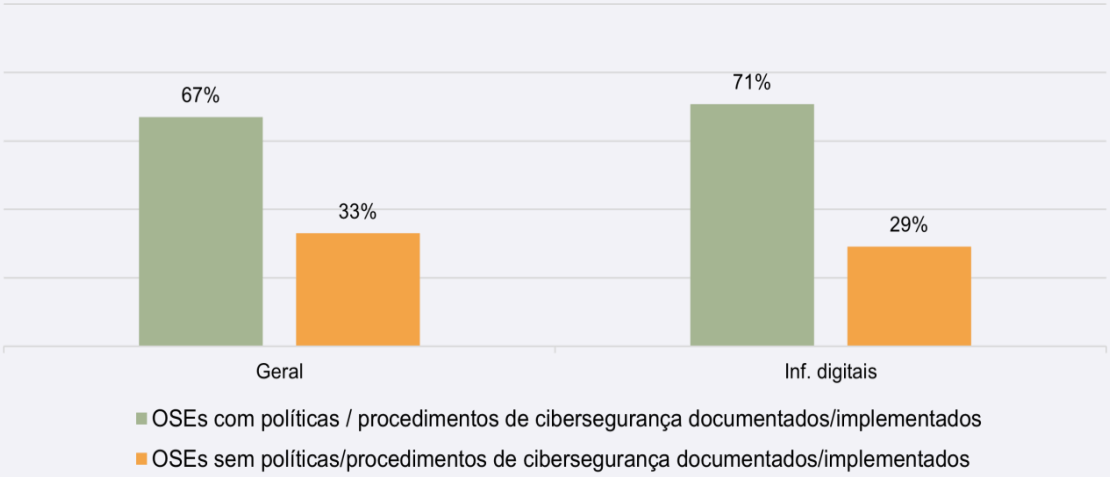
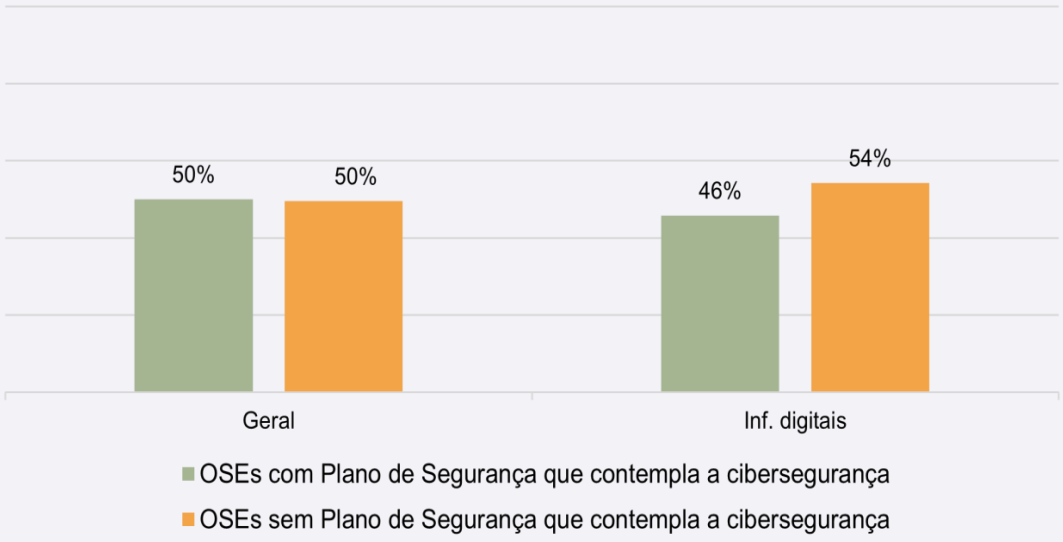


Gráfico 78 - Existência de Plano de Segurança que contemple a cibersegurança



Face a esta realidade, recomenda-se aos OSEs do setor que ainda não o tenham feito que elaborem e implementem uma política de cibersegurança que verse sobre:

