CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

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

Infraestruturas do Mercado Financeiro

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

O relatório elaborado atenderá aos seguintes pontos na análise setorial:

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

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

Contexto Geral

Tal como já referido, um OSE é "uma entidade pública ou privada que presta um serviço essencial[4] (...) para a manutenção de atividades societais ou económicas cruciais"[5].

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

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

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

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

- A entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais;
- A prestação desse serviço depende de redes e sistemas de informação; e
- Um incidente pode ter efeitos perturbadores importantes na prestação desse serviço[6].

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

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

Tabela 1 - Setores, Subsetores e Tipos de Entidades

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

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

Análise do questionário dirigido aos Reguladores de Serviços Essenciais

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

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

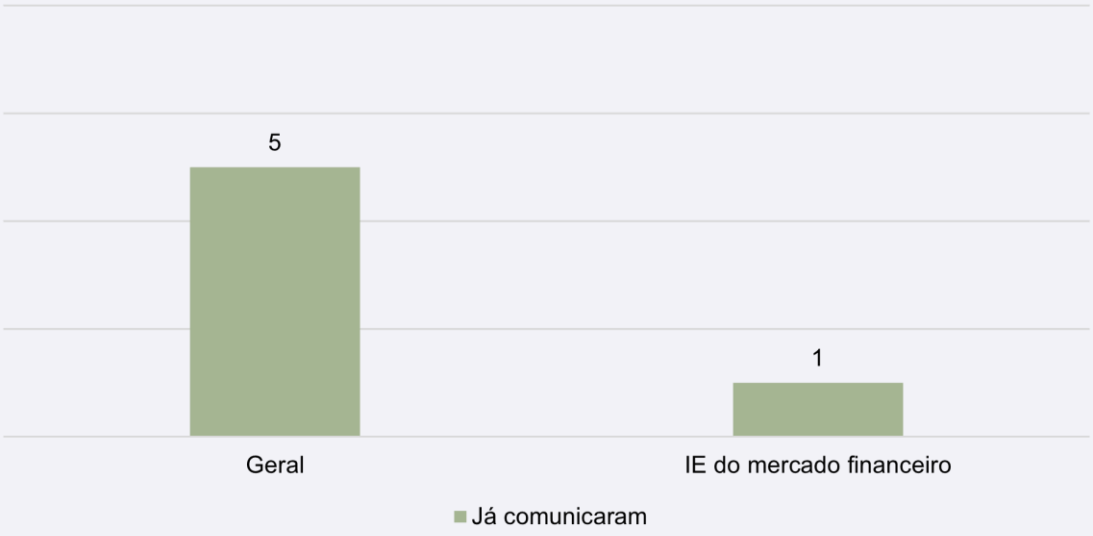
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez,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

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

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

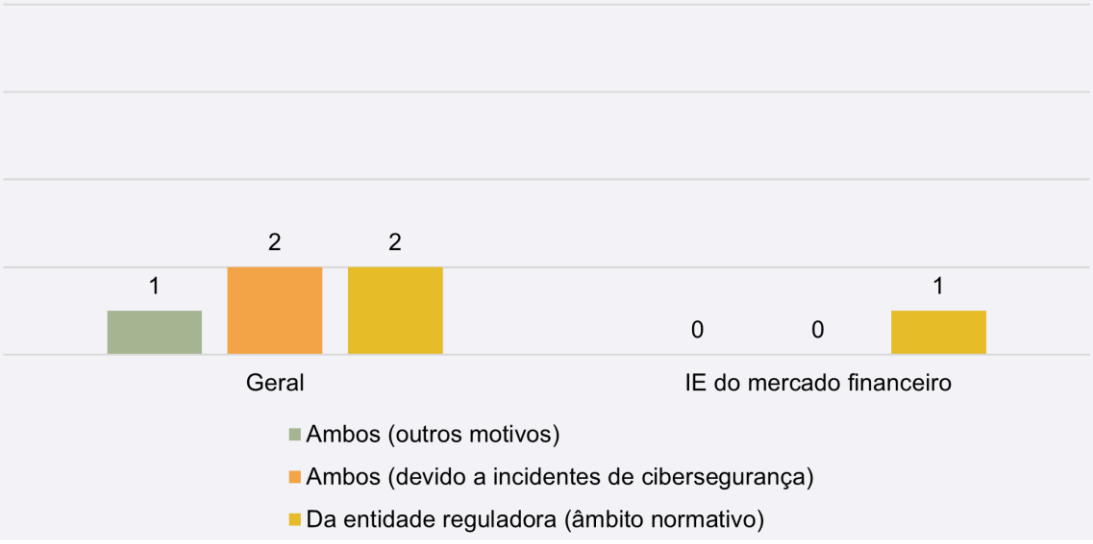
1. Comunicação entre OSE e respetivos Reguladores

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



Entre os oito reguladores que responderam, cinco indicaram já ter comunicado com os OSE sobre questões de cibersegurança. O regulador inquirido do setor das infraestruturas do mercado financeiro indicou ter realizado comunicações sobre estas matérias aos OSE por si regulados.

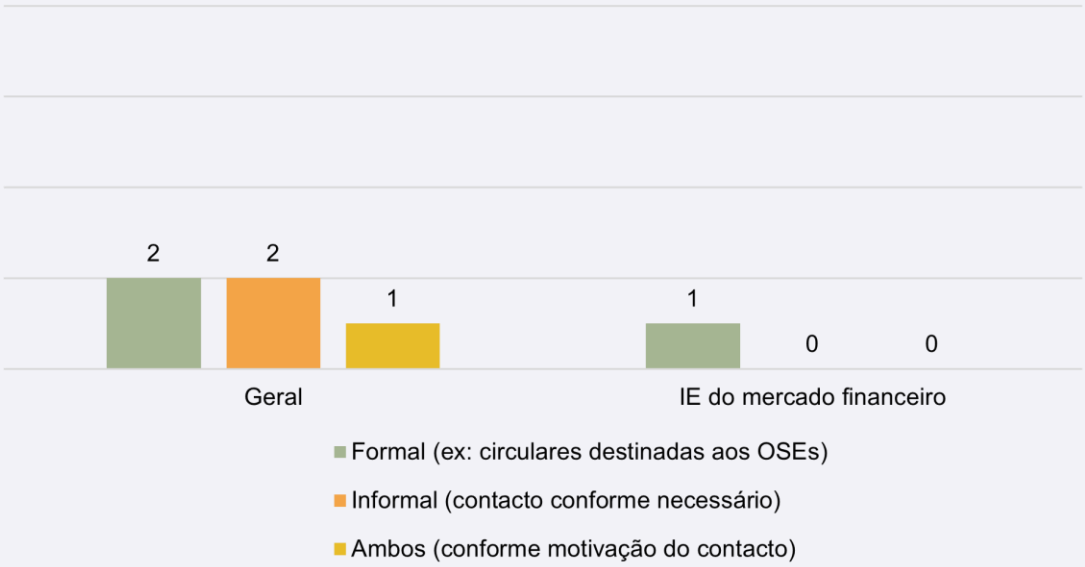
Gráfico 2 - Origem da comunicação sobre questões de cibersegurança



Relativamente à origem da comunicação sobre cibersegurança realizada por cinco dos reguladores, dois indicaram que a comunicação partiu dos próprios, em contexto de informação sobre normas do setor, sendo um deles o setor inquirido das infraestruturas do mercado financeiro. Dois responderam que houve comunicação que se gerou a partir dos dois lados, devido à ocorrência de incidentes de cibersegurança e apenas um (o regulador do setor bancário)

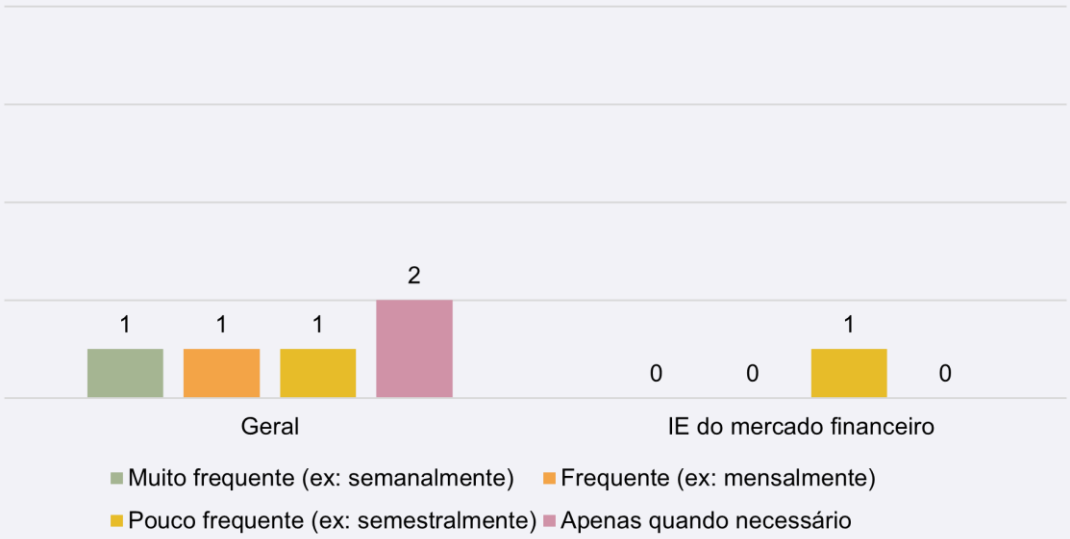
respondeu que houve comunicação sobre cibersegurança a ser realizada com os OSE devido a outros motivos.

Gráfico 3 - Formalidade da comunicação realizada



Entre os mesmos cinco reguladores, dois indicaram que a comunicação é geralmente feita de modo formal, um deles sendo o setor das infraestruturas do mercado financeiro), através de, por exemplo, circulares, outros dois responderam que a comunicação é sobretudo informal, consoante a necessidade e apenas o regulador do setor bancário indicou haver comunicação tanto de caráter formal como mais informal.

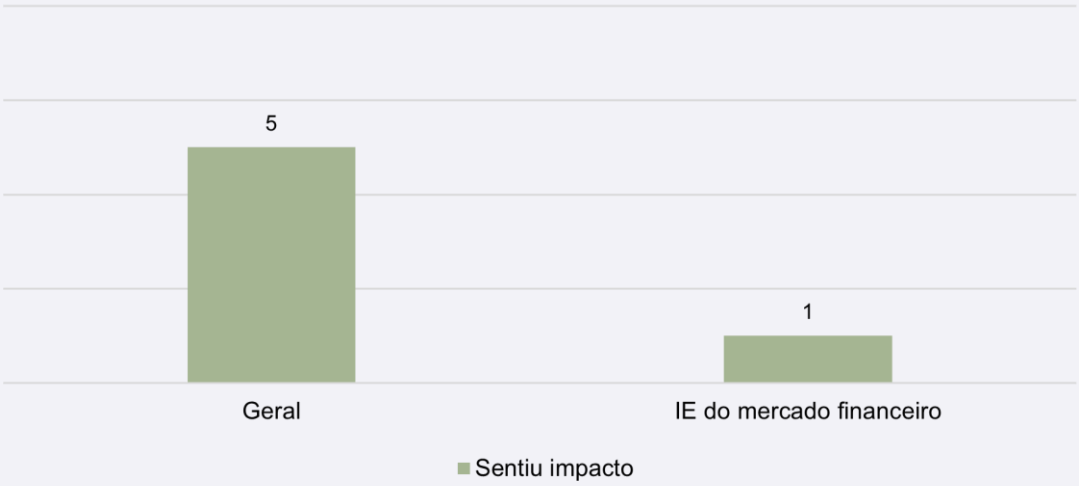
Gráfico 4 - Frequência da comunicação



No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. O regulador das IMF indicou que a frequência de comunicação com os OSE sobre questões de cibersegurança é pouco frequente, ocorrendo, por exemplo, semestralmente.

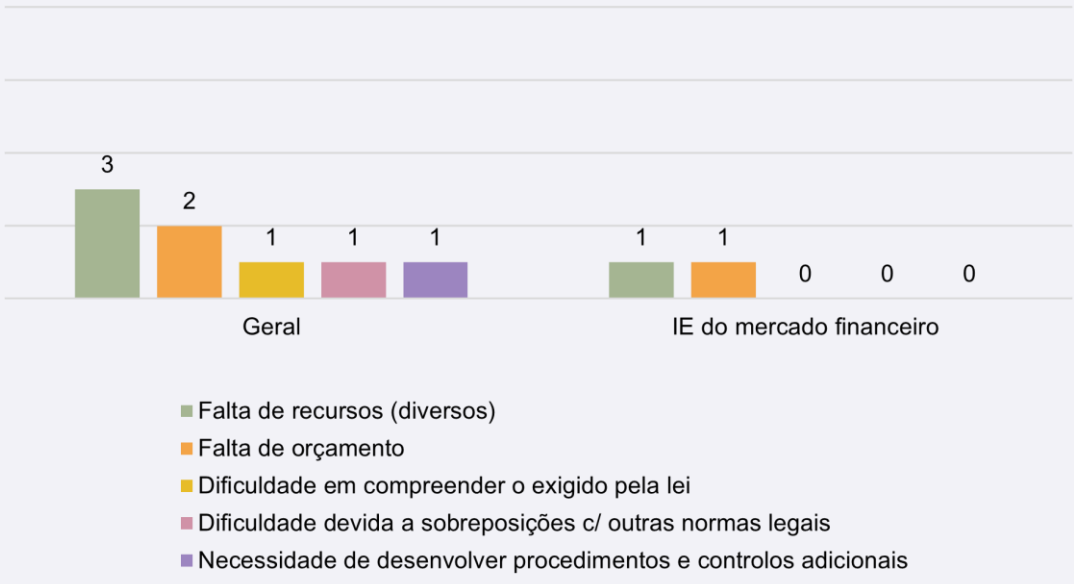
2. Impacto da publicação da Diretiva NIS ou da transposição da mesma (publicação da Lei n. º46/2018)

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



Questionou-se aos reguladores se sentiram impacto nas suas organizações e nos OSE por si regulados pela publicação da Diretiva NIS. Entre os oito reguladores que responderam, cinco indicaram ter sentido esse impacto. Esse impacto ter-se-á feito sentir no setor das infraestruturas do mercado financeiro. Ver-se-á, de seguida, quais foram os impactos sentidos.

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



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

O regulador das IMF indica também a falta de orçamento a conformidade com regime jurídico, como outra das dificuldades sentidas.

De acordo com um inquérito realizado pela ENISA, a implementação da diretiva NIS tem, normalmente, um efeito positivo nos OSE e provedores de serviços digitais. Este inquérito foi feito a 251 organizações (oriundas da França, Alemanha, Itália, Espanha e Polónia) e, destas, cerca de 58% já tinham estabelecido e completado a implementação da diretiva NIS. Cerca de 23% ainda estavam a implementar e 8% tinham planeado implementar a diretiva. Por outro lado, 10% não vão implementar a diretiva, mas vão usar a mesma como guia para o seu programa de segurança e só um referiu que não iria implementar a diretiva, nem seguir a mesma[7].

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

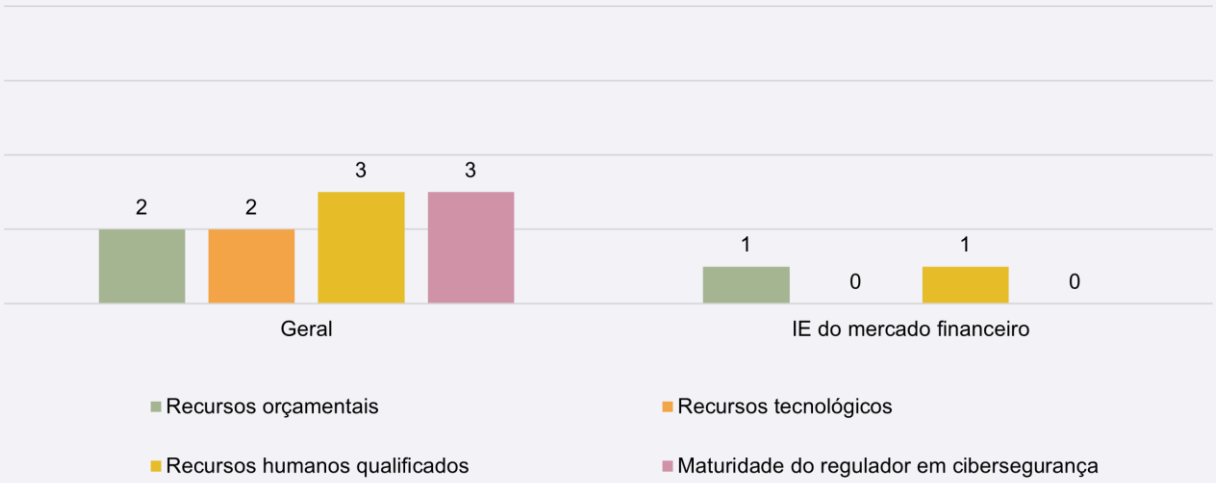
Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSE em matéria de cibersegurança, em caso de atribuição da competência

Foi questionado aos reguladores se teriam capacidade para realizar a supervisão dos operadores em matéria de cibersegurança. O número de respostas dividiu-se igualmente entre os que consideram ter a capacidade para realizar essa supervisão e os que não consideram tê-la (quatro reguladores consideram ter essa capacidade, outros quatro consideram não a ter).

O regulador do setor das infraestruturas do mercado financeiro indica não considerar ter essa capacidade.

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

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.

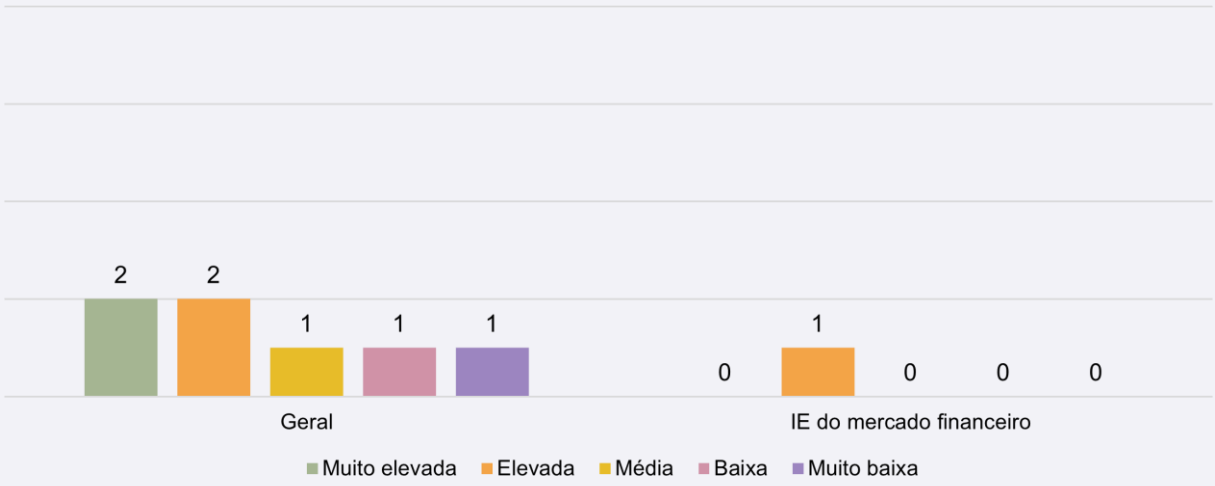
Nas infraestruturas do mercado financeiro, os principais recursos em falta para que essa supervisão possa ser realizada são recursos orçamentais e recursos humanos qualificados, já nas infraestruturas digitais, os principais recursos em falta indicados foram os recursos orçamentais e os recursos humanos qualificados.

A falta de recursos humanos qualificados em cibersegurança é um tema que surge repetidamente nas respostas tanto dos reguladores como dos OSE. Dados do Fórum Económico Mundial evidenciam uma escassez global de cerca 4 milhões de profissionais em cibersegurança[8], escassez essa que coloca diversas dificuldades não só aos reguladores e aos OSE dos setores em análise, mas também noutras organizações e setores de atividade. Este tema é explorado em maior detalhe na análise do **Gráfico 44**.

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

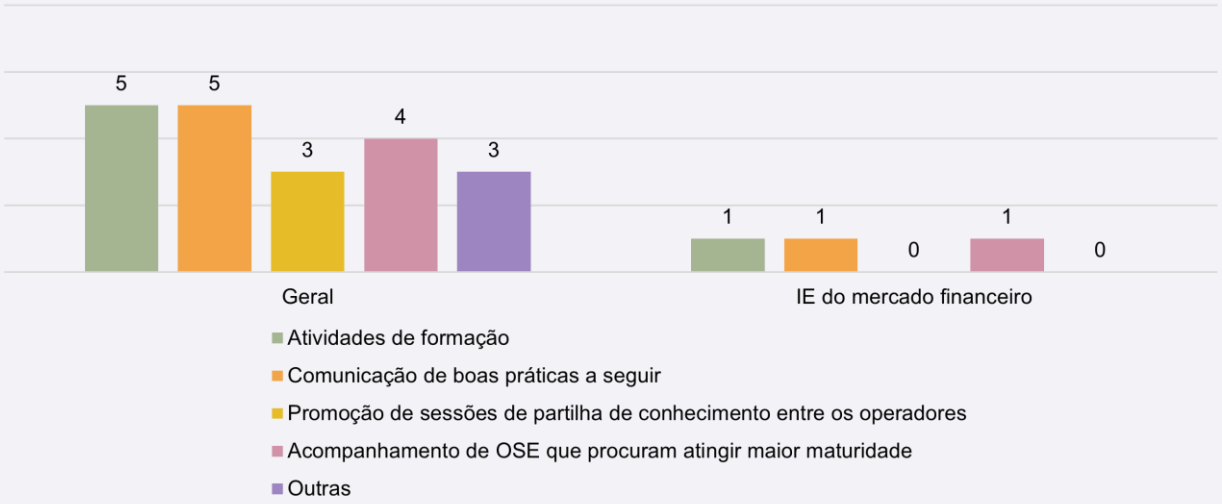
4. Maturidade em cibersegurança no setor

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



A perceção dos reguladores sobre a maturidade em cibersegurança dos operadores varia entre os diversos reguladores dos diferentes setores. Entre os inquiridos, apenas dois dos oito reguladores consideram que a maturidade nos seus setores é elevada. O regulador das infraestruturas do mercado financeiro considera que a maturidade é elevada.

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



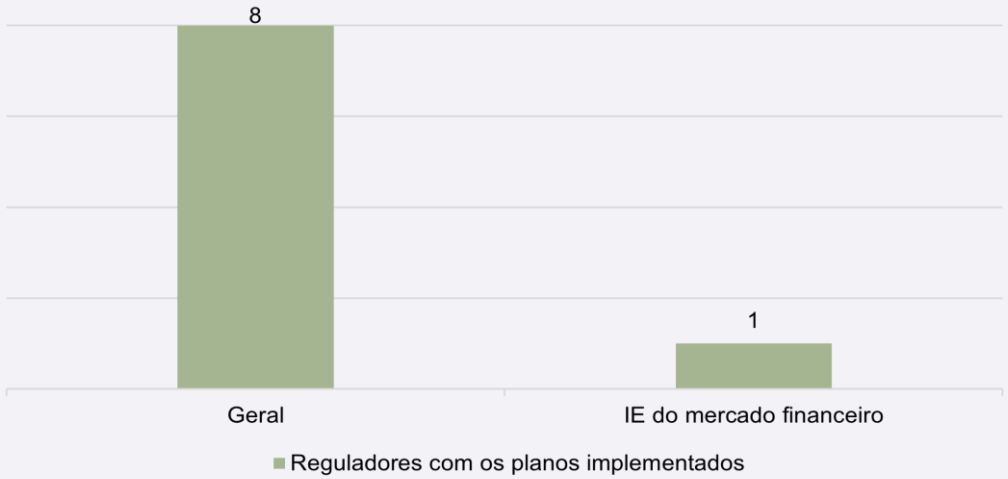
Os reguladores tentam promover a maturidade em cibersegurança nos seus respetivos setores através da adoção de diferentes medidas. Cinco dos reguladores inquiridos promovem atividades de formação num esforço para aumentar a maturidade no setor. Verifica-se o mesmo número de reguladores a recomendar boas práticas a seguir.

O regulador das IMF menciona adotar medidas como as atividades de formação, a comunicação de boas práticas a seguir bem como o acompanhamento de OSE que procuram atingir maior maturidade.

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

Apenas duas das entidades reguladoras inquiridas consideram ter suficientes profissionais capacitados em matéria de cibersegurança, enquanto os restantes seis não consideram ter suficientes profissionais capacitados na área. O regulador do setor das IMF é um dos que considera não ter profissionais suficientes. Novamente, estes resultados prender-se-ão com a escassez global de profissionais em cibersegurança já referida no **Gráfico 8** e que é analisada em detalhe no **Gráfico 44**.

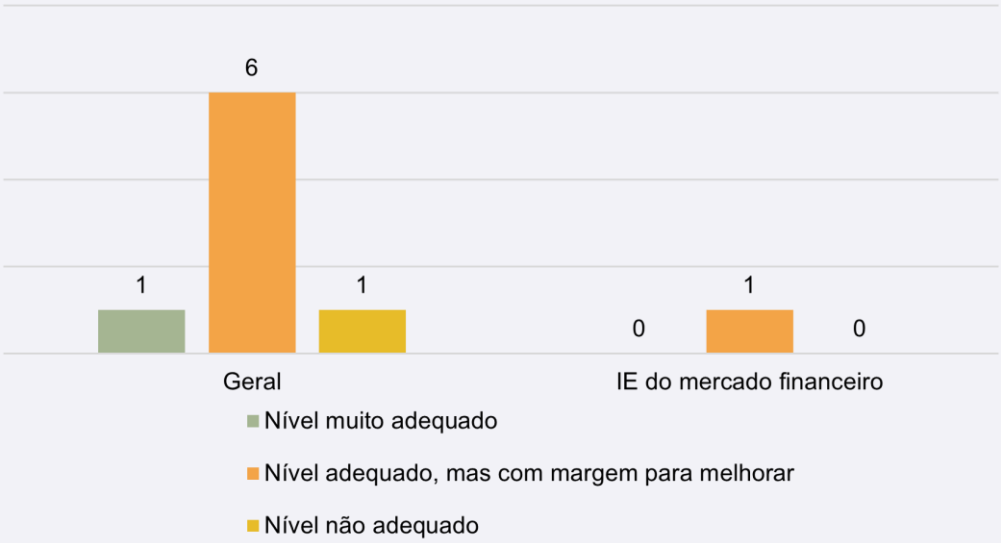
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados



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

5. Nível de segurança estabelecido pela legislação em vigor

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



Na generalidade, a maioria dos reguladores dos OSE, nomeadamente seis, consideram que a Diretiva NIS procura estabelecer um nível adequado de cibersegurança entre os OSE, mas com margem para melhorar face aos atuais desafios, perigos e ameaças nesta matéria, enquadrando o regulador das IMF nestes seis. Apenas um regulador considera que o nível de cibersegurança que a Diretiva NIS procura estabelecer é muito adequado, e outro regulador considera que a Diretiva não leva os operadores a estabelecerem um nível adequado de cibersegurança face aos atuais perigos, desafios e ameaças.

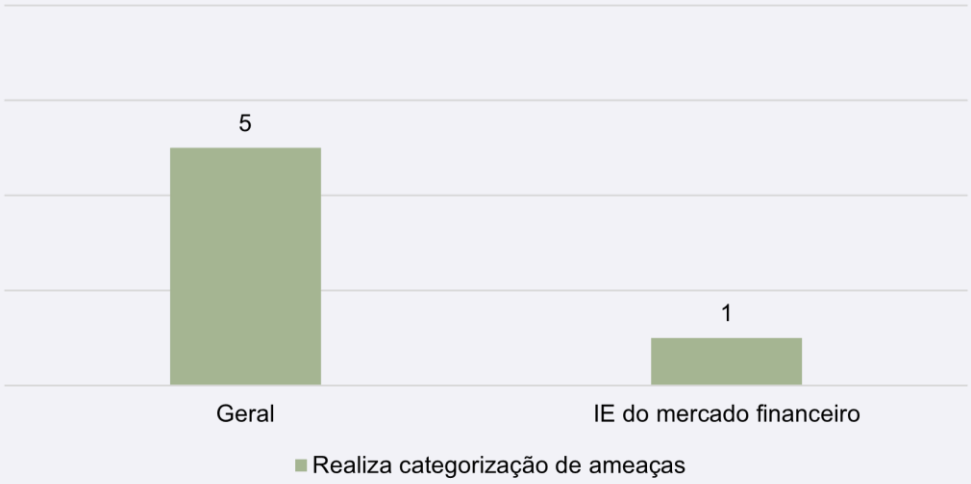
Uma questão semelhante foi colocada, em 2021, não aos reguladores, mas a diversos OSE na União Europeia, no âmbito do relatório *NIS Investments* 2021. As respostas recolhidas indicam que quase 50% (48,9%) dos operadores de serviços essenciais consideram que a Diretiva NIS teve um impacto positivo nas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

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

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

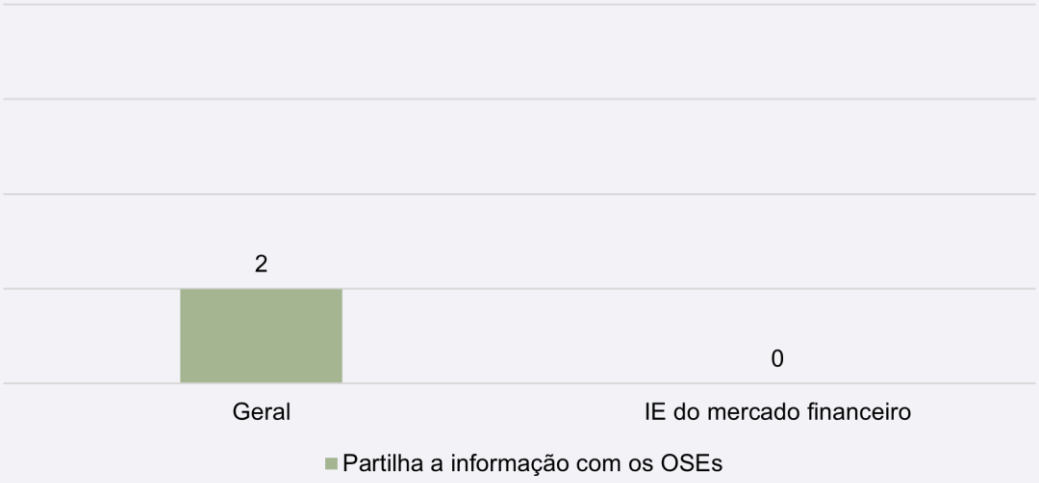
6. Categorização de ameaças

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



Cinco dos oito reguladores inquiridos realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores. O regulador do setor das infraestruturas do mercado financeiro é um dos cinco que realiza a categorização de ameaças.

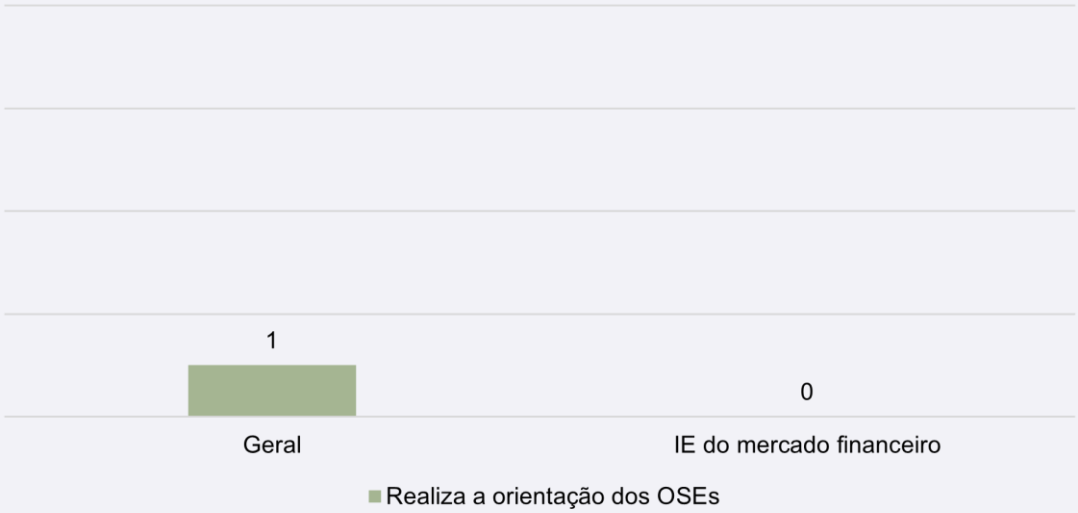
Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização



Dos cinco reguladores que realizam categorização de ameaças, apenas dois partilham informação relativa às ameaças com os OSE. Os restantes setores não efetuam a partilha de informação, sendo o regulador das infraestruturas do mercado um deles.

7. Orientação dos OSE por parte da entidade reguladora

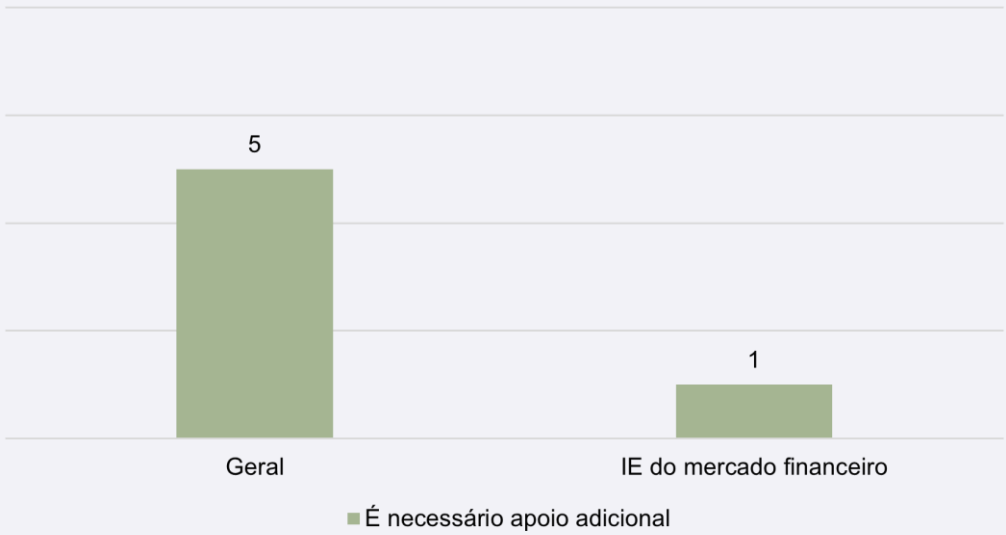
Gráfico 16 - Reguladores que orientam os OSE na digitalização de processos e na promoção de uma cultura digital



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

8. Apoio por parte do CNCS

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

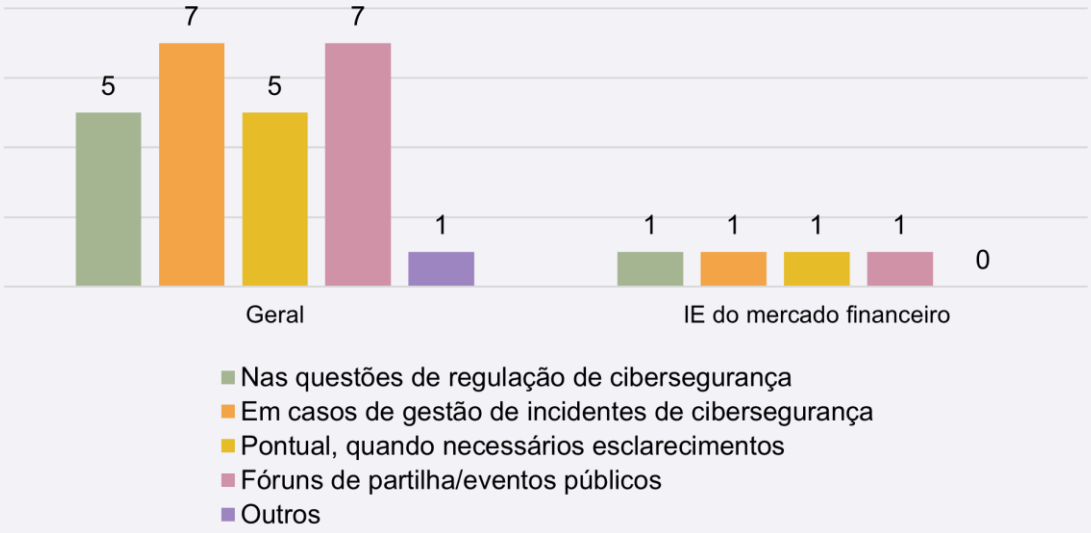


Entre os reguladores inquiridos, cinco (incluindo o setor das IMF) têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional.

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

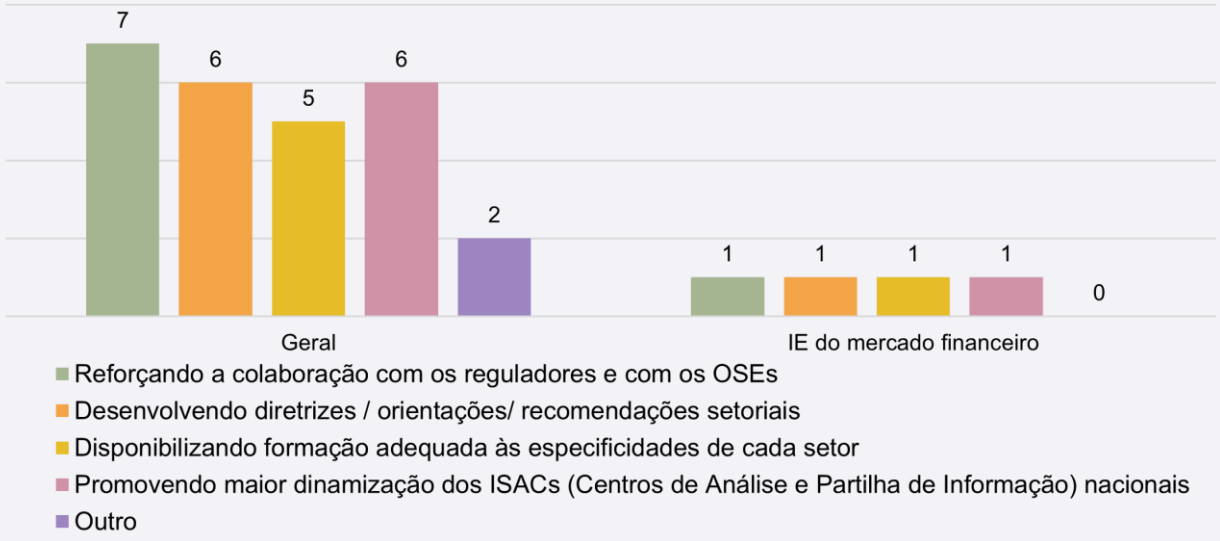
Entre os reguladores que consideram necessário apoio adicional do CNCS para que sejam atingidos níveis de maturidade em cibersegurança mais elevados nos vários setores, todos gostariam de ver mais ações de formação realizadas. Além destas, quatro destes reguladores gostariam que houvesse também mais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

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 regulador do setor das infraestruturas digitais menciona todas as interações com o CNCS.

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



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

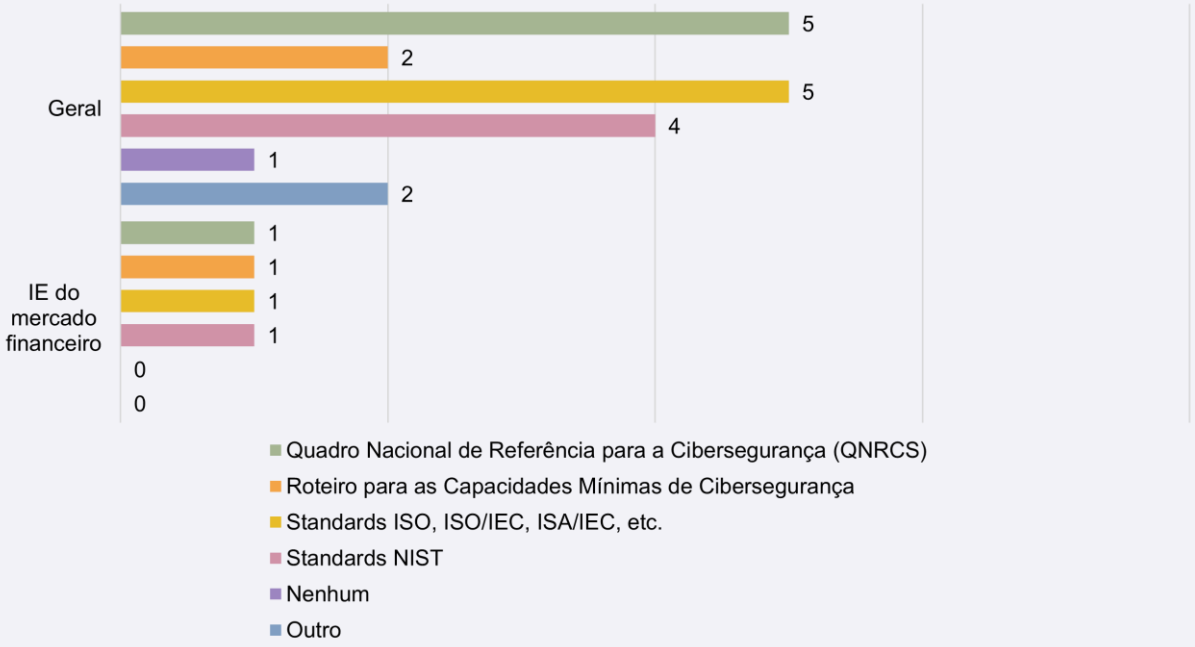
Nas infraestruturas do mercado financeiro, os reguladores inquiridos indicaram que gostariam de ver mais auxílio prestado ao nível do reforço da colaboração do CNCS com os reguladores e operadores, ao nível do desenvolvimento de diretrizes, orientações ou recomendações setoriais, da disponibilização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

O Centro Nacional de Cibersegurança lançou um desafio denominado por “Compromisso C-Academy” que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. As organizações poderão escolher, pelo menos, três formações até ao final de 2025. Alguns dos principais benefícios incluem: “Reforço da cibersegurança da organização, setor ou região, aumento da resiliência e da capacidade de resposta a ataques” e “Acesso a conteúdos formativos de elevada qualidade”[10].

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

9. *Standards* e boas práticas recomendadas

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



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

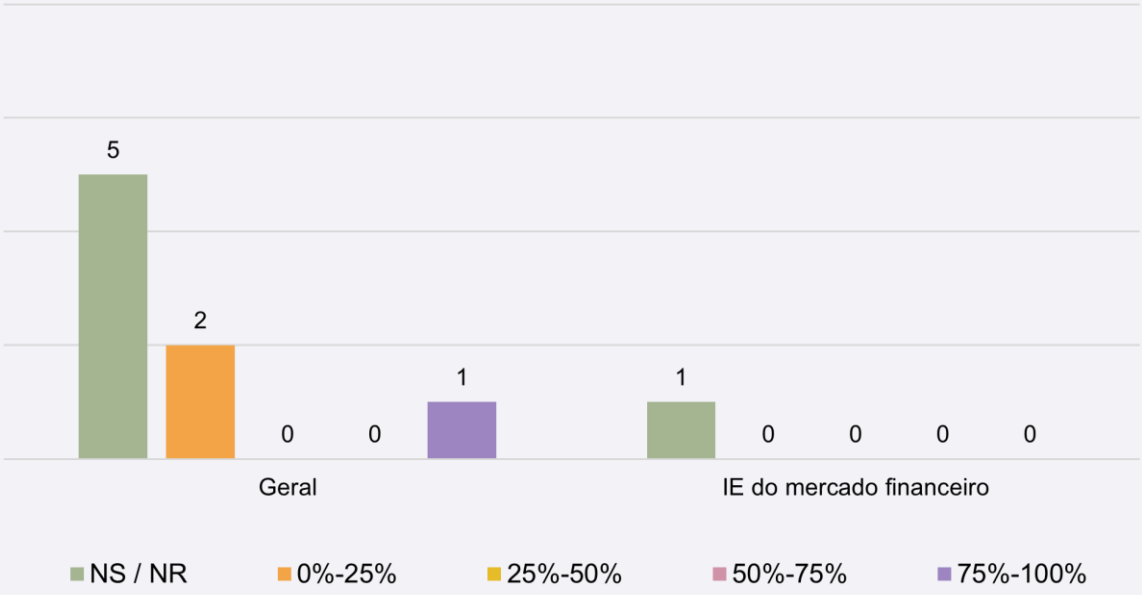
Na opção "outros", foram referidos *standards* da International Civil Aviation Organization (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain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

O regulador do setor das infraestruturas do mercado financeiro recomenda aos operadores o QNRCS, o Roteiro para as Capacidades Mínimas, *standards* ISO e *standards* NIST.

De acordo com um estudo realizado em 2023 pelo Departamento de Ciência, Tecnologia e Inovação do Governo do Reino Unido, o uso de boas práticas de cibersegurança diminuiu de 2021 para 2023. Nesta diminuição podem ser nomeados o decréscimo no uso de políticas de palavras-passe, onde se verificou uma redução de utilização pelos inquiridos de 79% para 70%, enquanto no uso de *Firewalls* se registou uma diminuição de 78% para 66%[11].

[11] Departamento de Ciência, Tecnologia e Inovação do Governo do Reino Unido, "Cyber security breaches survey 2023", 19 de abril de 2023, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

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



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

No setor de infraestruturas do mercado financeiro não conhecer a percentagem aproximada de operadores no setor certificados em normas internacionais do tipo referido.

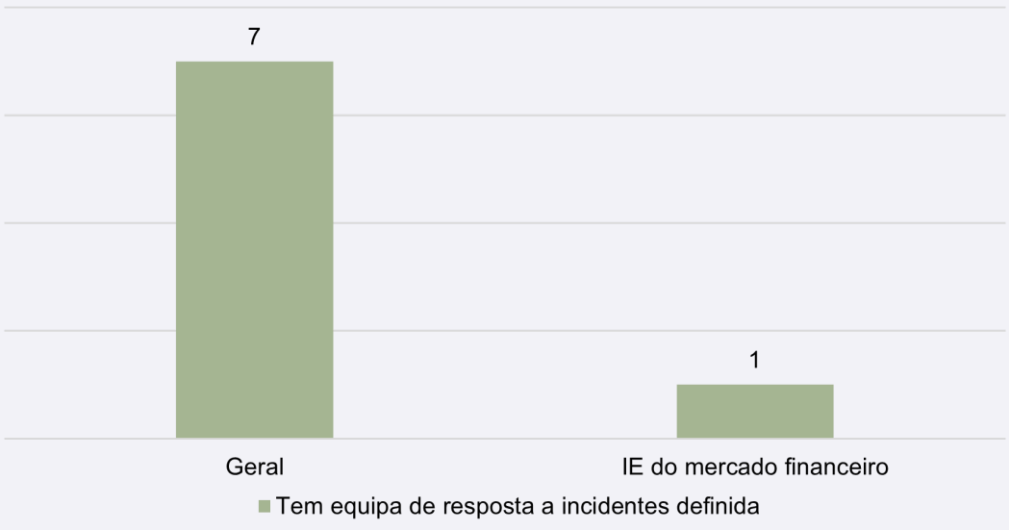
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança

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

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

10. Definição de equipa de resposta a incidentes de cibersegurança

Gráfico 23 - Reguladores com equipa de resposta a incidentes definida



Relativamente à definição de equipas de resposta a incidentes, a grande maioria dos reguladores inquiridos (sete) tem uma equipa definida. No setor das infraestruturas do mercado financeiro, o regulador inquirido informou ter definido a equipa de resposta a incidentes.

