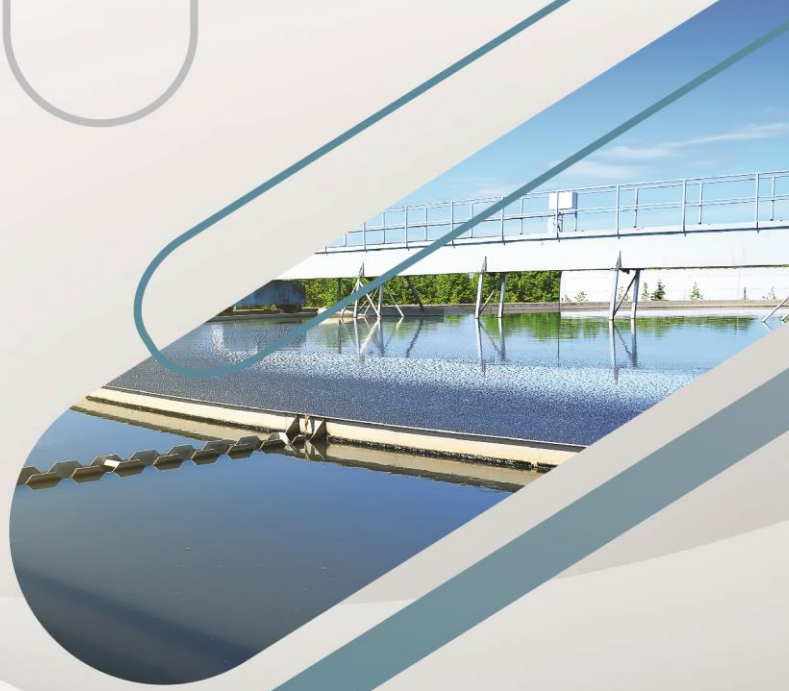
CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de **Cibersegurança**



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

Fornecimento e Distribuição de Água Potável

Caracterização, Regulamentação e Recomendações no Âmbito do Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

Índice

Índice de Gráficos

Índice de Figuras

Índice de Tabelas

Introdução

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

Foi neste contexto que surgiu a Diretiva NIS[1], derivada da necessidade formalizada pelo Parlamento Europeu e Conselho da UE da implementação e harmonização de medidas destinadas a garantir um elevado nível de segurança das redes e da informação em toda a UE. Esta necessidade advém, desde logo, da necessidade de garantir a fiabilidade, a segurança e a confiança nas atividades económicas e societais e no mercado interno.

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

A Diretiva NIS estabelece, entre outros, requisitos de segurança e de notificação para os Operadores de Serviços Essenciais (OSE), categorizando-os em setores e subsetores.

No contexto português, esta Diretiva foi transposta através da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC).

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

[1] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[2] Lei n.º 46/2018, de 13 de agosto, (art. 3º, al. g), Diário da República n.º 155/2018.

[3] Lei n.º 46/2018, de 13 de agosto, (art. 3º, al. t).

Os setores considerados para efeitos da consideração como OSE são os seguintes: 1) Energia; 2) Transportes; 3) Bancário; 4) Infraestruturas do mercado financeiro; 5) Saúde; 6) Fornecimento e distribuição de água potável; 7) Infraestruturas digitais. Cada um destes setores pode incluir subsetores a considerar, bem como tipos de entidades claramente identificados na lei. Estas considerações serão incluídas nos respetivos capítulos.

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

Contexto do relatório

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

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

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

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

Objetivos do relatório

Este relatório teve como principais objetivos:

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

O relatório elaborado atenderá aos seguintes pontos na análise setorial:

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

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

Contexto Geral

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

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

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

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

[4] Lei n.º 46/2018, de 13 de agosto, (Art. 3º, al. g).
[5] Lei n.º 46/2018, de 13 de agosto, (Art. 3º, al. t).

De um modo geral, a Diretiva NIS indica ainda que devem ser considerados os seguintes critérios para verificar se uma entidade é um OSE: A entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais; A prestação desse serviço depende de redes e sistemas de informação; e um incidente pode ter efeitos perturbadores importantes na prestação desse serviço[6].

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

Tabela 1 - Setores, Subsetores e Tipos de Entidades

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

[6] Lei n.º 46/2018, de 13 de agosto, (Art. 3º, al. t).

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

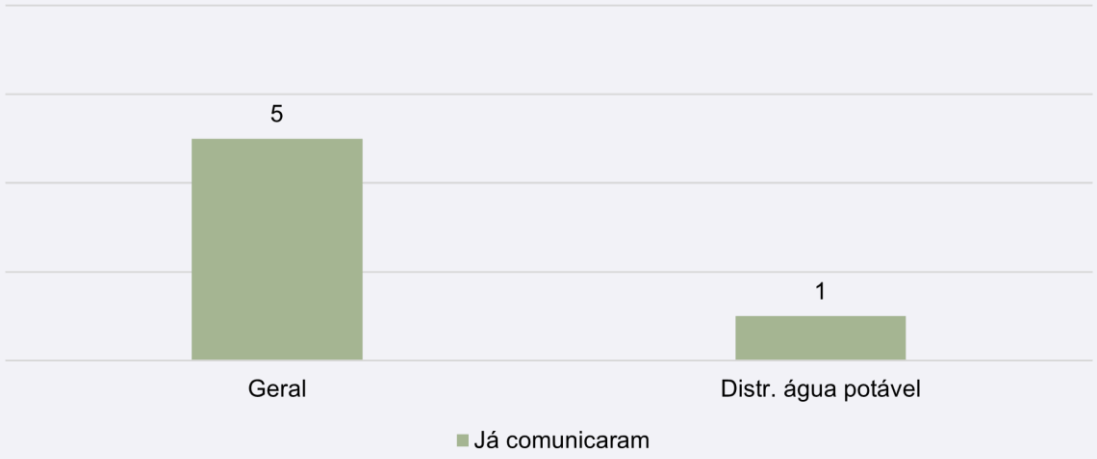
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez, 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, três das infraestruturas do mercado financeiro (IMF), 40 do setor saúde, **89 do setor do fornecimento e distribuição de água potável** e 25 do setor das infraestruturas digitais. Os resultados obtidos neste questionário são apresentados em percentagens.

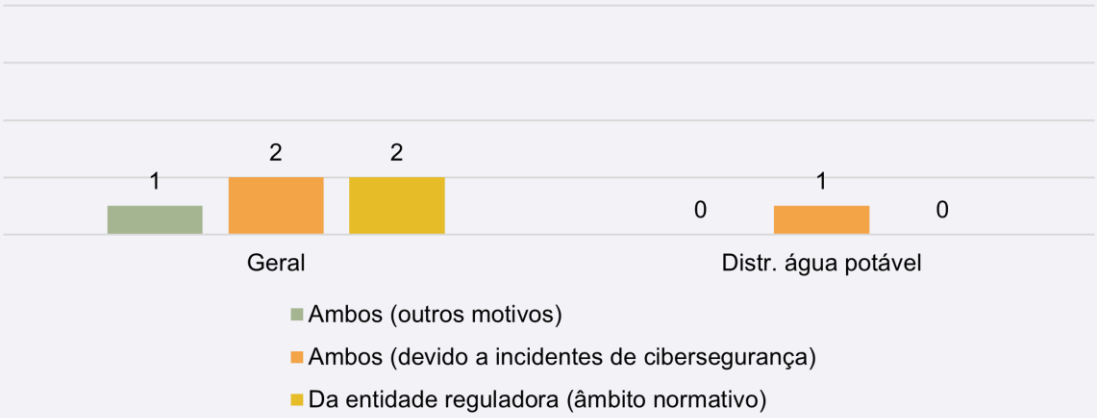
1. Comunicação entre OSE e respetivos Reguladores