- **Papéis e responsabilidades**: definindo claramente os papéis e responsabilidades dos colaboradores em matéria de cibersegurança, assegurando que todos entendem as suas funções e o impacto das suas ações na segurança geral;
- **Gestão de riscos**: implementando processos para a identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança, incluindo a realização de análises de risco periódicas;
- **Controlos de segurança**: através do estabelecimento de controlos de segurança rigorosos, como controlos de acesso lógicos e físicos, para proteger infraestruturas críticas e dados sensíveis;
- **Gestão de Incidentes**: com o desenvolvimento de um plano de resposta a incidentes, que inclua procedimentos para a deteção, identificação, resposta e recuperação de incidentes de cibersegurança. Também deve ser estabelecido um plano de comunicação de incidentes para notificar as partes interessadas;
- **Conformidade Legal**: garantindo que a organização cumpre todas as leis e regulamentos aplicáveis em matéria de cibersegurança, realizando auditorias regulares para verificar a conformidade;
- **Revisão e atualização da política de cibersegurança**: periodicamente (no mínimo, anualmente), para mantê-la alinhada com a evolução das ameaças de cibersegurança e as mudanças na organização;
- **Continuidade de Negócio**: através de uma política de continuidade de negócio que esteja alinhada com a política de cibersegurança, incluindo planos detalhados para assegurar a continuidade das operações em caso de incidentes significativos.

Estas medidas ajudarão a fortalecer a resiliência das infraestruturas digitais contra ciberataques, garantindo a continuidade e a integridade dos serviços essenciais prestados.

Face à baixa percentagem de OSEs do setor que indicaram possuir uma política de continuidade de negócio (27%), recomenda-se também a elaboração de uma política de continuidade de negócio alinhada com a política de cibersegurança. Deve incluir-se também a elaboração de uma política de comunicação, visto que se encontra abaixo dos 50%, tal como verificado na política de continuidade de negócio. Comparativamente com a média geral dos setores, apenas a política de gestão de risco se encontra acima da média. Recomenda-se a elaboração da política de gestão de acessos devido a encontrar-se com uma percentagem muito inferior em relação à média geral, assim como as políticas de comunicação e *backups* (**Gráfico 79 e gráfico 79.7**).

Gráfico 79 - Políticas incluídas no Plano de Segurança

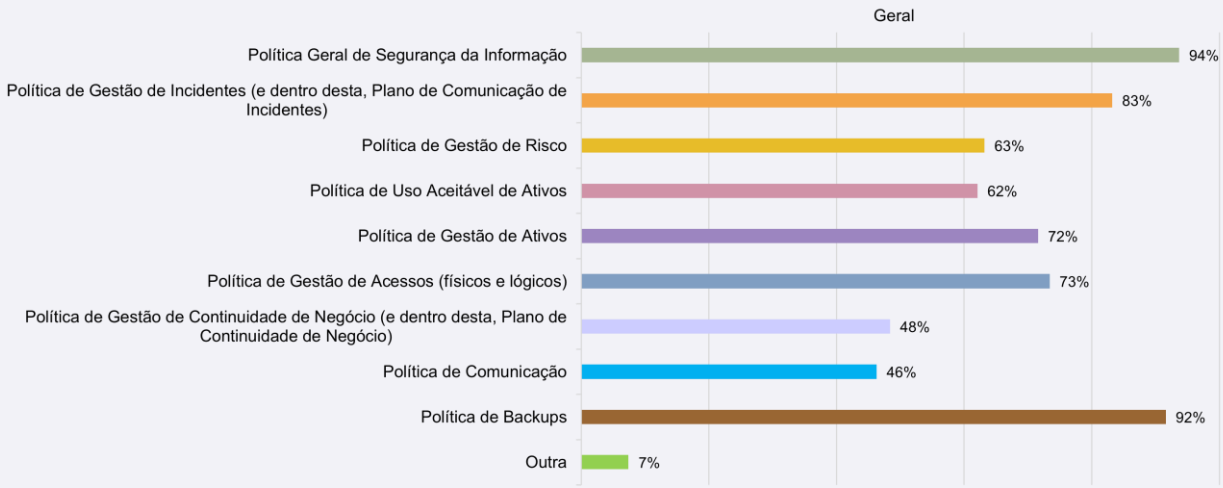
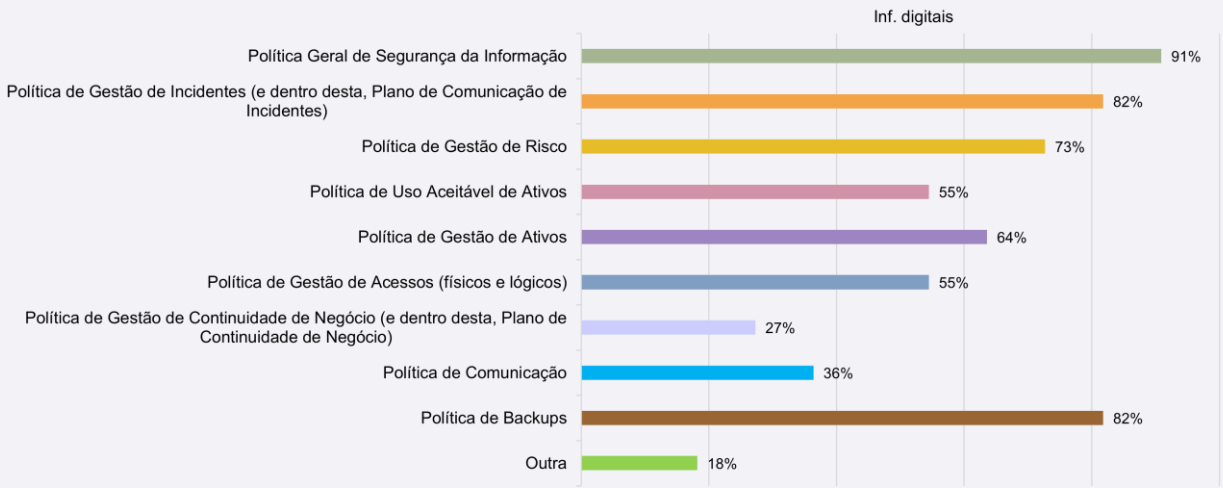