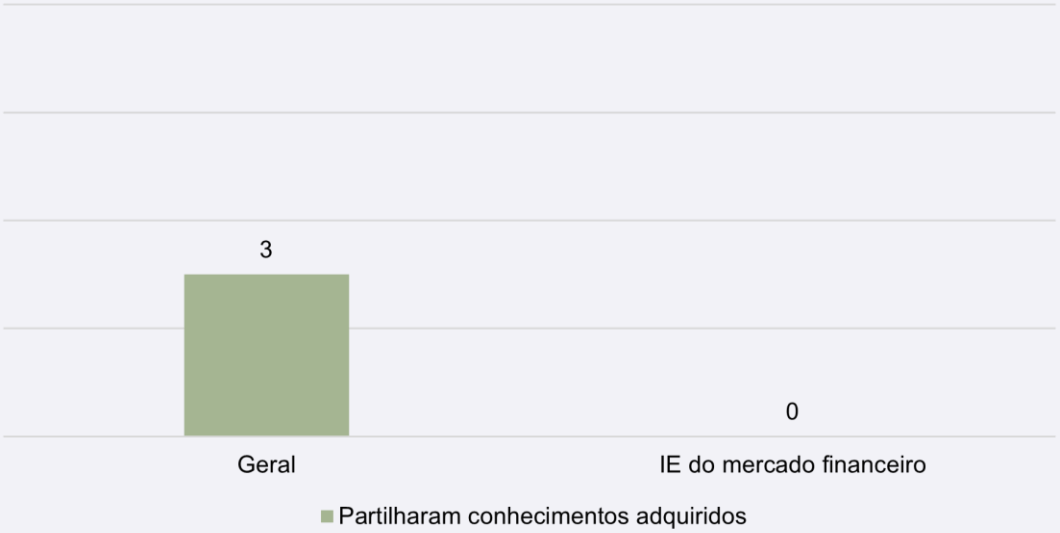
11. Sensibilização e consciencialização

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 inquirido do setor das infraestruturas do mercado financeiro informou estar ou já ter estado em programas de formação e sensibilização para os riscos no ciberespaço.

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

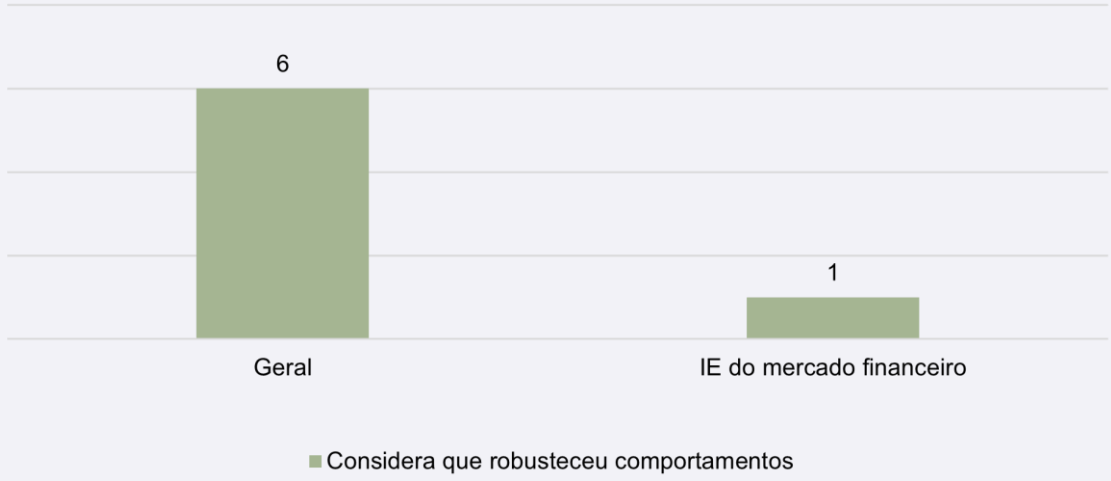


No seguimento da participação nos programas de formação e sensibilização para os riscos no ciberespaço, questionou-se se os conhecimentos adquiridos nesses programas foram partilhados com os OSE do setor. Os setores que fizeram essa partilha e os que não fizeram dividem-se igualmente.

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

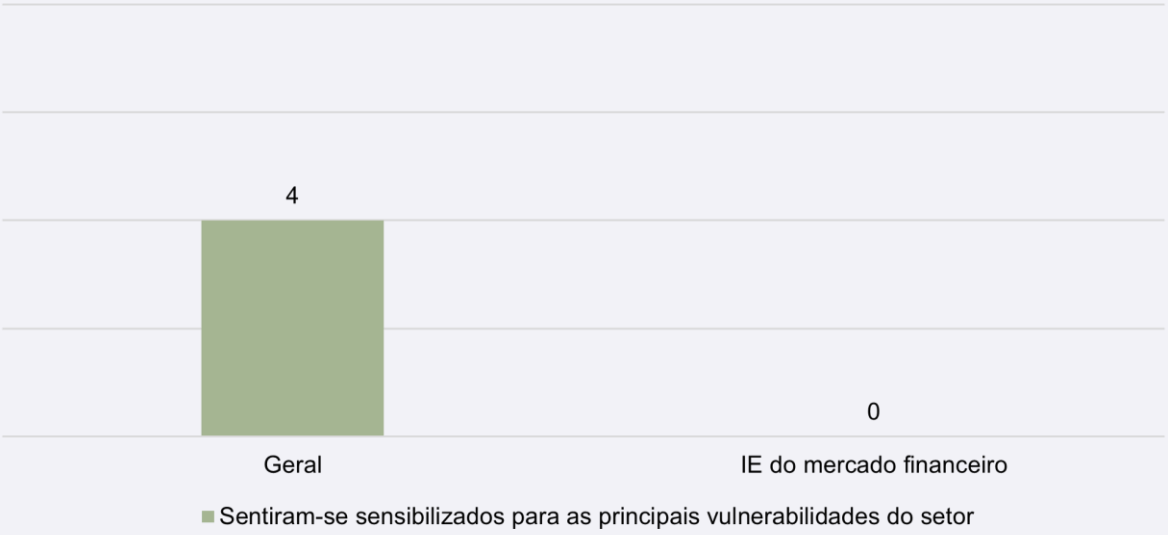
Nas infraestruturas do mercado financeiro o regulador não terá feito essa partilha com os operadores.

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.

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 regulador inquirido do setor das infraestruturas do mercado financeiro, este considera que a entidade formadora não o sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto.

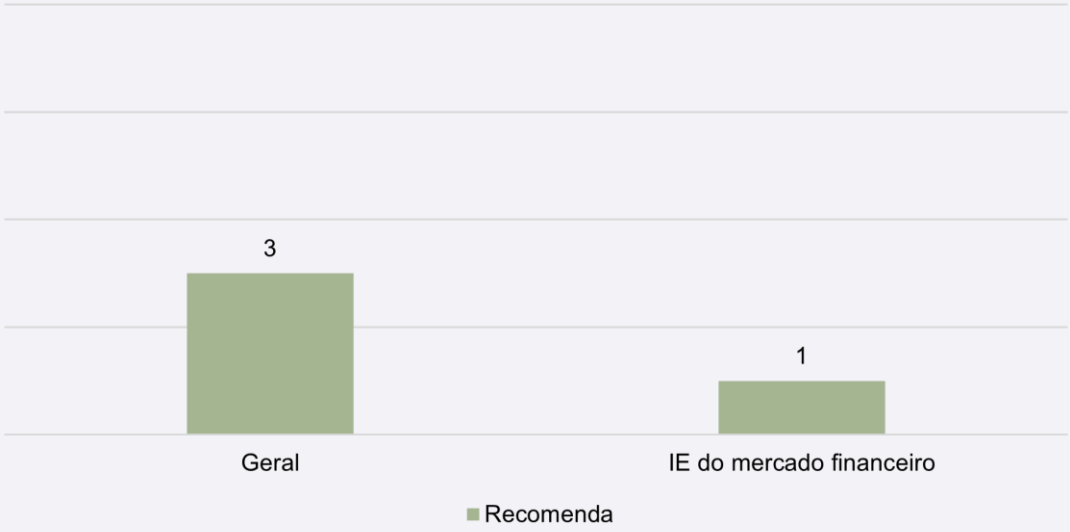
12. Cooperação nacional/internacional de proteção do ciberespaço

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 das infraestruturas do mercado financeiro insere-se no grupo da maioria, não fazendo parte de nenhuma estrutura do tipo.

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



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

No sector das infraestruturas do mercado financeiro, o regulador inquirido recomenda a participação em centros de partilha e análise de informação aos OSE.

13. Regulação de entidades e OSE

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

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

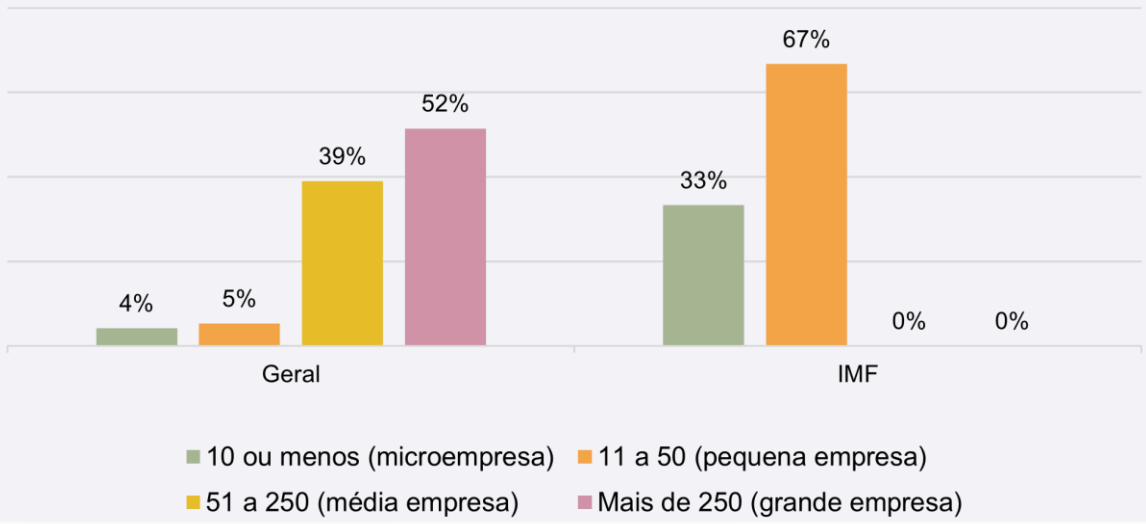
Setores	Estimativa
Energia	32
Transportes	> 19 000
Bancário	120
Infraestruturas do Mercado Financeiro	> 1 000
Distribuição de Água Potável	350
Infraestruturas Digitais	100

Tabela 4 - Número estimado das entidades reguladas que são OSE

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

Resultados do questionário dirigido aos Operadores de Serviços Essenciais

Gráfico 30 - Número de colaboradores na organização

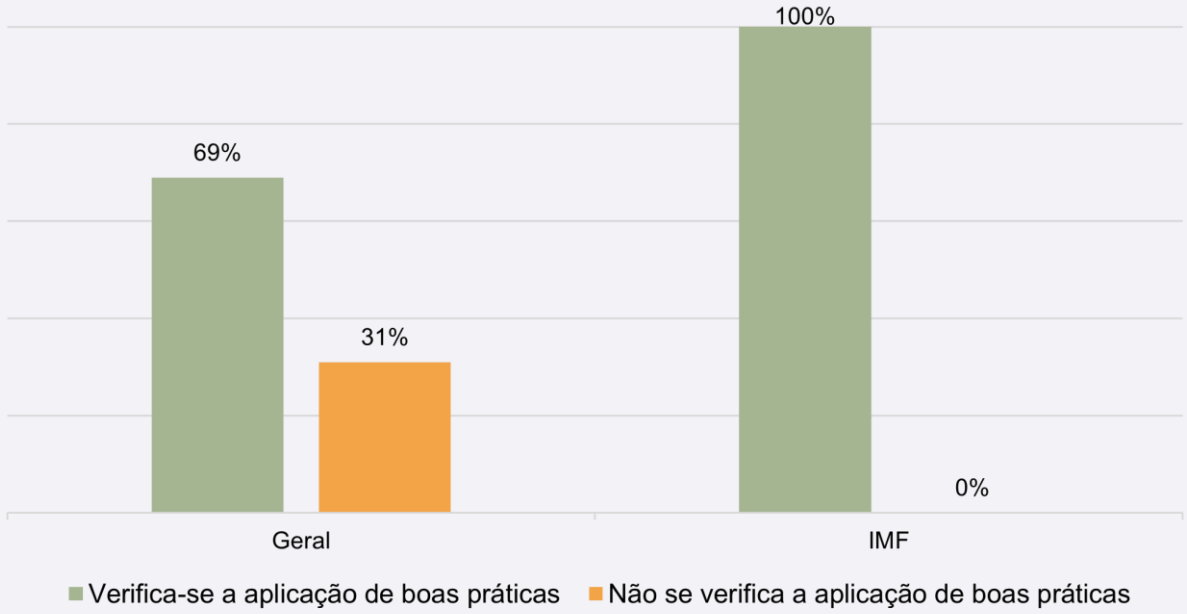


O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSE. As médias empresas representam 39% dos OSE, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas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

O setor das infraestruturas do mercado financeiro surge como o único a apresentar apenas micro e pequenas empresas.

A composição do tecido empresarial dos OSE difere grandemente daquele que é o tecido empresarial geral das empresas portuguesas. Enquanto entre os OSE mais de 50% destes são grandes empresas, 99,9% das demais empresas em Portugal são, segundo dados de 2022 da PORDATA, pequenas e médias empresas, com apenas 0,1% sendo grandes empresas[12].

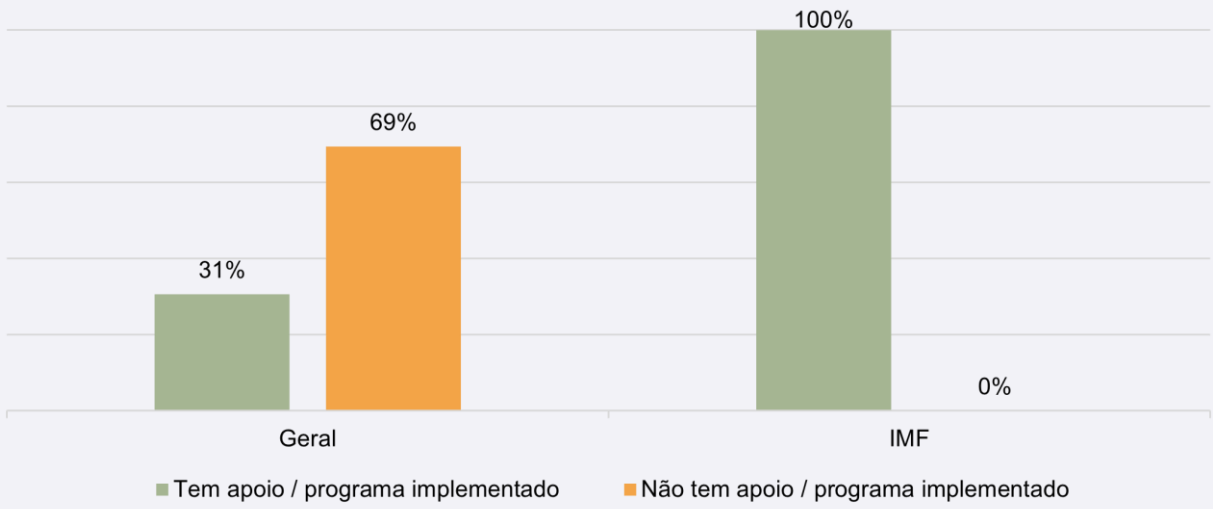
Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores



De um modo geral, os operadores percecionam a adoção de boas práticas de cibersegurança por parte dos seus colaboradores. Alguns exemplos dessas boas práticas são a não partilha de palavras-passe, o bloqueio do computador durante momentos de ausência da estação de trabalho, o cuidado com a informação confidencial do operador ou a denúncia de *e-mails* suspeitos/tentativas de *phishing*, entre outras. Na generalidade, dois terços dos operadores consideram que há uma efetiva adoção dessas boas práticas pelos seus colaboradores.
O setor das infraestruturas do mercado financeiro destaca-se por ser um setor onde 100% dos operadores consideram que boas práticas de cibersegurança são aplicadas pelos seus colaboradores.

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

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

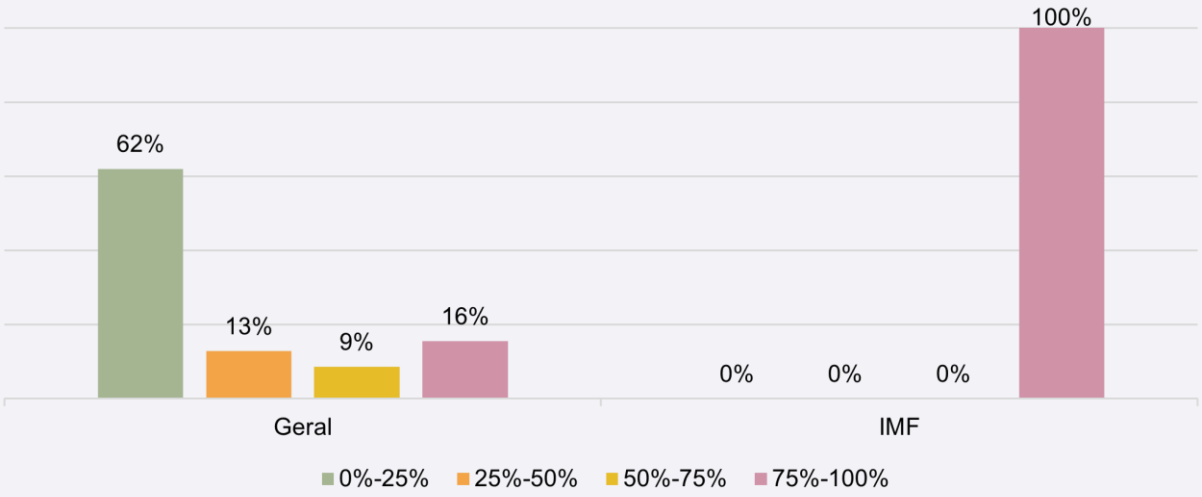


À data de realização do questionário, apenas um terço dos operadores tinham apoios ou programas próprios ou do Estado para colaboradores interessados em formação na área de cibersegurança.

O setor das infraestruturas do mercado financeiro destaca-se dos restantes setores em estudo, uma vez que, todos os operadores disponibilizam esses apoios ou programas.

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

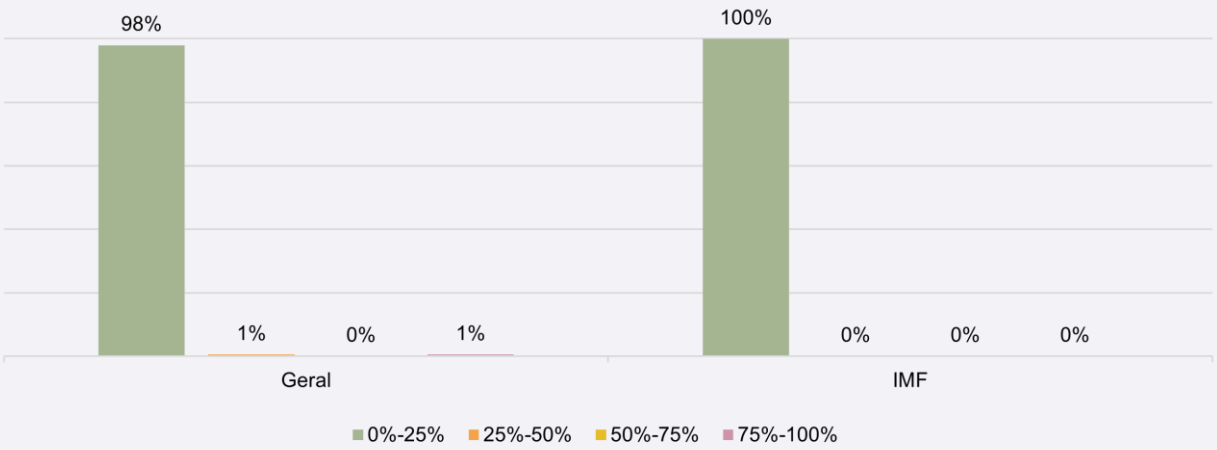
Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



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

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

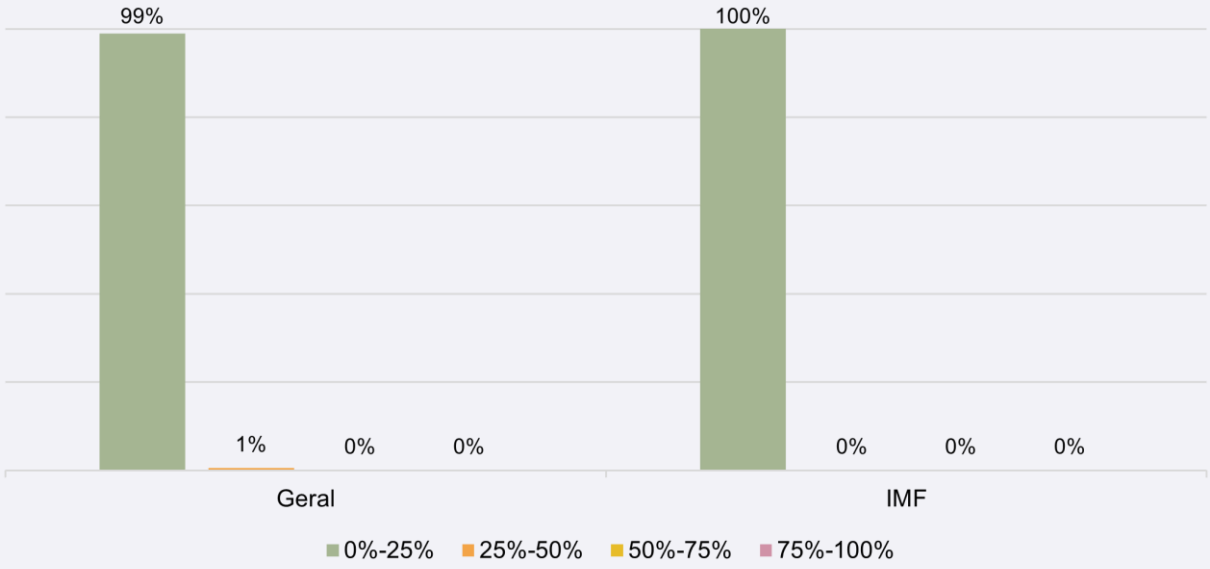
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



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. Em apenas dois setores foram registados 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

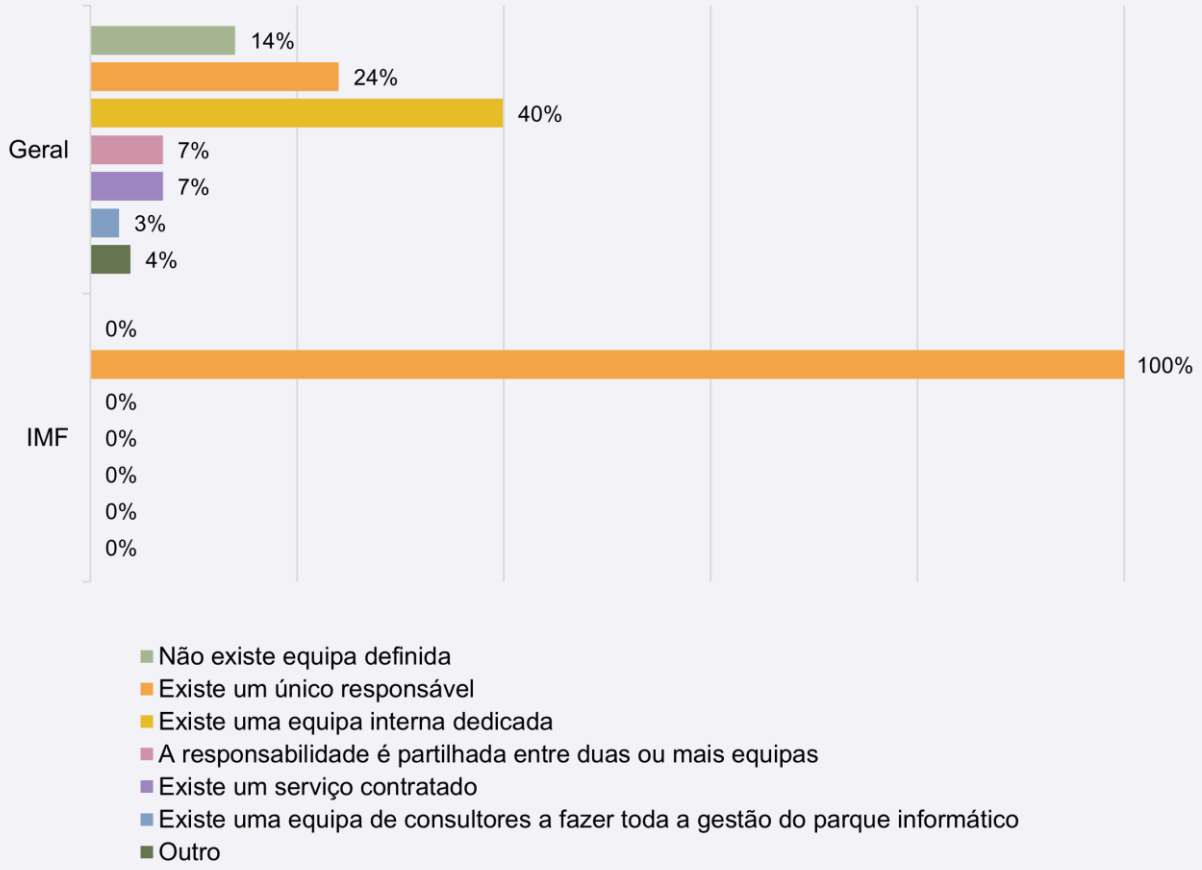


A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. Novamente, o resultado geral é um resultado expectável, uma vez que não se espera que colaboradores de outras áreas sejam certificados em cibersegurança.

De acordo com os dados disponíveis no relatório *NIS Investments* 2021, da ENISA, apenas 7,5% dos OSE na UE indicavam ter uma preocupação em certificar os colaboradores da própria organização. A nível setorial, no mesmo relatório, em nenhum dos setores se superava os 11% de OSE a certificar os seus próprios colaboradores[13].

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

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

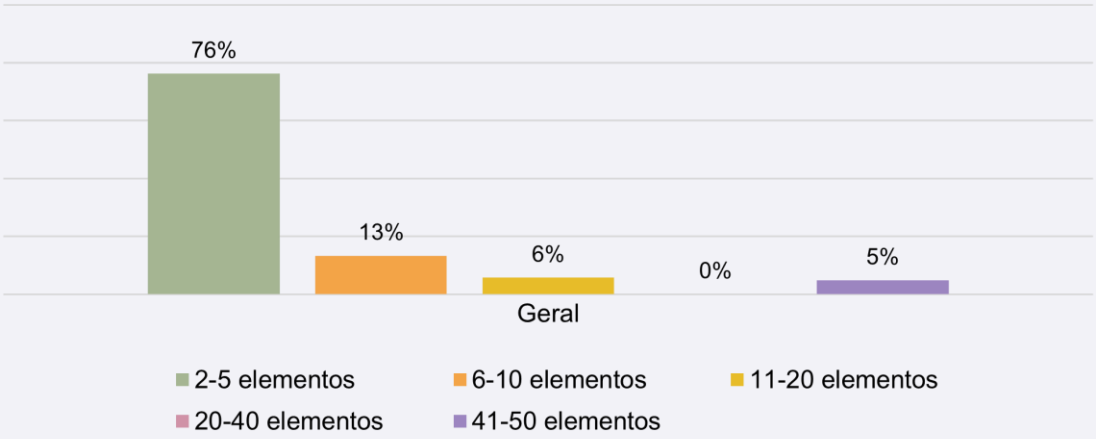


De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (25% dos casos).

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

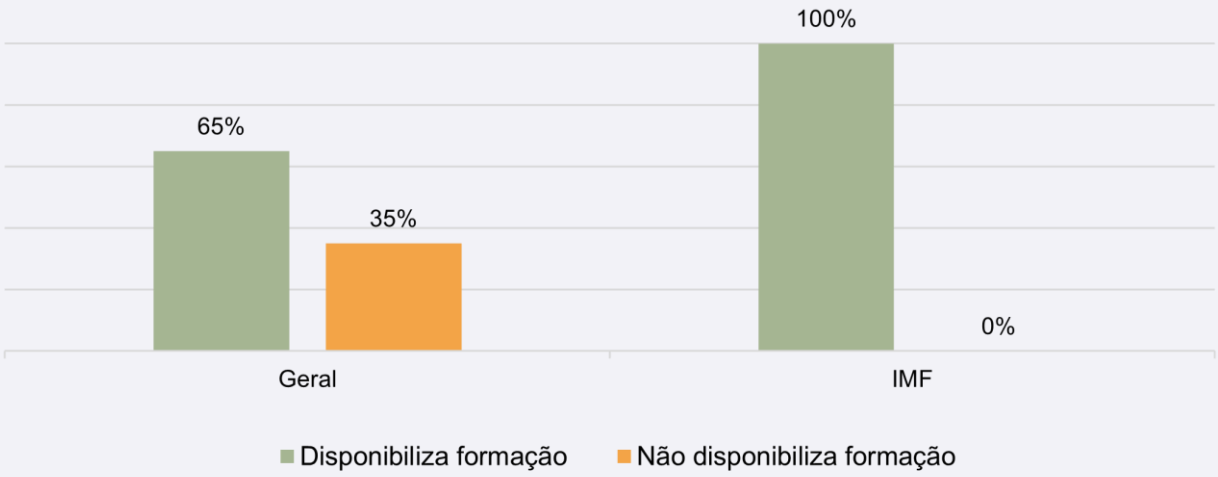
No setor infraestruturas do mercado financeiro, a responsabilidade é maioritariamente atribuída a um único responsável.

Gráfico 37 - Composição das equipas de *helpdesk*



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

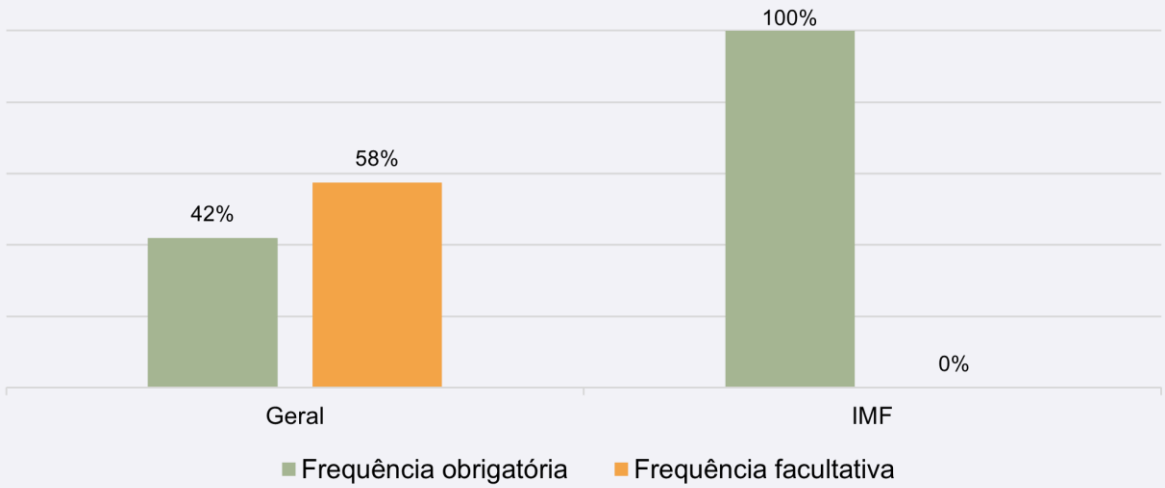
Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. Notavelmente, no setor das infraestruturas do mercado financeiro, todos os OSE indicaram disponibilizar formação em cibersegurança aos seus colaboradores.
Comparando com dados do Inquérito à Utilização das TIC nas Empresas (IUTICE) de 2022, realizado pelo Instituto Nacional de Estatística (INE), 63,3% das empresas em Portugal procuraram consciencializar os seus colaboradores sobre cibersegurança durante o ano de 2021[14]. Já um outro estudo, realizado pela Microsoft Portugal em setembro de 2023, intitulado "Estado da Cibersegurança em Portugal", indica que 84% das empresas portuguesas ministram formação de sensibilização para a cibersegurança. A discrepância nestes resultados poder-se-á dever à composição das amostras de cada estudo. Embora seja expectável que cada vez mais empresas disponibilizem formação em cibersegurança aos seus colaboradores, um crescimento de 20% em dois anos das entidades que disponibilizam formação em cibersegurança aos seus colaboradores é improvável.

[14] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 18, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=585250024&att_display=n&att_download=y

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

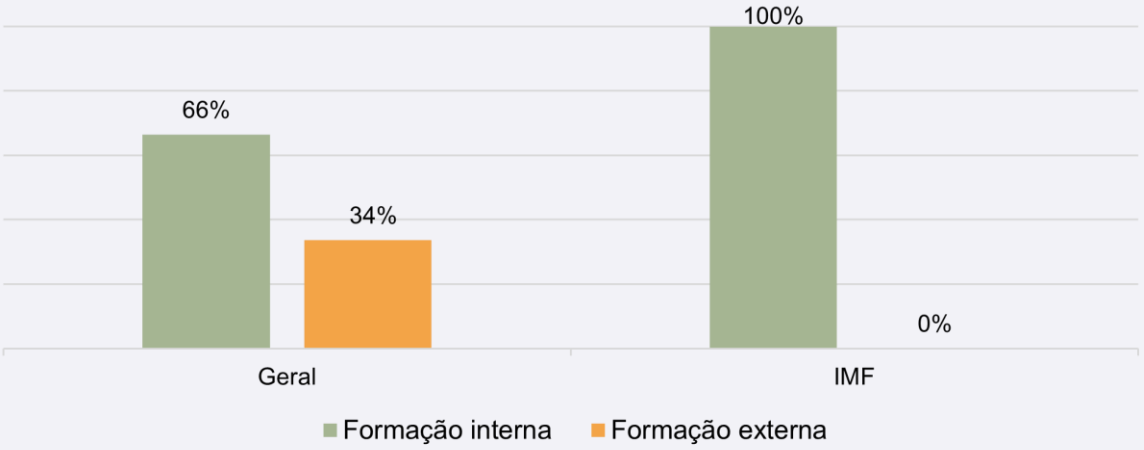


De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais esta tendência não se verifica. Destacam-se as elevadas percentagens de OSE nos quais a frequência das formações é obrigatória no setor das infraestruturas do mercado financeiro (100%).

Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre OSE e demais empresas em Portugal. Enquanto em 42% dos OSE que disponibilizam formação, esta é de caráter obrigatório, apenas em 19,2% das empresas portuguesas há formações obrigatórias. Já ao nível das de caráter facultativo (ou voluntário, nos termos do IUTICE), os resultados são mais similares aos do questionário realizado pelo CNCS, uma vez que estas se verificam em 58% dos OSE que disponibilizam formação e em 56,2% das empresas participantes no inquérito[15].

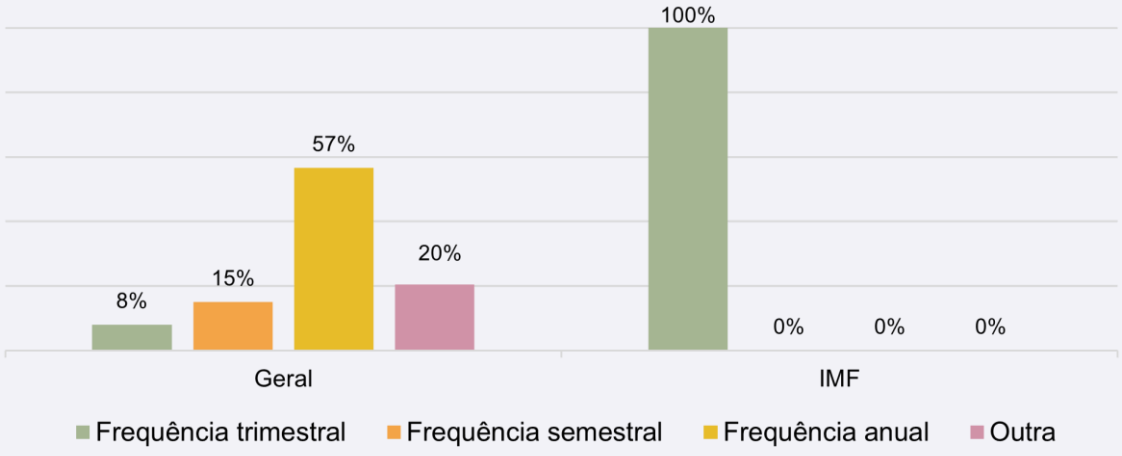
[15] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19.

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



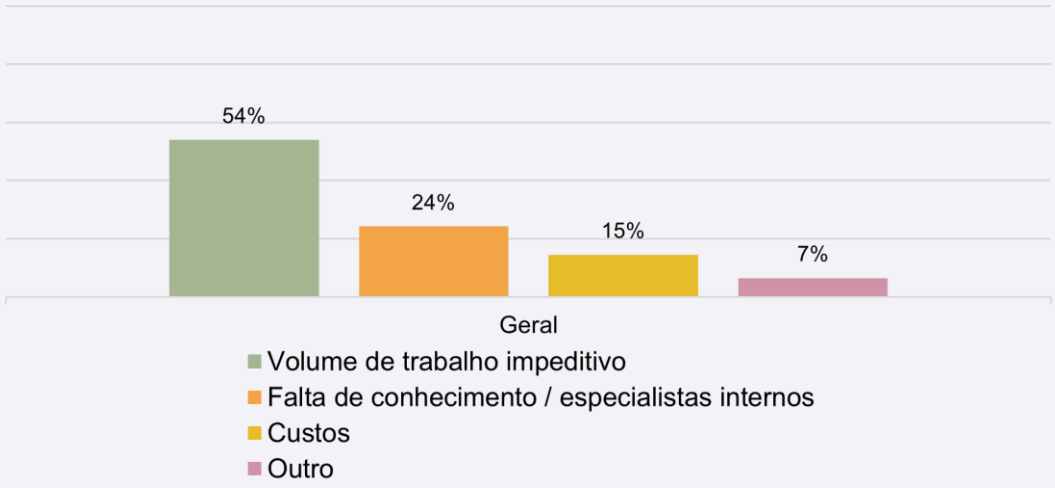
Neste gráfico, fica evidenciado o maior recurso à formação interna do que externa entre os OSE. A maioria dos inquiridos (66%) recorre aos meios internos para fins de formação aos colaboradores. Surgem em destaque o setor das infraestruturas do mercado financeiro, com as maiores percentagens de OSE a darem formação interna (100%, respetivamente).
Contudo, cerca de um terço dos OSE (34%) recorre a entidades externas para formar os seus colaboradores.

Gráfico 41 - Frequência média dos momentos de formação



Em termos gerais, a maioria dos OSE que disponibiliza formação (57%) indica que a frequência média dos momentos de formação é anual. Contudo, no setor das infraestruturas do mercado financeiro, todos os inquiridos indicaram que a frequência dos momentos de formação é trimestral. Entre os OSE que indicaram "Outra" frequência, tanto se registam frequências superiores à trimestral, chegando os momentos de formação a ser mensais ou mesmo semanais, como frequências inferiores à anual, onde não existe uma periodicidade definida e os momentos de formação sucedem de modo *ad hoc*.

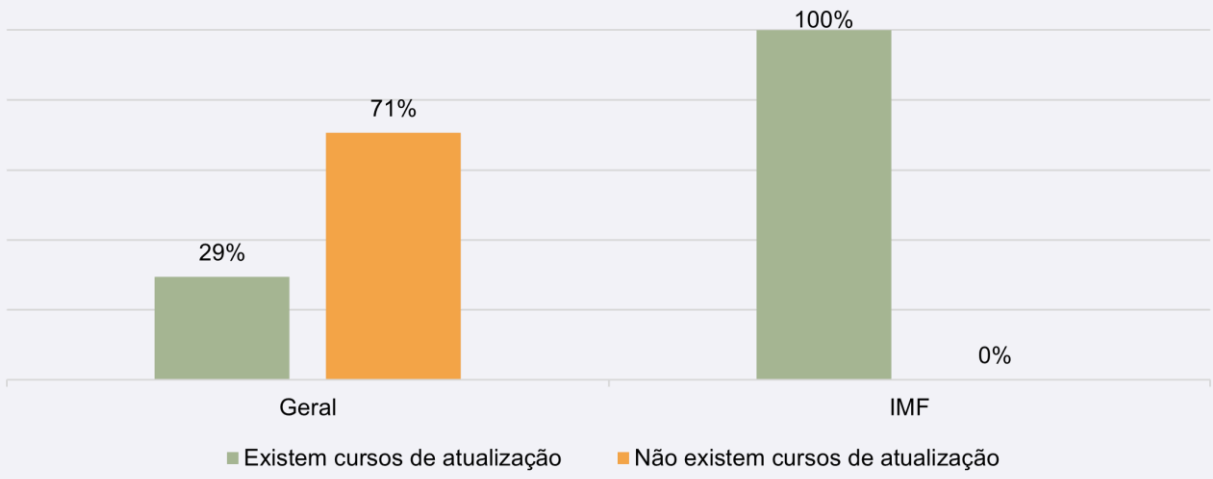
Gráfico 42 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam



Os motivos para a não disponibilização de formação são na sua maioria atribuídos ao volume de trabalho impeditivo, tendo este motivo sido indicado por 54% dos OSE que afirmaram não disponibilizar formação em cibersegurança aos seus colaboradores.

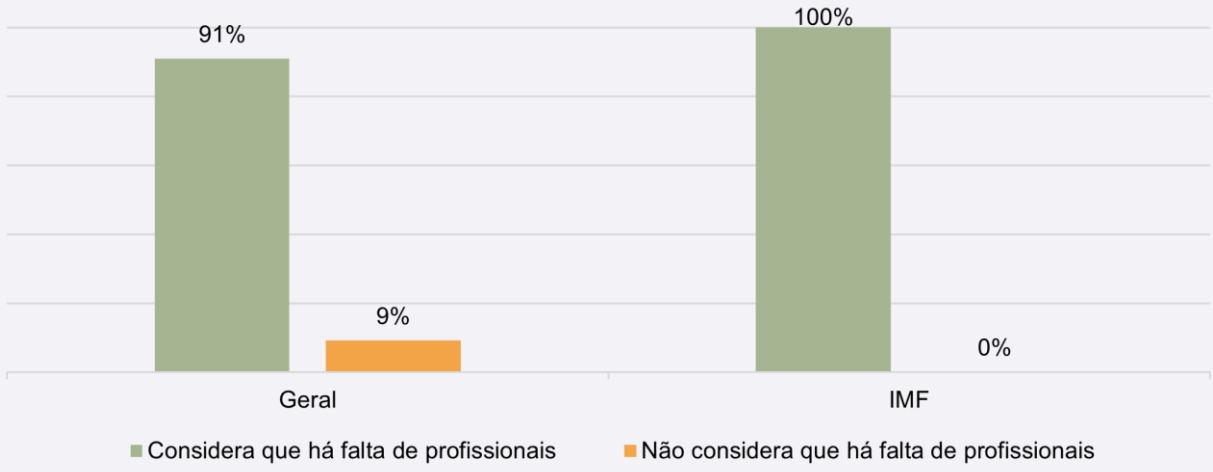
A questão não é aplicável ao setor das infraestruturas do mercado financeiro.

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



A oferta de cursos ou formações de atualização em cibersegurança para os colaboradores é escassa na generalidade, com apenas 29% dos OSE inquiridos a indicarem a existência destes cursos. Contudo, os setores das infraestruturas do mercado financeiro contrariam essa tendência geral, com a totalidade dos inquiridos indicarem que disponibilizam cursos de atualização.

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



A vasta maioria dos OSE inquiridos (91%) considera haver um cenário de escassez de profissionais de cibersegurança e áreas relacionadas no mercado de trabalho. Especificamente, no setor das infraestruturas do mercado financeiro, todos os OSE inquiridos consideram que há falta 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[16] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[17]. Esta falta de profissionais coloca aos empregadores na área desafios como conseguir pessoal qualificado, conseguir desenvolver equipas que possuam as capacidades técnicas desejadas e conseguir manter os bons profissionais encontrados[18]. De modo a combater esta escassez, organizações como o Fórum Económico Mundial e a ENISA têm feito diversas recomendações, que passam pela contratação de profissionais vindos de outras áreas de formação que não apenas as das TIC, engenharia e matemática, pela admissão de colaboradores menos experientes, ou mesmo sem experiência (sendo esta adquirida ao longo do desempenho das funções pretendidas), a admissão de colaboradores em trabalho totalmente remoto, e pela valorização dos profissionais, não só a nível salarial, mas também a nível das perspetivas de progressão de carreira e até mesmo do respeito pelos profissionais no local de trabalho[19] [20].

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

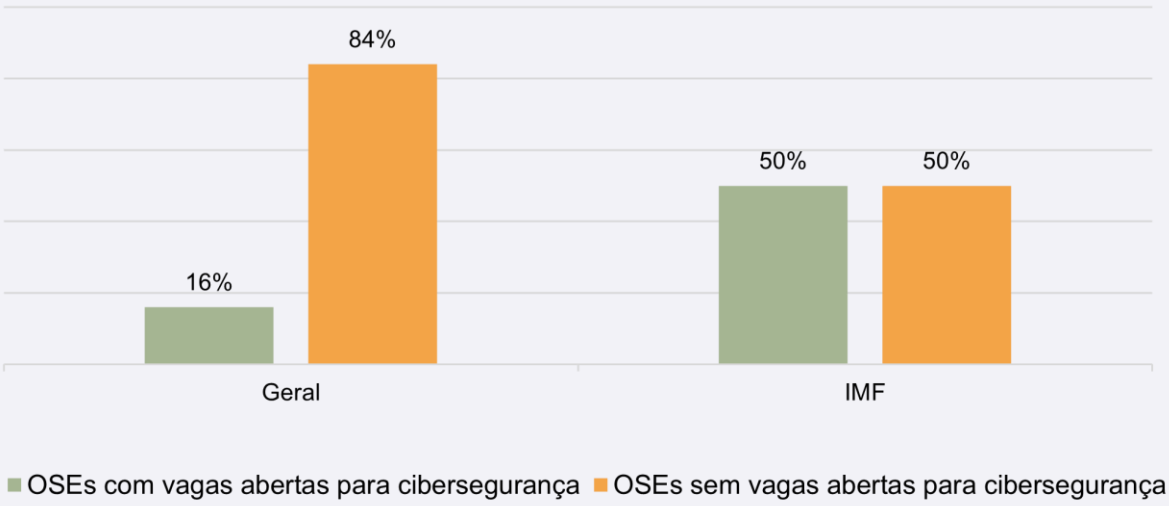
[17] ENISA, "Cybersecurity Skills Conference: Strengthening human capital in the EU", https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.