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



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

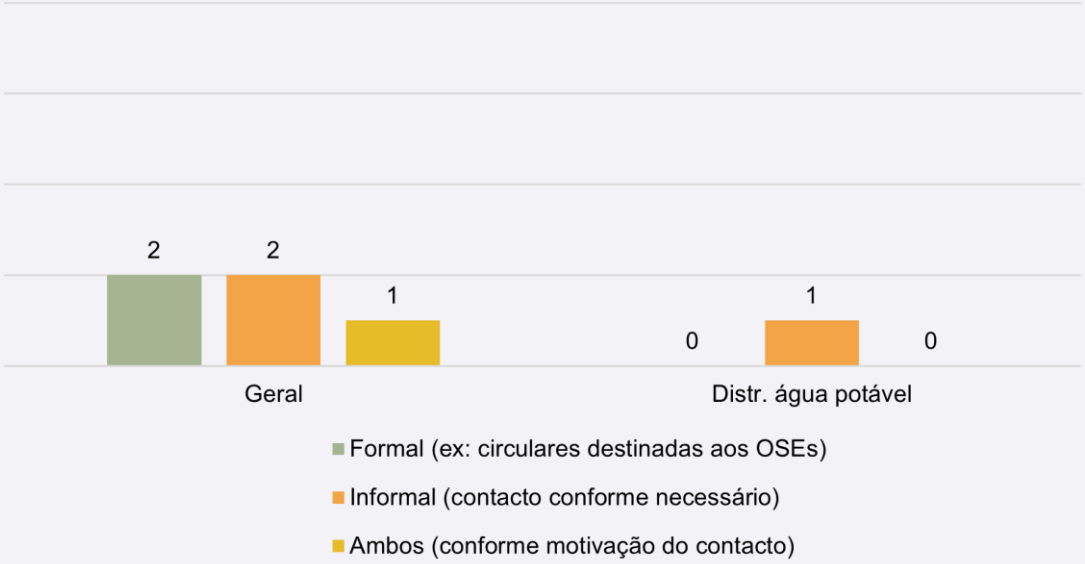
Gráfico 2 - Origem da comunicação sobre questões de cibersegurança



Relativamente à origem da comunicação sobre cibersegurança realizada por cinco dos reguladores, dois indicaram que a comunicação partiu dos próprios, em contexto de informação sobre normas do setor, outros dois responderam que houve comunicação que se gerou a partir dos dois lados, devido à ocorrência de incidentes de cibersegurança e apenas um respondeu que houve comunicação sobre cibersegurança a ser realizada com os OSE devido a outros motivos. O regulador inquirido do setor do fornecimento e distribuição de água potável refere que a comunicação se gerou de ambos os lados devido a incidentes de cibersegurança.

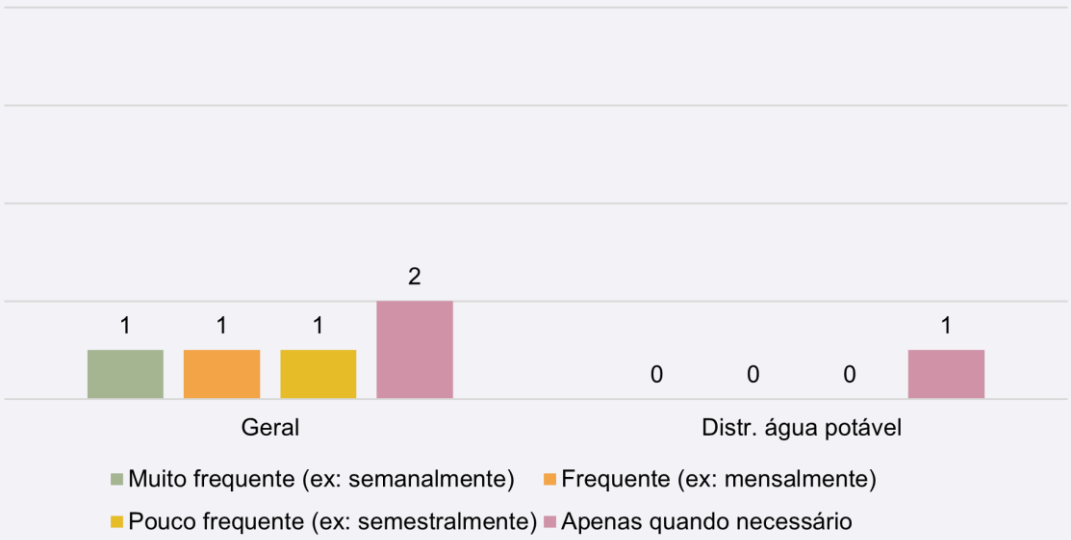
Por fim, há a comunicação realizada pontualmente através de instrumentos regulamentares emitidos pela entidade reguladora sobre matérias relevantes de forma transversal.

Gráfico 3 - Formalidade da comunicação realizada



Entre os mesmos cinco reguladores, dois indicaram que a comunicação é geralmente feita de modo formal, através de, por exemplo, circulares; outros dois responderam que a comunicação é sobretudo informal, outros dois indicam que a formalidade é aplicada consoante a necessidade, sendo um desses setores o setor da distribuição de água potável e apenas um regulador indicou haver comunicação tanto de caráter formal como mais informal.

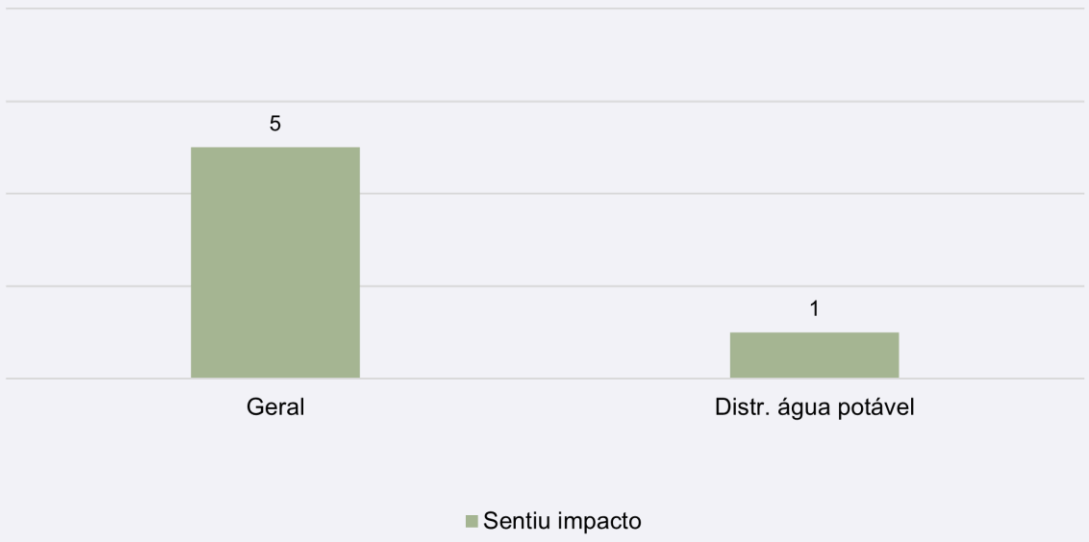
Gráfico 4 - Frequência da comunicação



No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. Apenas um regulador indicou que a comunicação é realizada muito frequentemente, praticamente de forma semanal. Já outro regulador indicou comunicar com os OSE sobre cibersegurança com uma frequência mensal. Por sua vez, outro regulador indicou que a frequência de comunicação com os OSE sobre questões de cibersegurança é pouco frequente, ocorrendo, por exemplo, semestralmente. Por fim, dois setores, sendo um deles o setor da distribuição de água potável, foram os que responderam que a comunicação é realizada apenas quando necessário, não havendo frequência ou periodicidade estimadas.