Gráfico 79.7 - Políticas incluídas no Plano de Segurança



Embora não exista obrigação legal no setor das infraestruturas digitais de realizar testes de intrusão (*pentesting*), é importante enfatizar que este setor também é alvo frequente de ciberataques, particularmente ataques de negação de serviço (DDoS), ataques de *ransomware* e violações de dados e, devido a isto, recomenda-se a realização de testes de intrusão.

Por fim, o CIS (*Center for Internet Security*) elaborou uma lista denominada *CIS Controls* e, nesta lista, constam todas as ações que o CIS considera fundamentais para manter a segurança de uma organização. Estes controlos estão divididos em três categorias:

- **Controlos básicos**: controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais**: controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais**: controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*[186].

No setor das infraestruturas digitais, os controlos fundacionais, relacionados com a segurança de rede, são particularmente críticos. Infraestruturas digitais, como *data centers*, serviços *cloud*, e redes de comunicação, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, a disponibilidade e a continuidade dos seus serviços. Qualquer falha ou configuração inadequada pode ser explorada para interromper serviços digitais essenciais, comprometer a segurança dos dados, desviar tráfego, ou provocar quedas na rede, afetando significativamente a atividade das organizações que dependem dessas infraestruturas.

[186] "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, https://www.cisecurity.org/controls/cis-controls-list.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos[187]:

Tabela 10 - Controlos de Segurança da CIS (Inf. Digitais)

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: "The 18 CIS Critical Security Controls", CIS Critical Security Controls, Center for Internet Security, https://www.cisecurity.org/controls/cis-controls-list.)

[187] "The 18 CIS Critical Security Controls".

Notas metodológicas

O presente relatório teve como propósito fazer uma extensa análise dos vários setores de operadores de serviços essenciais no âmbito do RJSC.

Com este propósito, foram realizados os questionários cujos resultados se apresentam no relatório, bem como uma aprofundada pesquisa sobre o contexto setorial, impacto socioeconómico, ameaças, capacitação e investimento em cibersegurança, legislação relevante, *standards* e boas práticas e desafios para cada setor em análise, procurando ter por base as mais confiáveis fontes académicas e científicas.

A análise das informações recolhidas e consequente produção e elaboração do relatório foram realizadas pela PwC, entidade parceira do CNCS na elaboração do presente documento.