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

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

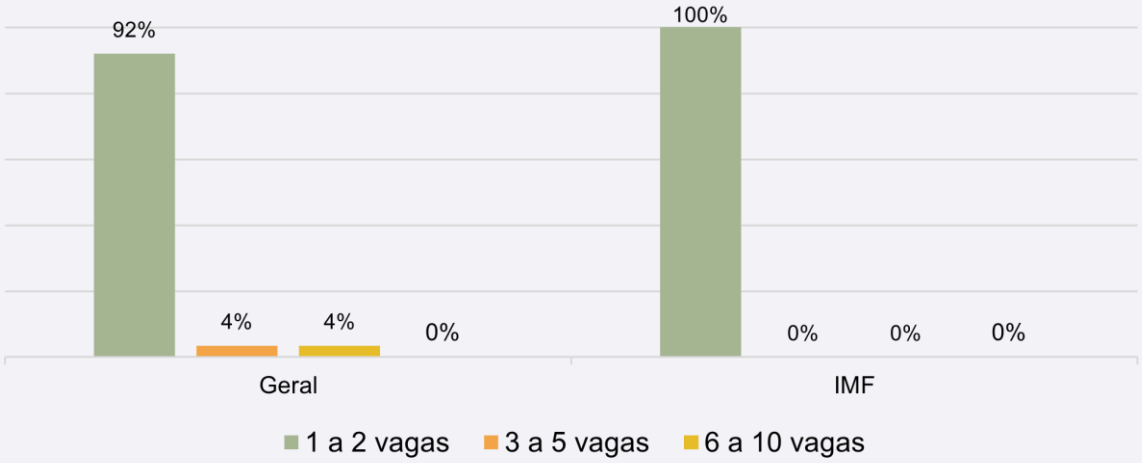
[20] Banco Mundial, "Strategic Cybersecurity Talent Framework", 22-25.

Gráfico 45 - Vagas abertas para a área de cibersegurança



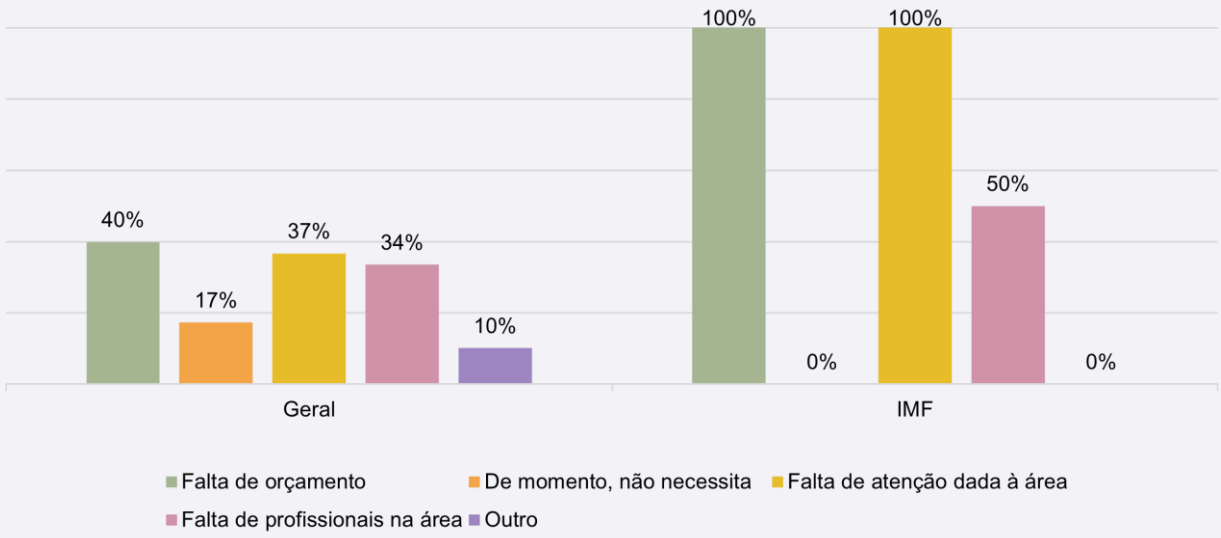
À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. Sectorialmente, registaram-se duas exceções, uma delas sendo o setor das infraestruturas do mercado financeiro, com 50% dos OSE a indicarem ter vagas em aberto.
Embora não se possa fazer uma 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 OSE com vagas abertas para a área de cibersegurança



Entre os 16% de OSE que tinham vagas abertas na área de cibersegurança, a maioria destes (92%) tinha 1 a 2 vagas por preencher. Tal era o caso para todos os OSE com vagas em aberto nos setores da energia, dos transportes, da banca e das infraestruturas do mercado financeiro. Apenas num setor foram registados OSE com 3 a 5 vagas em aberto e num outro setor houve indicação de haver entre 6 e 10 vagas em aberto.

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



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

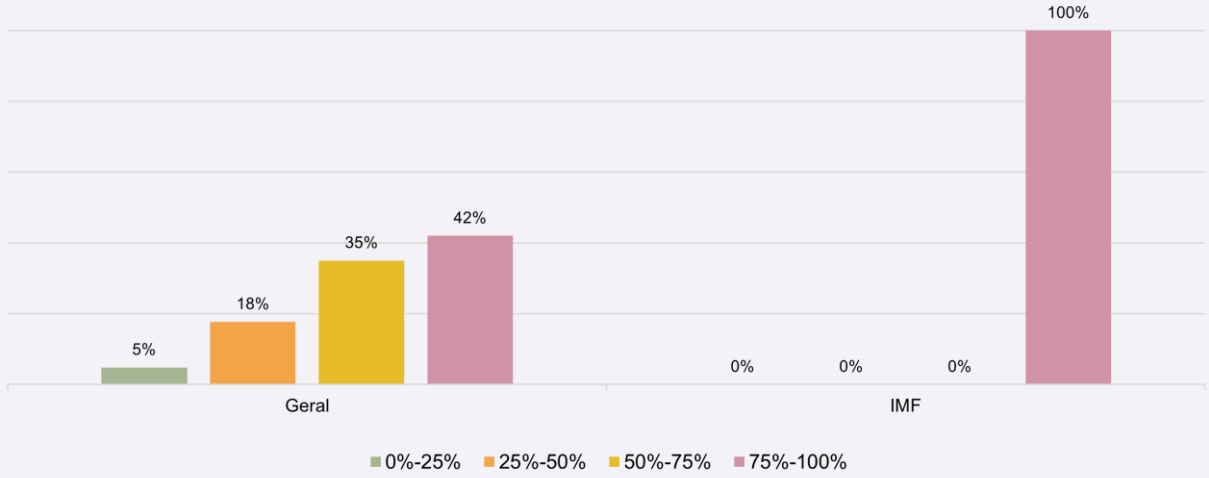
A resposta mais comum foi a falta de orçamento, indicada por 40% dos OSE sem vagas em aberto, seguida da falta de atenção dada à área (37%) e da falta de profissionais de cibersegurança (34%). Apenas em 17% dos casos foi indicado que não havia vagas em aberto por se considerar que de momento não eram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

No setor das infraestruturas do mercado financeiro os motivos apontados foram a falta de orçamento, a falta de atenção dada à área, e por uma certa percentagem a falta de profissionais na 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 OSE sem vagas em aberto é um dos aspetos mais preocupantes que surgem na análise. Um dos Objetivos Estratégicos (Objetivo 3) da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 passa por gerar e "garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço"[21], 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[22].

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



Apesar de predominar entre os OSE o intervalo 75%-100% de colaboradores com acesso a equipamentos digitais (indicado por 42% dos OSE), é visível que, com exceção de dois setores onde praticamente a sua totalidade tem acesso a equipamentos digitais, sendo um o setor das infraestruturas do mercado financeiro, há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos.

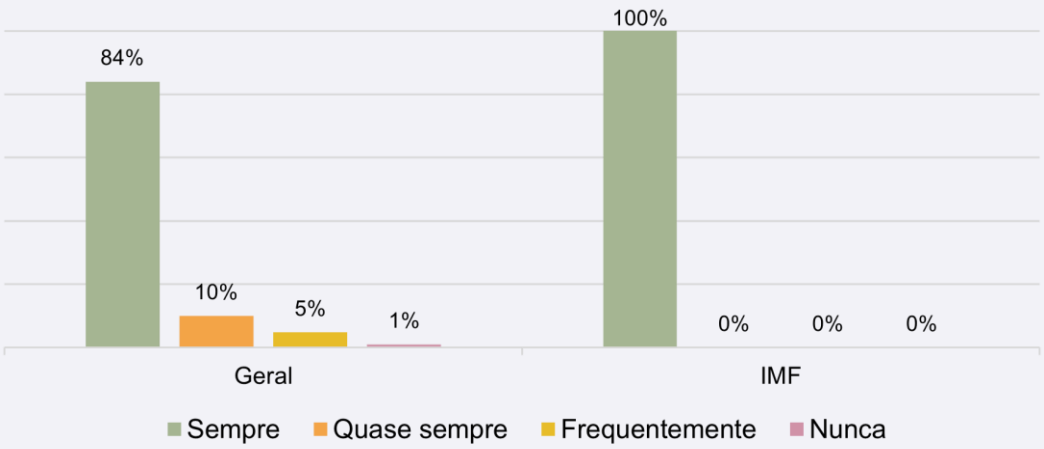
Segundo dados do IUTICE de 2022, em 2021, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais (+17,2 p.p. face a 2021), abrangendo 28,1% do pessoal ao serviço (+4,2 p.p. que em 2021). Neste ano, 74,7% das empresas tinham pessoal ao serviço com acesso remoto ao sistema de correio eletrónico da empresa[23].

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

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

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

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

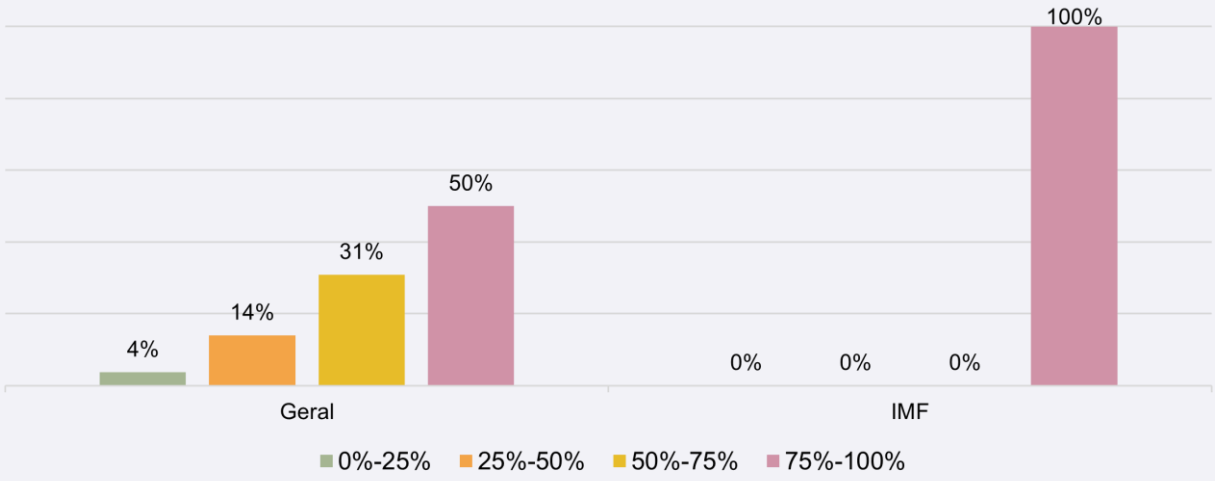


Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. Todos os operadores inquiridos nos setores das infraestruturas do mercado financeiro indicaram ser os próprios a fornecer sempre os equipamentos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

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[24].

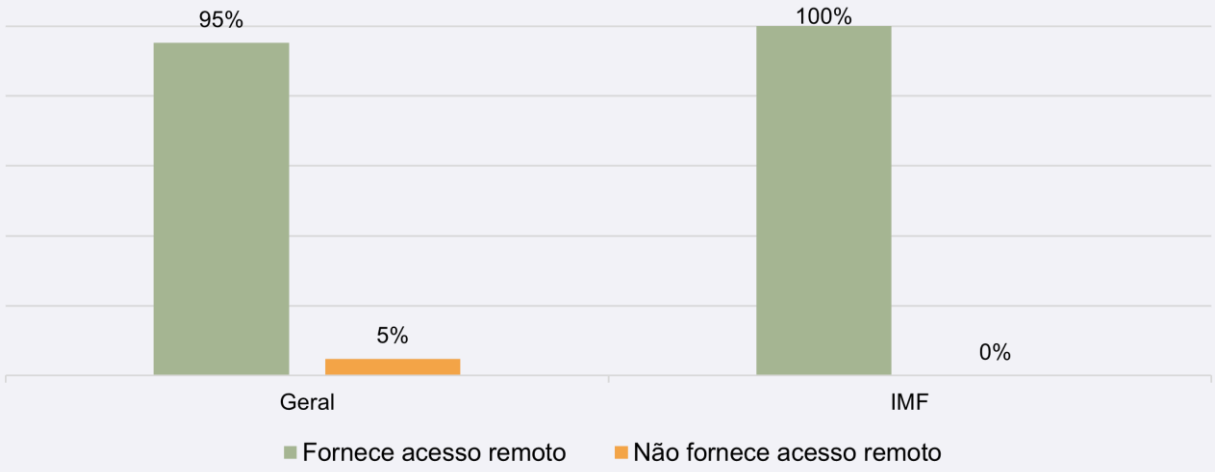
Gráfico 50 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções



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

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 IMF, verifica-se que todos os operadores fornecem esse acesso a pelo menos 75% dos colaboradores.
Voltando a comparar com dados do IUTICE, mas agora com o de 2023, verifica-se que há mais colaboradores com acesso à Internet no contexto específico dos OSE do que das várias empresas portuguesas. Juntando os dois intervalos onde mais de 50% dos colaboradores têm acesso à Internet, obtém-se 81% de OSE onde 50% dos colaboradores acedem à Internet no desempenho das suas funções. No contexto empresarial português, apenas 48,9% dos colaboradores têm acesso à Internet para fins de trabalho. Mesmo comparando setorialmente onde possível, como nos setores da energia e dos transportes, os OSE continuam a apresentar mais colaboradores com acesso à Internet: segundo o IUTICE, no setor da energia, há 39,8% de colaboradores com acesso à Internet, enquanto o questionário realizado demonstra que em 89% dos OSE desse setor, 50% dos colaboradores ou mais têm acesso à Internet; e no setor dos transportes, 56,6% dos colaboradores têm acesso à Internet no contexto empresarial português, enquanto no contexto dos OSE 88% indicam haver 50% ou mais colaboradores com acesso à Internet para fins de trabalho[25].

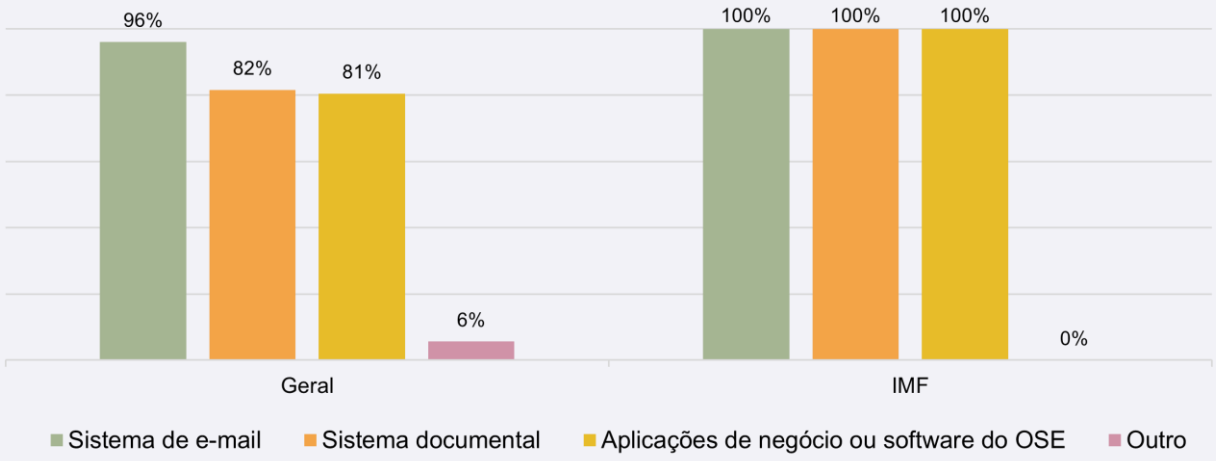
Gráfico 51 - Fornecimento de acesso remoto a sistemas (e-mail, aplicações ou documentos) dos OSE aos colaboradores



O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSE aos colaboradores é uma realidade em praticamente todos os OSE inquiridos (95%). Em quatro dos oito setores, sendo um deles o das infraestruturas do mercado financeiro, todos os OSE indicaram permitir o acesso remoto a esses sistemas por parte dos seus colaboradores.
Voltando a comparar com os dados do IUTICE de 2022, há uma maior percentagem de Operadores de Serviços Essenciais a fornecer acesso remoto ao sistema de e-mail do que na generalidade das empresas em Portugal. Enquanto 95% dos OSE indicaram dar esse acesso remoto, no contexto empresarial geral apenas 74,7% das empresas fornecem acesso remoto ao sistema de e-mail[26].

[25] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 3.
[26] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 6-7.

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



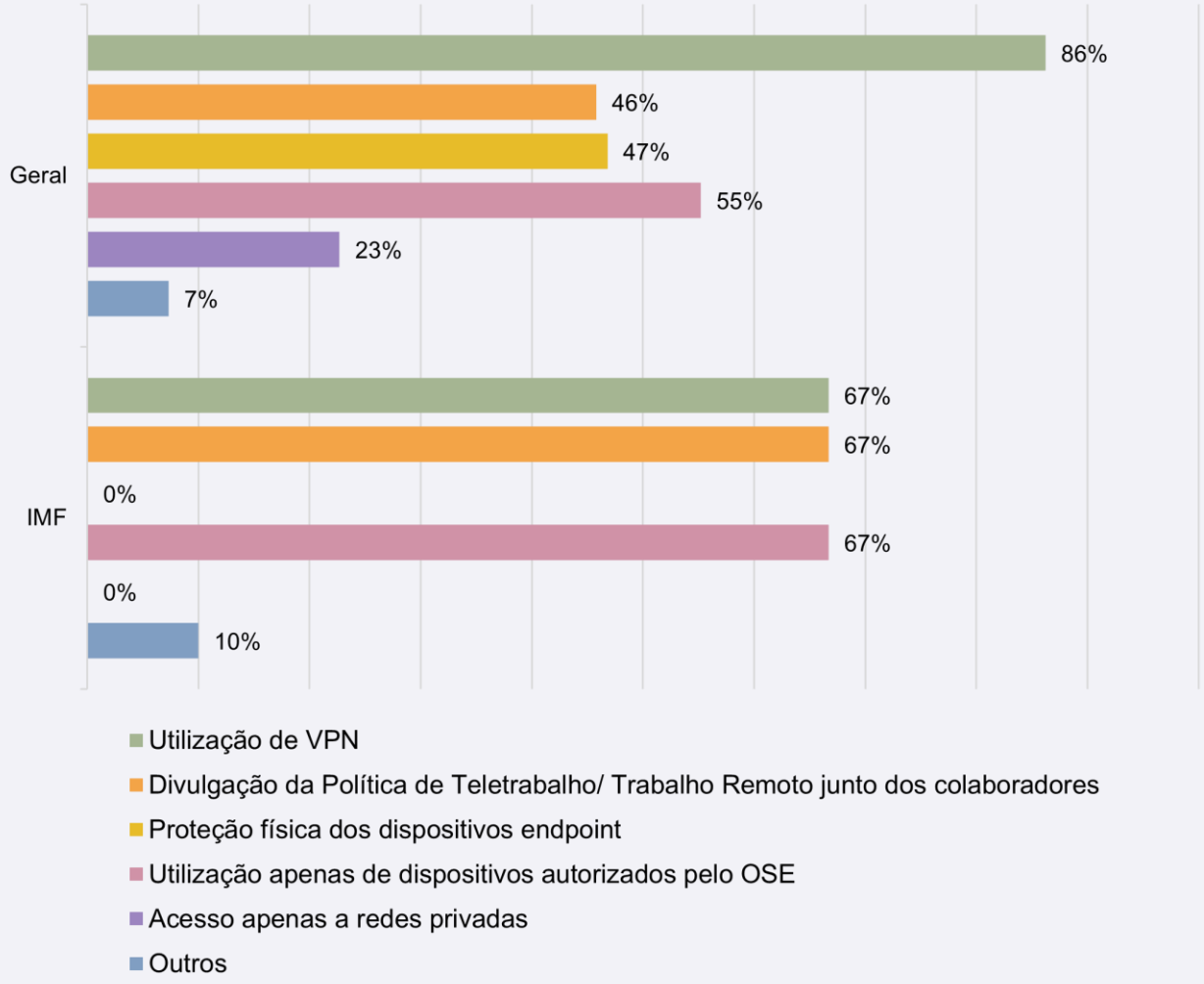
Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no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

No setor das IMF, os sistemas de e-mail, documentais e aplicações de negócio podem ser acedidos remotamente por todos os colaboradores.

Comparando novamente com dados do IUTICE de 2022, os OSE continuam a fornecer mais acesso remoto a diferentes sistemas do que a generalidade das empresas portuguesas. Tinha já sido vista a diferença na disponibilização geral de acesso remoto por parte dos colaboradores a sistemas entre OSE (95% a disponibilizar) e empresas (74,7% a disponibilizar). Revisitando essa comparação entre cada sistema, é visível que há mais OSE a dar acesso remoto aos documentos da organização do que empresas em geral (82% de OSE contra 65% de empresas) e também mais OSE a dar acesso remoto a aplicações ou *software* de negócio (81%) do que empresas (63,9%)[27].

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

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

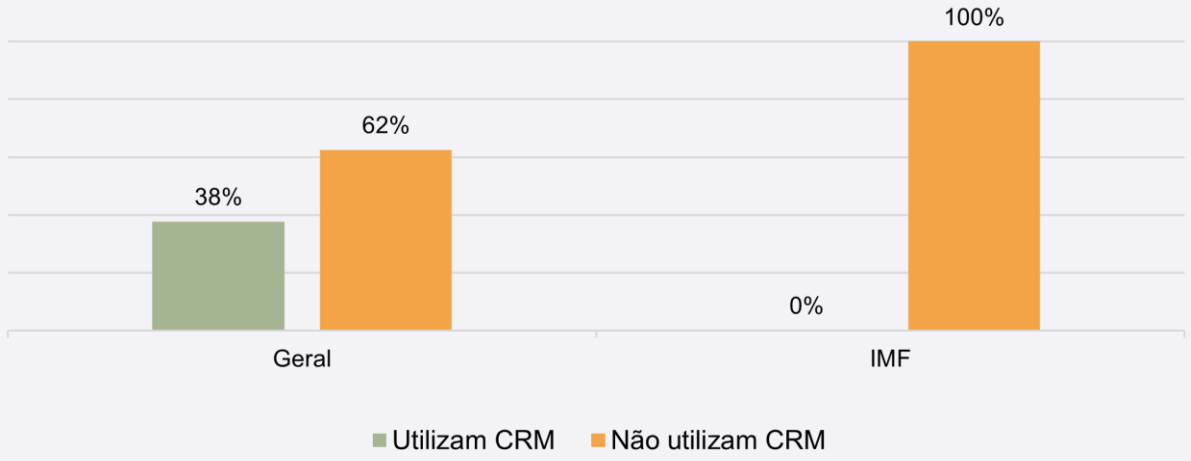


No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança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

A segunda boa prática mais aplicada é a utilização de dispositivos autorizados pelos OSE, mas com uma prevalência bem mais reduzida (verificada apenas em 55% dos casos). Medidas como a divulgação da Política de Teletrabalho/Trabalho Remoto, proteção física dos dispositivos *endpoint* e acesso apenas através de redes privadas verificam-se em menos de 50% dos operadores inquiridos. Os operadores que indicaram outras boas práticas mencionaram a utilização de autenticação multifator, máquinas virtuais a operar nos servidores do operador (VDI's: *Virtual Desktop Infrastructure*) e gestão de acessos privilegiados (PAM: *Privileged Access Management*).

O IUTICE questiona também quais as medidas de segurança aplicadas pelas empresas, embora não enquadre a questão no caso específico do acesso remoto. Apesar de se verificar uma elevada percentagem de empresas a utilizar medidas como palavras-passe seguras (84%) e backups em local distinto (73,7%), apenas 44,2% indicaram utilizar VPN, contrastando com os 86% de OSE que recorrem a esta medida.

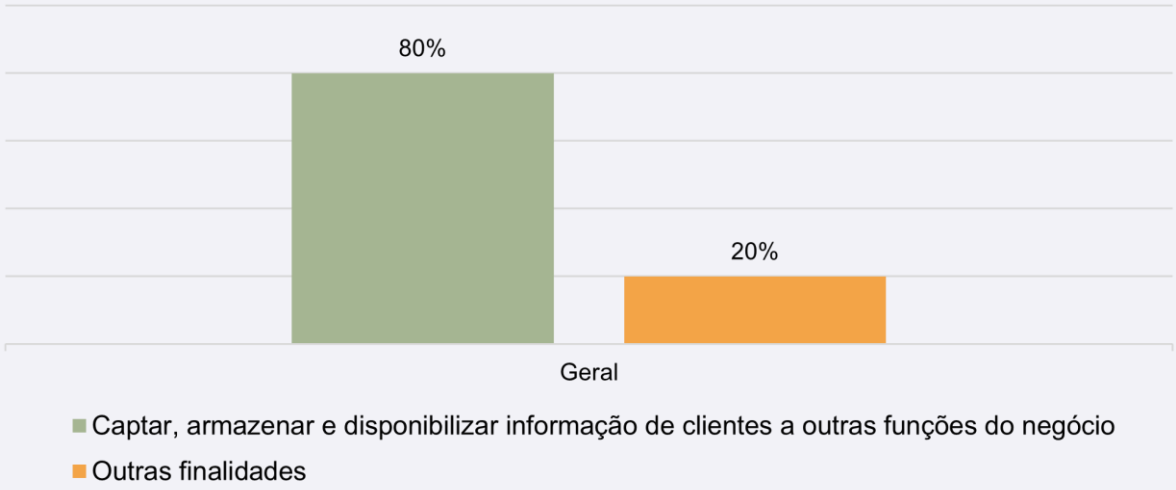
Gráfico 54 - OSE que utilizam Customer Relationship Management software (CRM)



São mais os operadores que não utilizam *software* de *Customer Relationship Management* (CRM)[28] - 62% - do que aqueles que utilizam - 38%. Curiosamente, nos dois setores da área financeira observa-se um grande contraste já que de todos os OSE do setor bancário utilizarem CRM e nenhum dos OSE das IMF utilizar este tipo de *software*.

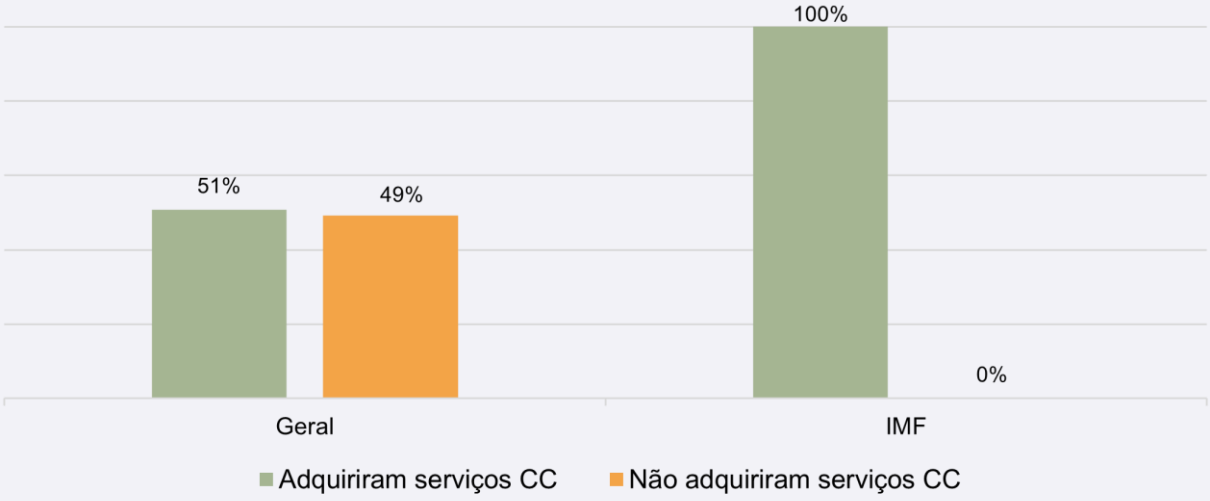
[28] *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos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

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



Entre os operadores que utilizam CRM, a maioria utiliza-o para captar, armazenar e disponibilizar informações de clientes a outras funções do negócio (80%). Os restantes 20% utilizam CRM para outros fins não especificados. Como o setor das infraestruturas do mercado financeiro mencionou não utilizar CRM, a questão não se aplica.

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



À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização.
Um dos setores que mais procurara este tipo de serviços foi o setor das infraestruturas do mercado financeiro, em que todos os inquiridos adquiriram este tipo de serviços.

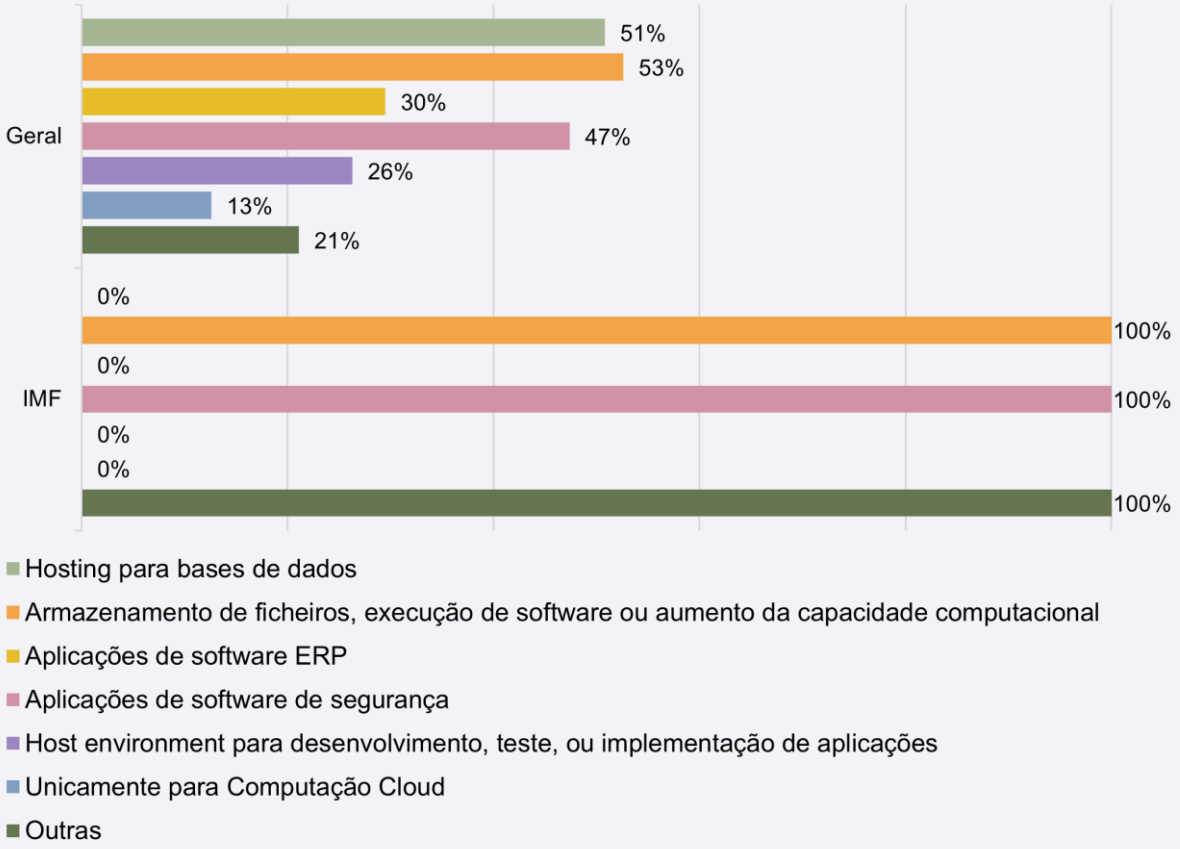
O relatório *NIS Investments* de 2022 demonstra que a procura por serviços *cloud* aumentou grandemente devido aos efeitos da pandemia, tendo sido uma prioridade de investimento nesse ano - cerca de 45% dos OSE colocaram o investimento em serviços *cloud* como um dos principais objetivos de 2021[29]. Em 2023, este tipo de serviços continuou a ser uma das áreas onde os OSE mais aumentaram o seu investimento (49% dos OSE inquiridos pela ENISA em 2023 indicaram ter aumentado os seus investimentos em plataformas *cloud*)[30]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[31].

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

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

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

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[32] aplicações de *software* de segurança, *host environment* para desenvolvimento, teste ou implementação de aplicações, e, por fim, exclusivamente para Computação *Cloud*.

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

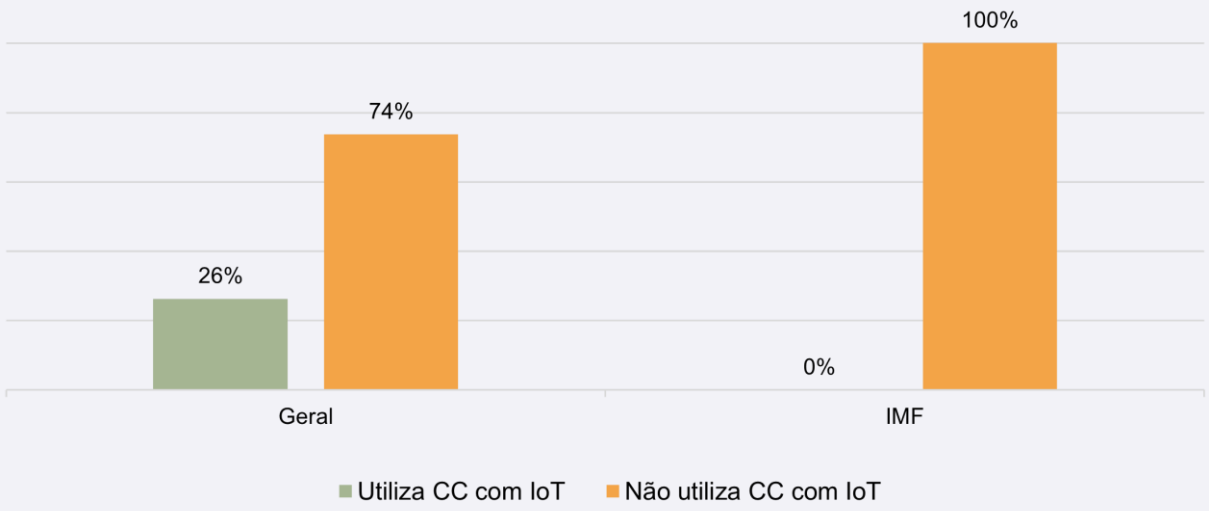
No setor das infraestruturas do mercado financeiro destacou-se a opção "Outras", que no caso deste setor contempla a utilização de Computação *Cloud* para suportar sistemas de e-mail e servidores DNS.

[32] *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.

A nível setorial, torna-se evidente que o armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional é uma das finalidades mais comuns no setor das infraestruturas do mercado financeiro, tendo sido indicada por 100% dos OSE deste setor. A utilização de serviços *cloud* para a utilização de *software* ou de aplicações de segurança é também uma das finalidades mais recorrentes neste setor, tendo sido indicada novamente por 100% dos OSE do mesmo.

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%)[33].

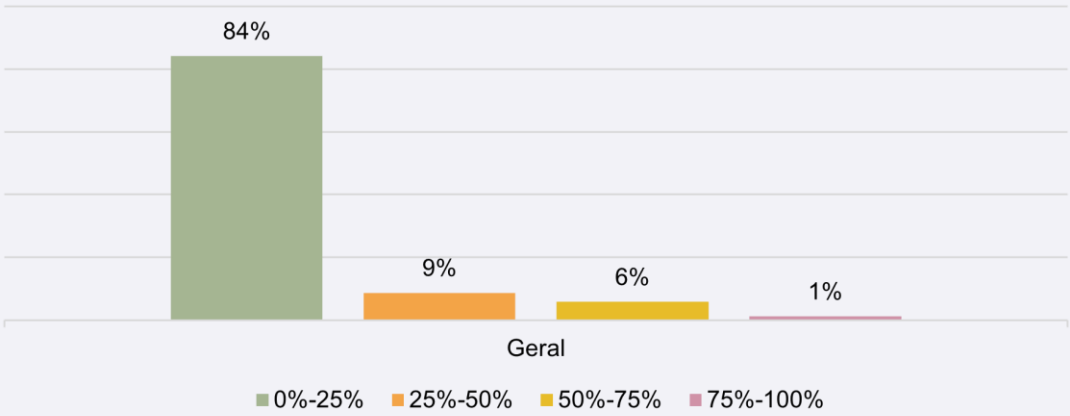
Gráfico 58 - Utilização de serviços de CC em conjunto com Internet of Things (IoT)



De modo geral, não é frequente, entre os OSE, a utilização de serviços de Computação *Cloud* (CC) em conjunto com a *Internet of Things* (IoT), embora alguns operadores o façam (26%). Especificamente, no setor das infraestruturas do mercado, nenhum operador utiliza CC com IoT.

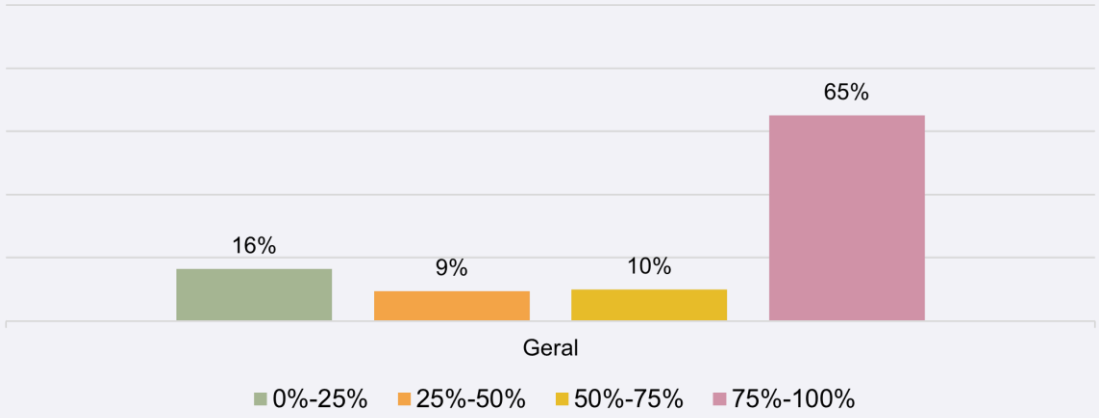
[33] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 59 - Percentagem de sistemas core em cloud



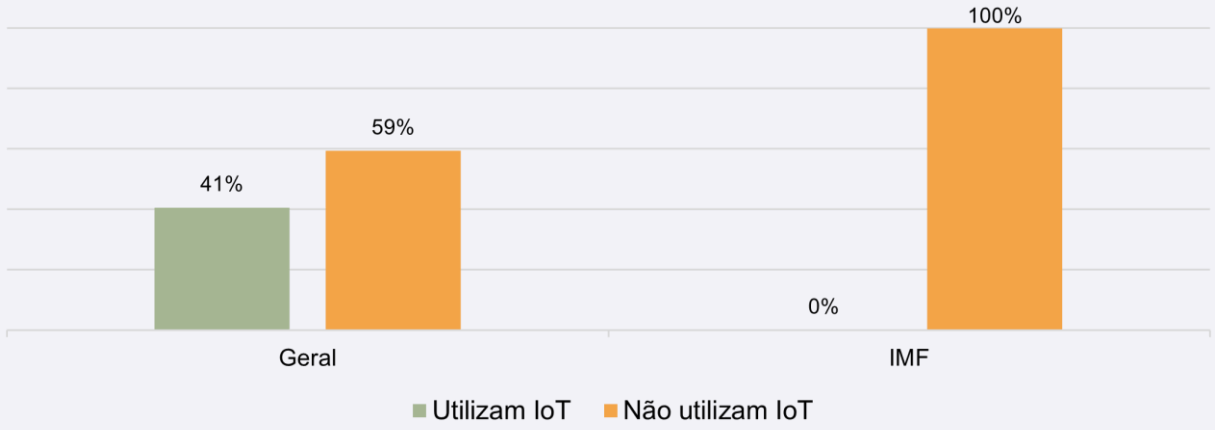
Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos.
No setor das infraestruturas do mercado financeiro, foi encontrado um erro nos dados obtidos, pelo que os mesmos tiveram de ser invalidados.

Gráfico 60 - Percentagem de sistemas core on-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. No setor das infraestruturas do mercado financeiro, foi encontrado um erro nos dados obtidos, pelo que os mesmos tiveram de ser invalidados novamente.

Gráfico 61 - Utilização de IoT pelos OSE

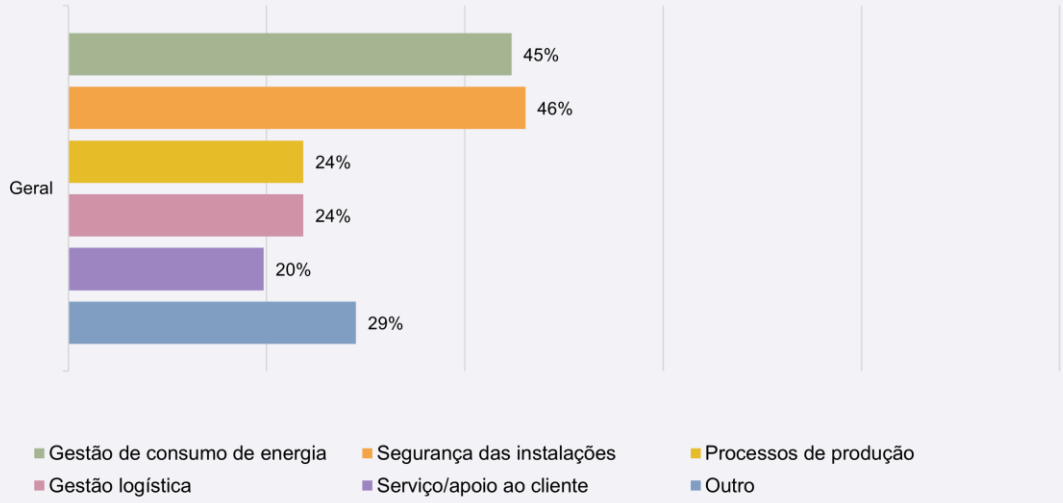


A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT. Destaca-se o setor das IMF, onde a totalidade dos inquiridos respondeu não utilizar de todo IoT.

De acordo com dados da ANACOM, no mercado empresarial, em 2021, aproximadamente 23% das empresas portuguesas com dez ou mais funcionários utilizaram dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente pela Internet, um aumento de 10 pontos percentuais em relação ao ano anterior. Portugal estava 6 p.p. abaixo da média da UE27, tendo ainda assim subido do 19.º para o 16.º lugar neste *ranking*. A utilização desses dispositivos tende a ser maior à medida que aumenta o tamanho da empresa, estando acima da média nas médias empresas (35%) e nas grandes empresas (46%). A estrutura do tecido produtivo português pode, portanto, explicar uma utilização relativamente menor dessas tecnologias em comparação com outros países. Por setor de atividade, a utilização de dispositivos interconectados monitorizados ou controlados remotamente pela Internet nos setores da eletricidade e da água foi de 41%[34].

[34] 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

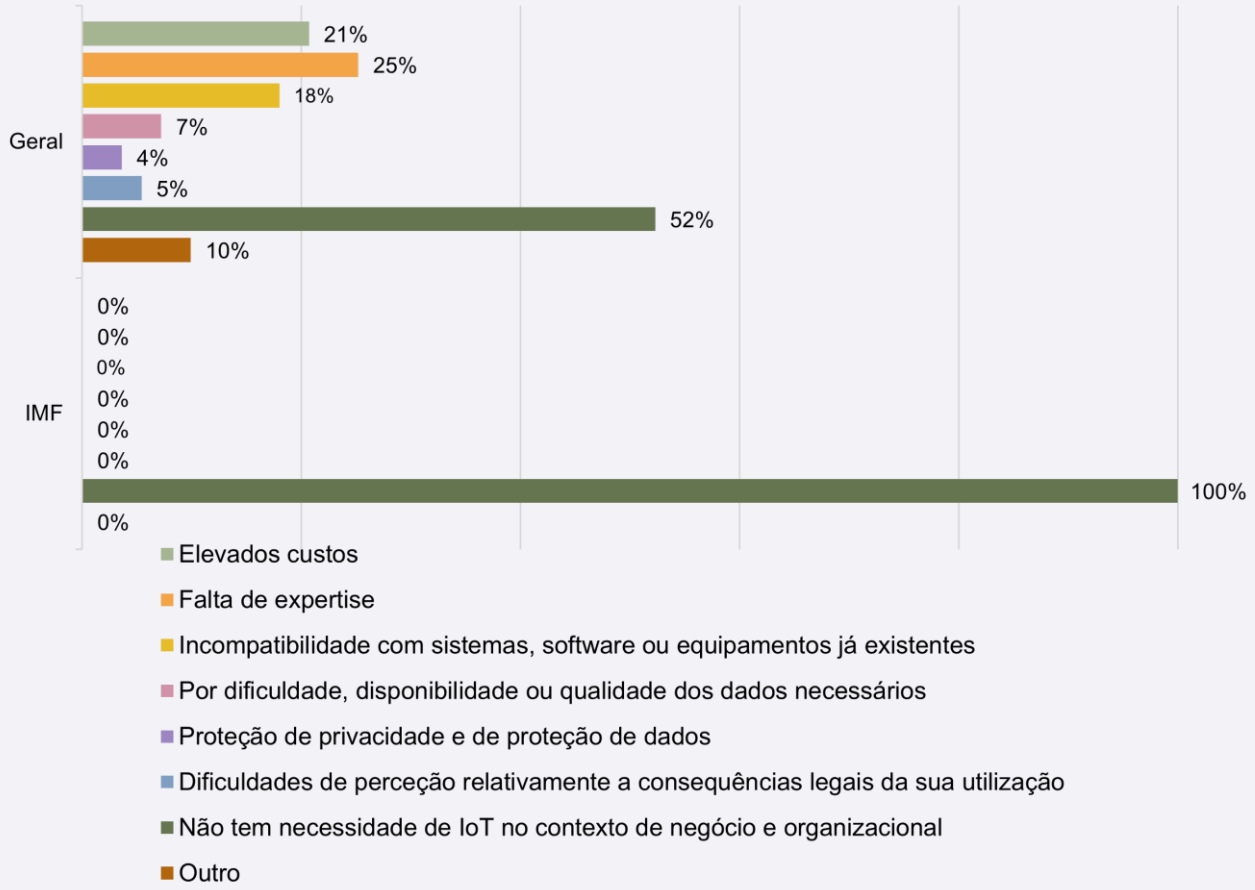


Dado que o setor das infraestruturas do mercado financeiro não possui operadores que utilizem IoT, não há dados relativos aos contextos da sua utilização nestes setores. De maneira geral, a utilização de IoT é mais comum nos contextos de gestão do consumo de energia e de segurança das instalações, respondido por cerca de 45% dos inquiridos, ao contrário da utilização de IoT para serviço/apoio ao cliente, que tem menos expressividade, cerca de 20%. A opção "Outro" contempla a utilização de IoT para fins de manutenção preditiva e de telemetria.