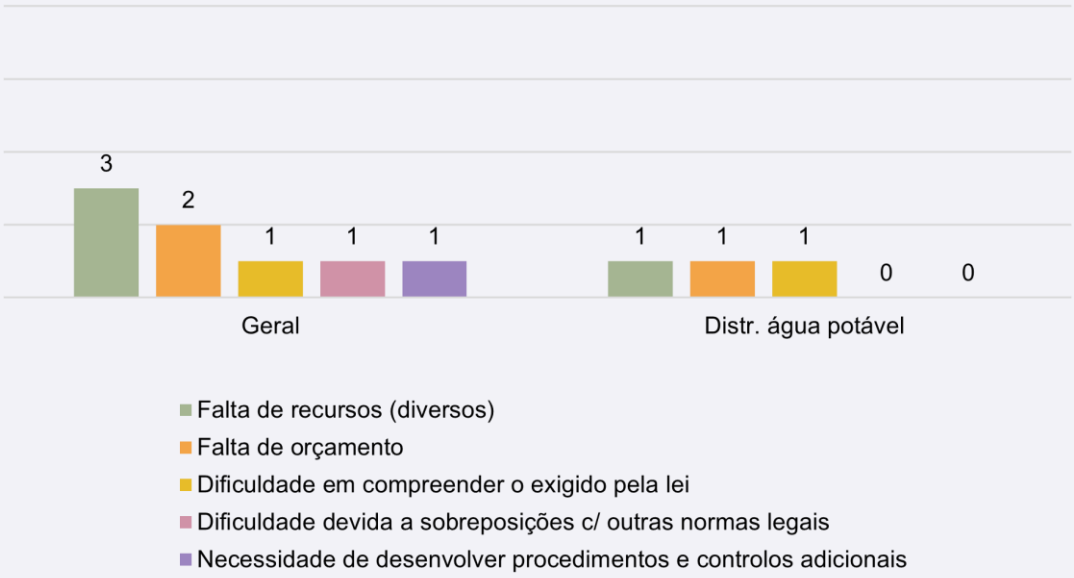
2. Impacto da publicação da Diretiva NIS ou da transposição da mesma (publicação da Lei n. º46/2018)

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



Questionou-se aos reguladores se sentiram impacto nas suas organizações e nos OSE por si regulados pela publicação da Diretiva NIS. Entre os oito reguladores que responderam, cinco indicaram ter sentido esse impacto. Esse impacto ter-se-á então feito sentir no setor da distribuição de água potável. 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



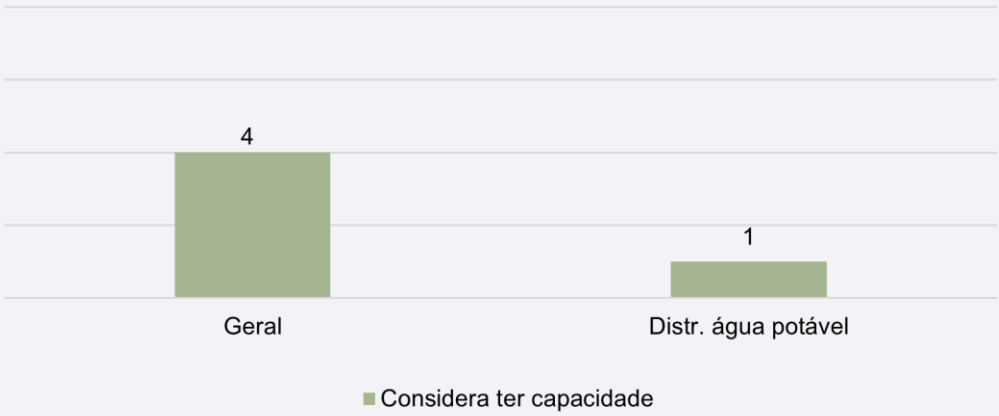
Três dos cinco reguladores que indicaram ter sentido impacto na sua organização ou nos OSE por si regulados devido à publicação da Diretiva NIS afirmaram que uma das dificuldades encontradas foi a falta de recursos diversos para estar em conformidade com a mesma, tendo sido uma dificuldade indicada pelo setor inquirido de distribuição de água potável, indicou também a falta de orçamento a conformidade com regime jurídico, como outra das dificuldades sentidas. Soma-se ainda, a dificuldade em compreender o que era exigido pela nova legislação, tendo este sido o único setor a apontar esta dificuldade.

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

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

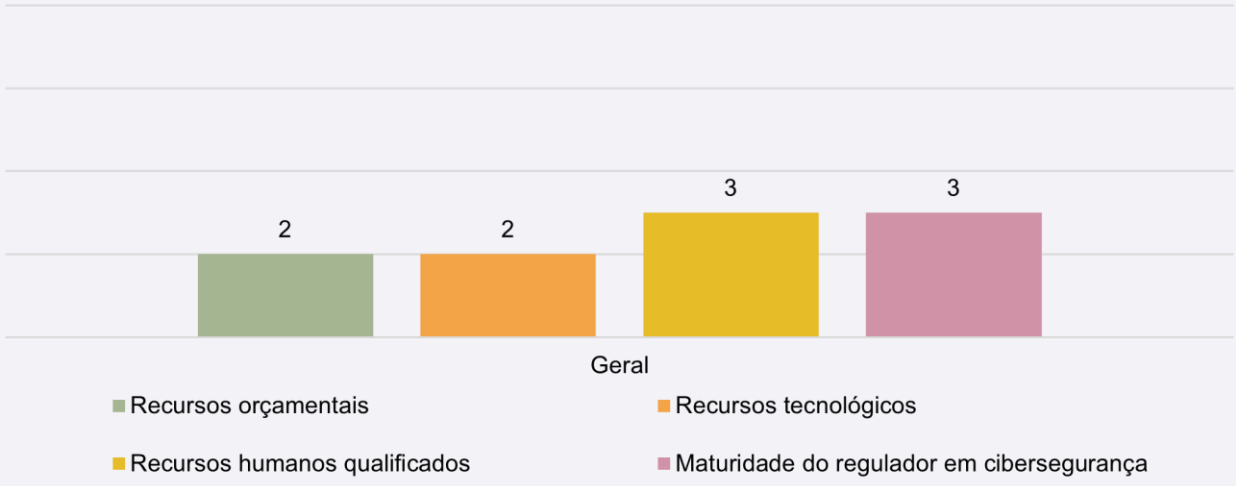
3. Supervisão dos OSE em matéria legislativa de cibersegurança por parte dos Reguladores

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



Foi questionado aos reguladores se teriam capacidade para realizar a supervisão dos operadores em matéria de cibersegurança. O número de respostas dividiu-se igualmente entre os que consideram ter a capacidade para realizar essa supervisão e os que não consideram tê-la (quatro reguladores consideram ter essa capacidade, outros quatro consideram não a ter). Posto isto, o regulador inquirido do setor da distribuição de água potável consideram ter a capacidade para realizar a supervisão dos operadores em matéria de cibersegurança.

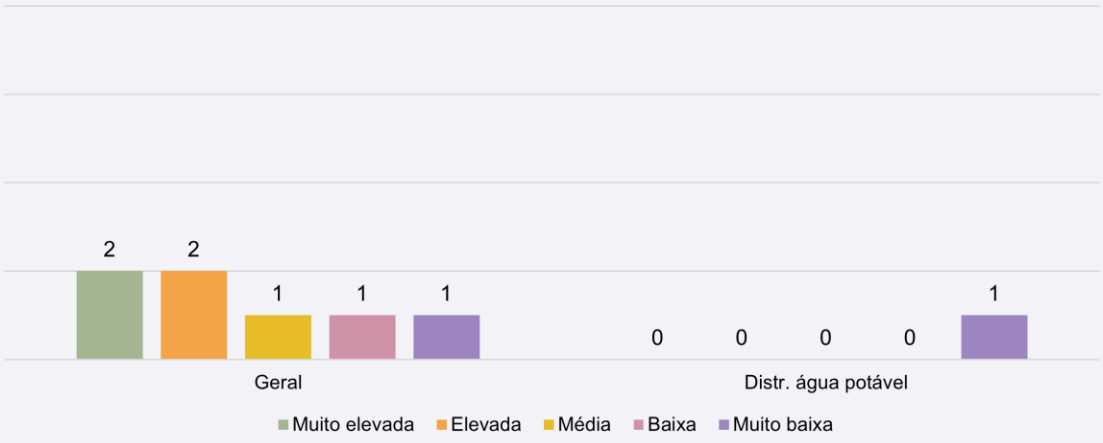
Gráfico 8 - Recursos em falta para a capacidade de supervisão em matéria de cibersegurança



Como os reguladores da distribuição de água potável referiram ter a capacidade necessária para realizar a supervisão, esta questão não se aplica.