Bibliografia

- .PT, “Relatório de Atividades e Contas 2022”. https://www.pt.pt/fotos/editor2/relatorios/relatorio_atividades_contas_2022.pdf.
- .PT. “História”. https://www.pt.pt/pt/historia/.
- .PT. “Quem somos”. https://www.pt.pt/pt/pt/quem-somos/.
- Abecasis, Miguel, Pedro Pereira, Dominic Field e Eduardo Bicacro. “O impacto do digital na economia portuguesa”, dezembro de 2018. https://web-assets.bcg.com/img-src/O-impacto-do-Digital-na-economia-portuguesa_tcm9-214461.pdf.
- Ahmed A. Thabit, Bassam H. Abd e Ahmed Alkhayyat. “Challenges and Solutions of 5G Technology”. 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 2021, pp. 54-59. https://ieeexplore.ieee.org/abstract/document/9717458.
- 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.
- ANACOM. “Interligação e Serviço Universal”, 23 de fevereiro de 2006. https://www.anacom.pt/render.jsp?categoryId=183071&languageId=0
- Anacom. “Telecomunicações e acesso à Internet de qualidade finalmente uma realidade em todo o País”, 6 de dezembro de 2023. https://www.anacom.pt/render.jsp?contentId=1769445.
- Baker, Paddy. “Coincheck Customers Fall Victim to Data Breach After Domain Account Error”. Coincheck, 3 de junho de 2020. https://www.coindesk.com/markets/2020/06/03/coincheck-customers-fall-victim-to-data-breach-after-domain-account-error/.
- Center for Internet Security. “The 18 CIS Critical Security Controls”, CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list.
- CIO. “What is ITIL? Your guide to the IT Infrastructure Library”. 16 de maio de 2022, https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html.
- 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. “Incidentes e Setores: 2019-2023”. Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024. https://www.cncs.gov.pt/pt/estatistica/.

- CNCS. "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança. https://www.cncs.gov.pt/pt/observatorio/#relatorios.
- CNCS. "Tecnologias Emergentes", maio de 2023. https://www.cncs.gov.pt/docs/rel-tecemer2023-observ-cncs.pdf.
- Comissão Europeia, "Broadband Coverage in Europe 2021", agosto de 2022. https://ec.europa.eu/newsroom/dae/redirection/document/88314.
- Comissão Europeia. "€1.3 billion from the Digital Europe Programme for Europe's digital transition and cybersecurity". https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity.
- Comissão Europeia. "Aliança Europeia para os Dados Industriais, a Edge e a Nuvem". *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/pt/policies/cloud-alliance.
- Comissão Europeia. "Aliança sobre processadores e tecnologias de semicondutores". *Shaping Europe's digital future.* https://digital-strategy.ec.europa.eu/pt/policies/alliance-processors-and-semiconductor-technologies .
- Comissão Europeia. "Década Digital da Europa: metas digitais para 2030". https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt.
- Comissão Europeia. "Programa Europa Digital", *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/pt/activities/digital-programme.
- Comissão Europeia. "Quantum Technologies Flagship", Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.
- Conselho Europeu, "Horizonte Europa". https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- *DatacenterDynamics*, "A economia dos Data Centers em Portugal: o que esperar para os próximos anos?", 26 de abril de 2023. https://www.datacenterdynamics.com/br/an%C3%A1lises/a-economia-dos-data-centers-em-portugal-o-que-esperar-para-os-proximos-anos-/.
- Decreto-Lei n.º 65/2021, de 30 de julho. *Diário da República*. https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.
- Deloitte e Universidade de Coimbra. "Avaliação do Potencial Económico da Transição Digital em Portugal", 2023. https://portugaldigital.gov.pt/wp-content/uploads/2023/05/Portugal-Digital_Avaliacao-Transicao-Digital_Documento-Final_v20230330_VF.pdf.
- Department for Science, Innovation & Technology, "Cyber security breaches survey 2023", 19 de abril de 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
- Dias, Manuel. "Estará no plano do próximo Governo colocar Portugal na vanguarda da Europa digital?". *Observador*, 3 de janeiro de 2024. https://observador.pt/opiniao/estara-no-plano-do-proximo-governo-colocar-portugal-na-vanguarda-da-europa-digital/.
- 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) 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 2002/19/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos (diretiva acesso). *Jornal Oficial das Comunidades Europeias*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0019