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%)"[35].

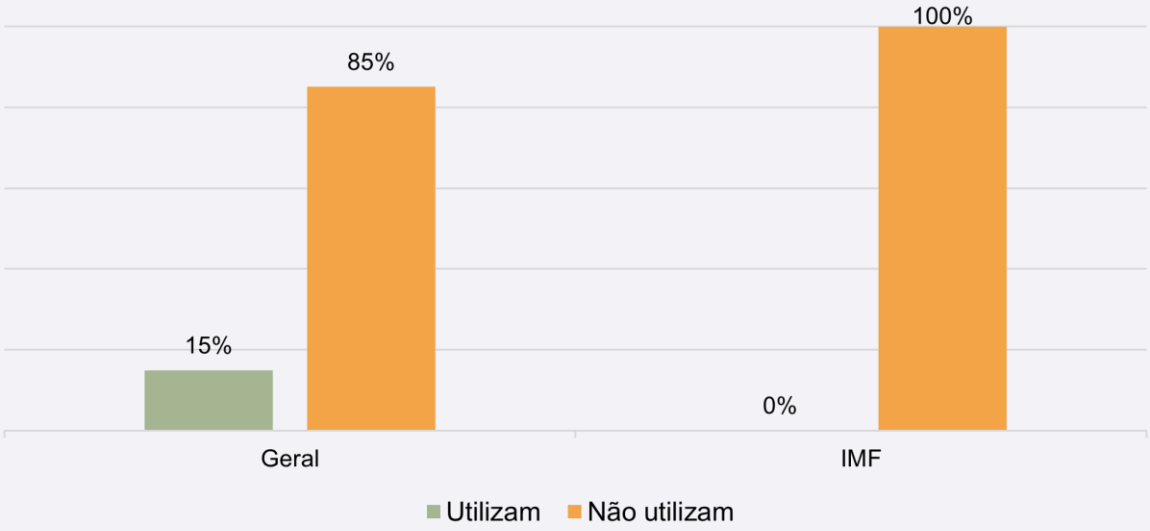
[35] ANACOM, "Utilização da Internet das Coisas (IoT - *Internet of Things*)", 2022, 17.

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%). O setor das infraestruturas do mercado financeiro menciona não sentir necessidade de IoT no contexto de negócio e organizacional.
Na opção “Outros”, foi sobretudo indicado que se estava a preparar a implementação de IoT na organização para os anos de 2024 e 2025.

Gráfico 64 - OSE que utilizam processos que recorrem a IA

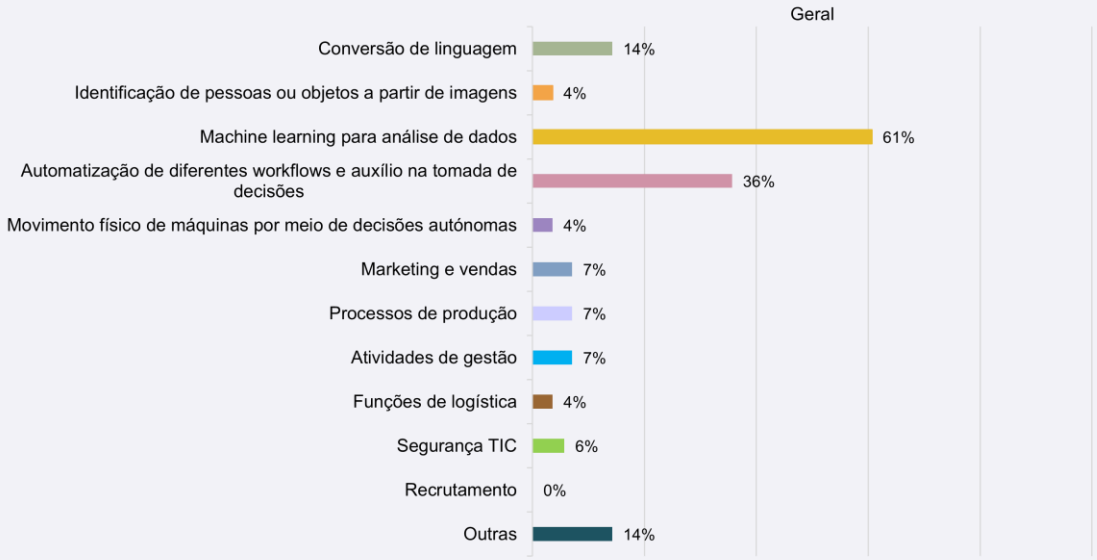


A utilização ou o recurso à IA é ainda reduzido entre os OSE. Apenas 15% dos inquiridos referem já utilizar ou recorrer a IA dentro das suas organizações.
Por norma, há pouca utilização de processos com recurso a Inteligência Artificial (IA) por parte dos operadores. Tal é verificável em todos os setores. Apenas no setor das infraestruturas do mercado financeiro não se registaram operadores a recorrer a Inteligência Artificial.

Comparando com dados do IUTICE de 2023, conclui-se que no universo dos Operadores de Serviços Essenciais há uma maior percentagem de empresas a já recorrer a Inteligência Artificial do que se se olhar para o panorama empresarial geral português. Enquanto 15% dos OSE indicaram já utilizar IA, apenas 7,9% das empresas declararam fazê-lo. Ainda no âmbito do IUTICE, o setor da indústria e energia continua a ser um dos que mais utiliza IA (8,8%), mas fica atrás de outros como o da informação e comunicação (29,8%)[36], quando no questionário do CNCS o setor da energia surge como aquele onde mais OSE utilizam Inteligência Artificial (33%). O IUTICE identifica também uma relação entre a dimensão das empresas e a utilização de IA - se separarem as empresas por dimensão (número de colaboradores), é possível constatar que são sobretudo as grandes empresas que já recorrem a IA (35,4%), e que essa utilização decresce quando se analisam PMEs: 16,4% das médias empresas utilizam IA e, no caso das pequenas empresas, esta percentagem é de apenas 5,8%[37].

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

Gráfico 65 - Funções para as quais utilizam IA



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

De acordo com os dados do IUTICE de 2023, entre as empresas que utilizam tecnologia de IA, 44,7% delas utilizam-na para identificar objetos ou pessoas através de imagens. Em seguida, 40,8% das empresas utilizam tecnologias que automatizam fluxos de trabalho ou auxiliam na tomada de decisão. Tecnologias para análise de linguagem escrita são utilizadas por 35% das empresas, apresentando um ligeiro. Já as tecnologias de aprendizagem automática para análise de dados, incluindo *deep learning*, são adotadas por 26,2% das empresas. A tecnologia de IA menos utilizada pelas empresas é a que permite a movimentação física de máquinas através de decisões autónomas baseadas na observação do meio ambiente, com apenas 8,3% de adoção.

No entanto, no setor da Indústria e Energia, essa tecnologia é mais prevalente, sendo utilizada por 15,3% das empresas que empregam IA[38].

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"[39]. 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%[40].

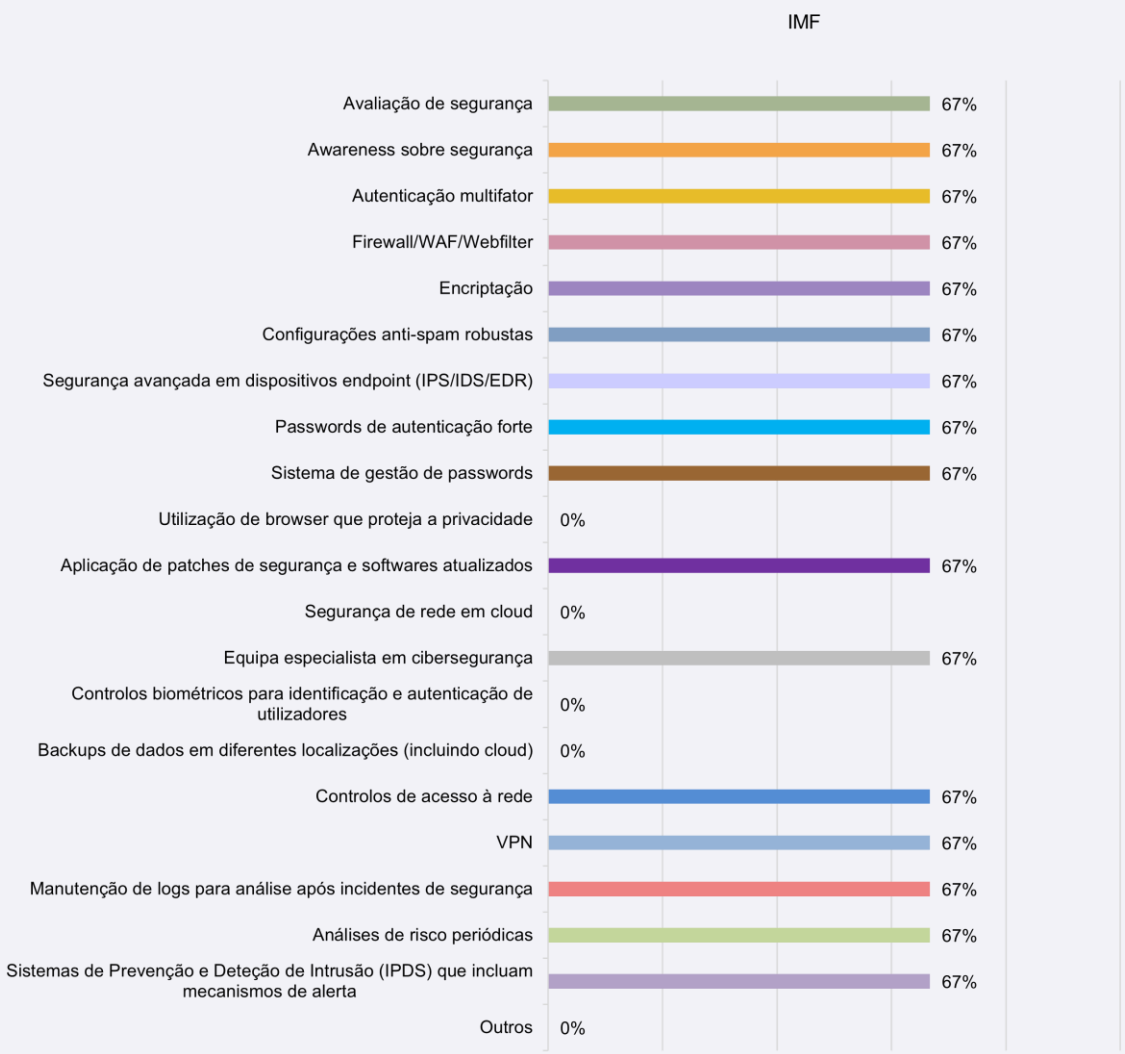
[38] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 17-18.

[39] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 9, https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.

[40] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 9.

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança

Gráfico 66.4 - 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.

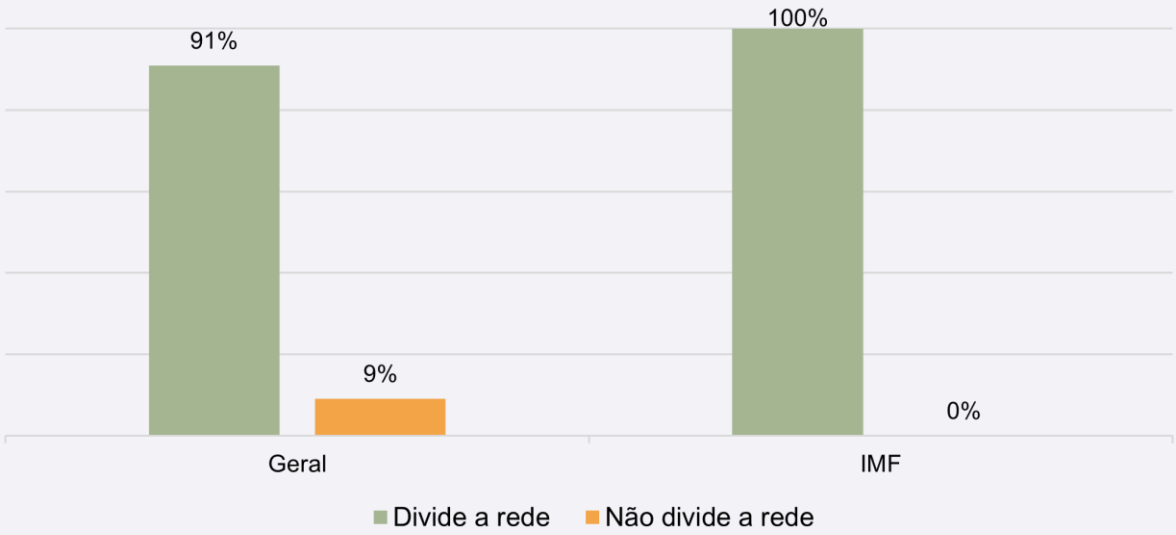
No setor das infraestruturas do mercado financeiro temos a exclusão da utilização de *browser* que projeta a privacidade, a segurança de rede em *cloud*, os controlos biométricos bem como os backups de dados.

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%[41].

Consta do estudo da Microsoft sobre o estado da cibersegurança em Portugal, que há um esforço já concretizado pelas organizações a nível nacional que importa destacar: 50% investiu mais em cibersegurança nos últimos anos, nomeadamente com a implementação de: antivírus e *malware* (81%), medidas de autenticação fortes para o acesso a sistemas críticos (71%), *firewalls* (61%), autenticação multifator (37%) e criptografia de dados, para proteger os ativos da empresa (36%)[42].

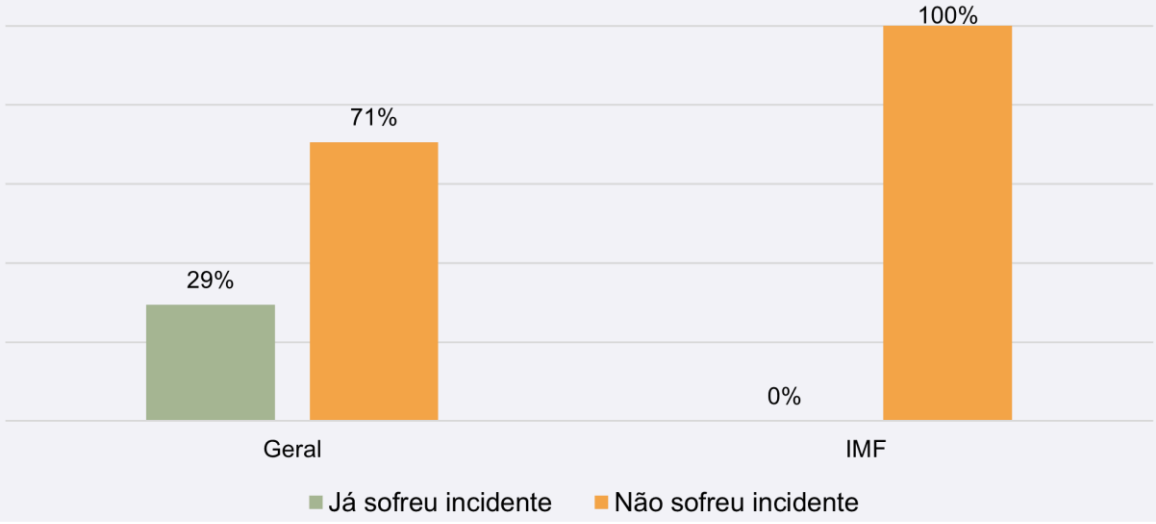
[41] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2022, 18.
[42] Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024, 7.

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%. Destaca-se o setor das infraestruturas do mercado financeiro onde 100% dos operadores referem fazer a divisão da rede.

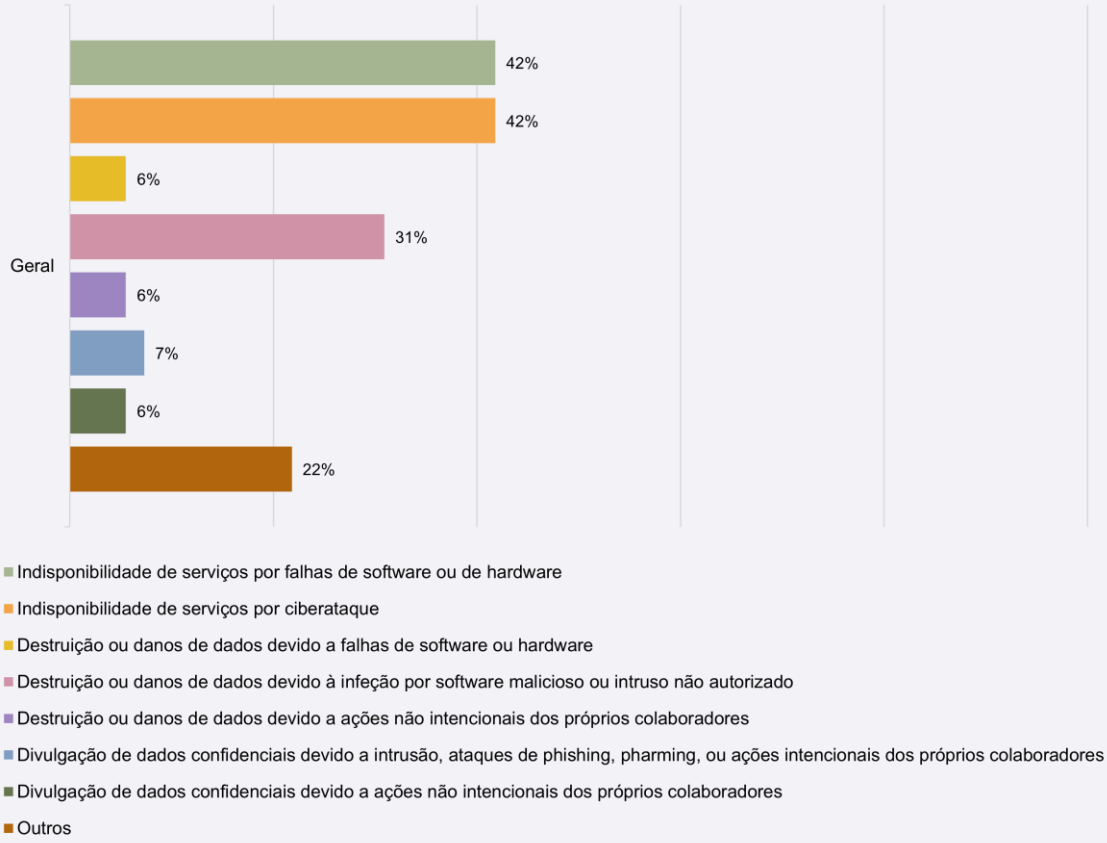
Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



Em contexto TIC, pelo observado no gráfico, conclui-se que a maioria dos OSE inquiridos (71%) não sofreu incidentes neste contexto. De acordo com os dados obtidos, o setor das infraestruturas do mercado financeiro não sofreu qualquer incidente.

Sendo o IUTICE de 2022, Portugal registou a segunda menor proporção de empresas com incidentes de segurança das TIC na União Europeia (UE). Em 2021, 89,7% das empresas em Portugal, e 91,8% no total da UE, utilizaram pelo menos uma medida para garantir a integridade, a disponibilidade e a confidencialidade dos seus dados e sistemas de Tecnologias de Informação e Comunicação (TIC)[43]. 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[44].

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.

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

[44] Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", janeiro de 2024, 5, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

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. O setor das infraestruturas do mercado financeiro mencionou nunca ter sofrido nenhum incidente logo a questão não se aplica.

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

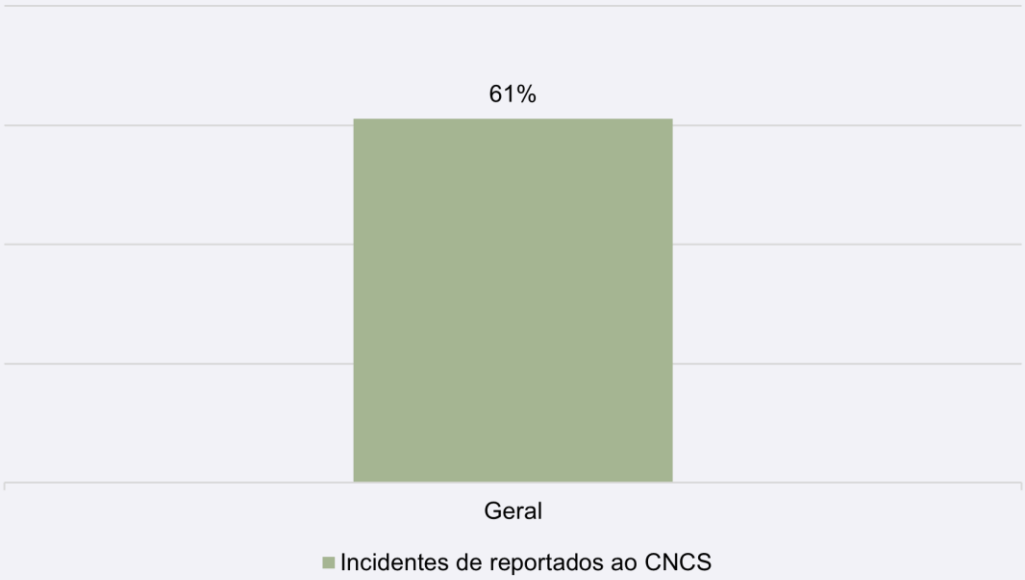
Segundo dados do IUTICE de 2022, em 2021, 11,5% das empresas experienciaram pelo menos um problema, seja de indisponibilidade de serviços TIC, de destruição ou corrupção de dados, ou de divulgação de dados confidenciais, devido a um incidente de segurança relacionado com as TIC. As consequências mais referidas destes incidentes foram a indisponibilidade de serviços TIC devido a falhas de *hardware* ou *software* e a ataques do exterior (8,3% e 2,5%, respetivamente), seguindo-se a destruição ou corrupção de dados devido a infeção de *software* malicioso ou intrusão não autorizada e devido a falhas de *hardware* ou *software* (2,1% e 1,8%, respetivamente)[45].

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[46].

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

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

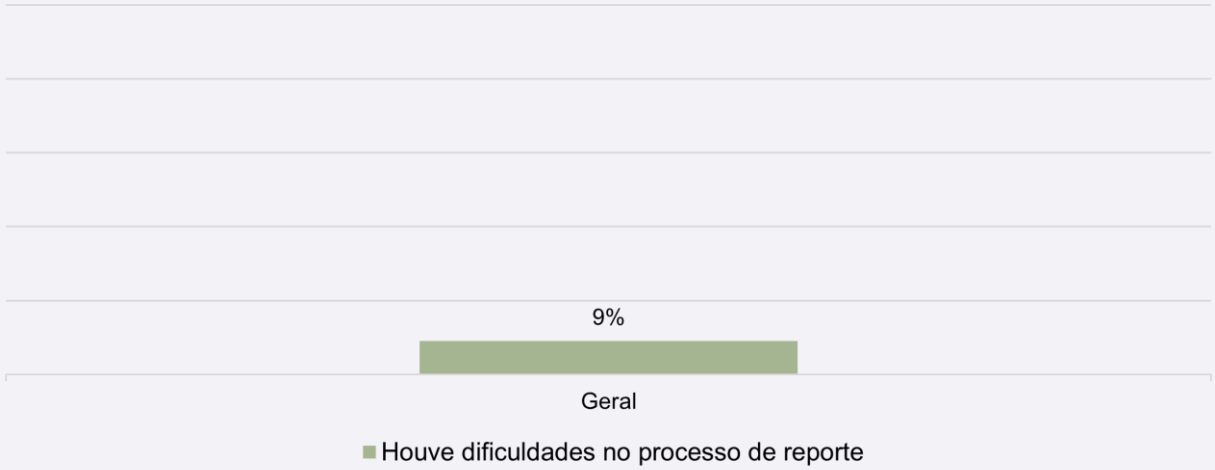
Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS



De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n. º1 do artigo 16.º da lei n. º46/2018, de 13 de agosto, os OSE estão apenas obrigados à notificação do incidente quando este tem "um impacto relevante na continuidade dos serviços essenciais por si prestados". A ausência desse impacto relevante na continuidade dos serviços foi um dos motivos para a não notificação do incidente, como se verificará no **Gráfico 75**.

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

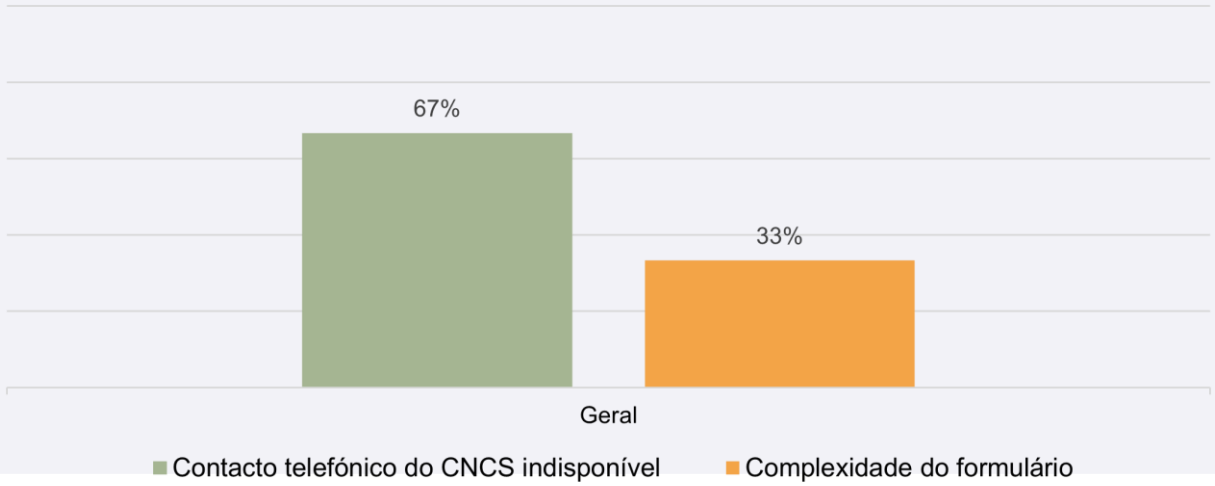
Gráfico 71 - Dificuldades no processo de notificação ao CNCS



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

Como o setor das infraestruturas do mercado financeiro não sofreu incidente, não existiram dificuldades no processo de notificação ao CNCS.

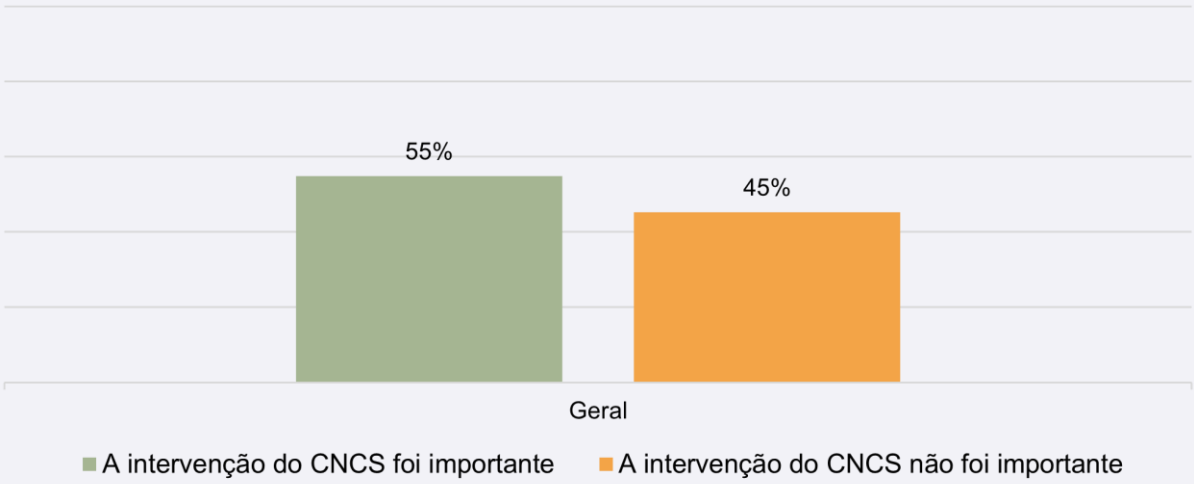
Gráfico 72 - Dificuldades encontradas pelos OSE durante a notificação de incidentes ao CNCS



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

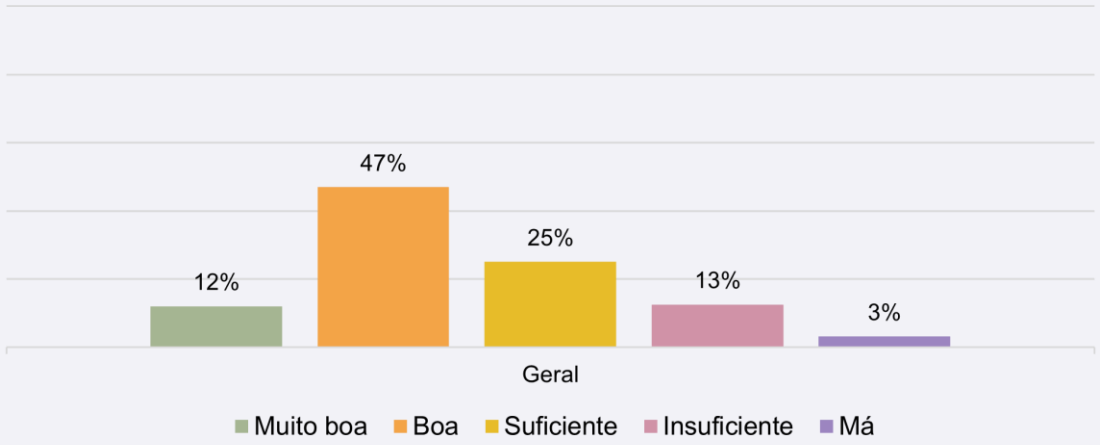
A questão anterior do setor das infraestruturas do mercado financeiro mantem-se.

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

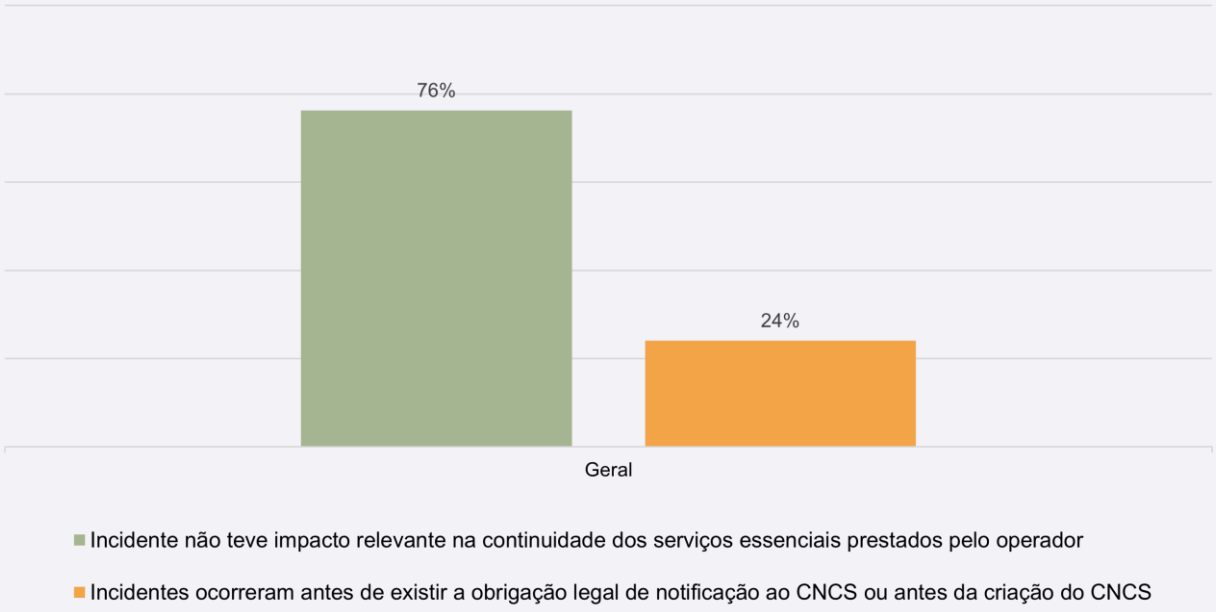
Gráfico 74 - Avaliação da resposta dada pelo CNCS



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%).

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

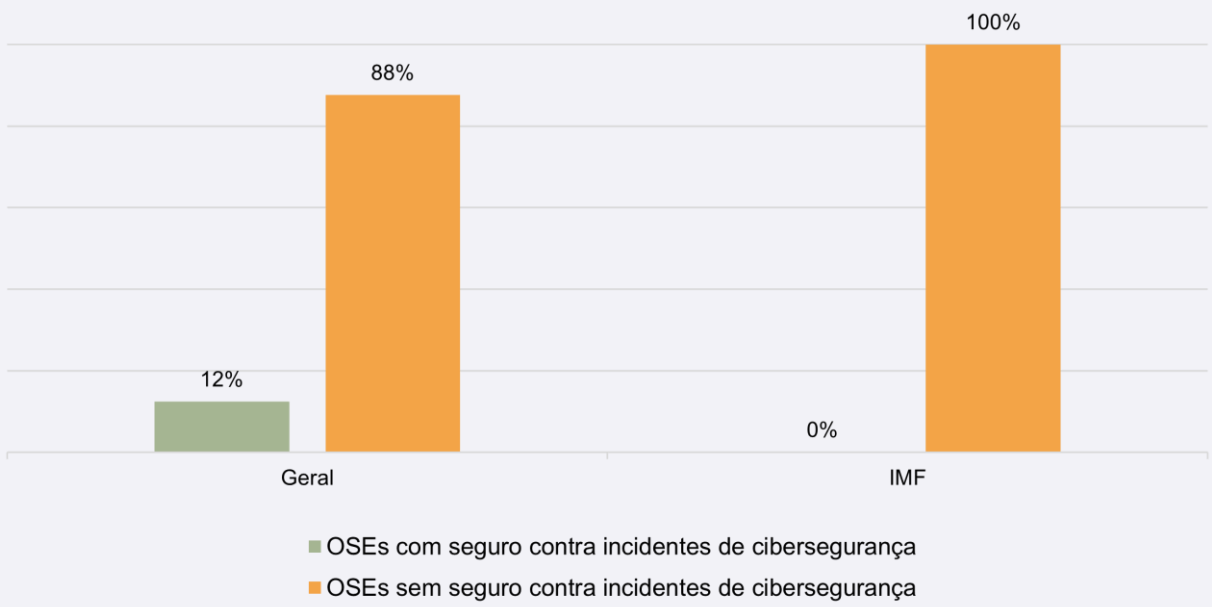
Gráfico 75 - Motivos para a não notificação de incidentes de cibersegurança ao CNCS



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

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

Gráfico 76 - Seguro contra incidentes de cibersegurança



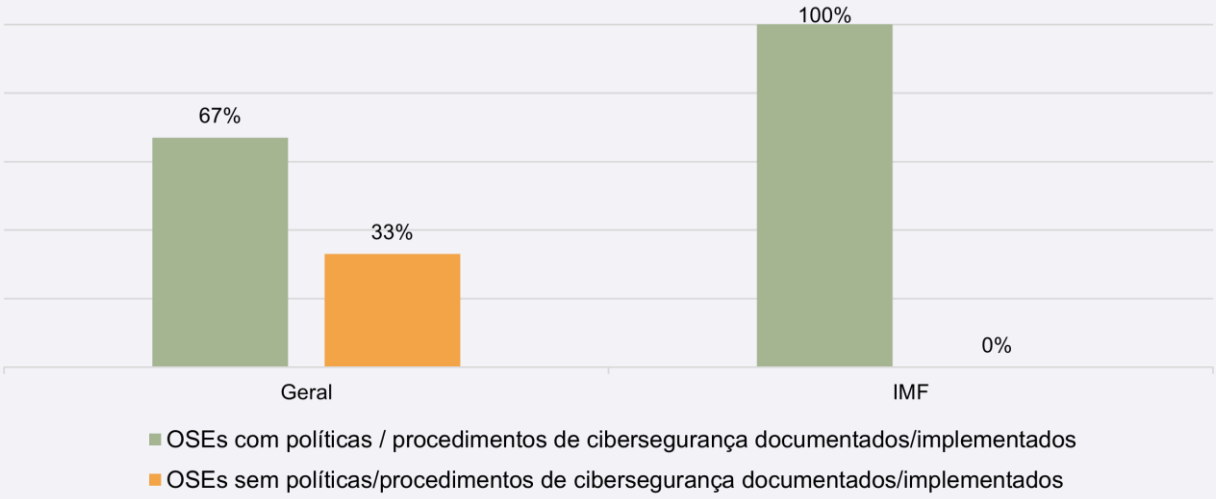
Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. Nenhum OSE do setor de infraestruturas do mercado financeiro possui seguro contra incidentes de cibersegurança.

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[47].

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[48].

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

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

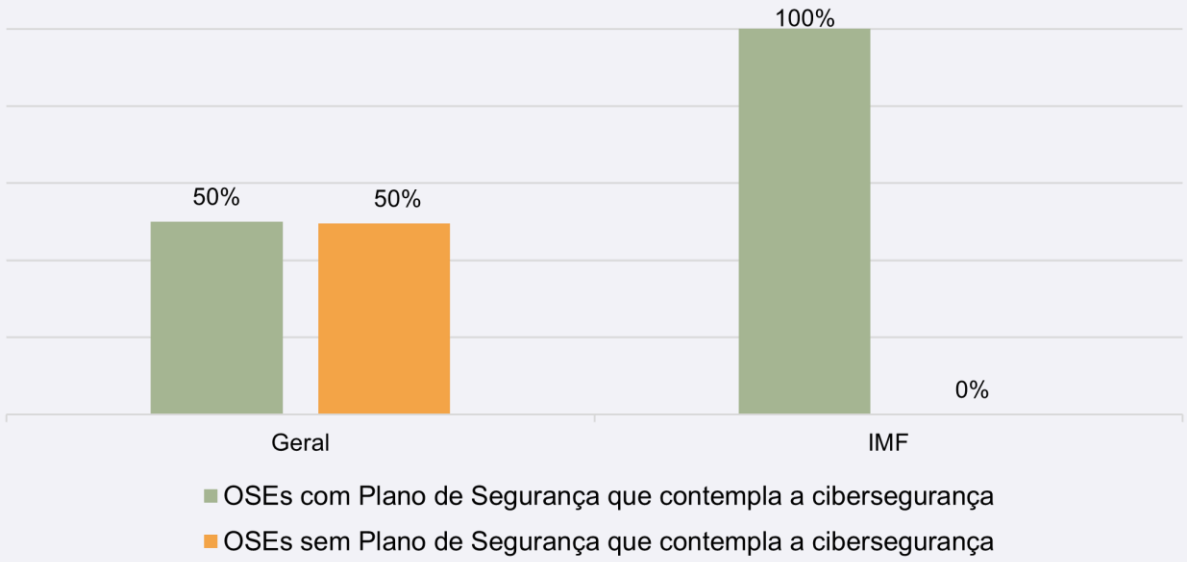


Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados. No setor das infraestruturas do mercado financeiro, todos os operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados.

Segundo dados do IUTICE, em 2022, cerca de 54.4% do total de empresas tinha documentos sobre medidas, práticas ou procedimentos em matéria de segurança[49].

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

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



O plano de segurança é obrigatório ao abrigo do decreto-lei n.º 65/2021, de 30 de julho. No entanto, metade dos operadores inquiridos, 50%, ainda não tem um plano de segurança que contemple a área da cibersegurança. O setor de infraestruturas do mercado financeiro é o único onde todos os inquiridos referem que já tem um plano de segurança que contemple a área da cibersegurança.

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[50].

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

Gráfico 79 - Políticas incluídas no Plano de Segurança

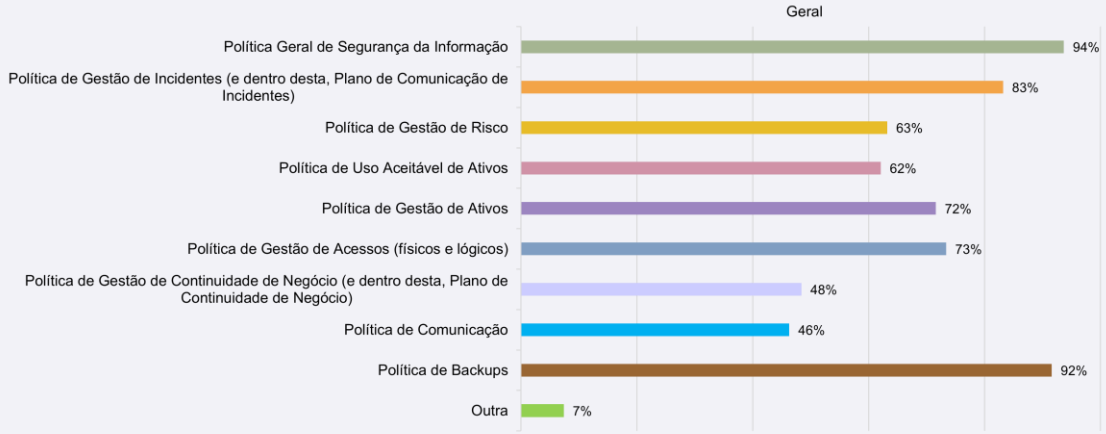
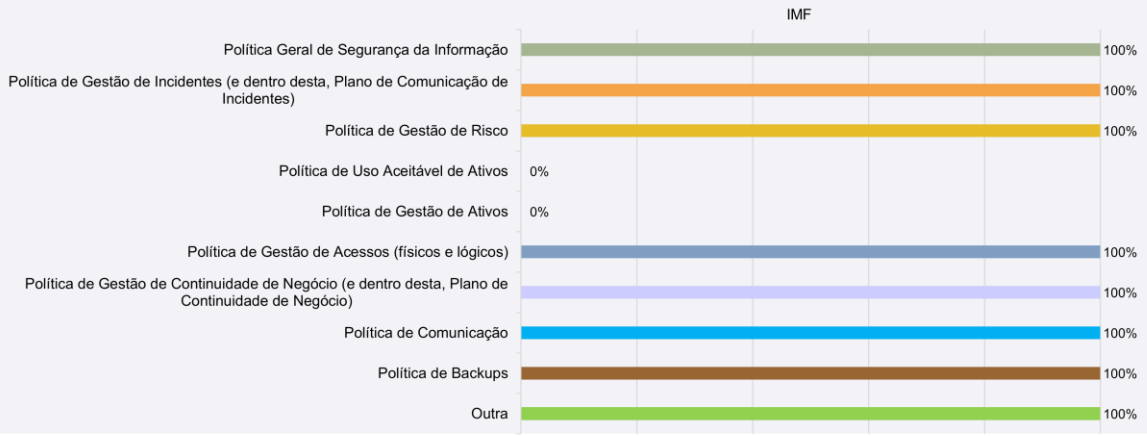


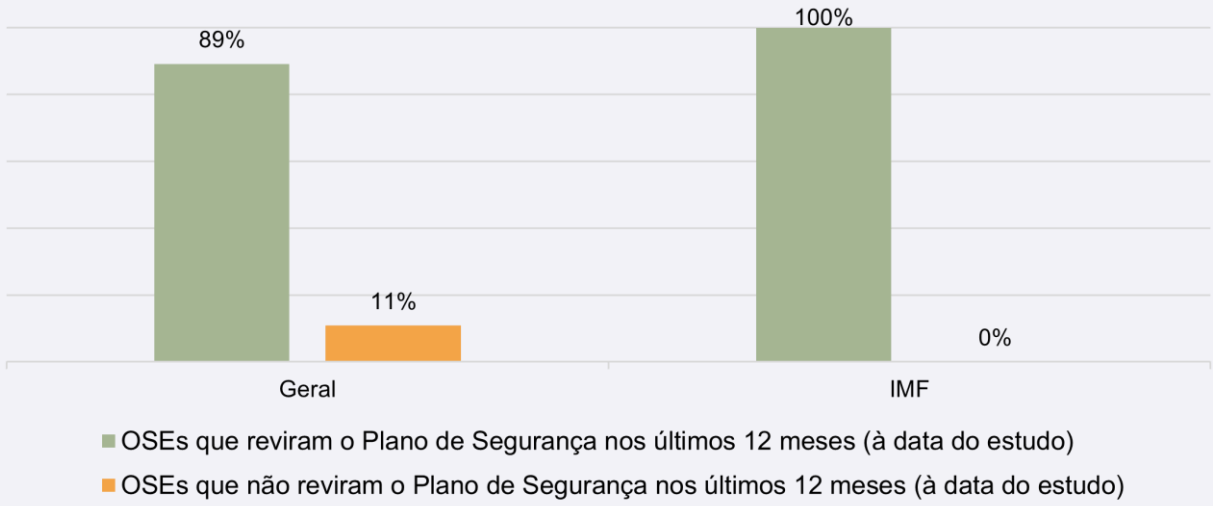
Gráfico 79.1 - Políticas incluídas no Plano de Segurança



Os gráficos acima representam a percentagem de operadores com plano de segurança que tem as diversas políticas elencadas elaboradas no âmbito desse mesmo plano.
As políticas mais comuns são a Política de Geral de SI (94%), a Política de Backups (92%), a Política de Gestão de Incidentes (83%), a Política de Gestão de Acessos (73%), a Política de Gestão de Ativos (72%), a Política de Gestão de Risco (63%) e a Política de Uso Aceitável de Ativos (62%). As políticas menos adotadas entre os operadores são a Política de Continuidade de Negócio (48%) e a Política de Comunicação (46%).
Entre as "outras" políticas (7%), contam-se a Política de Utilização de Correio Eletrónico, Política de *Passwords*, Política de Teletrabalho, Política de Classificação e Manuseamento de Informação, Política de Segurança Física, Política de Gestão de Alterações, Política de Criptografia, Política de Recursos Humanos para a Cibersegurança e Política de Privacidade e Proteção de Dados.

O setor das IMF não inclui no plano de segurança a política de uso aceitável de ativos nem a política de gestão de ativos.

Gráfico 80 - Revisão do Plano de Segurança



Cerca de 89% dos operadores com plano de segurança fizeram a revisão anual do mesmo nos últimos 12 meses, à data do estudo, seguindo as exigências do artigo 7º do decreto-lei nº 65/2021. Entre estes, destacam-se os operadores do setor das infraestruturas do mercado financeiro, no qual todos os operadores com plano de segurança realizaram a revisão anual deste.

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[51].