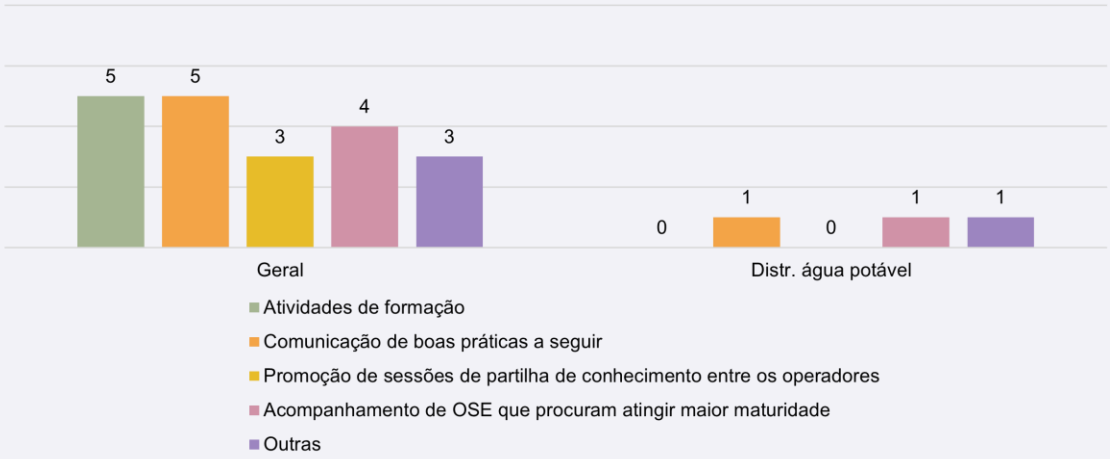
4. Maturidade em cibersegurança no setor

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



A perceção dos reguladores sobre a maturidade em cibersegurança dos operadores varia entre os diversos reguladores dos diferentes setores. Entre os inquiridos, apenas dois dos oito reguladores consideram que a maturidade nos seus setores é elevada. O regulador do setor da distribuição de água potável é o único a considerar que a maturidade do seu setor é muito baixa.

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, onde o setor de distribuição de água potável se encontra incluído.

Relativamente à promoção de sessões de partilha de conhecimento, apenas três reguladores indicaram fazê-lo. Quanto ao acompanhamento de OSE que procurem atingir maior maturidade em cibersegurança, quatro entidades referiram fazer esse acompanhamento, incluindo novamente o regulador do setor da distribuição de água potável.

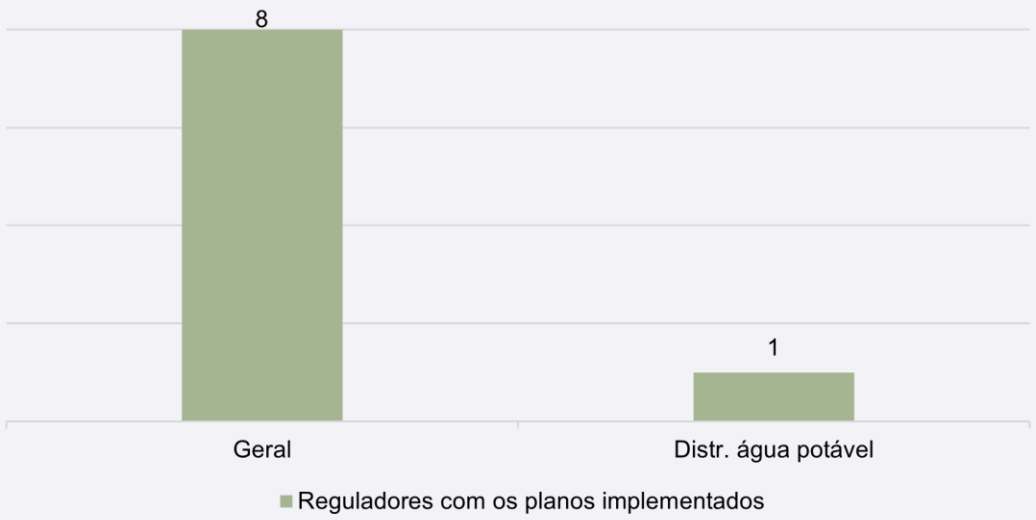
Gráfico 11 - Perceção sobre o número de profissionais capacitados em matéria de cibersegurança na entidade reguladora

Apenas duas das entidades reguladoras inquiridas consideram ter suficientes profissionais capacitados em matéria de cibersegurança, enquanto os restantes seis, contando com o setor do

fornecimento e distribuição de água potável, não consideram ter suficientes profissionais capacitados na área.

Novamente, estes resultados prender-se-ão com a escassez global de profissionais em cibersegurança e posteriormente analisada em detalhe no **gráfico 40**.

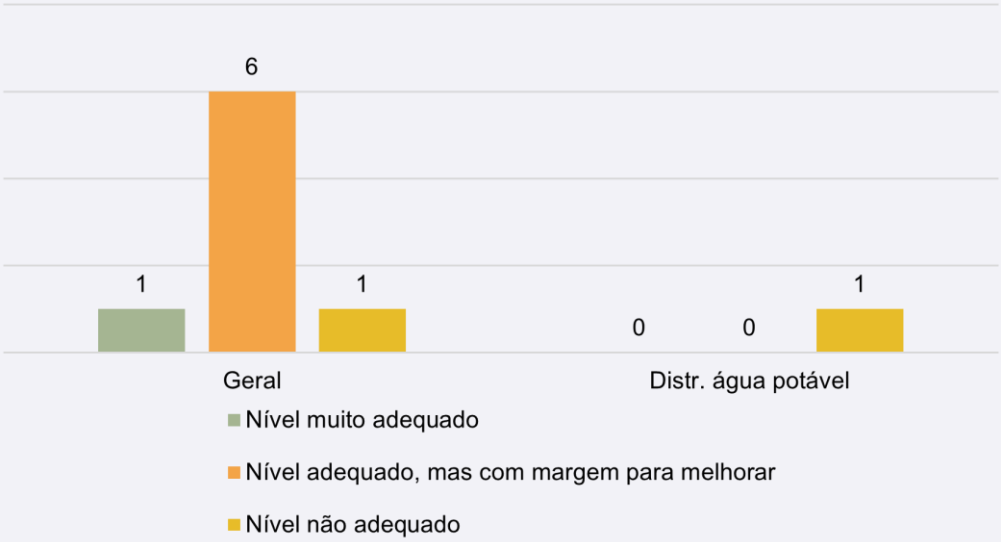
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados



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

5. Nível de segurança estabelecido pela legislação em vigor

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



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

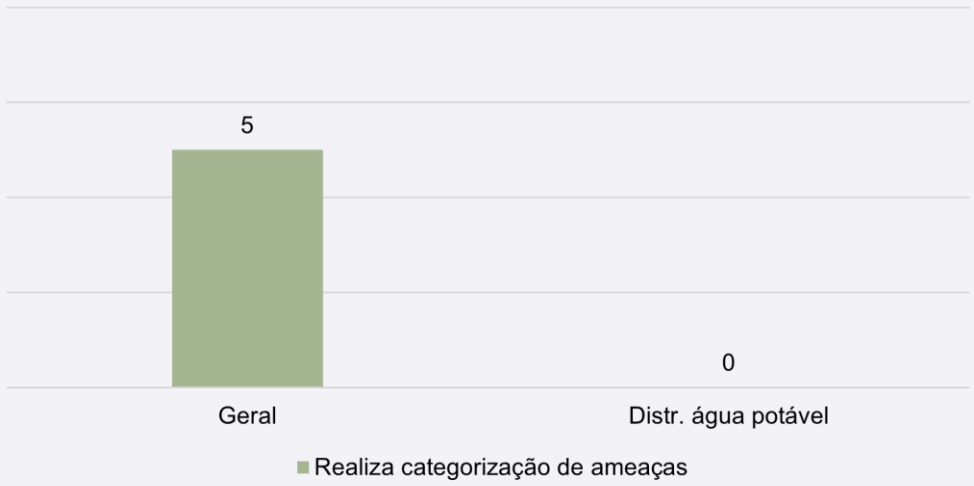
Uma questão semelhante foi colocada, em 2021, não aos reguladores, mas a diversos OSE na União Europeia, no âmbito do relatório *NIS Investments* 2021. As respostas recolhidas indicam que quase 50% (48,9%) dos operadores de serviços essenciais consideram que a Diretiva NIS teve um impacto positivo nas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