- Diretiva 2002/20/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa à autorização de redes e serviços de comunicações eletrónicas (diretiva autorização). *Jornal Oficial das Comunidades Europeias*. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:PT:PDF
- Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro). *Jornal Oficial das Comunidades Europeias*. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:pt:PDF.
- Diretiva 2002/22/CE do Parlamento Europeu e do Conselho de 7 de março de 2002 relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas (diretiva serviço universal). *Jornal Oficial das Comunidades Europeias*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0022.
- Duarte, Pedro. "O Desafio Digital". *Janus*, junho de 2022. https://repositorio.ual.pt/server/api/core/bitstreams/350ce9d5-f3e3-45e2-aa85-8c76378eb077/content.
- 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. "DNS Identity Verification and Authentication of Domain Name Owners", maio de 2023. https://www.enisa.europa.eu/publications/dns-identity.
- ENISA. "NIS Investments", 2021. https://www.enisa.europa.eu/publications/nis-investments-2021.
- ENISA. "Technical Guideline on Security Measures". https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures.
- Equinix. "LS1". https://www.equinix.com/data-centers/europe-colocation/portugal-colocation/lisbon-data-centers/ls1.
- Euro-IX. "IX-F – Best Practices", agosto de 2015. https://www.af-ix.net/sites/default/files/08%20-%20Bijal%20Sanghani%20-%20IX-F%20Best%20Practices.pdf.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), "Impact". https://www.ee-isac.eu/impact/#.
- Fátima Caçador. "Registo de domínios .pt com novo recorde em 2022. Foram registados mais de 150 mil", *Sapo TEK*, 4 de janeiro de 2023. https://tek.sapo.pt/noticias/internet/artigos/registo-de-dominios-pt-com-novo-recorde-em-2022-foram-registados-mais-de-150-mil.
- Fonseca, Pedro, Paul McCarthy e Marian-Andrei Rizoiu. *Registentes: Os primeiros domínios .pt.* Loures: Conclusão das Letras, julho de 2021. https://tictank.pt/wp-content/uploads/2021/08/2107-registentes_livro.pdf.
- ForeNova, "Cyber Threat Analysis Done the Right Way". https://www.forenova.com/threat-detection/how-to-conduct-a-cyber-threat-analysis.
- Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", janeiro de 2024.
- GigaPIX. "QUE FAZ O GIGAPIX?". https://gigapix.pt/pt/home/.
- GigaPIX. "Sobre nós". https://gigapix.pt/pt/sobre-nos/.
- Google. "Google Public DNS". https://dns.google/.

- Guerra, Juliana. “Impacto do 5G em Portugal pode chegar aos 3,6 mil milhões de euros”. *Ericsson*, 11 de junho de 2019. https://www.ericsson.com/pt/press-releases/2019/6/ericsson-mobility-report-a-adocao-da-tecnologia-5g-e-ainda-mais-rapida-do-que-esperada.
- Hudaib, Adam e Esra'a Hudaib. “DNS Advanced Attacks and Analysis”, 2014. https://www.academia.edu/download/35520765/DNS_Advanced_Attacks_and_Analysis.pdf.
- IAPMEI. “Transição Digital”, 23 de novembro de 2023. https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Industria-e-Sustentabilidade/Transformacao-digital.aspx.
- IEFP, Cheque-Formação + Digital. https://www.iefp.pt/cheque-formacao-digital.
- 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. “Estatísticas do emprego”, 8 de maio de 2024. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=665513779&att_display=n&att_download=y.
- INE. “Inquérito à utilização de tecnologias da informação e da comunicação nas empresas”, 21 de novembro de 2023. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637881953&att_display=n&att_download=y.
- ISO, “Information technology — Cloud computing — Overview and vocabulary”, 2014, https://www.iso.org/standard/60544.html.
- ISO, “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- ISO. “Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002”, 2008. https://www.iso.org/standard/43751.html.
- ISO. “Part 1: Service management system requirements”, 2018. https://www.iso.org/standard/70636.html.
- Kareem, Fairoz, Subhi Zeebaree, Hivi Dino, Mohammed Sadeeq, Zryan Rashid, Dathar Hasan e Karzan Sharif. “A Survey of Optical Fiber Communications: Challenges and Processing Time Influences”, abril de 2021. https://www.researchgate.net/profile/Subhi-Zeebaree/publication/351005349_A_Survey_of_Optical_Fiber_Communications_Challenges_and_Processing_Time_Influences/links/607ed8d48ea909241e10b11a/A-Survey-of-Optical-Fiber-Communications-Challenges-and-Processing-Time-Influences.pdf.
- Krebson Security. “Webnic Registrar Blamed for Hijack of Lenovo, Google Domains”, 26 de fevereiro de 2015. https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/.
- Lei n.º 16/2022, de 16 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298.
- Lei n.º 41/2004, de 18 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/41-2004-480710.
- Lei n.º 46/2018, de 13 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- Lei n.º 46/2018, de 13 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- Lei n.º 5/2004, de 10 de fevereiro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/5-2004-581061.
- Lei n.º 51/2011, de 13 de setembro, *Procuradoria-Geral Distrital de Lisboa*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=1515&pagina=1&ficha=1#.
- *LIS-IX*. “What is LIS-IX?”. https://lis-ix.pt/#what-is.
- McCarthy, Dave, Lara Greden, Jason Bremner, Brad Casemore, Jennifer Cooke, Stephen Elliot, Al Gillen, Phil Goodwin, Ashish Nadkarni, Adelaide O'Brien, Peter Rutten, Bjoern Stengel, Rick Villars, Natalya Yezhkova, Jevin Jensen, Mary Johnston Turner. “IDC FutureScape: Worldwide