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

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

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

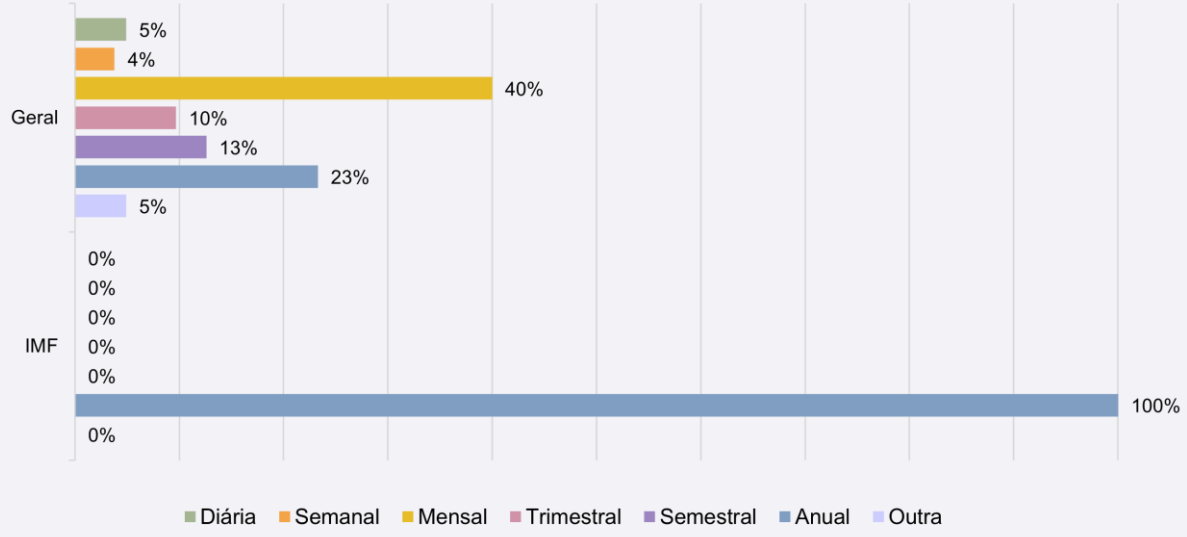
O setor das infraestruturas do mercado financeiro surge uma vez mais em destaque, uma vez que todos os operadores inquiridos realizam também procedimentos de deteção e gestão de vulnerabilidades.
Nos restantes setores, a percentagem de operadores que realiza estes procedimentos ultrapassa os 60%, com exceção de um, que fica aquém desse valor, fixando-se próximo dos 51%.

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

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

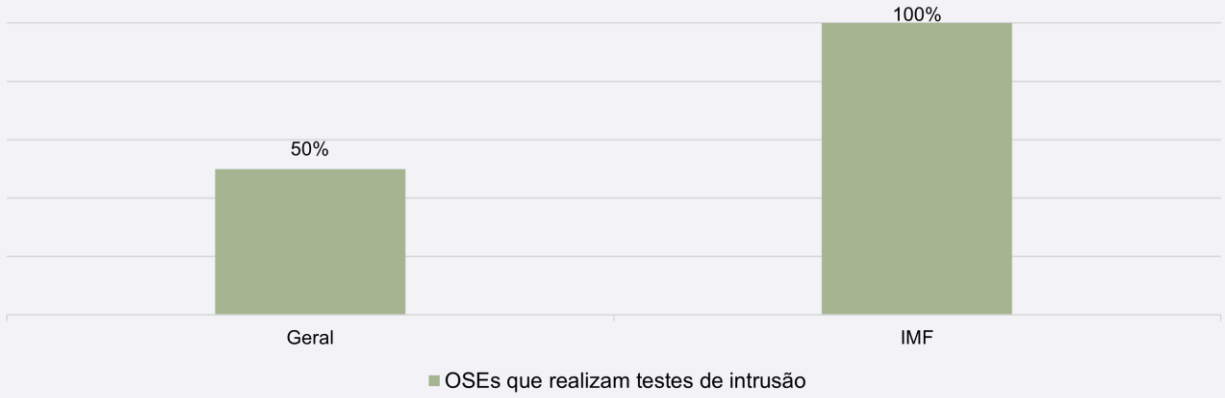
No setor das infraestruturas do mercado financeiro, todos os operadores que já realizavam procedimentos de deteção e gestão de vulnerabilidades, fazem também a análise das mesmas.

Gráfico 83 - Frequência da análise de vulnerabilidades



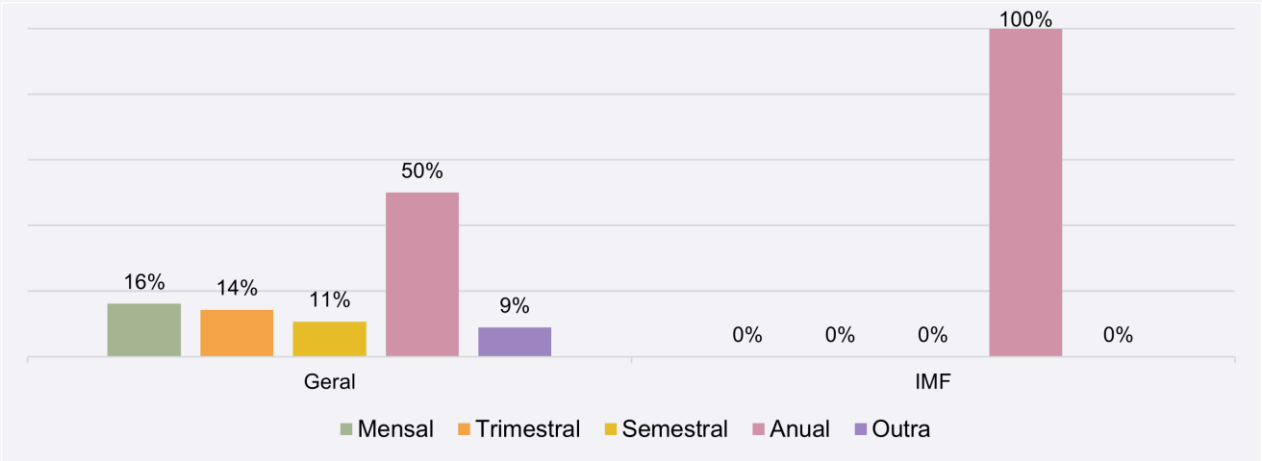
A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.
Destaca-se o setor das infraestruturas do mercado financeiro, no qual todos os operadores indicaram realizar análise de vulnerabilidades com frequência anual.
A frequência semanal é a menos observada, há ainda operadores, embora poucos, que realizam análise de vulnerabilidades diariamente.

Gráfico 84 - Realização de testes de intrusão



Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).
Há que destacar o setor das infraestruturas do mercado financeiro, no qual todos os inquiridos referiram realizar testes de intrusão.

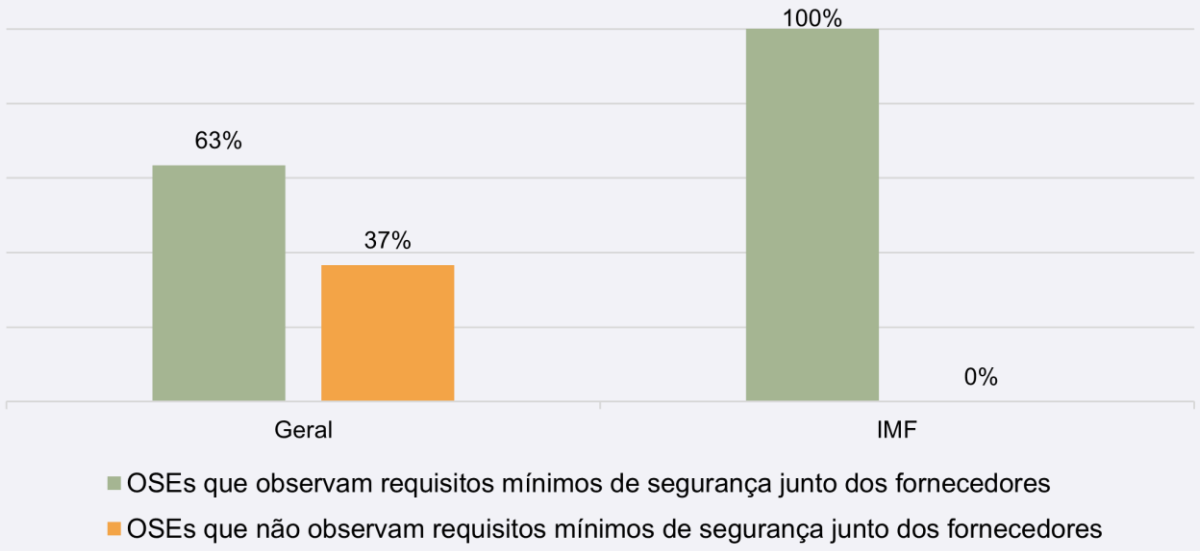
Gráfico 85 - Frequência de testes de intrusão



Com exceção de apenas dois setores, os operadores dos setores tendem a realizar testes de intrusão anualmente.
Uma das exceções verificadas prende-se com o facto de todos os operadores realizarem esses testes com uma frequência superior à anual e semestral. Entre os inquiridos, uma minoria realiza testes de intrusão pelo menos trimestralmente, sendo que a maioria realiza mensalmente ou de forma ainda mais frequente, para que os testes possam ser realizados por secções ou áreas da organização.

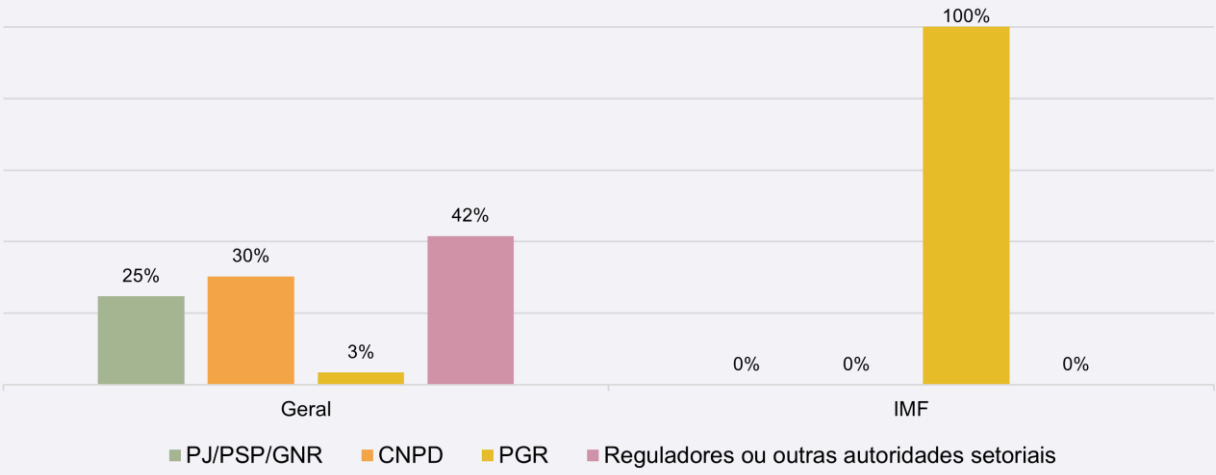
De salientar um dos setores onde 43% indicaram realizar testes de intrusão com uma frequência também superior à mensal porque há operadores que os realizam de forma contínua, operadores que conduzem estes testes sempre que as versões das aplicações utilizadas são atualizadas e operadores que realizam estes testes sempre que novos ativos são introduzidos.
Apenas no setor nas infraestruturas do mercado financeiro se registou a mesma frequência entre todos os operadores - os testes de intrusão são realizados anualmente.
Nos restantes setores, embora prevaleça a periodicidade anual para estes testes, é possível verificar operadores a optar por períodos mais curtos entre cada momento de teste.

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



Na generalidade, e também em cada setor, a maioria dos operadores (mais de 60%) procura que os seus fornecedores estejam alinhados com os requisitos mínimos de segurança por si exigidos. Novamente, destaca-se o setor das infraestruturas do mercado financeiro, no qual se verifica, para todos os operadores, a observação de requisitos mínimos de segurança por parte dos seus fornecedores.

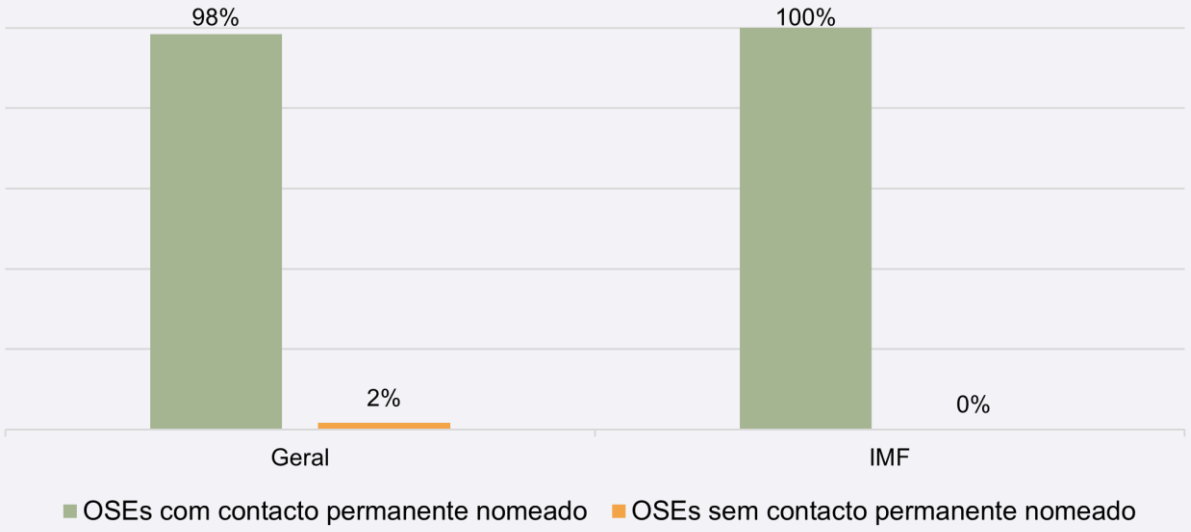
Gráfico 87 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS



Embora não seja obrigatório, cerca de 40% dos operadores optam por notificar as entidades reguladoras do seu setor ou outras autoridades setoriais caso sofram um ciberataque ou incidente de cibersegurança.
Apenas uma quantidade muito reduzida dos operadores tem previsto fazer qualquer tipo de notificação à Procuradoria-Geral da República (PGR).
A Comissão Nacional de Proteção de Dados (CNPD) surge em 2º lugar nas intenções de notificação em caso de ciberataque/incidente dos inquiridos, estando em 3º lugar as intenções de notificação à PJ/PSP/GNR.
Em caso de ciberataque os OSE concordam em contactar, para além do CNCS, os reguladores ou outras entidades setoriais. Verifica-se que contactar a PGR foi a opção com menos destaque seguida do CNPD.
Destaca-se os setores das infraestruturas do mercado financeiro, onde, no caso do primeiro, todos os inquiridos referem optar por contactar a PGR e, no caso do último, uma minoria. De referir que nenhum dos outros setores optou, em algum caso, contactar a PGR.

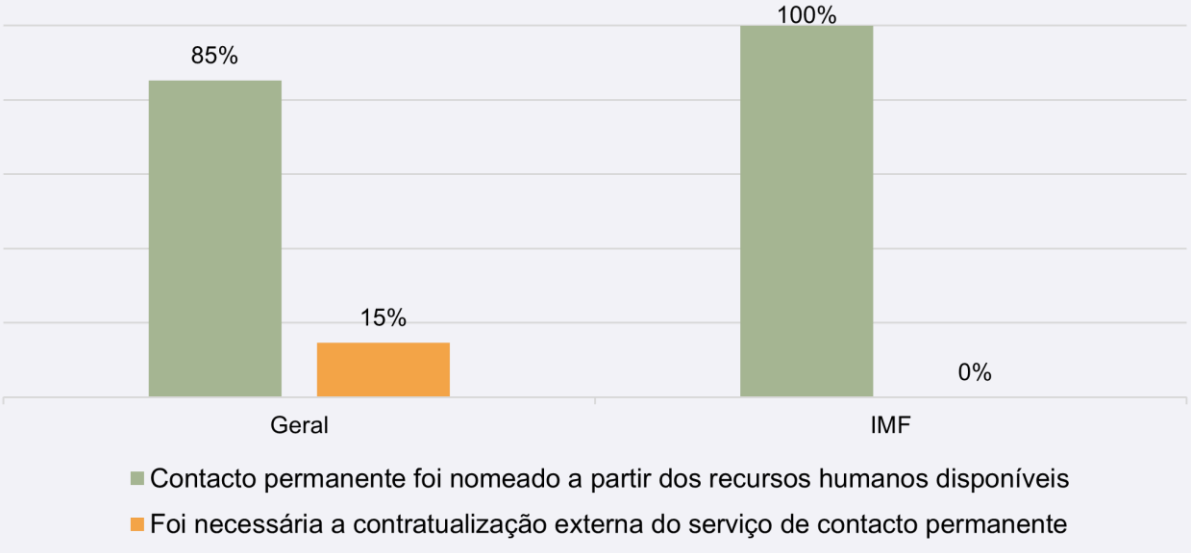
Os restantes setores privilegiam a notificação aos reguladores ou outras entidades setoriais em caso de ciberataque ou incidentes. Depois destas entidades encontra-se a PJ/PSP/GNR.

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



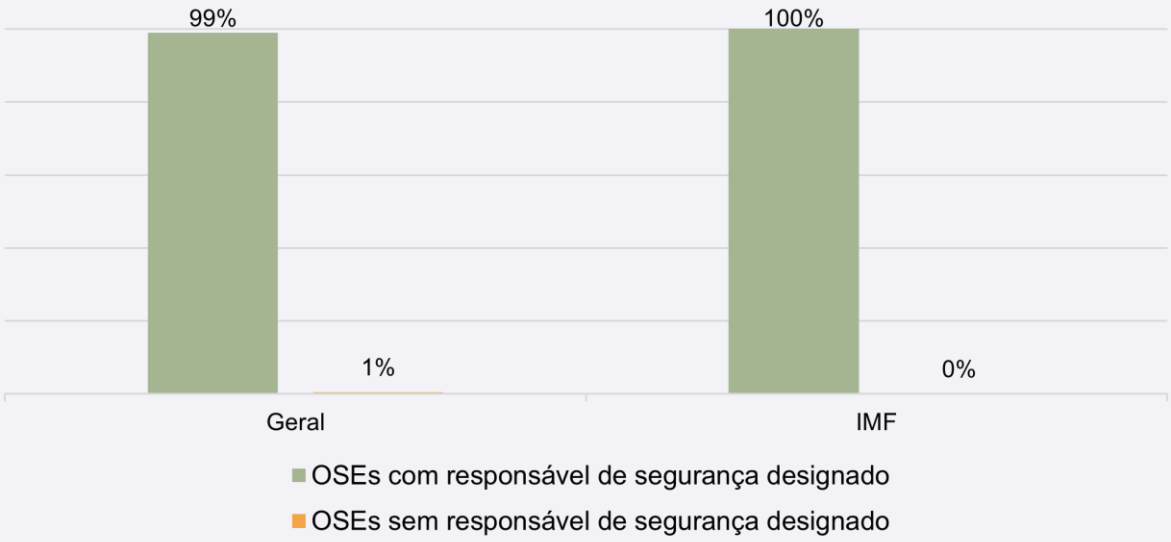
98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado.
Verificam-se exceções em dois setores onde houve uma entidade inquirida que ainda não tinha nomeado o contacto permanente.

Gráfico 89 - Designação do contacto permanente



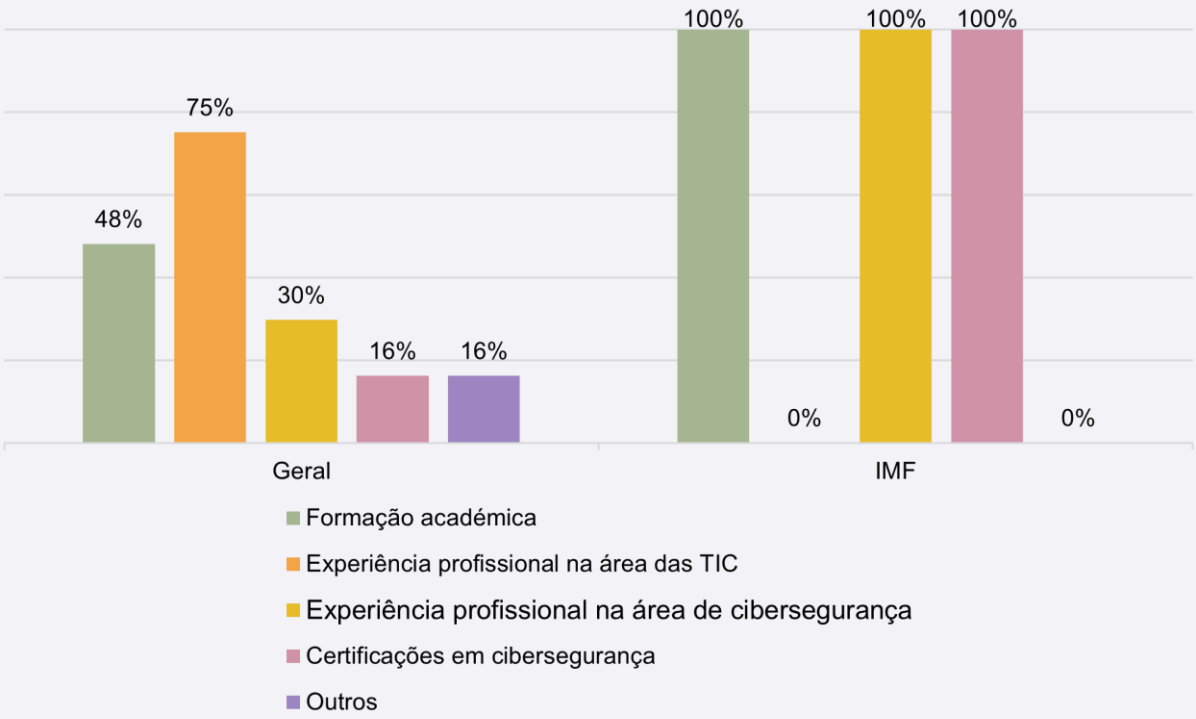
A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No entanto, houve ainda alguns operadores que tiveram de recorrer à contratualização externa do serviço de contacto permanente.
É de salientar, também, o setor das infraestruturas do mercado financeiro, no qual todos os inquiridos nomearam o contacto permanente a partir dos recursos humanos disponíveis.

Gráfico 90 - Designação do responsável de segurança



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

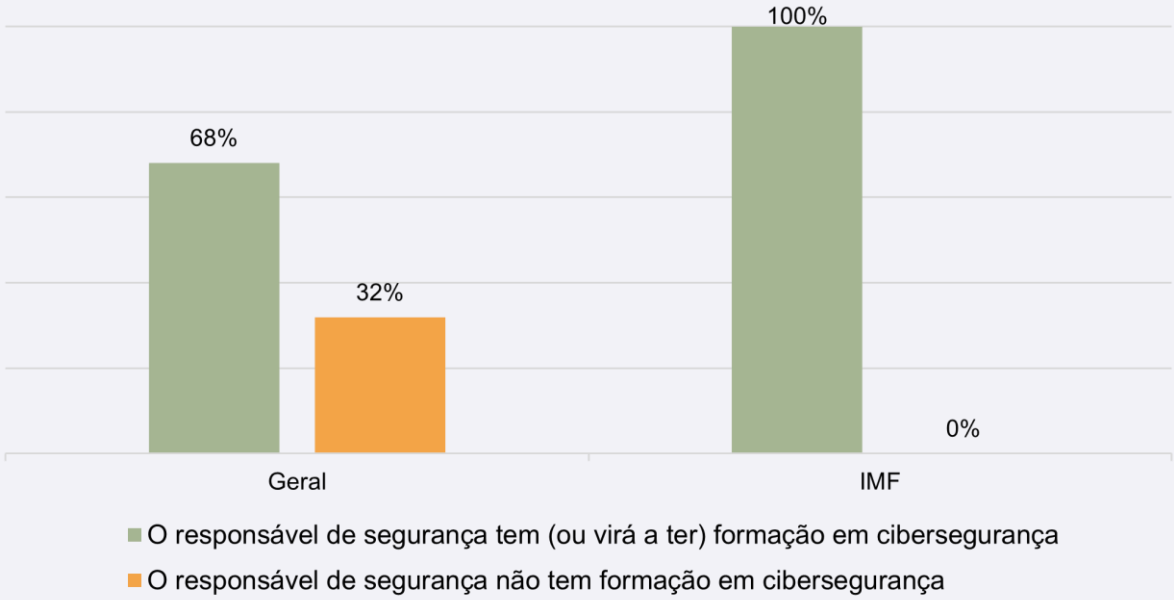
Gráfico 91 - Critérios utilizados para a designação do responsável de segurança



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

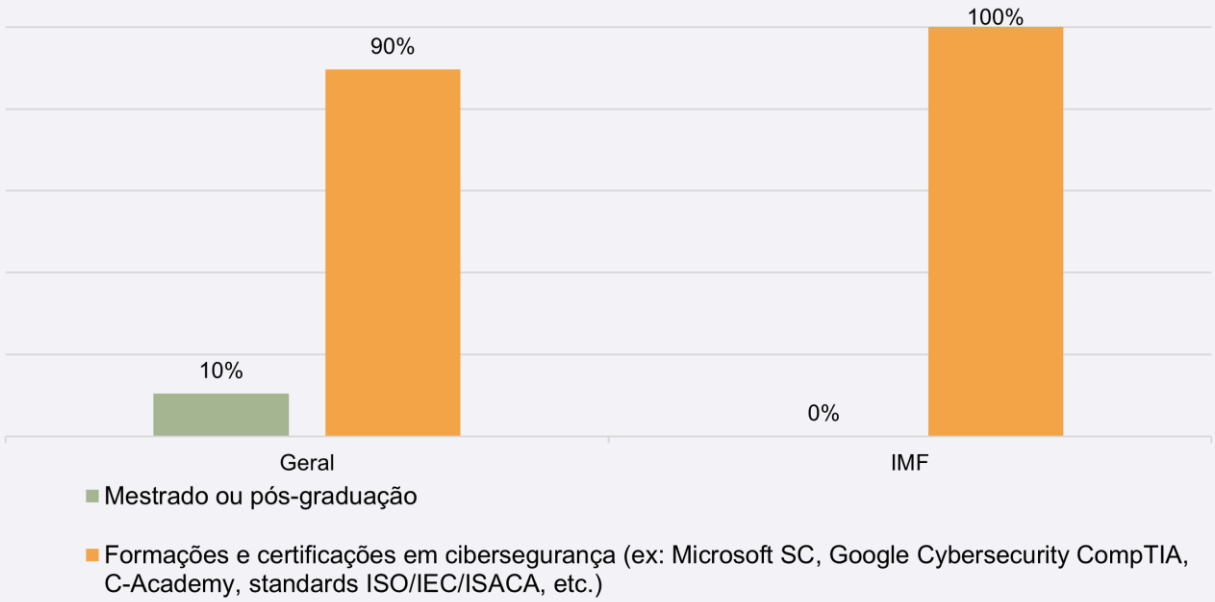
É também importante referir que se verificaram casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de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

Gráfico 92 - Formação específica de cibersegurança do responsável de segurança



Em cerca de 70% dos casos, o responsável de segurança tem ou virá a ter formação específica em cibersegurança. No setor das infraestruturas do mercado financeiro, todos os responsáveis de segurança designados têm ou virão a ter formação nesta área.

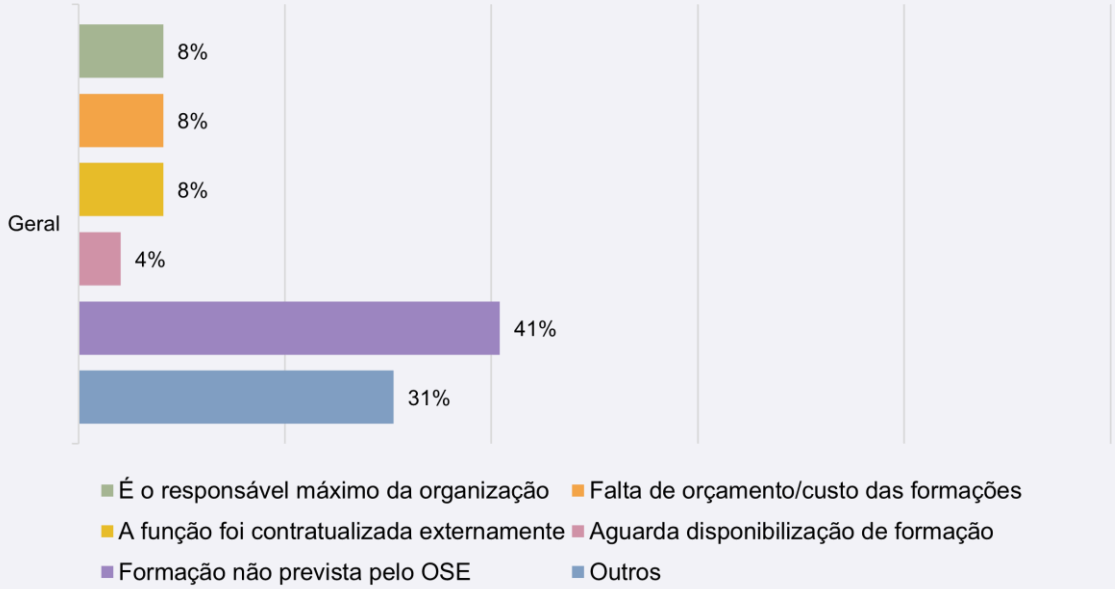
Gráfico 93 - Tipo de formação específica em cibersegurança



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.

De referir que no setor das infraestruturas do mercado financeiro, registam-se responsáveis de segurança somente com formações e certificações, sem mestrados ou pós-graduações.

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



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.

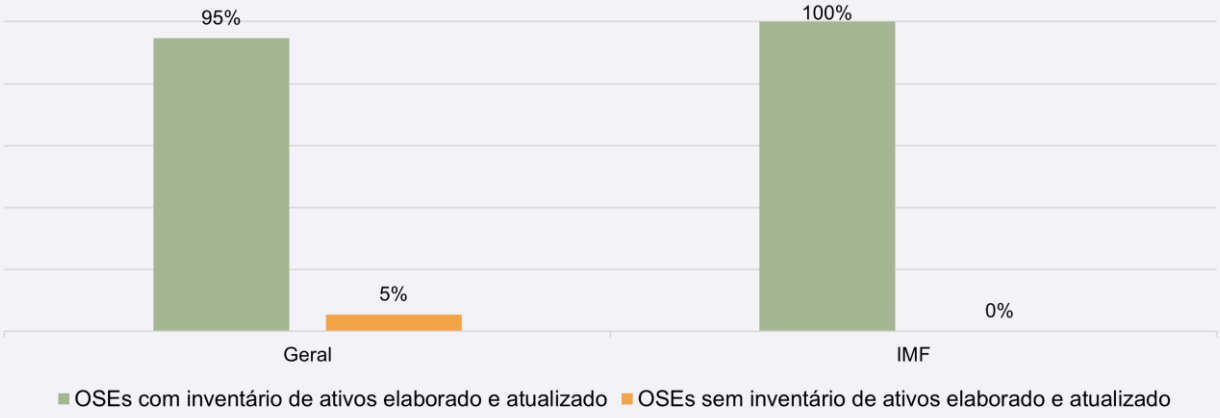
Tal como já referido, houve também situações em que a nomeação do responsável de segurança pouco teve que ver com a formação ou conhecimento em cibersegurança da pessoa nomeada, tendo em cerca de 10% dos casos sido nomeado o responsável máximo da organização. A falta de orçamento foi indicada também 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.

Visto a totalidade dos inquiridos do setor das infraestruturas do mercado financeiro terem formação em cibersegurança a questão não se aplica.

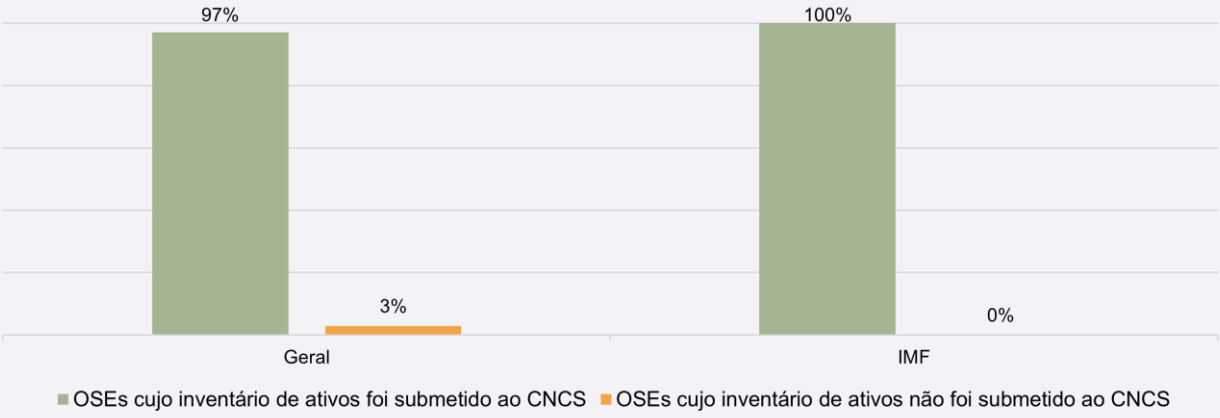
Como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado “Compromisso C-Academy” que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança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



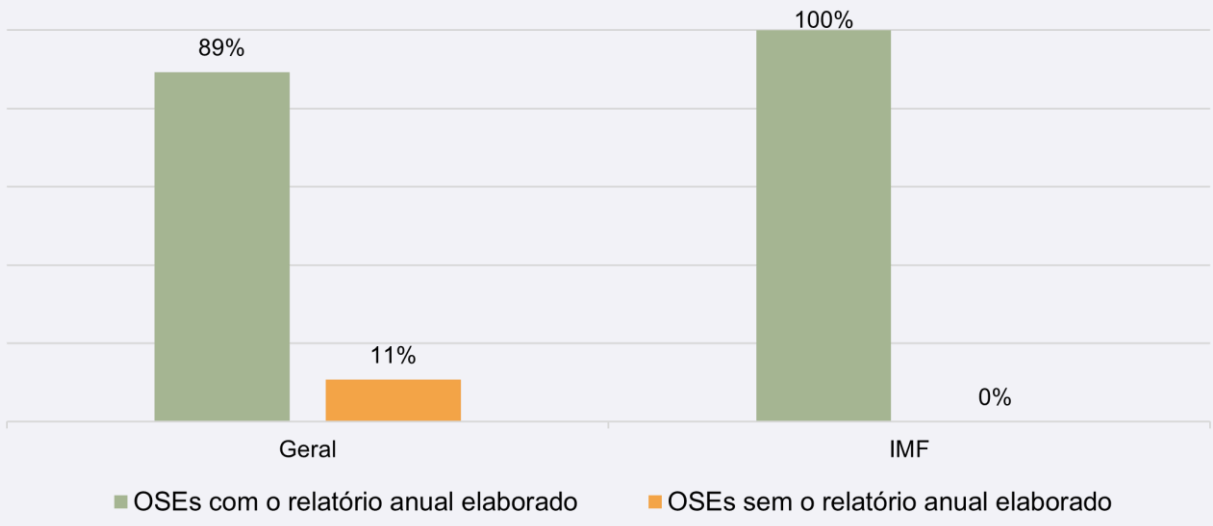
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. Destaca-se o setor das infraestruturas do mercado financeiro, no qual todos os operadores têm o seu inventário elaborado e atualizado.

Gráfico 96 - Submissão do inventário de ativos ao CNCS



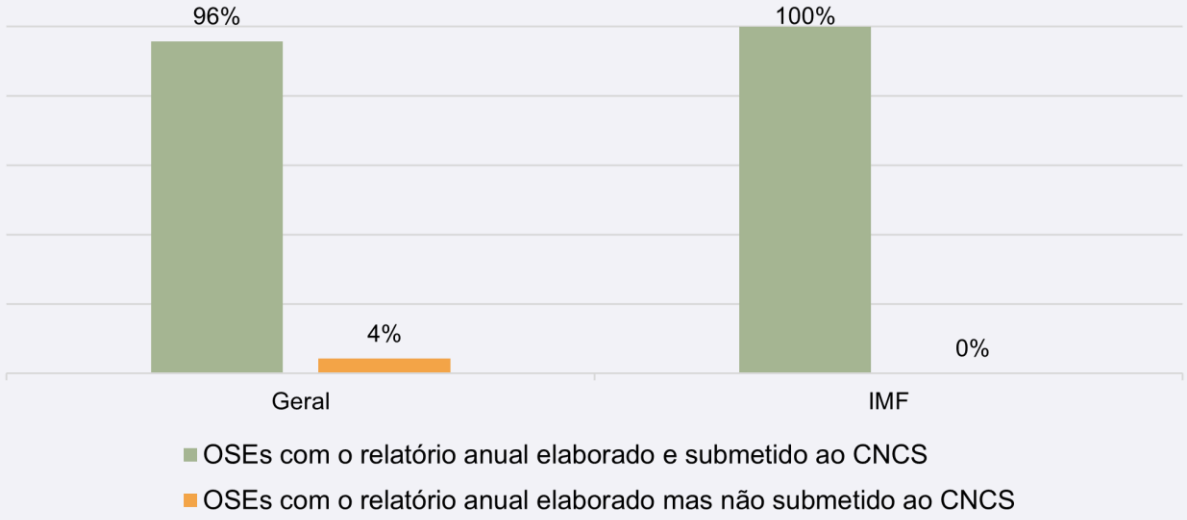
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. No setor das infraestruturas do mercado financeiro todos os operadores com inventário de ativos elaborado efetuaram a submissão do mesmo.

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



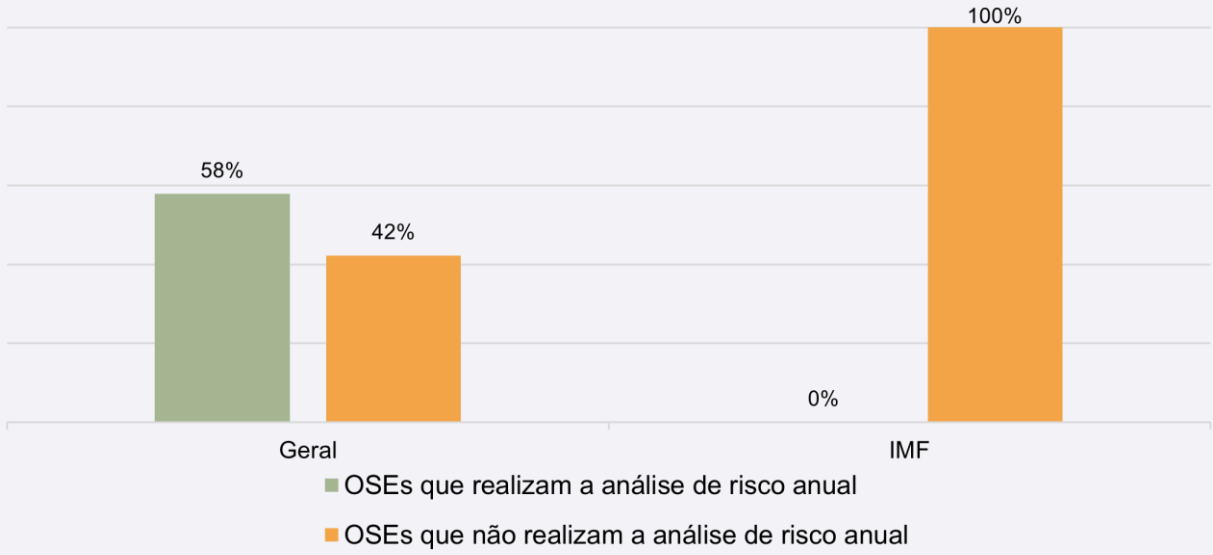
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. A totalidade dos operadores do setor das infraestruturas do mercado financeiro refere ter elaborado o relatório anual. Nos restantes setores, a percentagem de operadores que não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

Gráfico 98 - Submissão do relatório anual ao CNCS



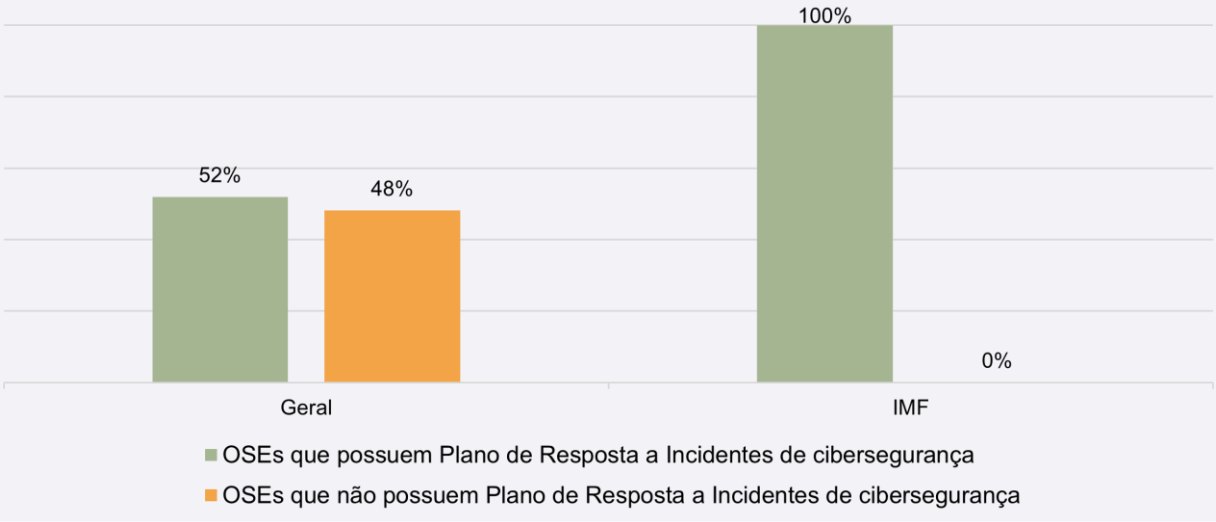
Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 97% submeteram-no ao CNCS. Destacam-se três setores, sendo um deles o das infraestruturas do mercado financeiro, nos quais todos os operadores com relatório elaborado submeteram o mesmo ao CNCS.

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



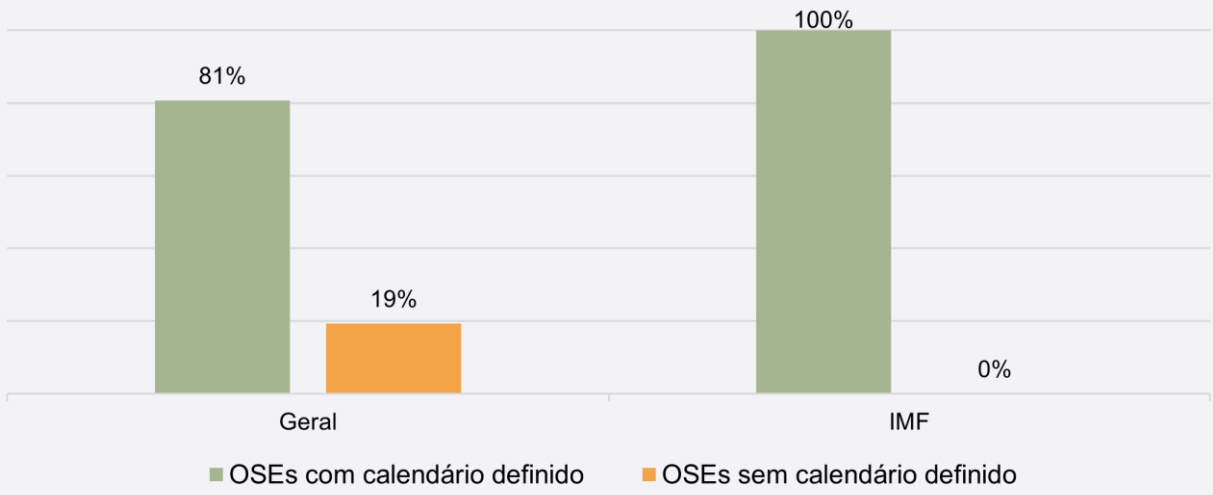
A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. No caso do setor das infraestruturas do mercado financeiro, no qual se tinha vindo a observar ampla conformidade com as obrigações decorrentes do decreto-lei, surpreende que nenhum dos inquiridos tenha referido realizar a análise de risco exigida.

Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança



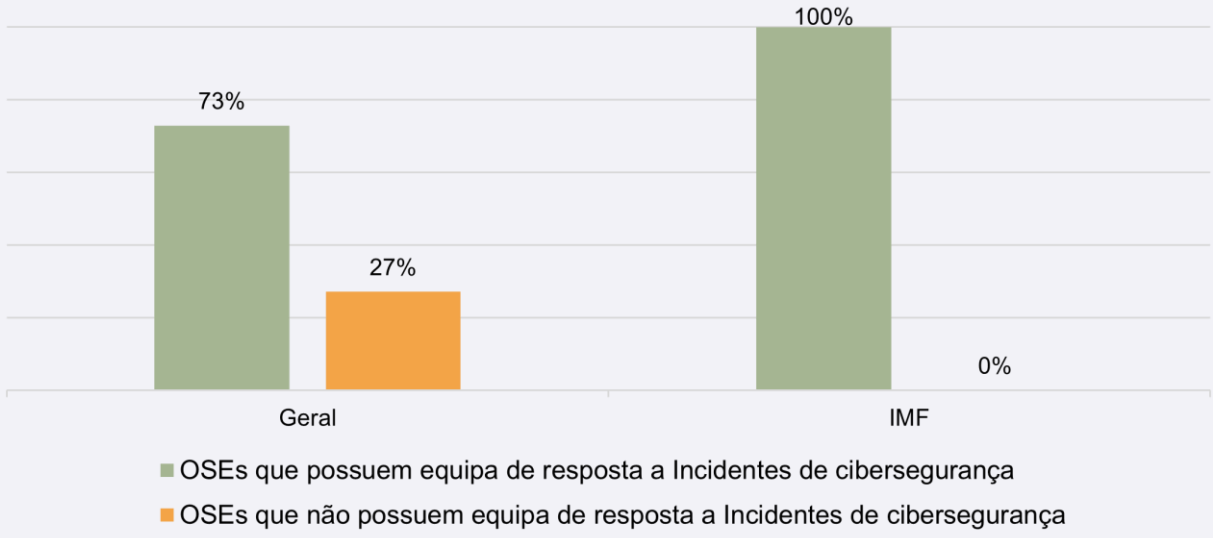
Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. Novamente, destaca o setor das infraestruturas do mercado financeiro, no qual todos os inquiridos indicam possuir esse plano.