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

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

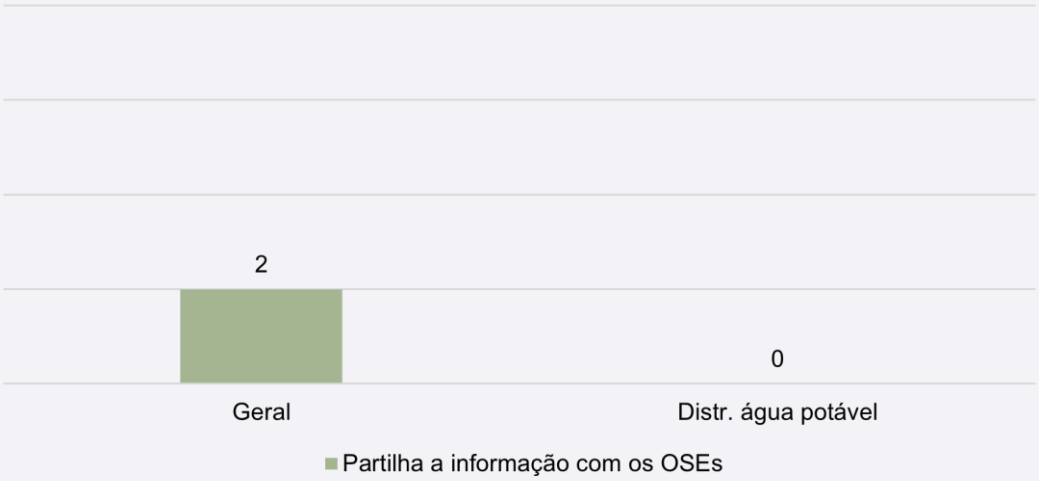
6. Categorização de ameaças

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



Cinco dos oito reguladores inquiridos realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores, sendo que um deles corresponde ao setor do fornecimento e distribuição de água potável.

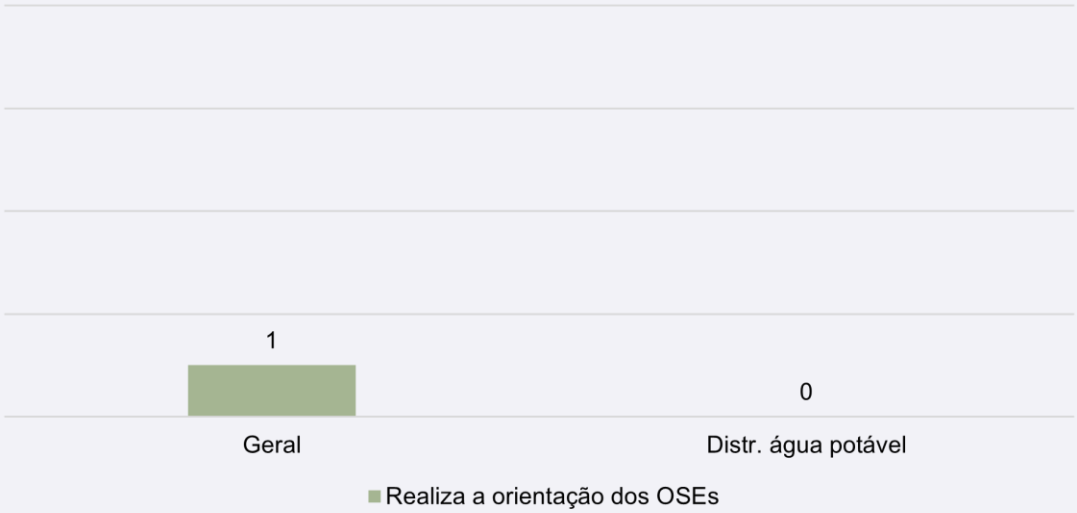
Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização



Dos cinco reguladores que realizam categorização de ameaças, apenas dois partilham informação relativa às ameaças com os OSE. Os restantes setores não efetuam a partilha de informação. No caso do setor de distribuição de água potável a questão não se aplica.

7. Orientação dos OSE por parte da entidade reguladora

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



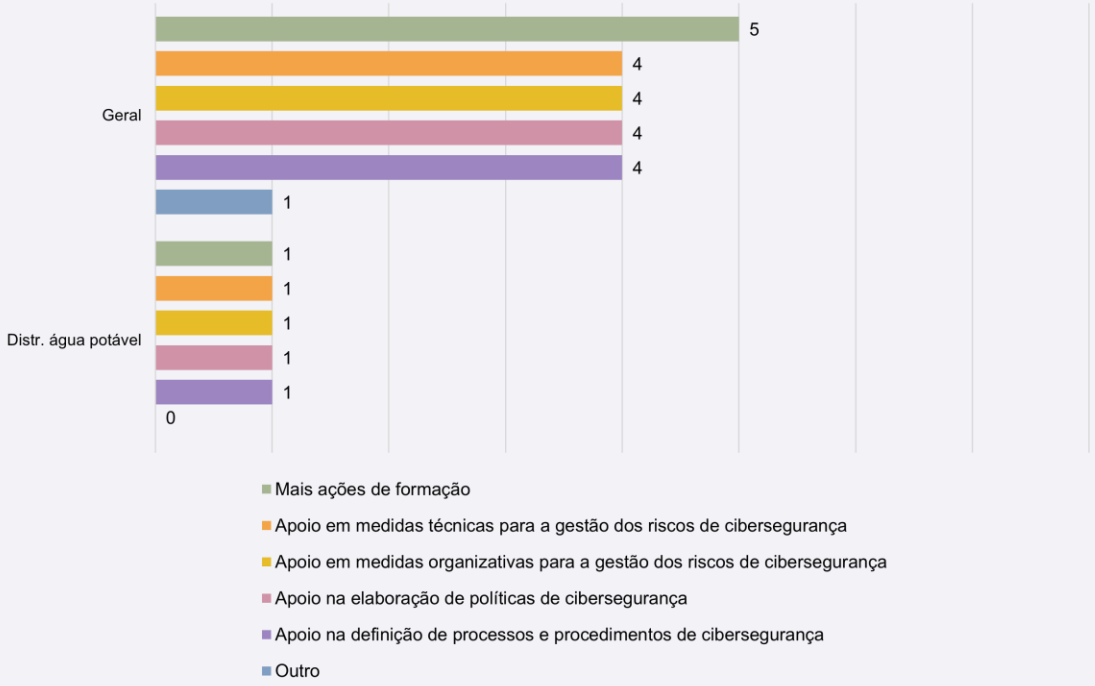
Apenas um dos reguladores indicou fornecer orientação aos OSE na digitalização de processos e na promoção de uma cultura digital, enquanto os restantes sete reguladores indicaram não fazer esse tipo de orientação.

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, sendo um deles o regulador do setor do fornecimento e distribuição de água potável, têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional.