Cloud 2023 Predictions", *IDC*, outubro de 2022. https://www.idc.com/getdoc.jsp?containerId=US48602322.

- Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- NIST. "NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral", fevereiro de 2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf.
- *Nordlayer*, "Which countries score the highest?". Última atualização a 22 de agosto de 2024. https://nordlayer.com/global-remote-work-index/#countries-score-table.
- Open DNS. "About Us". https://www.opendns.com/about/.
- Ott, David, Christopher Peikert, Mark Hill, Ann Drobnis e Chris Ramming. "Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility". *Computing Community Consortium*, setembro de 2019. https://arxiv.org/pdf/1909.07353.
- PORDATA, "Empresas: total e por dimensão", dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- Portugal 2030. "PT - Programa Regional de Lisboa 2021-2027". https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_lisboa.pdf.
- Portugal 2030. "PT - Programa Regional do Alentejo 2021-2027". https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_alentejo.pdf.
- Portugal 2030. "PT - Programa Regional do Algarve 2021-2027". https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_algarve.pdf.
- Portugal 2030. "PT - Programa Regional do Centro 2021-2027". https://www.adcoesao.pt/wp-content/uploads/sfc2021_pr_centro.pdf.
- Portugal Digital. "Plano de Ação para a Transição Digital de Portugal", 5 de março de 2020. https://portugaldigital.gov.pt/wp-content/uploads/2022/01/Plano_Acao_Transicao_Digital.pdf.
- Portugal Digital. "Sobre nós". https://portugaldigital.gov.pt/sobre-nos/.
- PORTUGAL.GOV.PT. "Fibra ótica vai chegar a todo o país até 2027", 12 de dezembro de 2023. https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=esta-aberto-o-concurso-para-levar-a-fibra-otica-a-todo-o-pais.
- PTSoc. Annual Report PTSOC 2023". https://ptsoc.pt.pt/en/relatorio-anual-ptsoc-2023/.
- Public DNS. "DNS servers in Portugal". https://public-dns.info/nameserver/pt.html.
- Recuperar Portugal. "TD-C16-i05 CAPACITAÇÃO E TRANSFORMAÇÃO DIGITAL DAS EMPRESAS DOS AÇORES". https://recuperarportugal.gov.pt/transicao-digital/empresas-4-0/td-c16-i05-capacitacao-e-transformacao-digital-das-empresas-dos-acores/.
- Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta. J*ornal Oficial da União Europeia*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015R2120.
- Silva, Alina, Ana Correia, Carolina Guimarães, Josefina Gomes, José Maria Azevedo, Manuela Oliveira, Paula Araújo da Silva, Paula Lopes, Paulo Santos, Pedro Figueiredo, Raquel Meira, Ricardo Sousa, Ruben Fernandes, Susana Pinto e Vasco Leite. "Estratégia de Desenvolvimento do Norte para Período de Programação 2021-27 das Políticas da União Europeia". PT - Programa Regional do Norte 2021-2027, Portugal 2030. https://www.ccdr-n.pt/storage/app/media/2021/CCDRN%202030-compactado.pdf.
- Sulaiman Asif, "Cyber Threat Analysis: Types, Benefits, Tools, Approaches", *Knowledge Hut*, September 5, 2023. https://www.knowledgehut.com/blog/security/threat-analysis.
- Telecommunications Industry Association. "ANSI/TIA-942 Standard". https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/.
- Três Em Um. "Sobre". https://3em1.pt/.
- World Bank. "Strategic Cybersecurity Talent Framework - White Paper", abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.

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