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



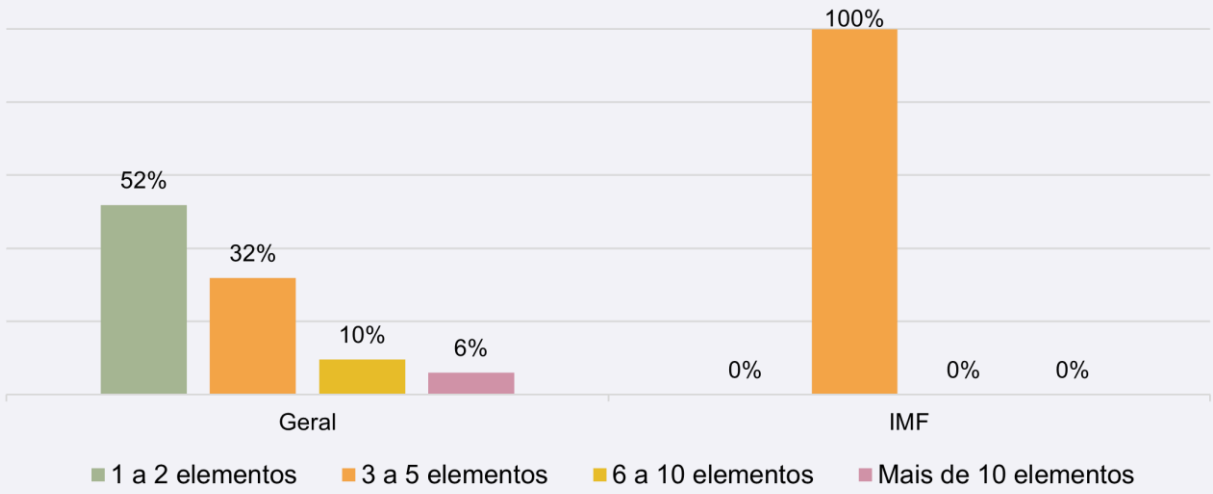
A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. No setor das infraestruturas do mercado financeiro todos os inquiridos indicam ter tal calendário definido. Há que salientar ainda que, tal como revelam 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%. Destacando mais uma vez o setor das infraestruturas do mercado financeiro, no qual todos os operadores inquiridos possuem equipa de resposta a incidentes de cibersegurança.

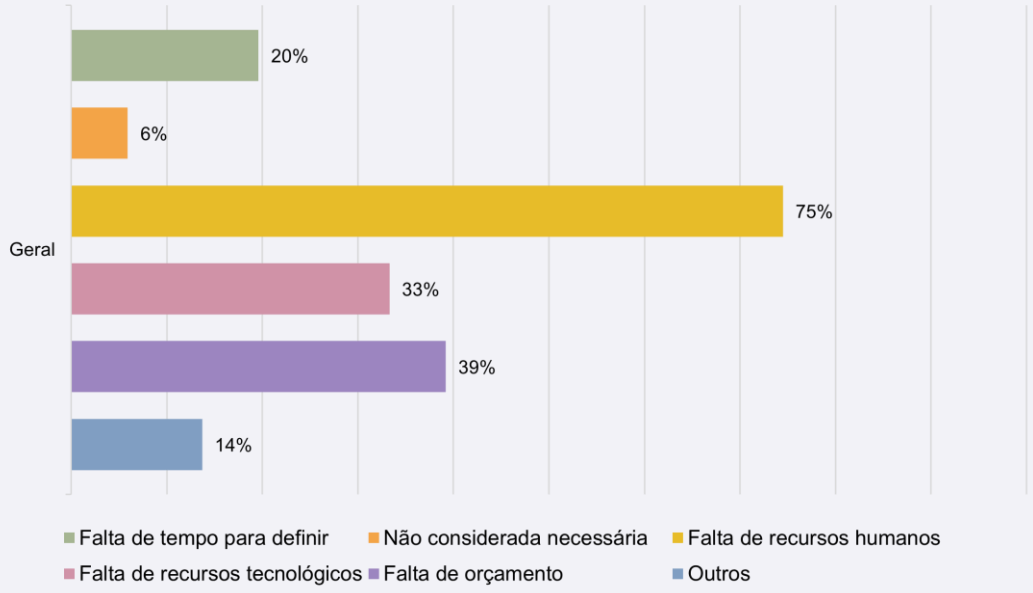
Gráfico 103 - Composição da equipa de resposta a incidentes de cibersegurança



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, nas infraestruturas do mercado financeiro, verifica-se que a totalidade das equipas é composta por 3 a 5 elementos em todos os operadores inquiridos. Ressalva-se ainda que embora equipas com 6 ou mais elementos se verifiquem menos vezes, estas chegam a verificar-se em até 40% dos operadores com equipa de resposta a incidentes.

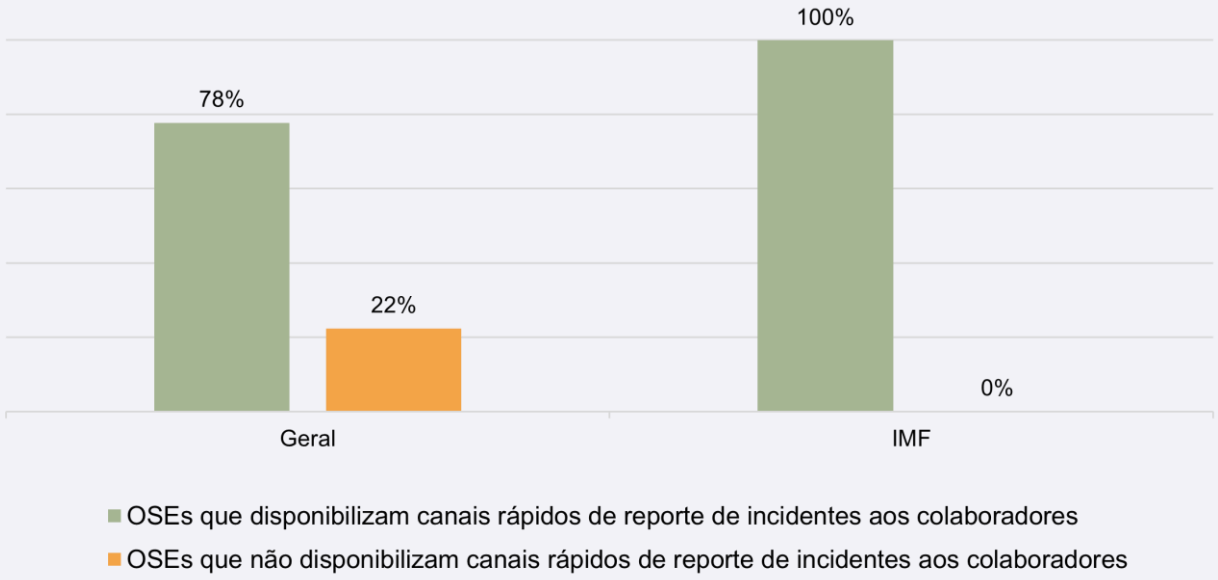
Em resumo, a composição das equipas de resposta a incidentes de cibersegurança tende a ser maioritariamente pequena.

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



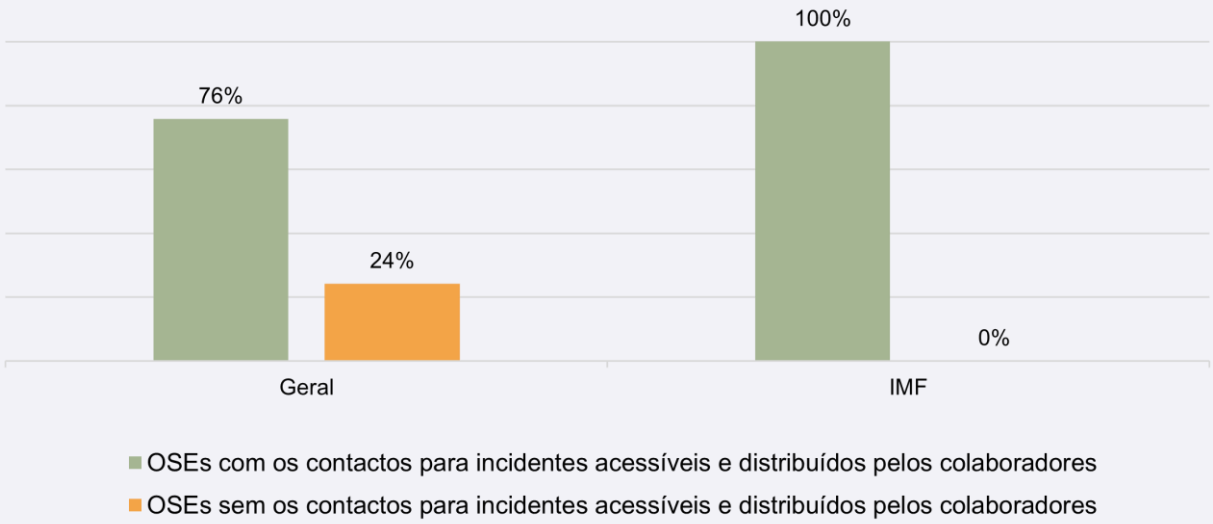
O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores 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. Visto a totalidade dos inquiridos do setor das infraestruturas do mercado financeiro apresenta equipa de resposta a incidentes a questão não se aplica.

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



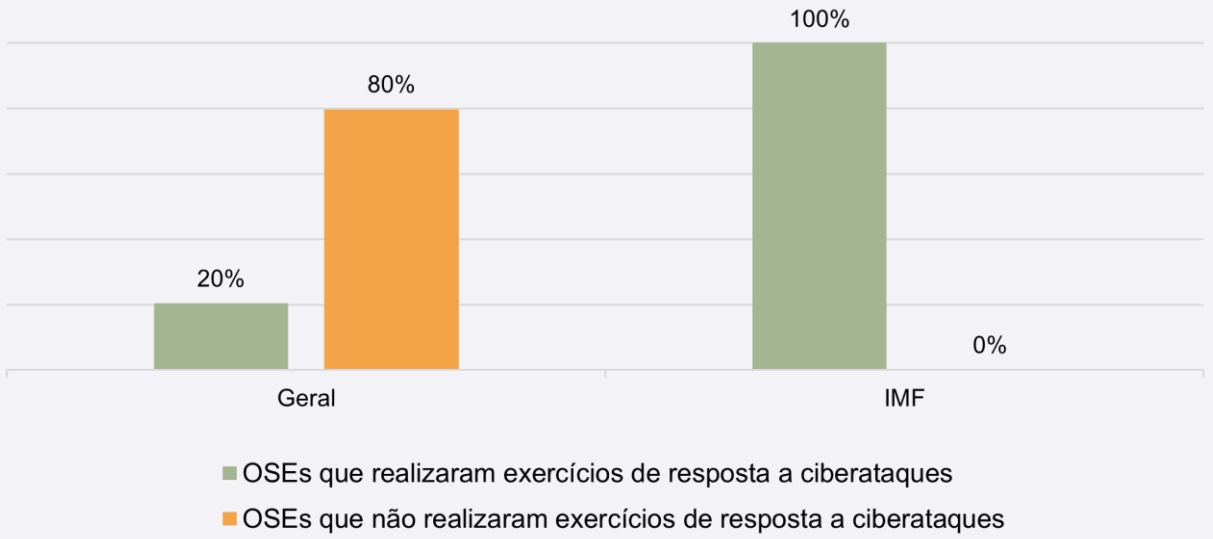
No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. Todos os operadores inquiridos do setor das IMF disponibilizam tais canais aos seus colaboradores.

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



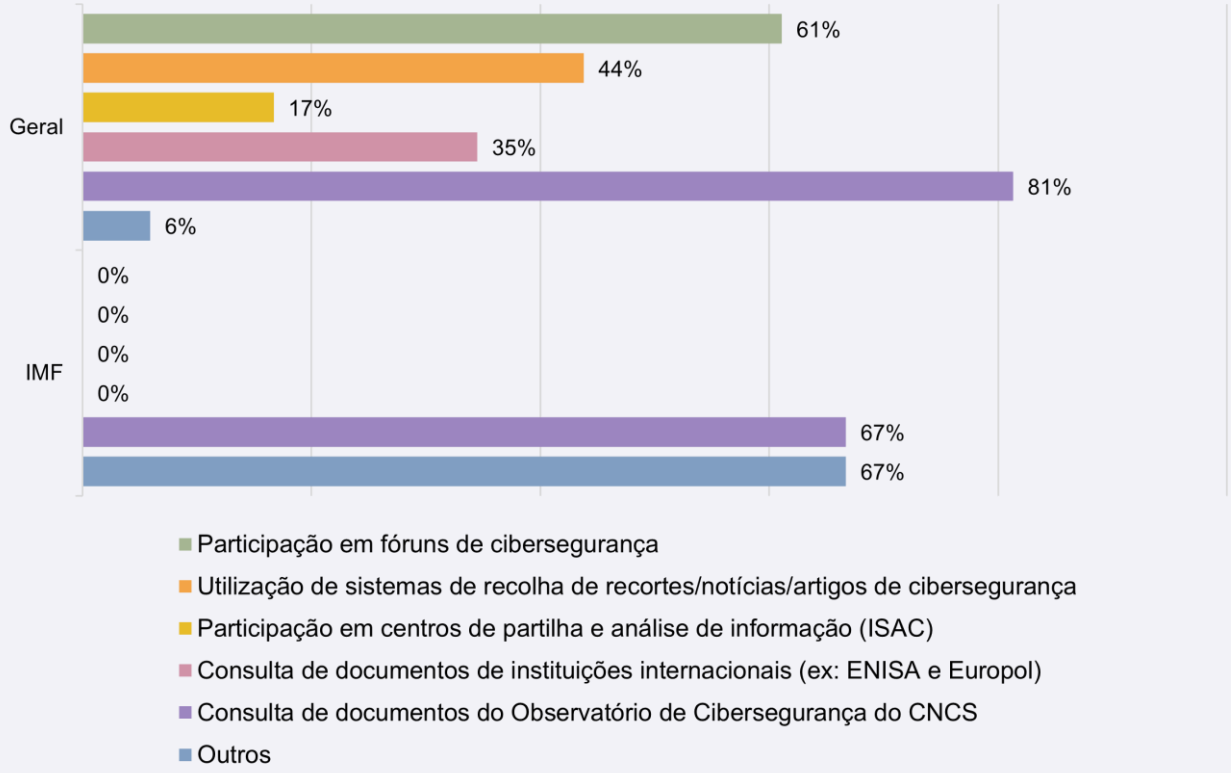
Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. Sectorialmente, todos os inquiridos do setor das infraestruturas do mercado financeiro responderam positivamente a esta questão.

Gráfico 107 - Realização de exercícios de resposta a ciberataques



De acordo com as respostas obtidas, apenas 20% dos operadores inquiridos realizam exercícios de resposta a ciberataques. No entanto, há ainda três setores que se destacam por a maioria dos operadores realizar estes exercícios. Um desses setores é o das infraestruturas do mercado financeiro, onde todos os inquiridos indicam realizar exercícios de resposta a ciberataques.

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



Independentemente dos métodos utilizados ou das fontes escolhidas para recolher informação sobre boas práticas relativas a riscos e incidentes de cibersegurança, verifica-se que a totalidade dos operadores inquiridos faz essa recolha. Os dois métodos mais comummente utilizados pelos operadores são a consulta de documentos do Observatório de Cibersegurança (cerca de 80%) e a participação em fóruns de cibersegurança (60%). Seguem-se a utilização de sistemas de recolha de notícias e artigos sobre cibersegurança, usada por 44% dos inquiridos, a consulta de documentos de instituições internacionais, como a ENISA e a Europol, praticada por cerca de 35% dos inquiridos. A participação em centros de partilha e análise de informação (ISACs) é a prática menos observada, sendo indicada por apenas 17% dos operadores inquiridos. Estes dados diferem grandemente dos registados pela ENISA, que dão conta de pelo menos 35% dos OSE em Portugal a participarem em ISACs[52].

No setor das infraestruturas do mercado financeiro, os operadores indicaram utilizar apenas os documentos produzidos pelo Observatório de Cibersegurança e "outros" métodos. Entre esses "outros", foi mencionado o recurso a uma entidade externa que presta serviços de cibersegurança, nos quais se inclui a recolha deste tipo de informações.

[52] 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"[53]. 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[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].

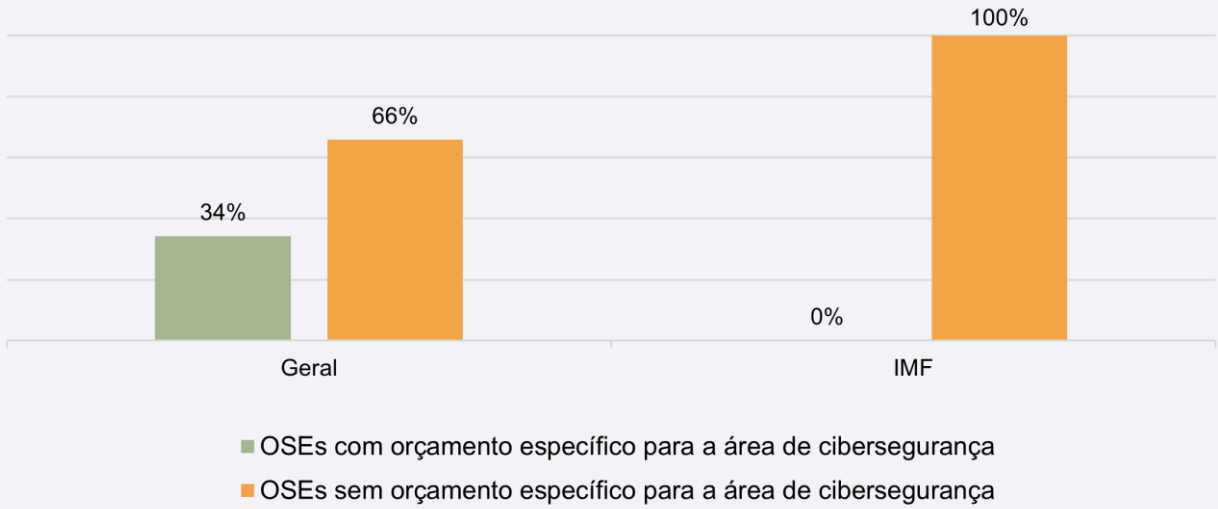
[53] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.

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

[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".

Gráfico 109 - Orçamento específico para a área de cibersegurança



Praticamente dois terços dos operadores inquiridos (66%) não possuem orçamento específico para a área de cibersegurança. O setor das infraestruturas do mercado financeiro foi o único onde nenhum dos inquiridos indicou ter orçamento específico para a área de cibersegurança.

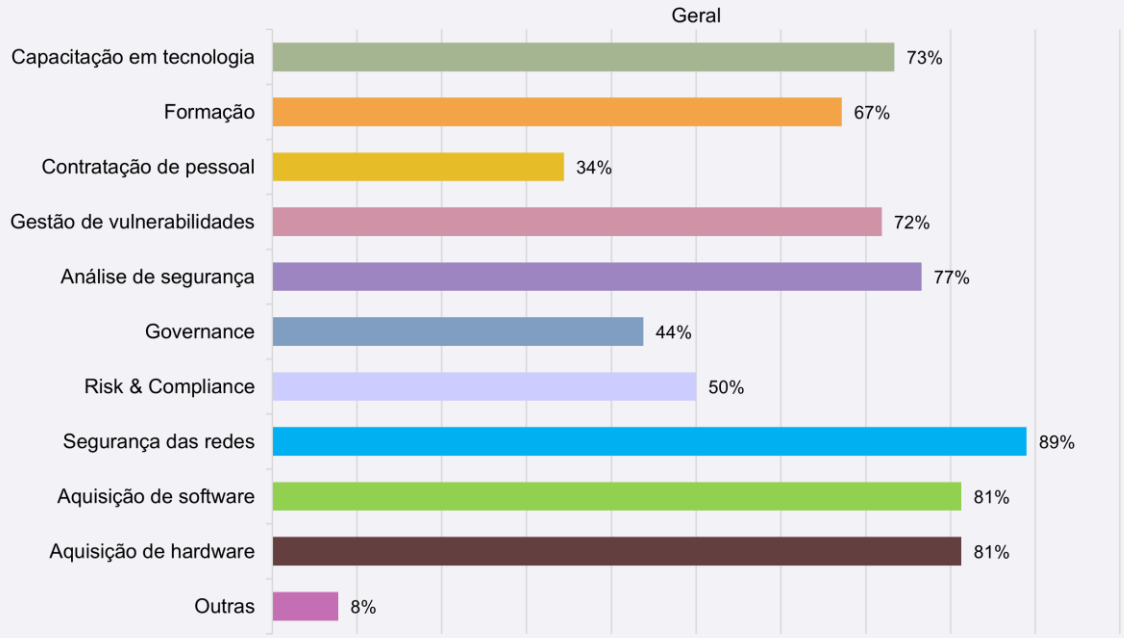
O Relatório *NIS Investments* de 2021 foi o último relatório da série da ENISA a analisar a questão de um orçamento específico para a cibersegurança, tendo os últimos dois relatórios, de 2022 e 2023, orientado o seu foco para orçamentos dedicados a riscos terceiros (*third-party risk*) e à formação em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

Importa também referir que a Diretiva NIS (RJSC) não obriga os OSE a ter orçamentos específicos para cibersegurança. No entanto, um estudo da Comissão Europeia e do Banco Europeu de Investimento (BEI) sobre a criação de uma plataforma de investimento em cibersegurança constatou que a ausência desses orçamentos específicos dificulta grandemente a análise do investimento realizado nesta área. Segundo o mesmo estudo, a própria UE não tinha, no ano de 2022, um orçamento dedicado ao financiamento da sua estratégia de cibersegurança[58].

[57] ENISA, NIS Investments, 2021, 7-8.
[58] Comissão Europeia e Banco Europeu de Investimento, “European Cybersecurity Investment Platform”, 2022, 29.

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].

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança



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

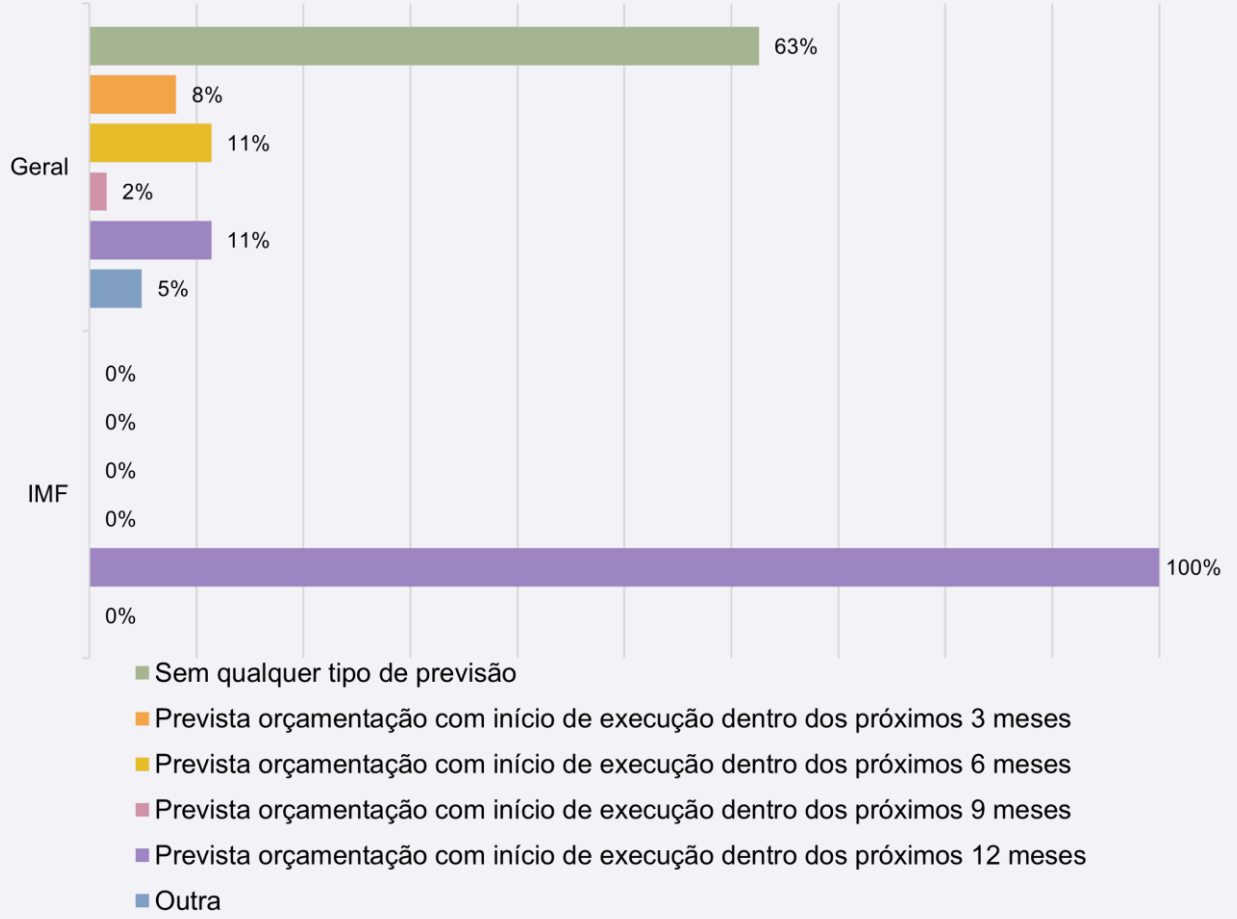
Como o setor das infraestruturas do mercado financeiro não apresentam orçamento para a área a questão não se aplica.

[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/.

A ENISA realizou um inquérito a 251 organizações OSE e prestadores de serviços digitais (oriundas da França, Alemanha, Itália, Espanha e Polónia). Segundo o inquérito, o orçamento médio para a implementação da diretiva NIS é 175 mil euros. A maioria das organizações do inquérito priorizaram os domínios de *Governance, Risk & Compliance* e Segurança das Redes.[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 OSE que não possuem orçamento específico para a área de cibersegurança



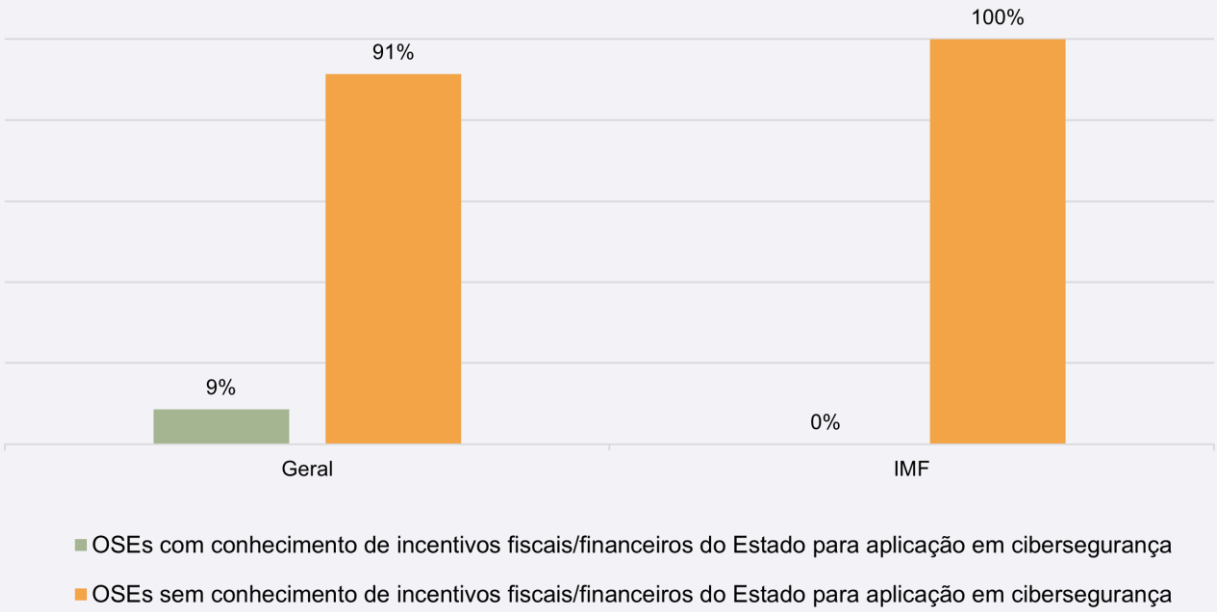
Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024. 63% destes não têm qualquer previsão de vir a ter tal orçamento. No setor das infraestruturas do mercado financeiro, todos os operadores sem orçamento específico para

[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

cibersegurança à data da realização do questionário tinham previsto iniciar a execução de um durante os 12 meses subsequentes, ou seja, até ao último trimestre de 2024.

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

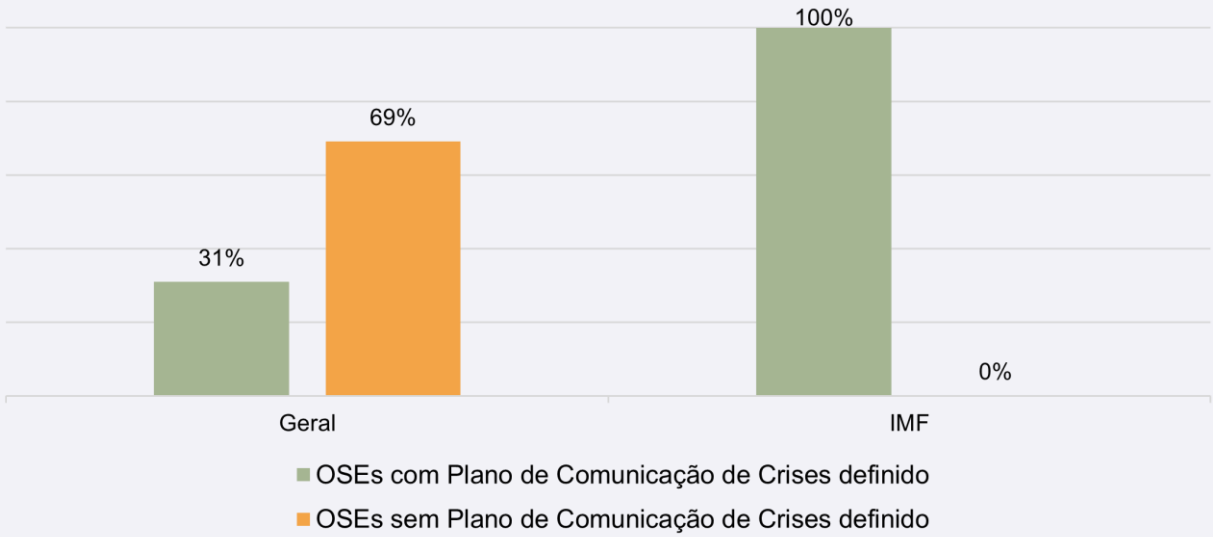


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. As percentagens de operadores com esse conhecimento nos vários setores são, contudo, reduzidas, variando entre os 4% e os 12%. No setor das infraestruturas do mercado financeiro não foram registados quaisquer operadores com conhecimento desses incentivos.

Cabe assim recordar que o Estado português lançou, em 2022, a medida Cheque-Formação + Digital, integrada no Programa Emprego + Digital 2025, que permite aos trabalhadores portugueses candidatarem-se a um cheque de formação digital de até 750 euros que pode ser aplicado em formações de 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 do mercado financeiro todos os inquiridos declaram ter plano de comunicação de crises definido. Tal deve-se ao facto de existir legislação setorial em vigor que obriga os operadores deste setor a terem este plano definido.

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises

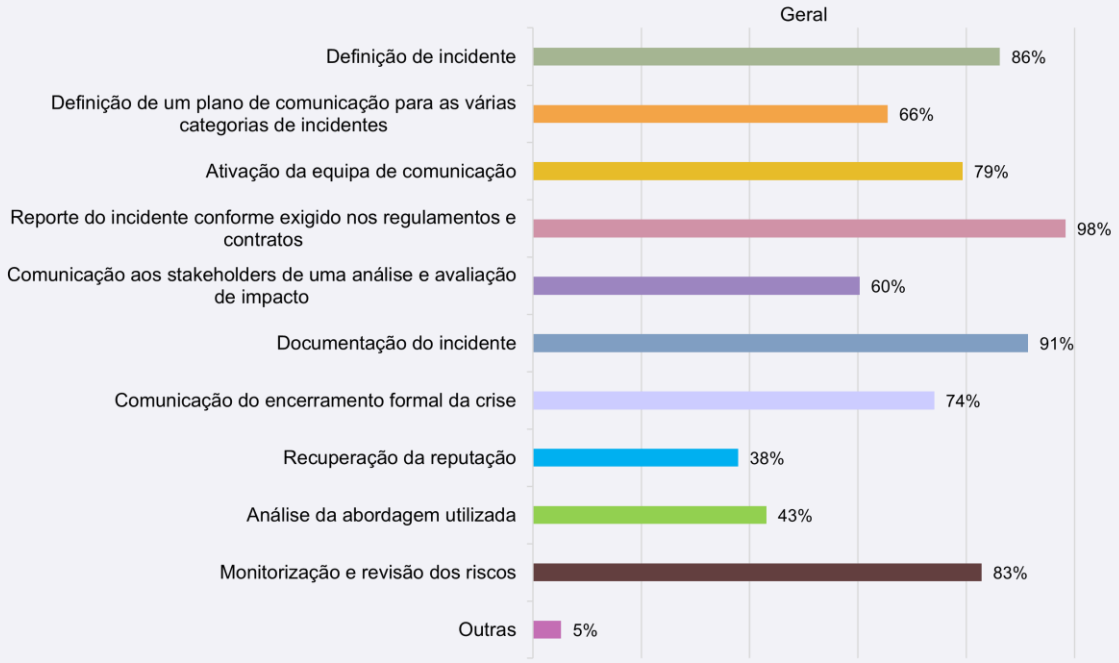
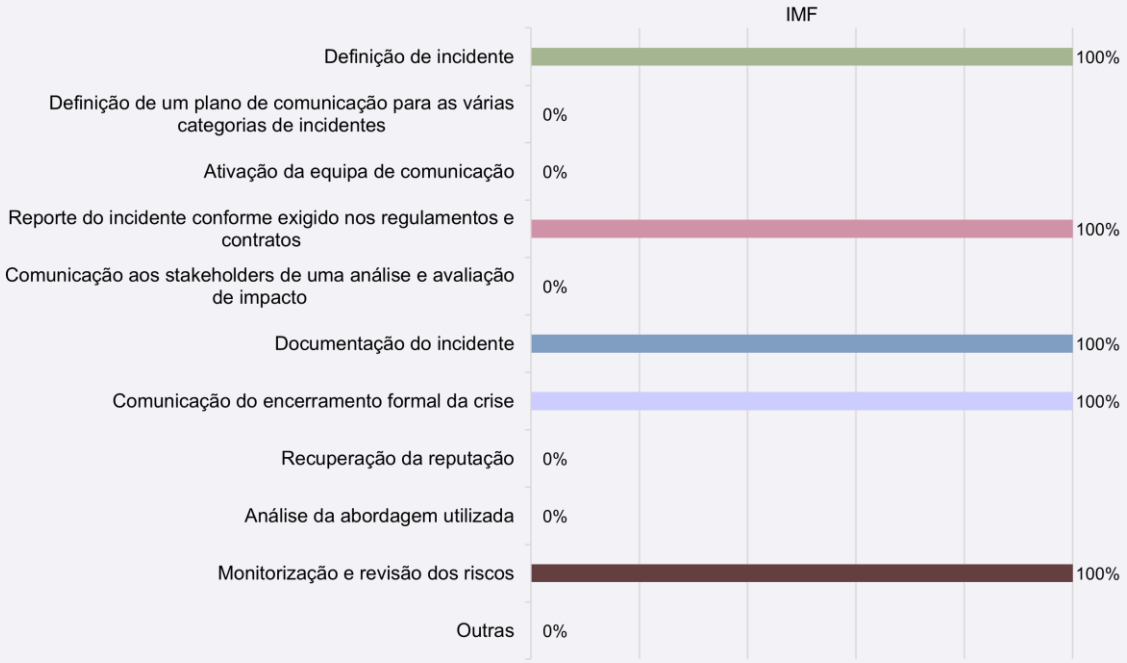


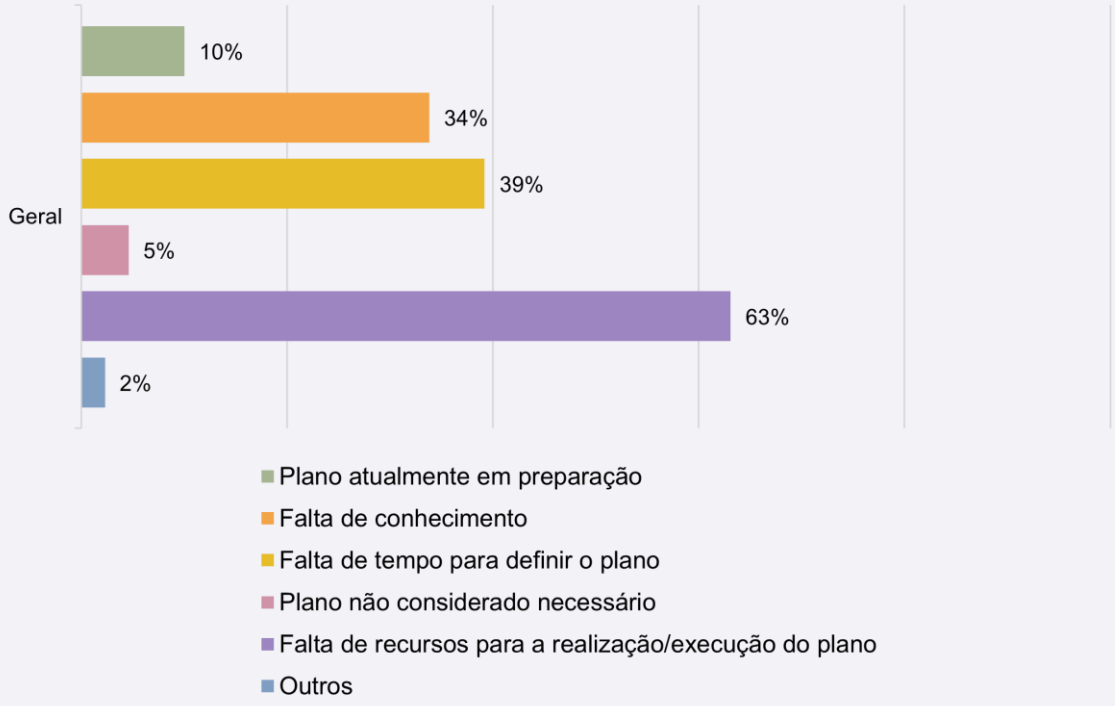
Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises



Na análise das secções incluídas nos planos de comunicação de crises, foram incluídas dez secções. Verifica-se que sete destas secções estão incluídas em pelo menos 60% dos planos já definidos.

As sete secções mais presentes são a definição de incidente, a definição de um plano de comunicação para várias categorias de incidentes, a ativação da equipa de comunicação, a notificação do incidente conforme exigido nos regulamentos e contratos, a comunicação aos grupos de interesse de uma análise e avaliação do impacto do incidente, a documentação do incidente e a análise da abordagem utilizada.
Por sua vez, as três secções que menos vezes estão incluídas nos planos de comunicação são as relacionadas com a comunicação do encerramento formal da crise, com a recuperação da reputação, e com a monitorização e revisão dos riscos.
No setor das infraestruturas do mercado financeiro, apesar de se verificarem cinco secções incluídas em todos os planos, há outras cinco que não constam em qualquer um dos planos definidos pelos operadores do setor.

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



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

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

O das infraestruturas de mercado financeiro afirma já ter o plano definido. Desta forma a questão não se aplica.

Análise Setorial

1. Infraestruturas do mercado financeiro

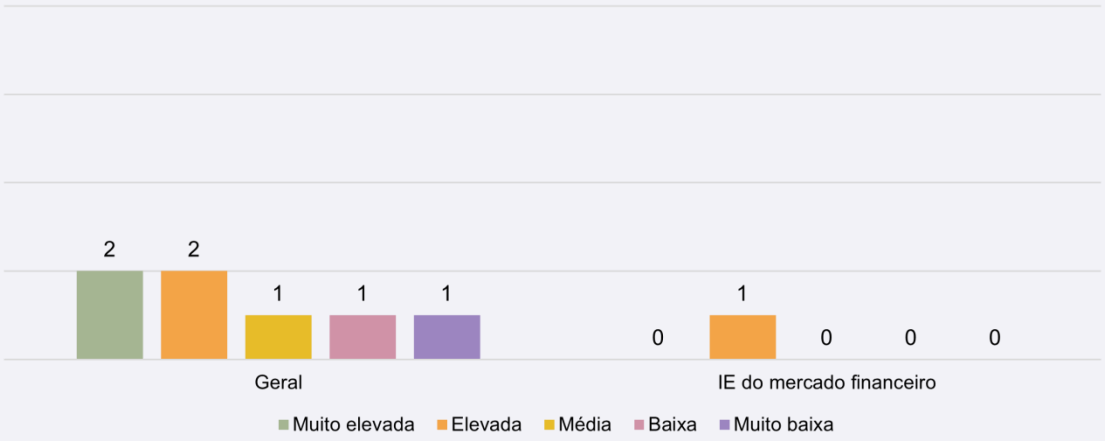
1.1. Contextualização setorial

No âmbito da Diretiva 2016/1148 e do Regime Jurídico da Segurança do Ciberespaço (RJSC, ou Lei n.º 46/2018, de 13 de agosto), que a transpõe, as infraestruturas do mercado financeiro são compostas por dois tipos de entidades: operadores de plataformas de negociação e contrapartes centrais (*Central Counterparties* - CCPs). Os operadores de plataformas de negociação são sociedades/entidades que, através de diferentes plataformas, permitem que um investidor aceda a diferentes mercados e instrumentos financeiros, tal como faz a Euronext Lisbon, mais vulgarmente conhecida por Bolsa de Lisboa. Já as contrapartes centrais, são infraestruturas do mercado financeiro que atuam como a contraparte em ambos os lados de uma transação financeira, efetuando operações de compensação em vários instrumentos financeiros. Um dos papéis principais das CCPs é então o de assegurar que as transações entre duas partes são realmente cumpridas. Estas entidades desempenham assim duas funções principais como intermediárias numa transação: a função de compensação e função de liquidação. Uma CCP atua como contraparte tanto para os vendedores quanto para os compradores, arrecadando dinheiro de cada um, o que lhe permite garantir os termos de uma negociação. Isto é, uma CCP suporta a maior parte do risco de crédito dos compradores e dos vendedores quando compensam e liquidam transações de mercado. Se um comprador ou vendedor não cumprir a sua parte no processo de transação, a CCP cobre as perdas resultantes da transação falhada. Nesses casos, a CCP compensa a transação falhada com o valor atual de mercado da mesma[64]. Em Portugal, existem contrapartes centrais dedicadas às operações no mercado de capitais nacional[65] e contrapartes centrais dedicadas exclusivamente a derivados do setor da energia (eletricidade e gás natural)[66]. Tanto as plataformas de negociação como as CCPs são reguladas em Portugal pela Comissão do Mercado de Valores Mobiliários - CMVM.

De acordo com o questionário realizado, o regulador do setor considera que a maturidade deste em cibersegurança é elevada e, no âmbito geral, apenas existem dois reguladores com maior perceção de maturidade em cibersegurança (**Gráfico 9**).

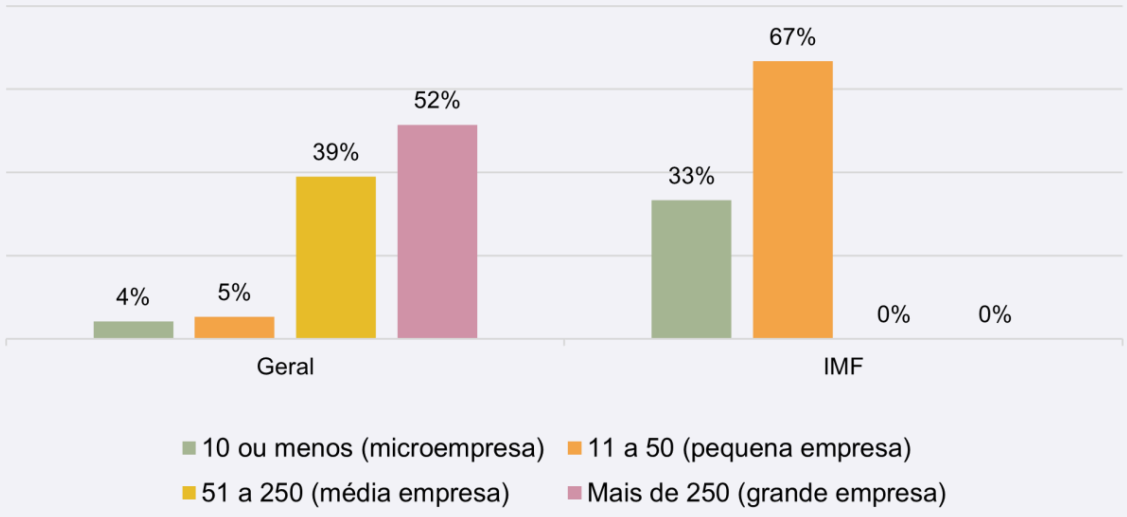
[64] Banco Central Europeu, "Central Counterparty Clearing Houses and Financial Stability", *Financial Stability Review*, 2005, 179, https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart200512_06.en.pdf.
[65] "Outros sistemas de liquidação", Infraestruturas de mercado, Banco de Portugal, https://www.bportugal.pt/page/outros-sistemas-de-liquidacao.
[66] "Quem somos", OMIClear, https://www.omiclear.pt/pt.