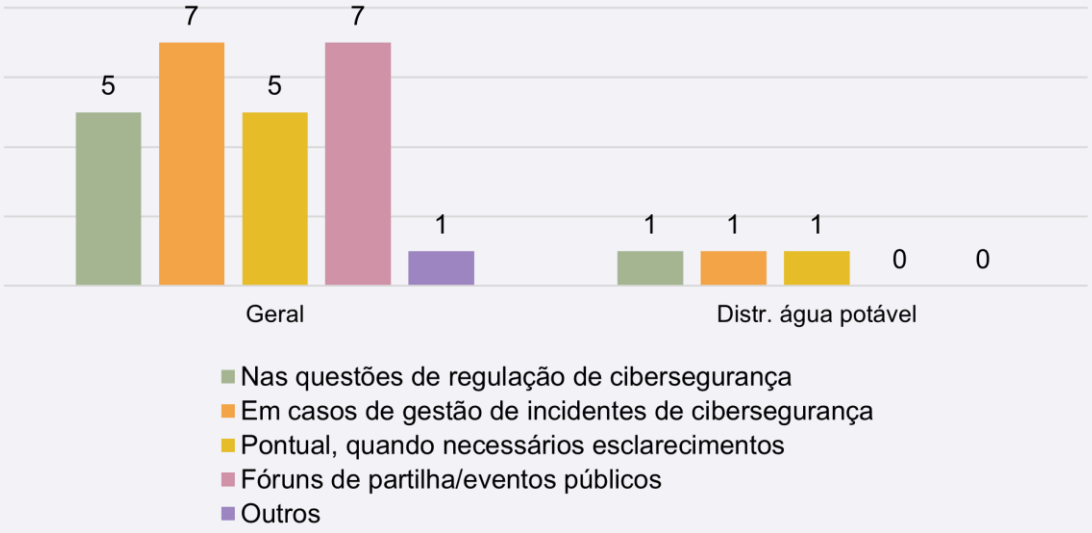
Gráfico 18 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS



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

No setor da distribuição de água potável, os reguladores inquiridos gostariam de ver esse apoio adicional traduzido em mais ações de formação, apoio em medidas técnicas e organizativas para a gestão dos riscos de cibersegurança, apoio na elaboração de políticas de cibersegurança e apoio na definição de processos e procedimentos de cibersegurança.

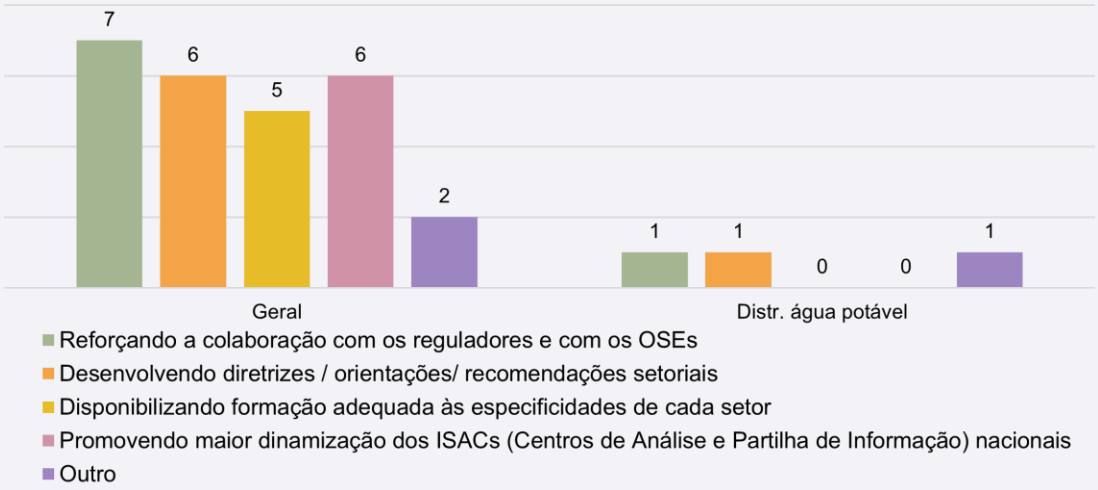
Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS



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.

No setor da distribuição de água potável, o regulador indica que por norma interagem com o CNCS no âmbito de questões relacionadas com a cibersegurança, em situação de gestão de incidentes de cibersegurança e em casos pontuais quando necessário. Apenas um dos reguladores referiu outro tipo de interação, relativo à definição de limites de reporte de incidentes.

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



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

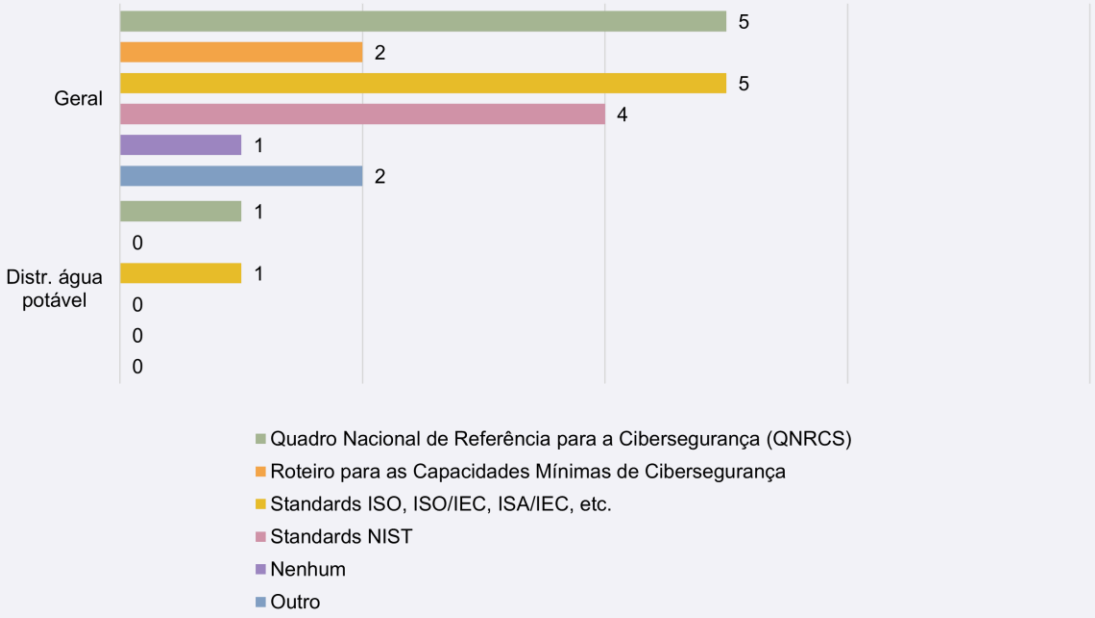
No caso do regulador do setor da distribuição de água potável, este respondeu que gostaria de ver o reforço da colaboração entre CNCS e entidades reguladoras e operadores, e o desenvolvimento de diretrizes/orientações/recomendações setoriais.

O Centro Nacional de Cibersegurança lançou um desafio denominado por “Compromisso C-Academy” que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. As organizações poderão escolher, pelo menos, três formações até ao final de 2025. Alguns dos principais benefícios incluem: “Reforço da cibersegurança da organização, setor ou região, aumento da resiliência e da capacidade de resposta a ataques” e “Acesso a conteúdos formativos de elevada qualidade”[9].

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

9. *Standards* e boas práticas recomendadas

Gráfico 21 - Standards e boas práticas recomendados aos 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.

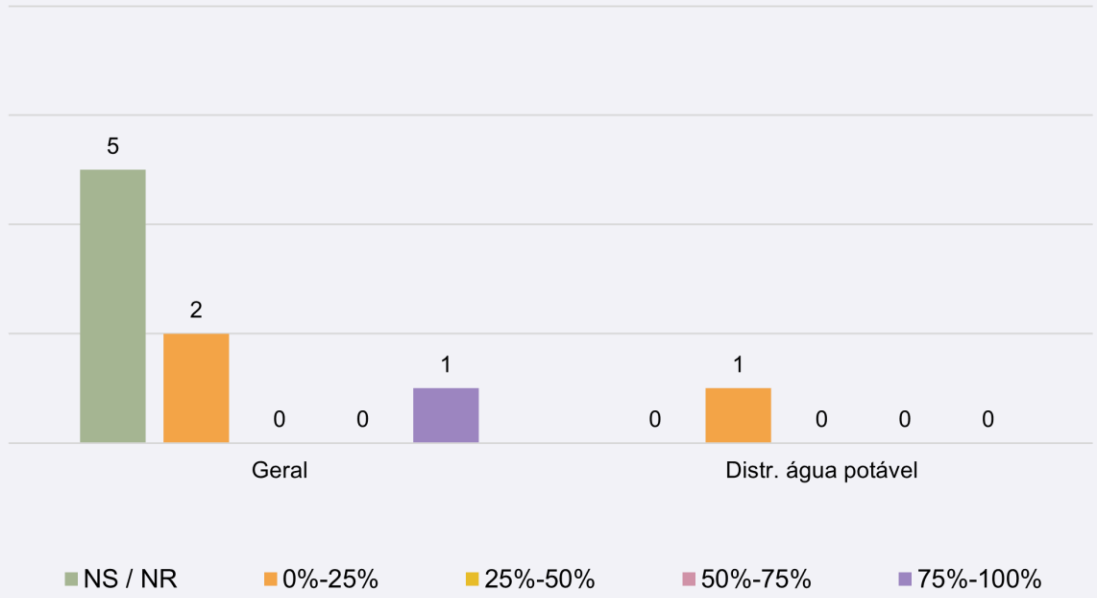
Na opção "outros", foram referidos *standards* da International Civil Aviation Organization (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain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

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

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

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

Gráfico 22 - Percentagem aproximada de 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 do fornecimento e distribuição de água potável, o regulador identifica entre 0%-25% de operadores certificados em normas internacionais ISO ou semelhantes.