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



O tecido empresarial dos OSE do setor das infraestruturas do mercado financeiro é sobretudo composto por pequenas empresas, com apenas entre 11 e 50 colaboradores, e as restantes são microempresas com 10 ou menos colaboradores (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



A perceção dos reguladores sobre maturidade em cibersegurança nos setores pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (100% contra 65% no geral) (vide **Gráfico 38**) e pelas medidas cibersegurança adotadas (**Gráfico 66.4**) Todas as medidas de proteção utilizadas têm o mesmo valor.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

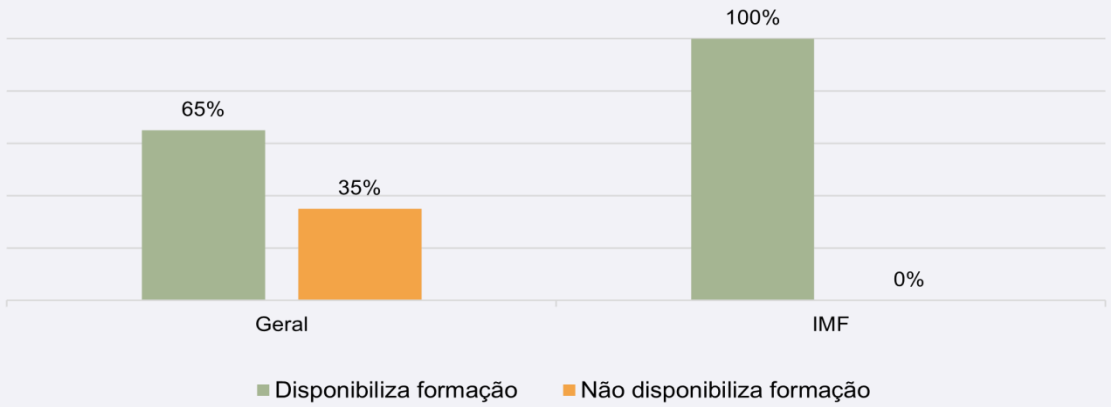
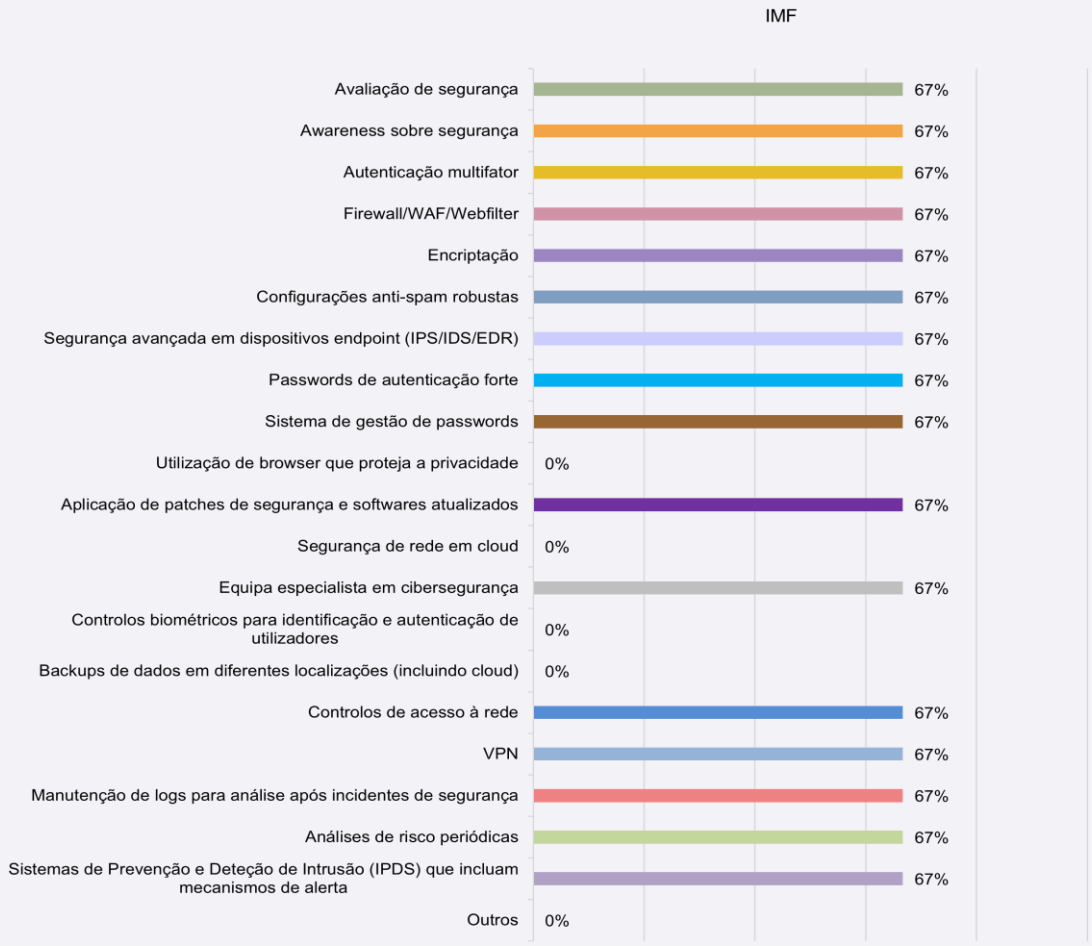
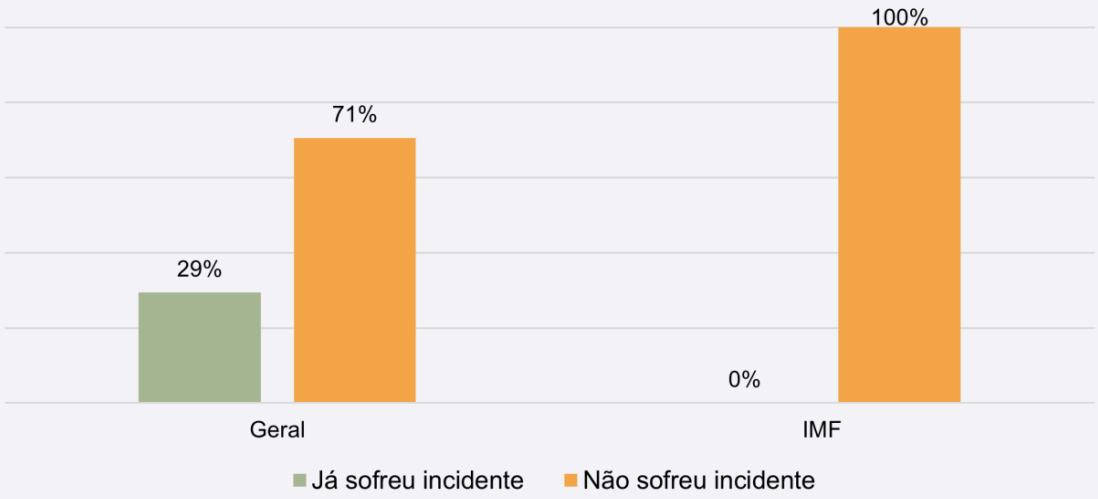


Gráfico 66.4 - Medidas de proteção contra ameaças de cibersegurança



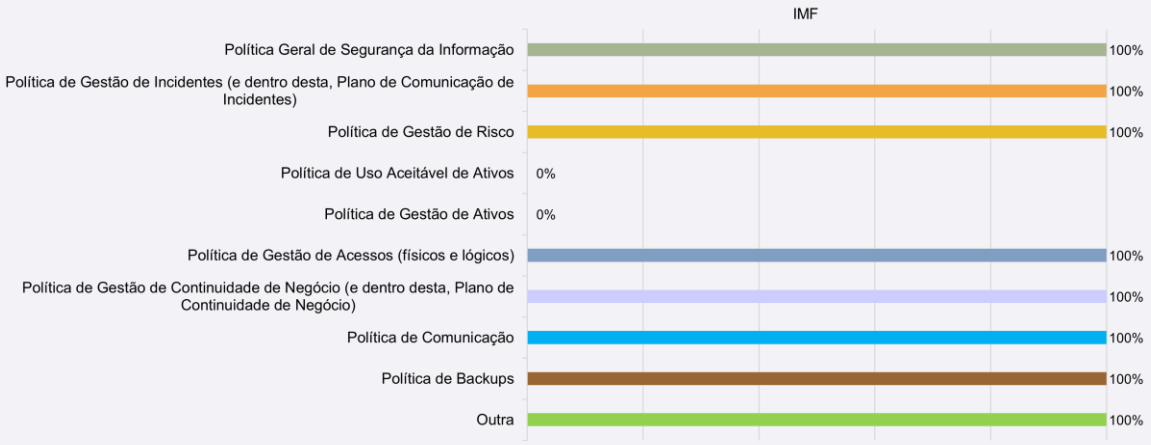
Mesmo não existindo orçamento de cibersegurança, este é o único setor onde não foram registados quaisquer incidentes de cibersegurança, estando assim acima da média geral que fica nos 71% (**Gráfico 68**).

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



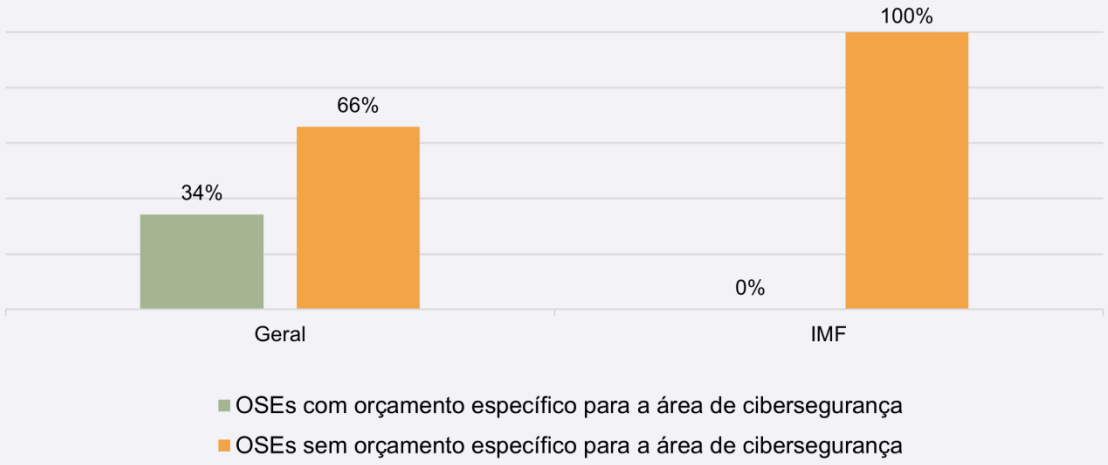
As políticas de cibersegurança e outras políticas relacionadas implementadas também suportam a afirmação anterior. O plano de segurança inclui todas as políticas tradicionalmente associadas à cibersegurança, com exceção de políticas relativas a ativos (**Gráfico 79.4**).

Gráfico 79.4 - Políticas Incluídas no Plano de Segurança



Embora cerca de 34% dos setores tenham um orçamento específico para a área de cibersegurança, não existem OSE neste setor a seguir esta prática (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



1.1.1. Impacto socioeconómico

As infraestruturas do mercado financeiro (as plataformas de negociação e as CCPs) desempenham um papel fundamental na economia nacional. Estas permitem pagamentos, compras, vendas, investimentos e sustentam o funcionamento da economia como um todo. São também estas que, muitas vezes, dão a necessária liquidez de capital a empresas, por exemplo, através da emissão de ações, recebendo as empresas dinheiro por cada ação vendida.

No caso específico das plataformas de negociação, o desempenho das empresas nas mesmas, como na Euronext Lisbon (Bolsa de Lisboa), pode desempenhar um papel crucial na atração de investimentos. Estas informações podem influenciar, impactando o nível de investimento interno e externo das empresas cotadas na bolsa nacional. É importante sublinhar que atrair investimento é importante em qualquer economia, uma vez que este é um impulsionador do crescimento económico e da produtividade[67].

Em 2019, o volume diário de negócios da Bolsa de Lisboa era de cerca de 86 milhões de euros. Em 2021, esse valor aumentou para os 112 milhões e, em 2022, o volume diário atingiu os 137 milhões de euros, tendo crescido percentualmente mais do que em outras praças europeias[68]. A maior parte do volume de negócios ainda vem de instituições internacionais, com 80% das transações a serem feitas por intermediários dora de Portugal, indicando um investimento estrangeiro.

[67] Pedro Bação et al., "Investimento Empresarial e o Crescimento da Economia Portuguesa", coord. Fernando Alexandre, *Fundação Calouste Gulbenkian* (2017): 7, https://gulbenkian.pt/wp-content/uploads/2017/11/Estudo_relatorio_Investimento_Empresarial_final_dez2017.pdf.

[68] Mariana Dias, "Euronext Lisboa cresce em 2022. Foram negociados 137 milhões de euros por dia", *Dinheiro Vivo*, 28 de fevereiro de 2023, https://www.dinheirovivo.pt/bolsa/euronext-lisboa-cresce-em-2022-foram-negociados-137-milhoes-de-euros-por-dia-15918612.html/.

No entanto, o crescimento do volume de negócios deve-se principalmente ao aumento de investidores individuais, que representam 15%, o triplo de 2019. Portugal tem atraído, sobretudo, investidores particulares norte-americanos, brasileiros e franceses[69].

Já no caso concreto das contrapartes centrais, estas ganharam particular relevância no seguimento da crise financeira de 2007-2008, iniciada nos Estados Unidos da América. Após o deflagrar dessa crise, a consequente insolvência de várias empresas e a falta de liquidez verificada levaram a uma grave quebra de confiança nas instituições financeiras por parte dos investidores e do público. Perante este cenário, iniciou-se uma profunda reforma das infraestruturas do mercado financeiro, na qual as CCPs desempenharam um importante papel. De forma sucinta, as CCPs passaram a ter um papel mais ativo nos procedimentos de compensação e liquidação[70], mitigando assim uma porção do risco de contraparte e do risco sistémico. Este novo papel surge no seguimento de desenvolvimentos legislativos na União Europeia tais como o Regulamento (UE) n.º 648/2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (também conhecido como *European Market Infrastructure Regulation* - EMIR), que impôs obrigações ao nível da partilha de dados entre CCPs e plataformas de negociação, ao nível da comunicação de informações sobre transações num repositório dedicado, bem como ao nível do capital mínimo para as CCPs poderem operar (7,5 milhões de euros de capital inicial e de capital permanente)[71]. A nova regulamentação, embora não tenha imposto a necessidade de incluir uma CCP na negociação de todo o tipo de ativos e derivados, impeliu a que mais plataformas de negociação celebrassem acordos com CCPs de modo a realizarem transações mais seguras. Dados do Banco Central Europeu demonstram que o número de transações seguras aumentou, entre 2008 e 2015, de cerca de 60% para praticamente 90% e que o envolvimento de CCPs nas transações aumentou, também, entre 2008 e 2015, de 40% para cerca de 65%[72]. A regulação das infraestruturas do mercado financeiro acabou por contribuir para um mercado mais seguro, embora a recuperação da confiança dos consumidores e investidores tenha sido lenta. Não obstante, as CCPs tornaram-se elementos indispensáveis à segurança e integridade dos mercados financeiros[73]. A nova regulamentação, juntamente com outras medidas, tais como as injeções de capital e a redução das taxas de juro, permitiram, lentamente, a recuperação da confiança dos investidores no mercado financeiro[74].

As infraestruturas do mercado financeiro são também um garante de igualdade no que diz respeito ao acesso ao mercado financeiro. As infraestruturas do mercado financeiro não são acessíveis apenas a investidores com um alto poder económico ou a grandes empresas. Estas permitem também investimentos de menores valores, alocações de poupanças individuais, com diferentes graus de risco, como por exemplo em fundos para a reforma, planos de poupança-reforma (PPR) e planos de poupança em ações (PPA), entre muitos outros.

---

69 Dias, "Euronext Lisboa cresce em 2022".

70 André Barata, "O Regime Europeu de Resolução de Contrapartes Centrais: a peça que faltava ao mercado dos derivados de balcão?", *Revista de Direito Financeiro e dos Mercados de Capitais*, dezembro de 2023, 201, https://rdfmc.com/wp-content/uploads/2024/01/Revista-de-Direito-Financeiro-e-do-Mercado-de-Capitais-2-20231.pdf.

71 Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, *Jornal Oficial da União Europeia*, 25, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012R0648.

72 Florian Heider, "Collateral, central clearing counterparties and regulation", *European Central Bank Research Bulletin 41*, 6 de dezembro de 2017, https://www.ecb.europa.eu/press/research-publications/resbull/2017/html/ecb.rb171206.en.html.

73 Barata, "O Regime Europeu de Resolução de Contrapartes Centrais", 270-271.

74 International Monetary Fund, "World Economic Outlook: Challenges to Steady Growth", outubro de 2018, 82, https://www.imf.org/-/media/Files/Publications/WEO/2018/October/English/main-report/Text.ashx.

As infraestruturas do mercado financeiro são também responsáveis pela promoção de uma maior transparência nos mercados, uma vez que as empresas cotadas em Bolsa são obrigadas a publicar informações financeiras de forma periódica e contínua[75]. A divulgação periódica de relatórios anuais detalhados, como balanços patrimoniais, demonstrações de resultados e de fluxos de caixa, bem como relatórios semestrais e trimestrais, que fornecem atualizações sobre a *performance* financeira e a situação económica das empresas contribuem para a transparência no mercado e para o aumento da confiança no mesmo por parte dos investidores[76].

1.1.2. Especificidades tecnológicas

As tecnologias utilizadas no setor financeiro, sobretudo as tecnologias inovadoras são comummente designadas como *fintech* (juntando o início das palavras inglesas *financial* e *technology*). Embora a origem do termo possa ser traçada até ao início da década de 90, foi somente nos anos de 2013 e 2014 que este começou a ganhar mais atenção e a ser mais amplamente utilizado[77].

O termo *fintech* engloba agora qualquer inovação tecnológica do setor financeiro, incluindo avanços em literacia financeira, consultoria e educação, bem como na simplificação da gestão de carteiras de investimentos, empréstimos, banca de retalho, *crowdfunding*, transferências/pagamentos e muito mais. Tecnologias como a *blockchain*, Inteligência Artificial (IA) e automatização de processos robóticos, estão cada vez mais integradas nas infraestruturas do mercado financeiro. Estas inovações impactam diretamente as organizações, pois exigem novas abordagens para garantir a segurança e resiliência das operações financeiras num ambiente cada vez mais digitalizado[78].

[75] "Financial Reporting", Issuer Disclosure, ESMA, https://www.esma.europa.eu/issuer-disclosure/financial-reporting.

[76] Shatha Hussain, Amer Alaya e Thana Azizi, "The impact of financial accounting disclosures on investors' reactions towards bad news: The moderating role of investors' sentiments", Cogent Economics and Finance, 16 de julho de 2023, 5, https://www.tandfonline.com/doi/pdf/10.1080/23322039.2023.2228087?download=true.

[77] Douglas Arner, "FinTech: Evolution and Regulation", Asian Institute of International Financial Law, University of Hong Kong, junho de 2016, https://law.unimelb.edu.au/__data/assets/pdf_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf.

[78] Maximilian Palmié et al., "The evolution of the financial technology ecosystem: an introduction and agenda for future research on disruptive innovations in ecosystems", University of Vaasa, 2020, 10 e 21, https://osuva.uwasa.fi/bitstream/handle/10024/10315/Osuva_Palmi%C3%A9_Wincent_Parida_Caglar_2020b.pdf?sequence=2&isAllowed=y.

Descrevem-se, de seguida, algumas das mais relevantes utilizadas no setor:

- ***Distributed Ledger Technology* (DLT) e *Blockchain***

Distributed Ledger[79] *Technology* (DLT) é uma tecnologia de registo descentralizado que permite o registo de transações de ativos em múltiplos locais simultaneamente. Esta descentralização, ao contrário das bases de dados tradicionais centralizadas, oferece maior resiliência e segurança contra falhas e ataques.

Quanto ao conceito de *blockchain*, este tem origem num artigo publicado em 2008[80]. A *blockchain* é uma rede formada por blocos encadeados onde cada um destes blocos contém uma "impressão digital", ou *hash* criptográfico, que se conecta ao bloco anterior. Como um tipo específico de DLT, a *blockchain* organiza os dados em blocos que são verificados e adicionados de forma imutável e segura. Este encadeamento por *hashes* criptográficos torna a *blockchain* interligada, permitindo rastrear todas as transações. Além disto, cada transação é visível para todos os envolvidos. Esta natureza descentralizada e distribuída da *blockchain* torna-a menos vulnerável a falhas: se algum bloco for removido, os demais já possuem uma cópia exata das informações, preservando a integridade dos dados. Da mesma forma, quando um novo nó se junta rede, o mesmo recebe uma cópia completa de todas as informações reforçando a confiabilidade e resiliência deste sistema[81].

O modo de funcionamento da tecnologia *blockchain* oferece um elevado nível de segurança às transações. Tentar modificar um bloco obrigaria a mudar o *hash* criptográfico de todos os blocos subsequentes, algo que exigiria um imenso poder computacional e que, mesmo assim, é altamente impraticável. Este modo de funcionamento torna virtualmente impossível a adulteração de dados e oferece uma plataforma segura para o armazenamento de dados sensíveis e para a realização de transações financeiras[82]. Para as organizações do setor das infraestruturas do mercado financeiro, as DLT podem ser fundamentais na modernização dos sistemas de transações, aumentando a transparência, reduzindo os riscos de manipulação de dados e melhorando a continuidade do negócio em caso de incidentes.

[79] Na língua inglesa, "*ledger*" é o termo utilizado para se referir a um livro de contas, no qual se registam as transações respeitantes a uma conta específica. Neste registam-se todas as transações de débito, crédito, de venda e de compra realizadas através dessa conta.

[80] Pornpit Wongthongtham et al., "Blockchain-enabled Peer-to-Peer energy trading", *Computers & Electrical Engineering* 94 (setembro de 2021): 1-9, https://doi.org/10.1016/j.compeleceng.2021.107299.

[81] Dejan Vujičić, Dijana Jagodić e Siniša Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview", *paper* apresentado no 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), Sarajevo, Bósnia e Herzegovina, de 21 a 23 de março de 2018, 1-6, https://ieeexplore.ieee.org/abstract/document/8345547/.

[82] Reza Soltani et al., "Distributed Ledger Technologies and Their Applications: A Review", *Applied Sciences* 12, 7898 (2022): 4, https://doi.org/10.3390/app12157898.

- **IA e *robo-advisors***

A Inteligência Artificial (IA) e os *robo-advisors* estão a ser cada vez mais aplicados no setor das infraestruturas do mercado financeiro para otimizar processos e melhorar a tomada de decisões. Embora a IA em si seja uma tecnologia ampla e não exclusiva deste setor, a sua aplicação específica em serviços como os *robo-advisors* tem transformado o modo como todas as instituições financeiras operam e interagem com os clientes. Os *robo-advisors*, que utilizam algoritmos baseados em IA, permitem a gestão automática de carteiras de investimento, oferecendo soluções personalizadas a baixos custos. Segundo um inquérito do Fórum Económico Mundial, em 2020 já 85% dos intervenientes no setor financeiro utilizavam IA e, no questionário realizado no âmbito deste relatório, todos os operadores inquiridos indicaram que utilizam IA. A Inteligência Artificial, segundo o mesmo inquérito, é amplamente utilizada no setor para diversos fins, como a automatização de processos, gestão de riscos, redução de custos, criação de novas fontes de receita, análise de dados, deteção de fraudes e anomalias, além de serviços de comunicação com clientes, como os *chatbots*[83]. Os mercados financeiros são, por natureza, intangíveis, e os diversos serviços que neles operam, como a execução de pagamentos, a emissão de ações e a compra e venda de ativos, dependem fundamentalmente do processamento de informação[84]. Este é um setor que emprega há décadas processos automatizados e algoritmos para realizar análises e previsões.

Quando um novo cliente se regista para utilizar serviços deste tipo, são-lhe pedidos diversos dados, tais como idade, género, vencimento, objetivos de investimento, atuais ativos de que disponha e o seu grau de tolerância ao risco. Com base nestes dados, e nas capacidades de análise e de previsão do mercado, como tendências de descidas e subidas de preços, o *robot* procura os melhores ativos onde investir e quais ignorar, em busca do cumprimento dos objetivos do cliente.

[83] Emmanuel Schizas et al., "Transforming Paradigms: A Global AI in Financial Services Survey", *World Economic Forum*, 29 de fevereiro de 2020, 25, https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf.

[84] Giacomo Calzolari, "Artificial Intelligence market and capital flows: Artificial Intelligence and the financial sector at crossroads", estudo para o Parlamento Europeu, maio de 2021, 25, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf.

- ***FIX (Financial Information eXchange)***

O setor das infraestruturas do mercado financeiro necessita de ter uma baixa latência nas suas operações de forma a garantir que as ordens são executadas no menor tempo possível. Para ajudar a garantir a menor latência, este setor utiliza o protocolo *FIX* (*Financial Information eXchange*). O protocolo *FIX*, foi desenvolvido em 1992 pela Goldman Sachs e pela Fidelity Investments, e é utilizado para facilitar as comunicações entre os diferentes sistemas de *trading* e define uma linguagem padrão que permite que diferentes sistemas comuniquem entre si sem a necessidade de criar interfaces específicas. Este protocolo baseia-se em mensagens pré-definidas que seguem um formato específico. Cada mensagem contém uma sequência de campos denominados por *tags*, onde cada campo transmite um dado específico, como por exemplo o preço de uma ação, a quantidade de ações, entre outros[85]. O *FIX* tem alguns benefícios, tais como[86]:

- **Velocidade e Eficiência**: O *FIX* facilita a transmissão rápida e precisa das informações, pois é um padrão de comunicação amplamente utilizado;
- **Interoperabilidade**: As empresas financeiras podem integrar os seus sistemas com os outros do mercado, independentemente do *software* ou *hardware* que estão a utilizar;
- **Redução de custos**: Como a comunicação fica padronizada, a necessidade de adaptações fica reduzida, permitindo uma configuração mais eficiente e, consequentemente, uma redução dos custos operacionais;
- **Segurança**: Este protocolo é adaptável às normas de segurança e oferece um suporte para a autenticação, proporcionando um ambiente seguro para as transações mais sensíveis.

Este protocolo é utilizado na gestão de ativos, na bolsa de valores e corretoras. Devido às mudanças regulatórias e ao aumento da complexidade nos mercados financeiros, este protocolo passou por várias atualizações, estando atualmente na versão 5.0 e continua a evoluir de forma a conseguir suportar novos tipos de transações e a aumentar a segurança do mesmo[87].

- ***RTGS (Real-Time Gross Settlement)***

Os mercados financeiros utilizam sistemas de liquidação bruta ("*gross settlement*") para processar e liquidar pagamentos de grande valor entre instituições de forma imediata e em tempo real. Estes sistemas são denominados de *RTGS* (*Real-Time Gross Settlement*) e, neste tipo de sistemas, as transações são processadas de forma individual e liquidadas de forma irrevogável, garantindo assim que o pagamento é finalizado assim que é executado[88].

---

[85] Hao Jia et al., "A Domain-Specific Accelerator for Ultralow Latency Market Data Distribution System," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, abril de 2023, 5466-5467, https://ieeexplore.ieee.org/abstract/document/9801674.

[86] True Tamplin, "Advantages of Financial Information Exchange (FIX)", *Finance Strategists*, 12 de julho de 2023, https://www.financestrategists.com/wealth-management/investment-management/financial-information-exchange-fix/#advantages-of-financial-information-exchange-fix.

[87] FIX Trading Community, "FIX 5.0 Specifications", https://www.fixtrading.org/standards/unsupported/fix-5-0/.

[88] Peter Allsopp, Bruce Summers e John Veale, "The Evolution of Real-Time Gross Settlement: Access, Liquidity and Credit, and Pricing", World Bank, fevereiro de 2009, 7-9, https://documents1.worldbank.org/curated/en/736521468331852042/pdf/490020WP0TheEv10Box338937B01PUBLIC1.pdf.

Existem vários tipos de sistemas *RTGS*. O *TARGET2* (*Trans-European Automated Real-time Gross Settlement Express Transfer System*) é um sistema utilizado pelos países da zona Euro para liquidação em Euros. É operado pelo Banco Central Europeu e bancos centrais nacionais[89]. Este sistema tem alguns benefícios, tais como[90]:

- **Eficiência**: Este sistema foi desenhado para processar um alto volume de dados em tempo real e, devido a isto, é possível fazer e receber pagamentos mais rápido e de forma eficiente;
- **Risco reduzido**: O sistema utiliza várias ferramentas de segurança para ter em conta que os pagamentos são seguros, reduzindo assim o risco de fraude ou de erro;
- **Transparência**: São fornecidas todas as informações dos pagamentos, incluindo o estado de cada transação;
- **Interoperabilidade**: É possível gerir diferentes tipos de pagamentos, podendo o sistema operar em diferentes regiões;
- **Redução de custos**: As taxas neste sistema são, normalmente, mais baixas em comparação com os sistemas alternativos de pagamentos.

Já o *Fedwire* é um sistema utilizado pelos Estados Unidos da América operado pela Federal Reserve para liquidação em dólares[91]. Este sistema também tem alguns benefícios[92]:

- **Velocidade**: O *Fedwire* processa as ordens de pagamento em tempo real, garantindo uma rapidez e segurança nas transações críticas;
- **Flexibilidade**: Este sistema oferece várias conexões para o envio e gestão de ordens de pagamento;
- **Segurança**: É garantida a segurança e uma alta disponibilidade, com *backups* regionais e testes regulares.

Por fim, o *CHAPS* (*Clearing House Automated Payment System*) é um sistema utilizado no Reino Unido, gerido pelo Banco de Inglaterra para liquidação em libras[93]. Tal como os outros sistemas, existem alguns benefícios na utilização do *CHAPS*. Nomeadamente, pagamentos de valor alto no mesmo dia de forma segura e eficiente, e uma infraestrutura de liquidação bruta que garante a resiliência operacional[94].

[89] Allsopp, Summers e Veale, "The Evolution of Real-Time Gross Settlement", 31.

[90] European Marchant Bank, "Target2 Explained: What is Target2?", 12 de junho de 2023, https://em.bank/blog/target2-explained-what-is-target2/.

[91] Allsopp, Summers e Veale, "The Evolution of Real-Time Gross Settlement", 13.

[92] Fedwire, "Fedwire Funds Service", https://www.frbservices.org/binaries/content/assets/crsocms/financial-services/wires/funds.pdf.

[93] Allsopp, Summers e Veale, "The Evolution of Real-Time Gross Settlement", 13-14.

[94] Bank of England, "CHAPS", https://www.bankofengland.co.uk/payment-and-settlement/chaps.

- **Plataformas de processamento de dados**

Com o crescente volume de dados a ser gerado neste setor, é necessário utilizar plataformas para gerir e processar estes dados. O principal desafio é conseguir extrair valor desta enorme quantidade de dados, pois os mesmos podem estar estruturados, semiestruturados ou não estruturados. A ferramenta mais utilizada para este fim é o Apache Hadoop[95]. Esta permite que os dados sejam processados e distribuídos por vários computadores utilizando modelos desenhados para serem escaláveis[96]. Existem outras ferramentas como o *HPCC*[97], o *Qubole*[98], que é uma ferramenta de fonte aberta ("*open-source*") que se gere e optimiza sozinha e a *HPE*[99].

Através do uso destes dados, é possível criar modelos analíticos que analisam grandes volumes de informações, tanto históricas como atuais. Estes modelos podem ajudar a antecipar os movimentos do mercado, permitindo que as empresas se ajustem a novas tendências e oportunidades.

A gestão de riscos também beneficia significativamente do uso de análises de dados. Com informações precisas e em tempo real, as organizações podem avaliar e mitigar potenciais riscos, desenvolvendo estratégias proativas. Por fim, a análise de dados pode otimizar vendas e apoiar decisões da equipa de *marketing*, ajudando as empresas a entender melhor o comportamento dos clientes e a personalizar as ofertas, resultando num aumento de receitas. Deste modo, a integração de ferramentas de processamento de dados e de análise torna-se fundamental para a competitividade e a eficiência no setor financeiro[100].

[95] "Apache Hadoop", The Apache Software Foundation, https://hadoop.apache.org/.

[96] Luben Boyanov, "Financial Data Processing in Big Data Platforms", Economic Alternatives 4, (2021): 537, https://www.unwe.bg/doi/eajournal/2021.4/EA.2021.4.03.pdf.

[97] "Home", HPCC Systems, https://hpccsystems.com/.

[98] "Platform", Qubole, https://www.qubole.com/platform.

[99] "HPE AI and data transformation services", Hewlett-Packard Enterprise, https://www.hpe.com/pt/en/services/consulting/big-data.html.

[100] Boyanov, "Financial Data Processing, 535.

1.2. Ameaças

Segundo o *Threat Landscape Report de 2023* da ENISA, os setores bancário e financeiro, apesar de não deixarem de ser um alvo, ficam atrás de outros alvos como a Administração Pública, o setor da saúde, as infraestruturas digitais, os transportes e os prestadores de serviços digitais[101].

É importante sublinhar que ataques significativos neste setor podem impactar todo o ecossistema financeiro, tanto a nível nacional como internacional, colocando a estabilidade financeira em risco[102]. Nos últimos anos, os ataques de cibersegurança neste setor têm vindo a aumentar, sendo agora mais sofisticados e destrutivos. Segundo o estudo "*Impact of cyber-attacks on the financial institutions*" a principal causa deste crescimento foi o acréscimo dos serviços remotos devido à pandemia[103].

Tanto este setor como o setor bancário estão interconectados com vários outros setores e, por esse motivo, estão suscetíveis a várias ameaças como o cibercrime e a ciberespionagem. Tal como referido anteriormente, os ataques neste setor são maioritariamente motivados pela parte financeira e, de acordo com o *Threat Landscape Report* de 2023 da ENISA, os principais ataques passam pelo comprometimento da disponibilidade dos serviços e da informação (ataques de negação de serviço: "*Denial of Service", DoS*), ataques de *ransomware*, contando-se ainda ameaças relativas a dados (*data breaches* e furto de dados)[104]. O ataque predominante foi o *ransomware*, onde 25% dos casos foram operações de um só grupo (*Lockbit*) e 87% dos casos vieram de apenas 20 grupos. Este setor e o setor bancário foram os alvos destes grupos em 6% dos casos[105].

Ciberataques em grande escala ameaçam a confiança no sistema financeiro e até mesmo na economia global. Nesses casos, são alvo de ataques os sistemas de pagamento, compensação ou liquidação, como o sistema *SWIFT*[106]. A interrupção desses serviços pode ter um impacto profundo no funcionamento dos mercados financeiros, comprometendo os fluxos de crédito. No contexto de um ecossistema financeiro cada vez mais interligado, um ataque a uma ou mais instituições ou infraestruturas críticas pode ter efeitos em cascata significativos. O Banco da Índia foi um dos afetados e sofreu um ciberataque em fevereiro de 2015, reportando um prejuízo de cerca de 9 milhões de dólares. Anteriormente, em janeiro do mesmo ano, o Banco del Austro, situado no Equador, sofreu também um ataque reportando também um prejuízo de 9 milhões de dólares[107].

---

[101] ENISA, "ENISA Threat Landscape 2023", 13.

[102] Banco Central Europeu, "Cyber resilience and financial market infrastructures", https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html.

[103] Olivér Gulyás e Gábor Kiss, "Impact of cyber-attacks on the financial institutions", *Procedia Computer Science* 219 (2023): 85, https://doi.org/10.1016/j.procs.2023.01.267.

[104] ENISA, "ENISA Threat Landscape 2023", 14.

[105] ENISA, "ENISA Threat Landscape 2023", 16 e 17.

[106] SWIFT: Society for Worldwide Interbank Financial Telecommunication, responsável pelo sistema de comunicações entre entidades financeiras para transferências internacionais.

[107] Abdul Stanikzai e Munam Shah, "Evaluation of Cyber Security Threats in Banking Systems", *paper* apresentado no 2021 IEEE Symposium Series on Computational Intelligence (SSCI),Orlando, FL, EUA, de 5 a 7 de dezembro 2021, 3, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9659862.

Os ataques a dados, nomeadamente à sua confidencialidade, integridade e disponibilidade, são também uma realidade no setor. As questões de confidencialidade surgem quando informações privadas dentro de uma empresa são divulgadas a terceiros, como no caso de violações de dados. As questões de integridade estão relacionadas com a utilização indevida dos sistemas, como é o caso da fraude, que leva a perdas financeiras diretas. Finalmente, os problemas de disponibilidade estão ligados a interrupções nos negócios que impedem as empresas de operar, resultando em perda de lucros[108].

Em 2011, um ataque de Negação de Serviço Distribuída ("*Distributed Denial of Service" - DDoS*) à Bolsa de Hong Kong interrompeu a divulgação de informações de mercado, forçando a paragem das atividades da mesma[109]. Em 2020, uma série de ataques do mesmo tipo à Bolsa de Valores da Nova Zelândia forçou a paragem das operações durante quatro dias consecutivos[110].

Em fevereiro de 2020, Christine Lagarde, presidente do Banco Central Europeu, veio a público, alertar que um ciberataque poderia originar uma crise financeira, afirmações estas que foram corroboradas pelo FSB (Financial Stability Board)[111]. De acordo com o Fórum Económico Mundial, o risco de ciberataques e de perdas monetárias subiu. Em 2017, houve cerca de 500 milhões de dólares em prejuízo no setor, enquanto em 2021 houve 2,5 mil milhões de dólares. Relativamente aos ataques, em 2017 houve cerca de 8 mil incidentes e em 2021 houve cerca de 11 mil incidentes[112].

[108] Antoine Bouveret, "Cyber Risk for the Financial sector: A Framework for Quantitative Assessment", *Working Paper* do Fundo Monetário Internacional, junho de 2018, 4, https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.

[109] "Hong Kong exchange trading disrupted as hackers target website", *Reuters*, 10 de agosto de 2011, https://www.reuters.com/article/technology/hong-kong-exchange-trading-disrupted-as-hackers-target-website-idUSTRE7792FT/.

[110] "New Zealand stock exchange disrupted by fourth 'offshore' cyber attack", *The Guardian*, 28 de agosto de 2020, https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack.

[111] Tim Maurer e Arthur Nelson, "The Global Cyber Threat to Financial Systems", FINANCE & DEVELOPMENT, março de 2021, 2, https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

[112] Johnny Wood, "Global financial stability at risk due to cyber threats, IMF warns. Here's what to know", *World Economic Forum*, 15 de maio de 2024, https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/.

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos[113], 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[114].
- **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[115].
- ***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[116].
- **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[117]. No caso, consideraram-se os colaboradores internos maliciosos.

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

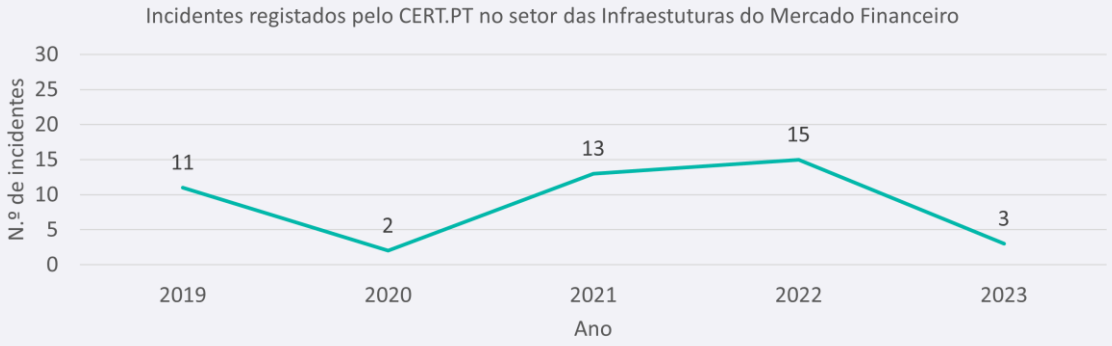
Tabela 5 - Agentes de ameaça mais prováveis (IMF)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Ransomware	■	■	■	■
Malware	■	■	■	■
Vulnerabilidades	■	■	■	■
Phishing e *Smishing*	■	■	■	
Acesso indevido a dados pessoais	■	■	■	■
DDoS	■	■	■	
Manipulação de Sistemas (TI)	■	■		■

Legenda:
■ - Agente de ameaça provável

No questionário realizado, nenhum dos inquiridos indicou ter sofrido qualquer tipo de incidente de segurança. Contudo, esse resultado contraria os números do CNCS e do CERT.PT, que registaram, entre 2019 e 2023, um total de 44 incidentes no setor financeiro[118].

Figura 1 - Número de incidentes no setor das Infraestruturas do Mercado Financeiro anualmente



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

[118] CNCS, "Relatório Riscos e Conflitos" (2023), 10.

1.3. Capacitação

As infraestruturas do mercado financeiro, têm, em Portugal, procurado capacitar-se em cibersegurança de duas formas: através da contratação de profissionais, devido à falta de profissionais na área (**Gráfico 44**) e da aquisição de tecnologia para dar resposta às ameaças visto que 100% do setor tem acesso a equipamentos digitais na realização do seu trabalho (**Gráfico 48**) bem como acesso à internet (**Gráfico 50**). Relativamente à média geral, este setor tem maior percentagem no acesso a equipamentos digitais na realização do seu trabalho e à internet, ambos com 100%.

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

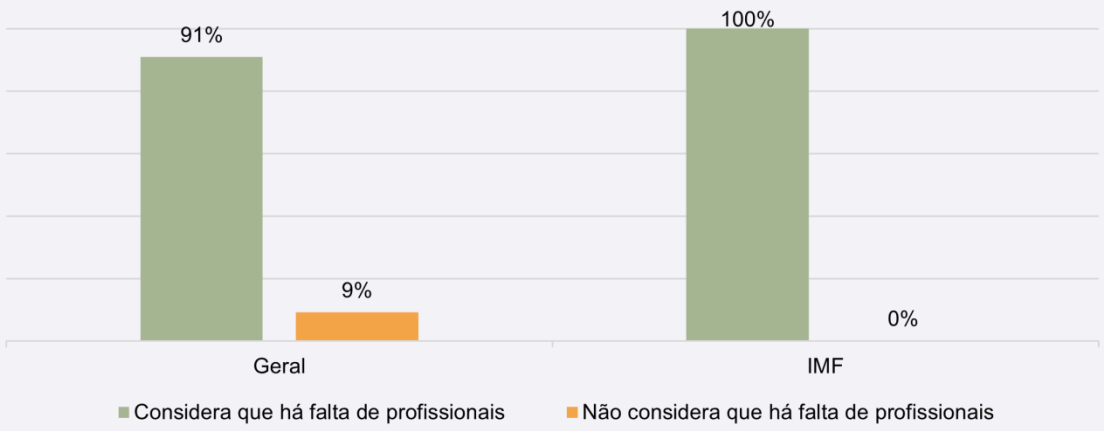


Gráfico 48 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho

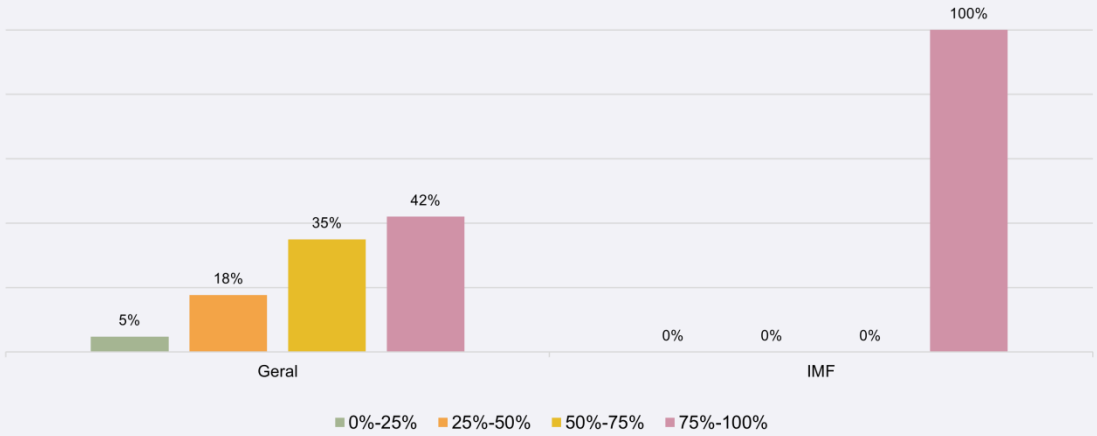
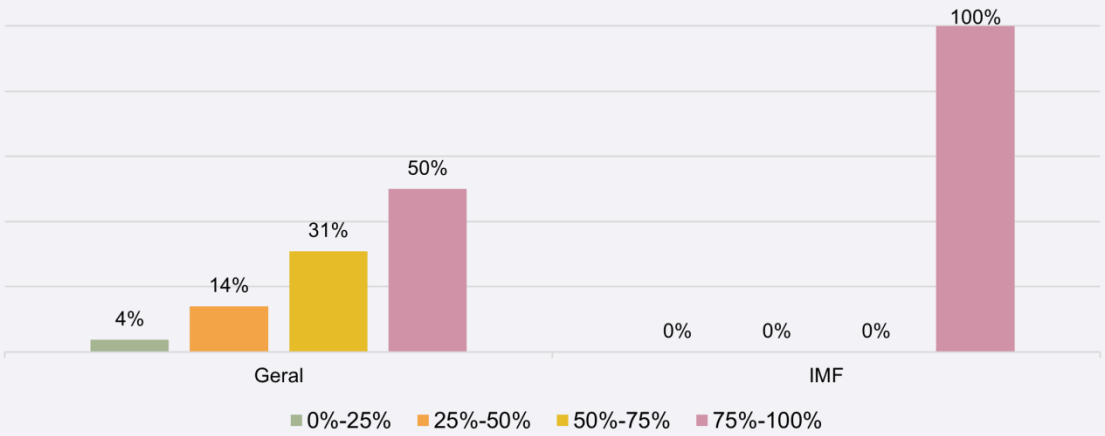


Gráfico 50 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções



Desde 2017, ano em que o Centro Tecnológico da Euronext foi transferido de Belfast para o Porto, a plataforma pan-europeia de Bolsas, que também opera em Portugal, tem aumentado continuamente a equipa dedicada à cibersegurança. Inicialmente, o centro no Porto contava com cerca de 70 profissionais, mas em 2021 esse número já aumentou para aproximadamente 180 trabalhadores. Com o objetivo de fortalecer ainda mais as defesas de cibersegurança, a Euronext planeou contratar mais 50 profissionais em 2022 e pretende adicionar várias dezenas de novos colaboradores até final de 2024[119].

Quanto à aquisição de tecnologia, também a Euronext conta, desde 2018, com a plataforma "*Cymulate Breach & Attack Simulation*", da empresa Cymulate, que permite aos profissionais do grupo realizar uma série de testes, nomeadamente simulam ataques cibernéticos (de cibersegurança) reais para identificar vulnerabilidades e melhorar a postura de segurança da organização aos seus próprios mecanismos de segurança e assim melhorar a sua postura face a ciberataques[120].

[119] Miguel Nogueira,"Centro tecnológico da Euronext no Porto vai contratar para continuar 'história de sucesso'", *Porto.*, 12 de novembro de 2021, https://www.porto.pt/pt/noticia/centro-tecnologico-da-euronext-no-porto-vai-contratar-para-continuar-historia-de-sucesso.

[120] "Euronext adota solução da Cymulate para melhorar resposta a ameaças", *IT Channel*, 28 de novembro de 2019, https://www.itchannel.pt/news/negocios/euronext-adota-solucao-da-cymulate-para-melhorar-resposta-a-ameacas.

No caso das câmaras de compensação e CCPs, a capacitação tem, pelo menos desde 2021, passado pela contratualização externa do serviço de *Security Operations Center* (*SOC*)[121] e de *Cyber Threat Intelligence* (*CTI*)[122], bem como pela mitigação de quaisquer vulnerabilidades identificadas pelo CNCS e ainda pela implementação de melhorias nos controlos de segurança (melhorias nos acessos à *cloud*, filtragem dos acessos à Internet, implementação de autenticação multifator, segmentação de redes). Têm também apostado na formação teórica e prática e na realização de exercícios de cibersegurança[123].

Atualmente, a União Europeia (UE) está a trabalhar num projeto com o objetivo de fortalecer o mercado financeiro, "melhorando assim o acesso ao financiamento a pequenas e médias empresas (PMEs) e os investimentos transfronteiriços. Esta iniciativa, denominada por União dos Mercados de Capitais (UMC)", é destinada a criar um verdadeiro mercado único de capitais, assegurando o livre fluxo de investimento entre todos os Estados-Membros. Esta iniciativa tem três pilares principais:

- Apoiar a recuperação económica ecológica, digital, resiliente e inclusiva das empresas;
- Tornar a UE um espaço mais seguro para o investimento a longo prazo;
- Assegurar a integração dos mercados num único mercado[124].

[121] Responsável pela deteção, resposta e prevenção às ameaças de cibersegurança de uma organização. (Fonte: https://www.ibm.com/topics/security-operations-center)

[122] Informações sobre ameaças que foram agregadas, transformadas, analisadas, interpretadas ou enriquecidas para fornecer o contexto necessário e auxiliar processos de tomada de decisão. (Fonte: "Threat Intelligence", Glossary, NIST, https://csrc.nist.gov/glossary/term/threat_intelligence)

[123] OMI, "Relatório Integrado OMI 2022", maio de 2023, 47, https://www.omie.es/sites/default/files/2023-05/omi_reporting_integrado_2022_PT_4.pdf.

[124] Conselho Europeu, "Construção da União dos Mercados de Capitais da UE", última revisão a 12 junho de 2024, https://www.consilium.europa.eu/pt/policies/what-the-eu-is-doing-to-deepen-its-capital-markets/.

1.4. Investimento em cibersegurança

A par do que tem sido feito ao nível da capacitação no setor, é possível verificar, através dos relatórios de atividades, que têm sido realizados outros esforços no âmbito do reforço da cibersegurança. No caso da Euronext, o grupo revalidou, em 2022, as suas certificações na ISO 22301 (sobre Continuidade de Negócio) e ISO 27001 (sobre Sistemas de Gestão de Segurança da Informação). Tem também sido prestada particular atenção dentro do grupo à preparação para a conformidade com legislação europeia como o *Digital Operational Resilience Act* (DORA), destinado aos setores bancário e financeiro, e com o quadro TIBER-EU[125], um quadro que oferece orientações sobre como as entidades destes dois setores, autoridades e prestadores de serviços de CTI e *Red Team* devem trabalhar em conjunto para testar a sua resiliência num cenário controlado de ciberataque.

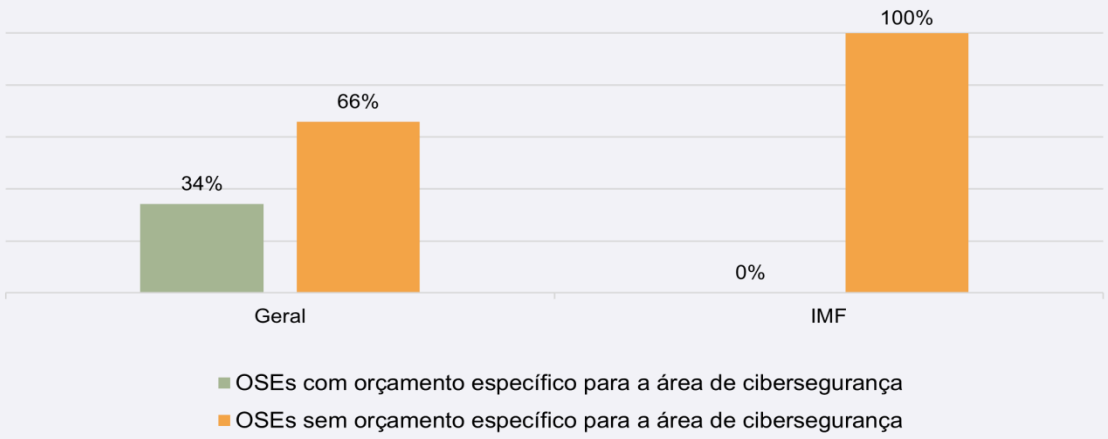
Além disso, o Banco de Portugal e a Comissão do Mercado de Valores Mobiliários (CMVM) têm desenvolvido iniciativas para reforçar a resiliência cibernética. Em 2023, o Banco de Portugal publicou o relatório "Relatório de Estabilidade Financeira" em novembro 2023[126], destacando a importância da cibersegurança na estabilidade financeira e detalhando as medidas implementadas para aumentar a resiliência do sistema financeiro nacional.

Outras iniciativas incluem parcerias entre instituições financeiras e empresas de tecnologia para desenvolver soluções avançadas de cibersegurança. A SIBS, por exemplo, investiu em sistemas de monitorização e deteção de ameaças no ciberespaço, além de participar de exercícios de simulação de ciberataques para testar e aprimorar sua resposta a incidentes. A SIBS participa ativamente em debates e eventos sobre segurança e cibersegurança[127].

[125] Euronext, "Financial Statements as of 31 December 2022", 14, https://www.euronext.com/sites/default/files/2023-06/cassa_di_compensazione_e_garanzia_spa_financial_statement_31.12.2022_eng.pdf.
[126] Banco de Portugal, "Relatório de Estabilidade Financeira", novembro de 2023, 50-51, https://www.bportugal.pt/sites/default/files/documents/2024-02/ref_11_2023_pt.pdf.
[127] SIBS, "Relatório e Contas 2023: Contas Consolidadas", julho de 2024, 42, https://sibs-sites.sibs.pt/sibs/wp-content/uploads/sites/13/2024/07/RC_2023_SIBS_CONSOLIDADO.pdf

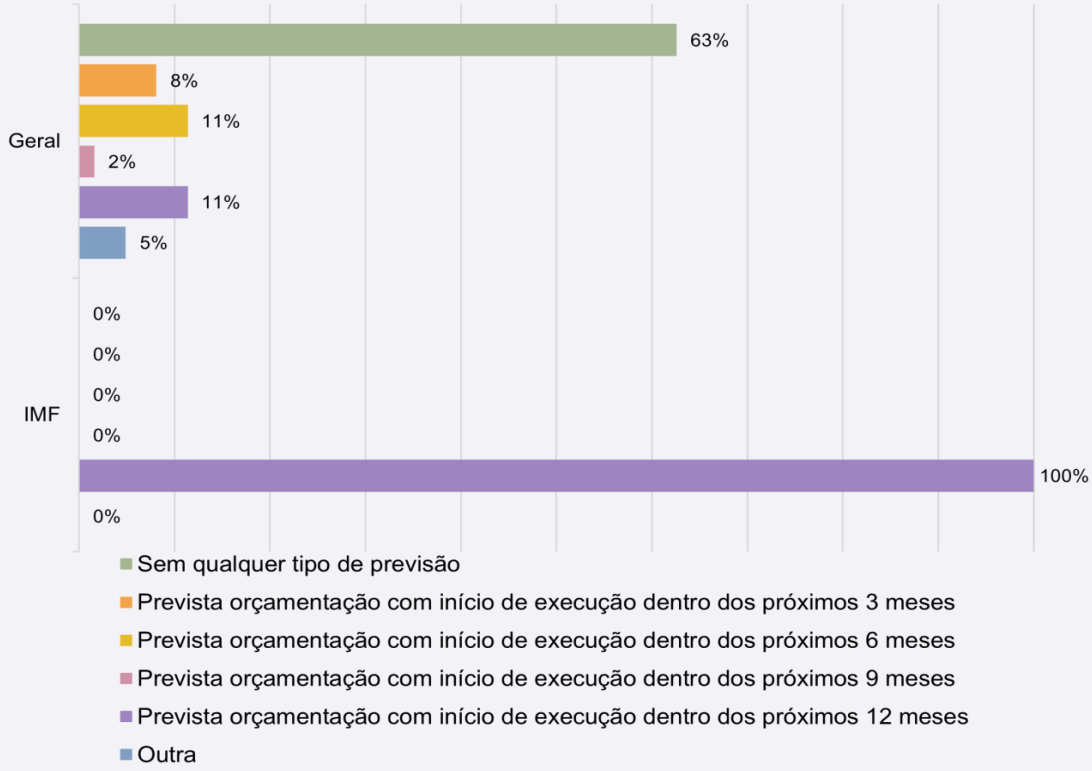
Deste setor, nenhuma das entidades tem um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 66% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



Todas as entidades têm previsto a orçamentação dentro dos próximos 12 meses (**Gráfico 111**).

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



Apesar desses esforços, não foram divulgados números concretos sobre os valores investidos em cibersegurança, dificultando uma avaliação precisa do nível de investimento no setor.

1.5. RJSC e legislação setorial

O setor das infraestruturas do mercado financeiro está sujeito a diversas obrigações legais e regulamentares no âmbito da cibersegurança. A legislação existente é maioritariamente de âmbito europeu, mesmo sendo depois transposta para o ordenamento jurídico nacional (como é o caso das diretivas europeias, cuja transposição é obrigatória). A nível nacional, e de forma a complementar a legislação europeia, o setor é sobretudo orientado por regulamentos e circulares produzidos pela entidade reguladora - a CMVM.

Veja-se então primeiro o que tem sido feito a nível europeu. Em 2012, o Regulamento da União Europeia n.º 648/2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, também conhecido como *European Market Infrastructure Regulation* (EMIR), apesar de não versar exclusivamente sobre cibersegurança, impôs às contrapartes centrais o dever de "manter sistemas informáticos adequados para lidar com a complexidade, variedade e tipo de serviços e atividades desenvolvidos, a fim de assegurar elevados padrões de segurança e a integridade e confidencialidade das informações que detêm"[128].

Por sua vez, em maio de 2014, foi publicada a Diretiva 2014/65/UE, relativa aos mercados de instrumentos financeiros, que impõe às infraestruturas do mercado financeiro a obrigação de "aplicar mecanismos de segurança sólidos para garantir a segurança e a autenticação dos meios de transferência das informações, minimizar o risco de corrupção de dados e de acesso não autorizado e para evitar fugas de informação, mantendo a confidencialidade dos dados em todos os momentos"[129]. Esta diretiva foi transposta para o ordenamento jurídico nacional através da lei n.º 35/2018, de 20 de julho[130].

Também em 2014, em julho, foi publicado o Regulamento da UE n.º 909/2014, relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs), que impôs às CSDs a obrigação de manter "ferramentas de tecnologias de informação adequadas, que garantam um elevado grau de segurança e fiabilidade operacional e que disponham de capacidade suficiente"[131], devendo as "ferramentas de tecnologias de informação ser adequadas para lidar com a complexidade, a variedade e o tipo de serviços e atividades desenvolvidas, de modo a garantir normas de segurança elevadas e a integridade e confidencialidade das informações conservadas"[132].

---

[128] Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, *Jornal Oficial da União Europeia*, 30, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:201:0001:0059:PT:PDF.

[129] Diretiva 2014/65/UE do Parlamento Europeu e do Conselho de 15 de maio de 2014 relativa aos mercados de instrumentos financeiros, *Jornal Oficial da União Europeia*, 173, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014L0065.

[130] Lei n.º 35/2018, de 20 de julho, *Procuradoria-Geral Distrital de Lisboa*, https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2920&tabela=leis&so_miolo=.

[131] Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs), *Jornal Oficial da União Europeia*, 46, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0909.

[132] Regulamento (UE) n.º 909/2014.

Surgiria depois, em 2016, a Diretiva n.º 2016/1148[133] (a Diretiva NIS, cuja transposição para o ordenamento jurídico nacional corresponde à Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço[134]). Foi com esta Diretiva e lei que os operadores do setor das infraestruturas do mercado financeiro foram identificados como Operadores de Serviços Essenciais, sendo-lhes colocadas diversas obrigações ao nível da segurança dos sistemas e redes, bem como ao nível de reporte de incidentes[135]. O RJSC viria a ser complementado pelo Decreto-Lei n.º 65/2021, de 30 de julho, que o regulamenta, e impõe obrigações como a designação de um ponto de contacto permanente, um responsável de segurança, a elaboração e manutenção de um inventário de ativos, a elaboração e implementação de um plano de segurança, a elaboração de um relatório anual que inclua as principais atividades desenvolvidas em matéria de cibersegurança e estatísticas análises agregadas dos incidentes relevantes ocorridos, bem como a realização de uma análise de risco anual[136].

A nível europeu, surge ainda o Regulamento n.º 2022/2554, relativo à resiliência operacional digital do setor financeiro, mais conhecido por DORA (*Digital Operational Resilience Act*). Este regulamento destina-se a várias entidades financeiras, desde bancos, a empresas de seguros, passando também pelas plataformas de negociação e contrapartes centrais. Deste decorrem diversas obrigações, tais como obrigações afetas à gestão do risco associado às tecnologias da informação e comunicação (TIC), gestão dos serviços e ferramentas TIC prestados por terceiros, obrigações ao nível dos sistemas, protocolos e ferramentas TIC, das atividades de proteção e prevenção, deteção, resposta e recuperação em situação de incidente, reporte de incidentes, testes de resiliência operacional, o que inclui a realização de análises de vulnerabilidades, avaliações da segurança das redes, análises da segurança física, revisões do código fonte, testes baseados em cenários, testes de compatibilidade, testes de desempenho, testes de extremo a extremo e testes de penetração[137]. A aplicação deste regulamento será obrigatória a partir de 17 de janeiro de 2025.

Seis anos depois da publicação da Diretiva NIS, foi publicada em 2022 a Diretiva (UE) 2022/2555[138], mais amplamente conhecida como NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: "setores de importância crítica"[139] e "outros setores críticos"[140]. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

---

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

[134] Lei n. º46/2018, de 13 de agosto, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.

[135] Lei n. º46/2018.

[136] Decreto-Lei n. º65/2021, de 30 de julho, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.

[137] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro, Jornal Oficial da União Europeia, 29-51, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554

[138] 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

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

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

Apesar de a Diretiva NIS 2 abranger mais entidades nalguns setores, tal não se verifica no setor das infraestruturas do mercado financeiro. À semelhança do setor bancário, continuam a ser abrangidas as mesmas entidades já visadas pela Diretiva NIS 1. Ao nível de novas obrigações, a Diretiva NIS 2 vem reforçar a necessidade de as medidas de gestão dos riscos de cibersegurança deverem ser do conhecimento dos órgãos de direção das entidades e aprovadas pelos mesmos[141]. 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[142].

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança. O Regulamento DORA inclui provisões semelhantes incentivando este tipo de acordos para o intercâmbio de "informações específicas e sensíveis relativas a ciberataques, nomeadamente indicadores de comprometimento dos sistemas ou dos dados, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração"[143]. Já a Diretiva NIS 2 estabelece que as informações partilhadas à luz destes acordos podem ser relacionadas com "ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques"[144].

Como referido, a nível nacional o setor é sobretudo orientado pelos regulamentos, instruções, recomendações e circulares da CMVM. O Regulamento da CMVM n.º 7/2023 sobre a Regulamentação do Regime da Gestão de Ativos, estabelece sobre as entidades reguladas a obrigação de comunicar, no prazo máximo de 24 horas, "a ocorrência de incidentes relacionados com a segurança de informação e comunicação que impactem o normal funcionamento da sua atividade ou que constituam risco elevado para [o seu] funcionamento"[145]. Já circulares como a 005/2023[146] e a Circular 003/2024 - Circular Anual de Gestão de Ativos 2024[147] reforçam a importância da cibersegurança, as ações de supervisão executadas nessa matéria por parte da CMVM sobre as entidades reguladas e, simultaneamente, alertam as entidades financeiras para a necessidade de estarem em conformidade com o regulamento DORA a partir de 17 de janeiro de 2025.

---

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

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

[143] Regulamento (UE) 2022/2554, artigo 45.º, n.º 1.

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

[145] Regulamento da CMVM n.º 7/2023 Regulamentação do Regime da Gestão de Ativos, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/regulamento-cmvm/7-2023-835896543

[146] Circular 005/2023 - Gestão de Ativos e Empresas de Investimento | Tecnologias da Informação e Comunicação: Cibersegurança - CMVM, https://www.cmvm.pt/PInstitucional/Content?Input=C6DE3F376C5004D8E490034ED0FAA70C0A71D3AE04178CDC0170C5EC472B7D19#.

[147] Circular 003/2024 - Gestão de Ativos – Circular anual de gestão de ativos 2024 - CMVM, https://www.cmvm.pt/PInstitucional/Content?Input=C1B8E11C9FC436AFE660445BDC7E1867050C25D72FD472228ABA2E3FEA4A338B#.

1.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor de infraestruturas de mercado, segundo a ENISA, que define o setor como "*Financial and Banking*". Neste sentido, os *standards* e as boas práticas aplicadas a este setor são, muitas vezes, os mesmos seguidos que o setor bancário, por trabalharem em várias circunstâncias com sistemas, ativos e métodos semelhantes[148].

Tabela 6 - Standards e Boas Práticas (Infraestruturas do Mercado Financeiro)

Standards	Boas práticas
• Gramm–Leach–Bliley Act; • Sarbanes–Oxley Act; • Diretiva (UE) 2015/2366, relativa aos serviços de pagamento no mercado interno (PSD2); • EBA - Orientações definitivas sobre a segurança dos pagamentos efetuados através da Internet; • American National Standards Institute (ANSI) X9 series.	• Payment Card Industry Data Security Standard (PCI DSS); • Basel II; • EBA - Orientações definitivas sobre a segurança dos pagamentos efetuados através da Internet; • CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure; • SEC OCIE Cybersecurity.

Na tabela anterior estão os *standards* e boas práticas referentes à área das infraestruturas do mercado financeiro. De seguida, apresenta-se um breve sumário de cada um:

- **Gramm–Leach–Bliley Act:** Lei dos EUA que exige que instituições financeiras protejam a confidencialidade e a segurança das informações dos clientes[149];
- **Sarbanes–Oxley Act:** Lei dos EUA com disposições que afetam a governação das empresas, a gestão de riscos, auditorias e os relatórios financeiros das empresas públicas, incluindo disposições destinadas a dissuadir e punir a fraude e a corrupção[150].
- **Diretiva (UE) 2015/2366, relativa aos serviços de pagamento no mercado interno (PSD2):** Diretiva da UE com o objetivo de modernizar os serviços de pagamento na Europa, promovendo a inovação e aumentando a segurança nas transações[151];
- **EBA - Orientações definitivas sobre a segurança dos pagamentos efetuados através da Internet:** Orientações da EBA para melhorar a segurança dos pagamentos pela Internet, reduzindo riscos de fraude e aumentando a proteção ao consumidor[152];

[148] ENISA, "Mapping of OES Security Requirements to Specific Sectors", 18 de janeiro de 2018, 28 https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors.

[149] "Gramm-Leach-Bliley Act", Business Guidance: Privacy and Security, United States Federal Trade Commission, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[150] "The Sarbanes-Oxley Act", Sarbanes Oxley Act, https://sarbanes-oxley-act.com/.

[151] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, *Jornal Oficial da União Europeia*, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366.

[152] "Orientações definitivas sobre a segurança dos pagamentos efetuados através da internet", EBA, https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/558993c7-c253-472c-bae3-f897f6c6038a/EBA-GL-2014-12_PT_rev1%20GL%20on%20Internet%20Payments.pdf.

- **American National Standards Institute (ANSI) X9 series:** Conjunto de normas que definem padrões de segurança para transações financeiras, garantindo a integridade e confidencialidade das mesmas[153];
- **Payment Card Industry Data Security Standard (PCI DSS):** Conjunto de padrões de segurança para proteger as informações dos cartões de pagamento e evitar fraudes[154];
- **Basel II:** Acordo internacional que estabelece normas para a regulação bancária[155];
- **EBA - Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2):** Orientações preliminares para medidas de segurança e gestão de riscos operacionais nos serviços de pagamento sob a PSD2[156];
- **CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure:** Diretrizes para aumentar a resiliência de cibersegurança das infraestruturas dos mercados financeiros[157];
- **SEC OCIE Cybersecurity:** Diretrizes da SEC (Securities and Exchange Commission - EUA) para avaliar a postura de cibersegurança das empresas financeiras[158].

[153] "X9: Accredited Standards Committee X9, Inc.", ANSI Webstore, American National Standards Institute, https://webstore.ansi.org/sdo/x9?source=blog&_gl=1*v6wen5*_gcl_au*NzI0ODc2NzI1LjE3MjU1NTU5ODc.

[154] "PCI Data Security Standard (PCI DSS)", Standards, Security Standards Council, https://www.pcisecuritystandards.org/standards/pci-dss/.

[155] "Basel II: Revised international capital framework", Basel Committee on Banking Supervision, Bank for International Settlements, https://www.bis.org/publ/bcbsca.htm.

[156] "Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)", EBA, 12 de janeiro de 2018, https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf.

[157] "Guidance on cyber resilience for financial market infrastructures", BIS e IOSCO, junho de 2016, https://www.bis.org/cpmi/publ/d146.pdf.

[158] "OCIE Cybersecurity and Resiliency Observations", U.S. Securities and Exchange Commission, https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

1.7. Desafios

As infraestruturas do mercado financeiro enfrentam desafios semelhantes aos do setor bancário. São alvos apetecíveis para ciberataques, sobretudo os que podem vir a afetar a disponibilidade dos serviços e da informação, como ataques de *DDoS* e de *ransomware*, bem como os que podem comprometer a segurança e integridade dos dados, como *data breaches*. São também um setor onde os ciberataques podem ter um efeito em cadeia, tornando-se impossível circunscrever os impactos de um ciberataque a uma organização ou a um território, comprometendo assim a estabilidade financeira internacional.

Adicionalmente, são um setor que tem de navegar uma regulamentação extensa e complexa e encetar diversos esforços para estar em conformidade com tudo o que a regulamentação e legislação lhe exige. Por exemplo, o regulamento DORA, em vigor desde janeiro de 2023, e que será de cumprimento obrigatório para as entidades dos setores bancário e financeiro a partir de janeiro de 2025, traz novas exigências ao nível da gestão do risco das TIC, gestão do risco das TIC com terceiros, testes de resiliência operacional digital, incidentes relacionados com as TIC, da partilha de informação e da supervisão dos prestadores de serviços terceiros críticos. Diversas entidades estão já a tomar as medidas necessárias para estarem em conformidade com o regulamento a partir de janeiro de 2025.

1.8. Recomendações

O Conselho Nacional de Supervisores Financeiros (CNSF) destaca a importância da Gestão da Continuidade de Negócio (Business Continuity - BC) no setor financeiro, particularmente para as infraestruturas do mercado financeiro. A continuidade de negócio é essencial para assegurar a manutenção ou rápida recuperação de funções críticas em caso de interrupções operacionais, minimizando impactos nos mercados financeiros. Este enfoque reflete-se nas orientações e normativos do CNSF, que visam fortalecer a resiliência operacional no setor face a riscos como ciberataques ou desastres naturais.

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

Tabela *7* - Cenários de risco (IMF)

Cenários de risco
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento.
Campanha de PHISHING dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
COLABORADOR que, por vingança, por razões financeiras ou por negligência, expõe informação sensível da entidade ou instala *software* malicioso que compromete a organização com *spyware*, *ransomware* ou outro tipo de ameaça.
FUGA DE INFORMAÇÃO da organização, causada eventualmente por violação de dados e ação intencional de um colaborador, expondo nos media e ao público em geral dados pessoais, dados financeiros, trocas de emails, propriedade intelectual, entre outras.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

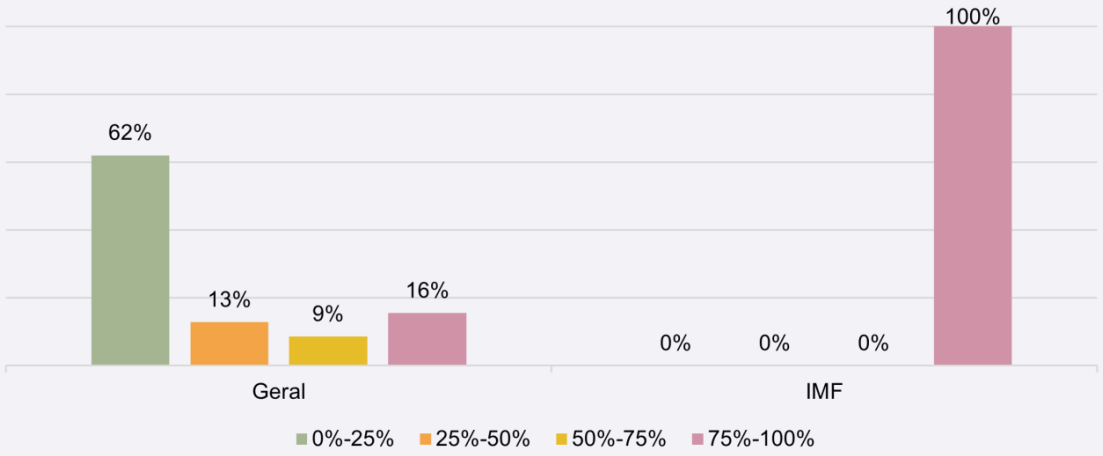
(Fonte: CNCS, "Riscos & Conflitos 2021", última atualização em 30 de agosto de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf)

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

Formação

As ameaças mais prevalentes neste setor são o *ransomware* e as ameaças relativas a dados pessoais dos clientes, sendo estas ameaças concretizadas, normalmente, através de ataques bem-sucedidos de *phishing*. A sensibilização para este tipo de riscos e a formação para identificar estes riscos são essenciais para impedir que estas se concretizem, pois a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Este setor está à frente da média geral, dado que em os OSE, 75%-100% trabalhadores têm formação básica em cibersegurança quando, no âmbito geral, apenas 16% dos setores estão nesse patamar (**Gráfico 33**).

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



Os resultados do questionário evidenciam que a totalidade dos OSE do setor disponibiliza formação em cibersegurança aos seus colaboradores (**Gráfico 38**), sendo que todas são de carácter obrigatório (**Gráfico 39**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

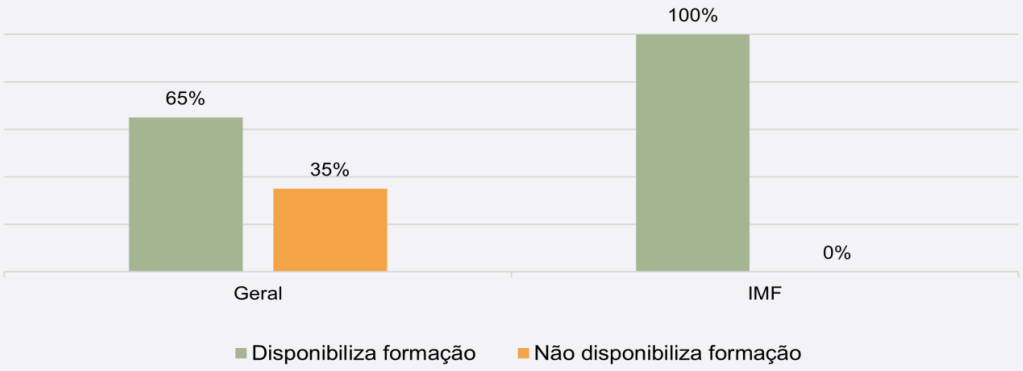
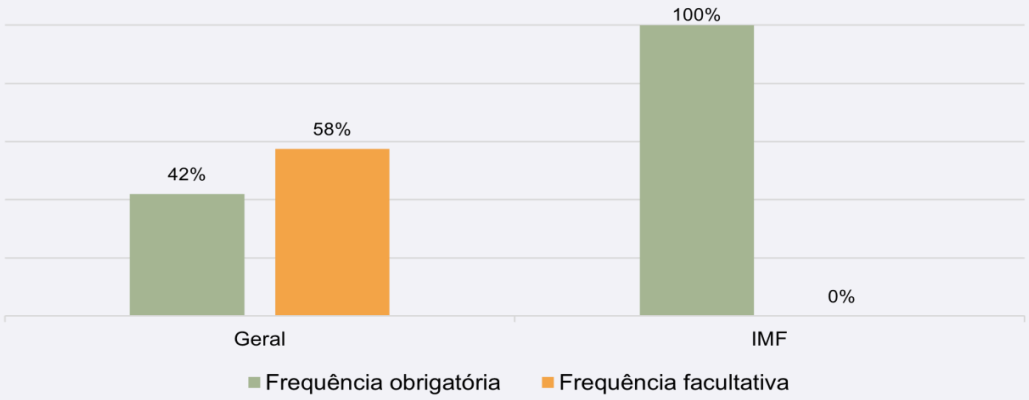
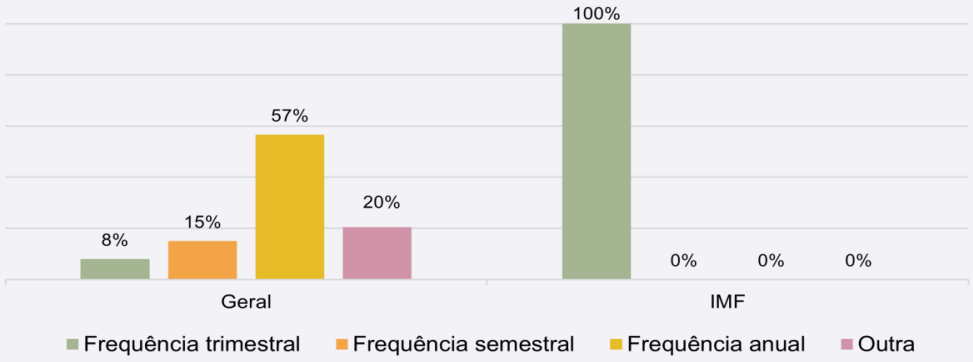


Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



Além disso, em todas as entidades, os momentos de formação têm frequência trimestral (**Gráfico 41**), o que no contexto do setor assegura a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores.

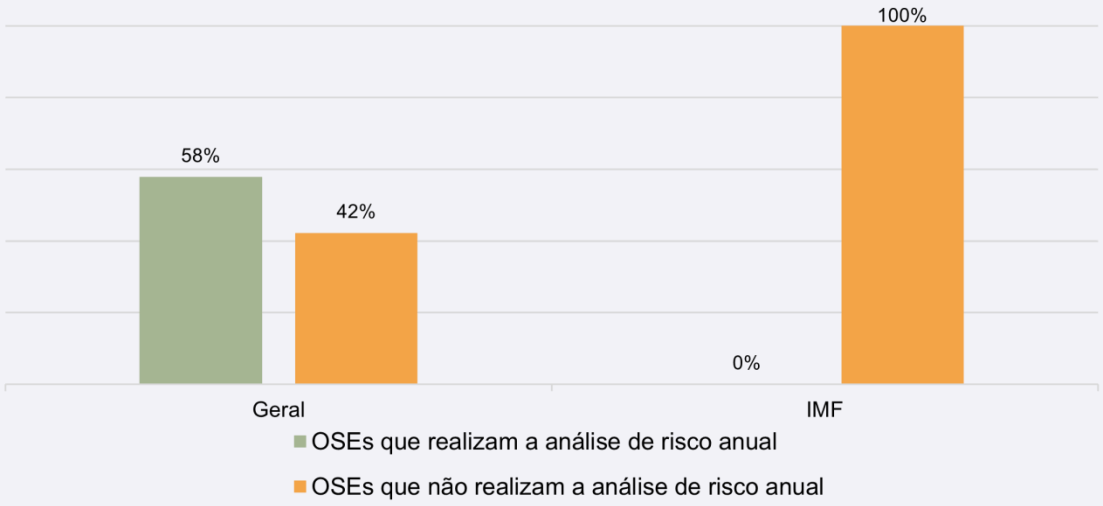
Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que este setor, comparativamente com os restantes, está acima da média, com exceção na utilização de *browser* que proteja a privacidade, segurança de rede em *cloud*, controlos biométricos para identificação e autenticação de utilizadores e *backups* de dados em diferentes localizações. Este setor é o único onde não se realiza avaliações de segurança anuais no âmbito de cibersegurança (**Gráfico 99**).

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



Nesse sentido, recomenda-se aos OSE do setor das infraestruturas do mercado financeiro que:

- Realizem avaliações de segurança, em todas as entidades, pelo menos anualmente;
- Realizem análises de risco pelo menos anualmente;
- Implementem, onde possível, controlos biométricos para identificação e autenticação de utilizadores;
- Implementem *backups* de dados em diferentes localizações.

Políticas, procedimentos e planos de cibersegurança

Com base nos dados reunidos no questionário, 100% dos OSE do setor possuíam políticas e procedimentos de cibersegurança documentados e implementados. Todos os inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Diante desta situação, apesar de todos OSE do setor terem uma política de segurança, é importante que a mesma verse sobre:

- Os diversos papéis e responsabilidades dos vários colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, como os controlos de acesso (lógico e físico);
- A gestão de incidentes, incluindo a elaboração de um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação, além de um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir, que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização periódica da política (pelo menos anualmente), para manter a mesma atualizada conforme a evolução das ameaças de cibersegurança e as mudanças na organização.

Considerando que nenhum dos OSE do setor indicaram possuir uma política de uso aceitável de ativos e uma política de gestão de ativos, recomenda-se também a elaboração de uma política de gestão de ativos alinhada com a política de cibersegurança.

Análise de vulnerabilidades e realização de testes de intrusão (*pentesting*)

Todos os OSE do setor das infraestruturas do mercado financeiro realizam procedimentos de deteção e gestão de vulnerabilidades, sendo este ponto importante tendo em vista a diminuição e antecipação de possíveis ataques. A deteção e análise, e correção de vulnerabilidades é uma prática importante para a proteção proativa e preventiva dos sistemas e aplicações em utilização em qualquer setor de atividade.

Quanto à realização de testes de intrusão, todos os OSE realizam os mesmos. É importante a realização deste tipo de testes, pois é mais uma maneira de identificar vulnerabilidades, corrigi-las e tornar os OSE mais resilientes em matéria de cibersegurança.

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

- **Controlos básicos**: controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais**: controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais**: controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*[159].

No setor das infraestruturas de mercado financeiro, os controlos fundacionais, relacionados com a segurança da rede, desempenham um papel particularmente crítico. Infraestruturas essenciais, como sistemas de compensação e liquidação, plataformas de negociação e redes de pagamento, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para assegurar a integridade, disponibilidade e continuidade dos serviços financeiros. Falhas ou configurações inadequadas podem ser exploradas para interromper transações financeiras, comprometer a segurança de dados sensíveis, ou desviar operações críticas, colocando em risco a estabilidade e a confiança nos mercados financeiros.

[159] "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[160]:

Tabela 8 - Controlos de Segurança da CIS (IMF)

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)

[160] "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

- Allsopp, Peter, Bruce Summers e John Veale. “The Evolution of Real-Time Gross Settlement: Access, Liquidity and Credit, and Pricing”. World Bank, fevereiro de 2009. https://documents1.worldbank.org/curated/en/736521468331852042/pdf/490020WP0TheEv10Box338937B01PUBLIC1.pdf.
- American National Standards Institute. “X9: Accredited Standards Committee X9, Inc.”. ANSI Webstore. https://webstore.ansi.org/sdo/x9?source=blog&_gl=1*v6wen5*_gcl_au*NzI0ODc2NzI1LjE3MjU1NTU5ODc.
- 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. “Utilização da Internet das Coisas (IoT - Internet of Things)”, 2022.
- Arner, Douglas. “FinTech: Evolution and Regulation”, Asian Institute of International Financial Law, University of Hong Kong, junho de 2016. https://law.unimelb.edu.au/__data/assets/pdf_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf.
- Bação, Pedro, Carlos Carreira, João Cerejeira, Gilberto Loureiro, António Martins e Miguel Portela. “Investimento Empresarial e o Crescimento da Economia Portuguesa”. Coordenação de Fernando Alexandre. Fundação Calouste Gulbenkian, 2017. https://gulbenkian.pt/wp-content/uploads/2017/11/Estudo_relatorio_Investimento_Empresarial_final_dez2017.pdf.
- Banco Central Europeu. “Central Counterparty Clearing Houses and Financial Stability”. Financial Stability Review, 2005. https://www.ecb.europa.eu/pub/pdf/fsr/art/ecb.fsrart200512_06.en.pdf.
- Banco Central Europeu. “Cyber resilience and financial market infrastructures”. https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html.
- Banco de Portugal. “Outros sistemas de liquidação”. Infraestruturas de mercado. https://www.bportugal.pt/page/outros-sistemas-de-liquidacao.
- Banco de Portugal. “Relatório de Estabilidade Financeira”, novembro de 2023. https://www.bportugal.pt/sites/default/files/documents/2024-02/ref_11_2023_pt.pdf.
- Bank for International Settlements e International Organization of Securities Commissions. “Guidance on cyber resilience for financial market infrastructures”, junho de 2016. https://www.bis.org/cpmi/publ/d146.pdf.
- Bank for International Settlements. “Basel II: Revised international capital framework”, Basel Committee on Banking Supervision. https://www.bis.org/publ/bcbsca.htm.
- Bank of England. “CHAPS”. https://www.bankofengland.co.uk/payment-and-settlement/chaps.

- Barata, André. “O Regime Europeu de Resolução de Contrapartes Centrais: a peça que faltava ao mercado dos derivados de balcão?”. Revista de Direito Financeiro e dos Mercados de Capitais, dezembro de 2023. https://rdfmc.com/wp-content/uploads/2024/01/Revista-de-Direito-Financeiro-e-do-Mercado-de-Capitais-2-20231.pdf.
- Bouveret, Antoine. “Cyber Risk for the Financial sector: A framework for Quantitative Assessment”. *Working Paper* do Fundo Monetário Internacional, junho de 2018. https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.
- Boyanov, Luben. “Financial Data Processing in Big Data Platforms”. Economic Alternatives 4, 2021. https://www.unwe.bg/doi/eajournal/2021.4/EA.2021.4.03.pdf.
- Calzolari,Giacomo. “Artificial Intelligence market and capital flows: Artificial Intelligence and the financial sector at crossroads”. Estudo para o Parlamento Europeu, maio de 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf.
- Center for Internet Security. “The 18 CIS Critical Security Controls”, CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list.
- CMVM. “Circular 003/2024 - Gestão de Ativos – Circular anual de gestão de ativos 2024”. https://www.cmvm.pt/PInstitucional/Content?Input=C1B8E11C9FC436AFE660445BDC7E1867050C25D72FD472228ABA2E3FEA4A338B#.
- CMVM. “Circular 005/2023 - Gestão de Ativos e Empresas de Investimento | Tecnologias da Informação e Comunicação: Cibersegurança”. https://www.cmvm.pt/PInstitucional/Content?Input=C6DE3F376C5004D8E490034ED0FAA70C0A71D3AE04178CDC0170C5EC472B7D19#.
- 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. “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. “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancacncs.pdf.
- CNCS. “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2023”. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf.
- CNCS. “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança. https://www.cncs.gov.pt/pt/observatorio/#relatorios.
- CNCS. ISAC. https://www.cncs.gov.pt/pt/isac/.
- 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.
- Conselho Europeu, “Horizonte Europa”. https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Conselho Europeu. “Construção da União dos Mercados de Capitais da UE”, última revisão a 12 junho de 2024. https://www.consilium.europa.eu/pt/policies/what-the-eu-is-doing-to-deepen-its-capital-markets/.

- Conselho Europeu. “Horizonte Europa”. https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Decreto-Lei n.º 65/2021, de 30 de julho. Diário da República. https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.
- Department for Science, Innovation & Technology, “Cyber security breaches survey 2023”, 19 de abril de 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
- Department 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, Mariana. “Euronext Lisboa cresce em 2022. Foram negociados 137 milhões de euros por dia”, Dinheiro Vivo, 28 de fevereiro de 2023. https://www.dinheirovivo.pt/bolsa/euronext-lisboa-cresce-em-2022-foram-negociados-137-milhoes-de-euros-por-dia-15918612.html/.
- Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366.
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.
- Diretiva (UE) 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 2014/65/UE do Parlamento Europeu e do Conselho de 15 de maio de 2014 relativa aos mercados de instrumentos financeiros, Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014L0065.
- EBA. “Orientações definitivas sobre a segurança dos pagamentos efetuados através da internet”. https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/558993c7-c253-472c-bae3-f897f6c6038a/EBA-GL-2014-12_PT_rev1%20GL%20on%20Internet%20Payments.pdf.
- EBA. “Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)”, 12 de janeiro de 2018. https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf.
- 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. “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. “ENISA Threat Landscape 2023”, 19 de outubro de 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.
- ENISA. “Mapping of OES Security Requirements to Specific Sectors”, 18 de janeiro de 2018. https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors.
- ENISA. “NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist”, 11 de dezembro de 2020. https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist.
- ENISA. “NIS Investments”, 2021. https://www.enisa.europa.eu/publications/nis-investments-2021.
- ENISA. “NIS Investments”, 2022. https://www.enisa.europa.eu/publications/nis-investments-2022.
- ENISA. “NIS Investments”, 2023. https://www.enisa.europa.eu/publications/nis-investments-2023.
- ESMA. “Financial Reporting”. Issuer Disclosure. https://www.esma.europa.eu/issuer-disclosure/financial-reporting.
- Euronext, “Financial Statements as of 31 December 2022”. https://www.euronext.com/sites/default/files/2023-06/cassa_di_compensazione_e_garanzia_spa_financial_statement_31.12.2022_eng.pdf.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), “Impact”. https://www.ee-isac.eu/impact/#.
- FIX Trading Community. “FIX 5.0 Specifications”. https://www.fixtrading.org/standards/unsupported/fix-5-0/.
- 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.
- Gulyas, Oliver e Gabor Kiss. “Impact of cyber-attacks on the financial institutions”, Procedia Computer Science 219, 2023. https://doi.org/10.1016/j.procs.2023.01.267.
- Heider, Florian. “Collateral, central clearing counterparties and regulation”, European Central Bank Research Bulletin 41, 6 de dezembro de 2017. https://www.ecb.europa.eu/press/research-publications/resbull/2017/html/ecb.rb171206.en.html.
- Hewlett-Packard Enterprise. “HPE AI and data transformation services”. https://www.hpe.com/pt/en/services/consulting/big-data.html.
- HPCC Systems. “Home”. https://hpccsystems.com/.
- https://www.anacom.pt/streaming/relatorioInternet_dasCoisas_IoT2022.pdf?contentId=1737940&field=ATTACHED_FILE.
- Hussain, Shatha, Amer Alaya e Thana Azizi. “The impact of financial accounting disclosures on investors’ reactions towards bad news: The moderating role of investors’ sentiments”. Cogent Economics and Finance, 16 de julho de 2023. https://www.tandfonline.com/doi/pdf/10.1080/23322039.2023.2228087?download=true.
- 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. “Inquérito à Utilização das TIC nas Empresas”, 2022. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=585250024&att_display=n&att_download=y.
- INE. “Inquérito à utilização de tecnologias da informação e da comunicação nas empresas”, 21 de novembro de 2023. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637881953&att_display=n&att_download=y.
- International Monetary Fund. “World Economic Outlook: Challenges to Steady Growth”, outubro de 2018. https://www.imf.org/-/media/Files/Publications/WEO/2018/October/English/main-report/Text.ashx.
- ISO, “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- ISO. “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- IT Channel. “Euronext adota solução da Cymulate para melhorar resposta a ameaças”, 28 de novembro de 2019. https://www.itchannel.pt/news/negocios/euronext-adota-solucao-da-cymulate-para-melhorar-resposta-a-ameacas.
- Jia, Hao, Yuxiang Huan, Chen Ding, Yulong Yan, Jianjun Cui e Jiachen Wang. "A Domain-Specific Accelerator for Ultralow Latency Market Data Distribution System," IEEE Transactions on Industrial Informatics, vol. 19, no. 4, abril de 2023. https://ieeexplore.ieee.org/abstract/document/9801674.
- Lei n.º 35/2018, de 20 de julho, Procuradoria-Geral Distrital de Lisboa. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2920&tabela=leis&so_miolo=.
- Lei n.º 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.
- Maurer, Tim e Arthur Nelson. “The Global Cyber Threat to Financial Systems”, FINANCE & DEVELOPMENT, março de 2021. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.
- Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- NIST. “Threat Intelligence”. Glossary. https://csrc.nist.gov/glossary/term/threat_intelligence.
- Nogueira, Miguel. “Centro tecnológico da Euronext no Porto vai contratar para continuar ‘história de sucesso’”. Porto., 12 de novembro de 2021. https://www.porto.pt/pt/noticia/centro-tecnologico-da-euronext-no-porto-vai-contratar-para-continuar-historia-de-sucesso.
- OMI, “Relatório Integrado OMI 2022”, maio de 2023. https://www.omie.es/sites/default/files/2023-05/omi_reporting_integrado_2022_PT_4.pdf.
- OMIClear. “Quem somos”. https://www.omiclear.pt/pt.
- Palmié, Maximilian, Joakim Wincent; Vinit Parida e Umur Caglar. “The evolution of the financial technology ecosystem: an introduction and agenda for future research on disruptive innovations in ecosystems”. University of Vaasa, 2020. https://osuva.uwasa.fi/bitstream/handle/10024/10315/Osuva_Palmi%C3%A9_Wincent_Parida_Caglar_2020b.pdf?sequence=2&isAllowed=y.
- PORDATA, “Empresas: total e por dimensão”, dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.

- PORDATA. “Empresas: total e por dimensão”, dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- Qubole. “Platform”. https://www.qubole.com/platform.
- Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554.
- Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012R0648.
- Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0909.
- Regulamento da CMVM n.º 7/2023 Regulamentação do Regime da Gestão de Ativos. Diário da República. https://diariodarepublica.pt/dr/detalhe/regulamento-cmvm/7-2023-835896543.
- Reuters. “Hong Kong exchange trading disrupted as hackers target website”. 10 de agosto de 2011. https://www.reuters.com/article/technology/hong-kong-exchange-trading-disrupted-as-hackers-target-website-idUSTRE7792FT/.
- Sarbanes Oxley Act. “The Sarbanes-Oxley Act”, https://sarbanes-oxley-act.com/.
- Schizas, Emmanuel, Rui Hao, Keith Bear, Massimo Preziuso, Elizabeth Seger, Robert Wardrop, Raghavendra Rau, Pradeep Debata, Philip Rowan, Nicola Adams, Mia Gray e Nikos Yerolemou. “Transforming Paradigms: A Global AI in Financial Services Survey”. World Economic Forum, 29 de fevereiro de 2020. https://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf.
- Security Standards Council. “PCI Data Security Standard (PCI DSS)”. Standards. https://www.pcisecuritystandards.org/standards/pci-dss/.
- SIBS. “Relatório e Contas 2023: Contas Consolidadas”, julho de 2024. https://sibs-sites.sibs.pt/sibs/wp-content/uploads/sites/13/2024/07/RC_2023_SIBS_CONSOLIDADO.pdf.
- Soltani, Reza, Marzia Zaman, Rohit Joshi e Srinivas Sampalli. “Distributed Ledger Technologies and Their Applications: A Review”, Applied Sciences 12, 2022. https://doi.org/10.3390/app12157898.
- Stanikzai, Abdul e Munam Shah. "Evaluation of Cyber Security Threats in Banking Systems". Paper apresentado no 2021 IEEE Symposium Series on Computational Intelligence (SSCI),Orlando, FL, EUA, de 5 a 7 de dezembro 2021. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9659862.
- Sulaiman Asif, “Cyber Threat Analysis: Types, Benefits, Tools, Approaches”, Knowledge Hut, September 5, 2023. https://www.knowledgehut.com/blog/security/threat-analysis.
- Tamplin, True. “Advantages of Financial Information Exchange (FIX)”. Finance Strategists, 12 de julho de 2023. https://www.financestrategists.com/wealth-management/investment-management/financial-information-exchange-fix/#advantages-of-financial-information-exchange-fix.
- The Apache Software Foundation. “Apache Hadoop”. https://hadoop.apache.org/.
- The Guardian. “New Zealand stock exchange disrupted by fourth 'offshore' cyber attack”, 28 de agosto de 2020. https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack.
- U.S. Securities and Exchange Commission. “OCIE Cybersecurity and Resiliency Observations”.

https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

- United States Federal Trade Commission. “Gramm-Leach-Bliley Act”. Business Guidance: Privacy and Security. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.
- Vujičić,Dejan, Dijana Jagodić e Siniša Ranđić. "Blockchain technology, bitcoin, and Ethereum: A brief overview”. Paper apresentado no 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), Sarajevo, Bósnia e Herzegovina, de 21 a 23 de março de 2018. https://ieeexplore.ieee.org/abstract/document/8345547/.
- Wongthongtham, Pornpit, Daniel Marrable, Bilal Abu-Salih, Xin Liu e Greg Morrison. “Blockchain-enabled Peer-to-Peer energy trading”. Computers & Electrical Engineering 94, setembro de 2021. https://doi.org/10.1016/j.compeleceng.2021.107299.
- Wood, Johnny. “Global financial stability at risk due to cyber threats, IMF warns. Here's what to know”. World Economic Forum, 15 de maio de 2024. https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/.
- World Bank. “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.
- World Economic Forum. “Global Cybersecurity Outlook 2024”, janeiro de 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

www.cncs.gov.pt/

Observatório
de **Cibersegurança**