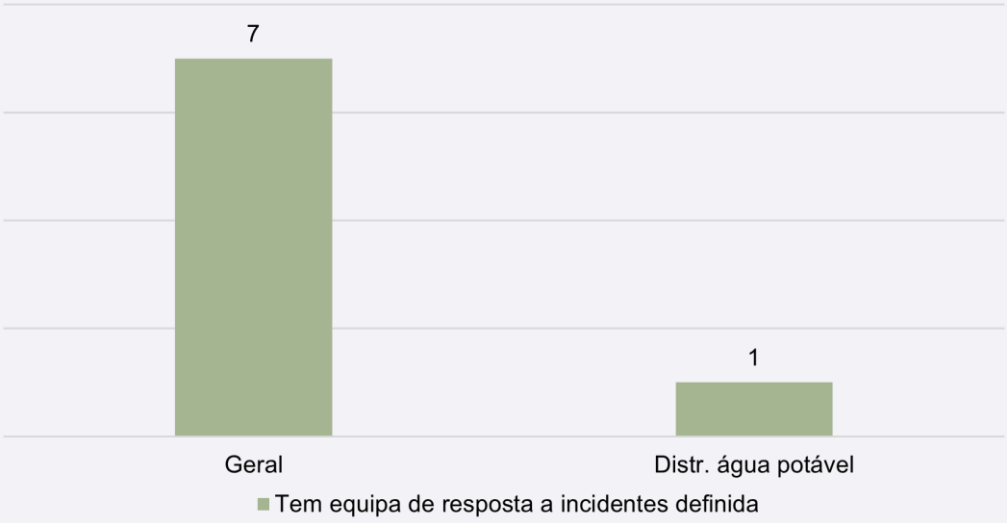
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança

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

Foi também questionado aos reguladores que normativos setoriais específicos nacionais ou europeus em matéria de cibersegurança estavam em vigor nos respetivos setores. Partindo das suas respostas, obteve-se a **Tabela 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 da distribuição de água potável, o regulador inquirido informa ter definido a equipa de resposta a incidentes.

11. Sensibilização e consciencialização

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

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

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.

O regulador do setor da distribuição de água potável não terá feito essa partilha com os operadores.

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

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

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

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

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

Quanto ao setor de distribuição de água potável a situação aplicável é a mesma que a anterior.

12. Cooperação nacional/internacional de proteção do ciberespaço

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

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

O regulador do setor da distribuição de água potável 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 caso do regulador inquiridos do setor da distribuição de água potável, este não recomenda aos operadores a participação em centros de partilha de informação.

13. Regulação de entidades e OSE

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

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

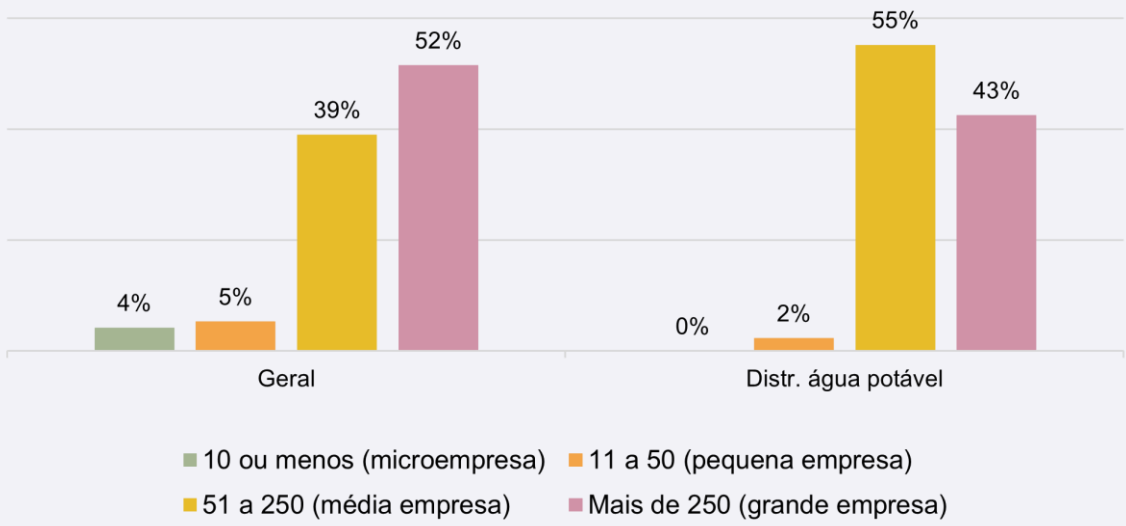
Setores	Estimativa
Energia	32
Transportes	> 19 000
Bancário	120
Infraestruturas do Mercado Financeiro	> 1 000
Distribuição de Água Potável	350
Infraestruturas Digitais	100

Tabela 4 - Número estimado das entidades reguladas que são OSE

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

Resultados do questionário dirigido aos Operadores de Serviços Essenciais

Gráfico 30 - Número de colaboradores na organização

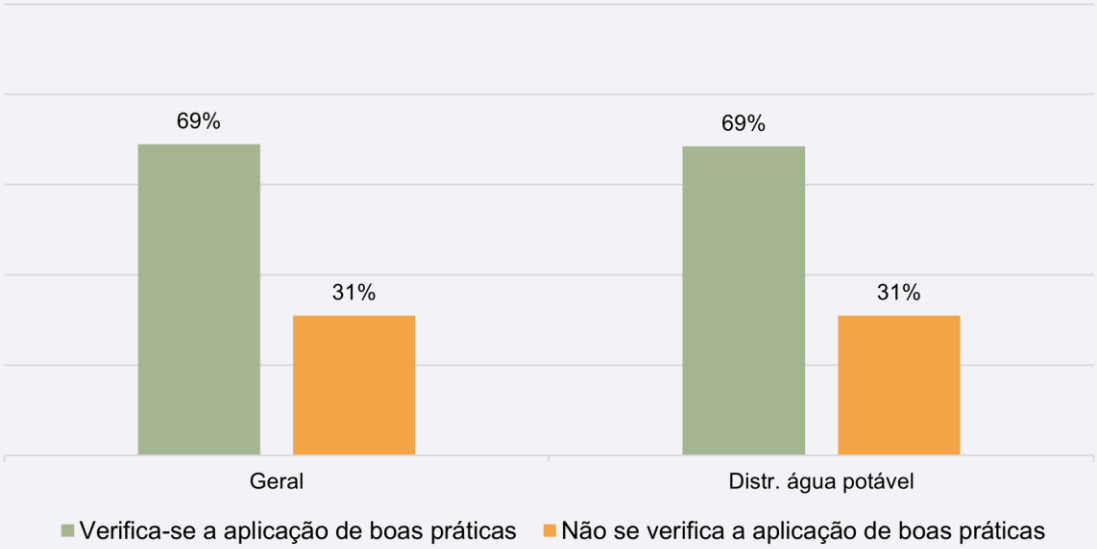


O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSE. As médias empresas representam 39% dos OSE, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas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

Contrariamente à maioria, no setor do fornecimento e distribuição de água potável, são mais comuns as médias empresas.

A composição do tecido empresarial dos OSE difere grandemente daquele que é o tecido empresarial geral das empresas portuguesas. Enquanto entre os OSE mais de 50% destes são grandes empresas, 99,9% das demais empresas em Portugal são, segundo dados de 2022 da PORDATA, pequenas e médias empresas, com apenas 0,1% sendo grandes empresas[11].

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

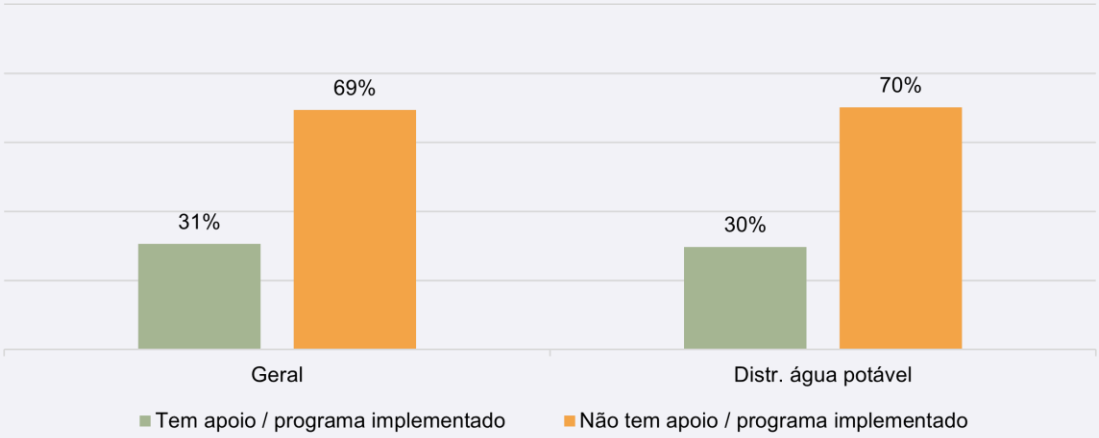


De um modo geral, os operadores percecionam a adoção de boas práticas de cibersegurança por parte dos seus colaboradores. Alguns exemplos dessas boas práticas são a não partilha de palavras-passe, o bloqueio do computador durante momentos de ausência da estação de trabalho, o cuidado com a informação 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 da distribuição de água potável, a perceção de que estas boas práticas são aplicadas espelha a generalidade.

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

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

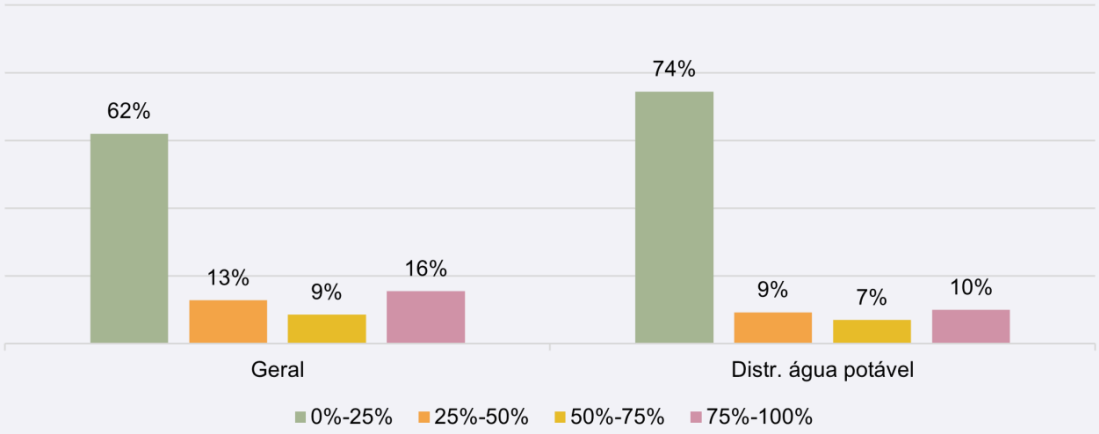


À data de realização do questionário, apenas um terço dos operadores tinham apoios ou programas próprios ou do Estado para colaboradores interessados em formação na área de cibersegurança.

No fornecimento e distribuição de água potável, mais de dois terços dos operadores não têm apoios ou programas próprios ou do Estado para colaboradores que desejem formação em cibersegurança, correspondendo a 70% dos OSE.

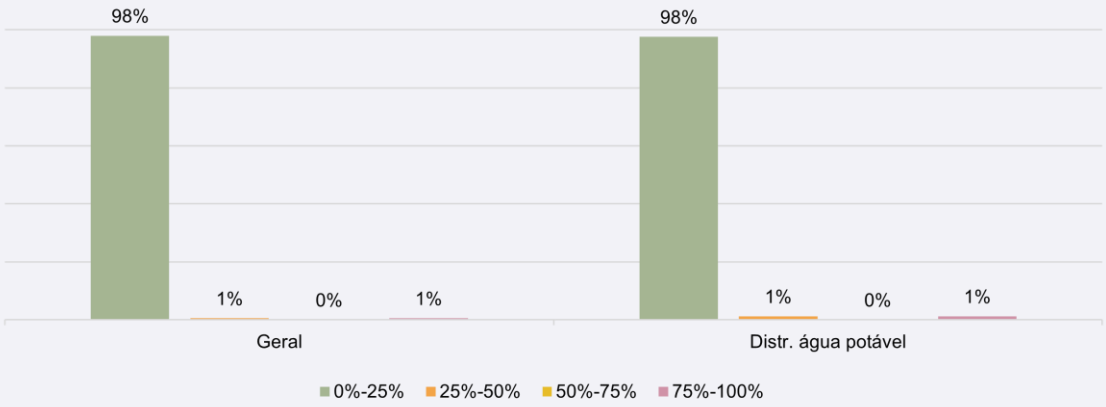
Importa sublinhar, que estas respostas não significam que não seja dada formação em cibersegurança aos colaboradores. O que acontece é que muita da formação disponibilizada pelos operadores aos colaboradores não está inserida num programa de formação específico, ou então não existem apoios para colaboradores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

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



Na maioria dos OSE (62%), a percentagem de colaboradores com formação básica em cibersegurança não ultrapassa os 25%. No setor do fornecimento e distribuição de água potável, a percentagem de operadores onde três quartos dos colaboradores ou mais têm formação básica em cibersegurança é relativamente baixa, nunca ultrapassando os 10%.

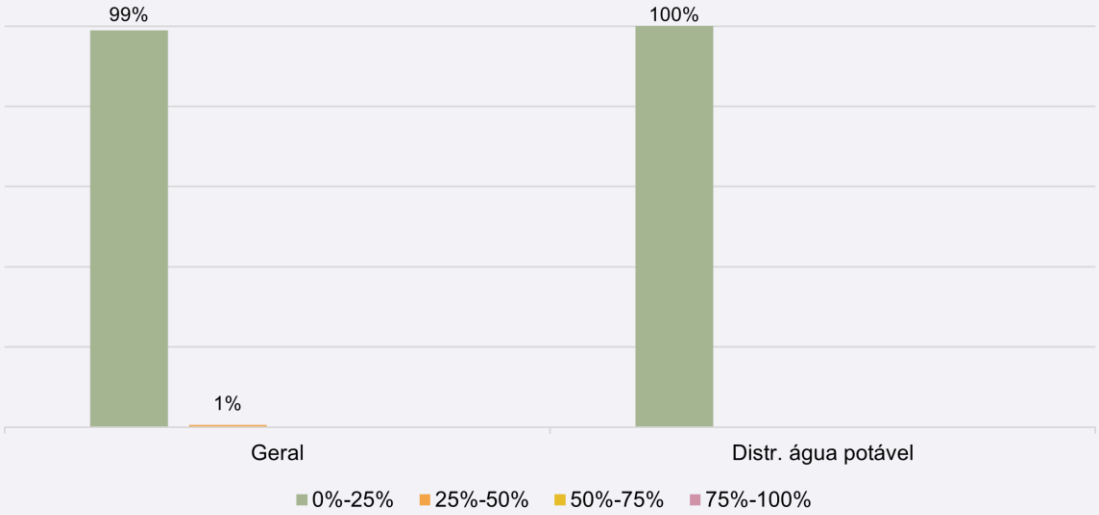
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



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

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

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

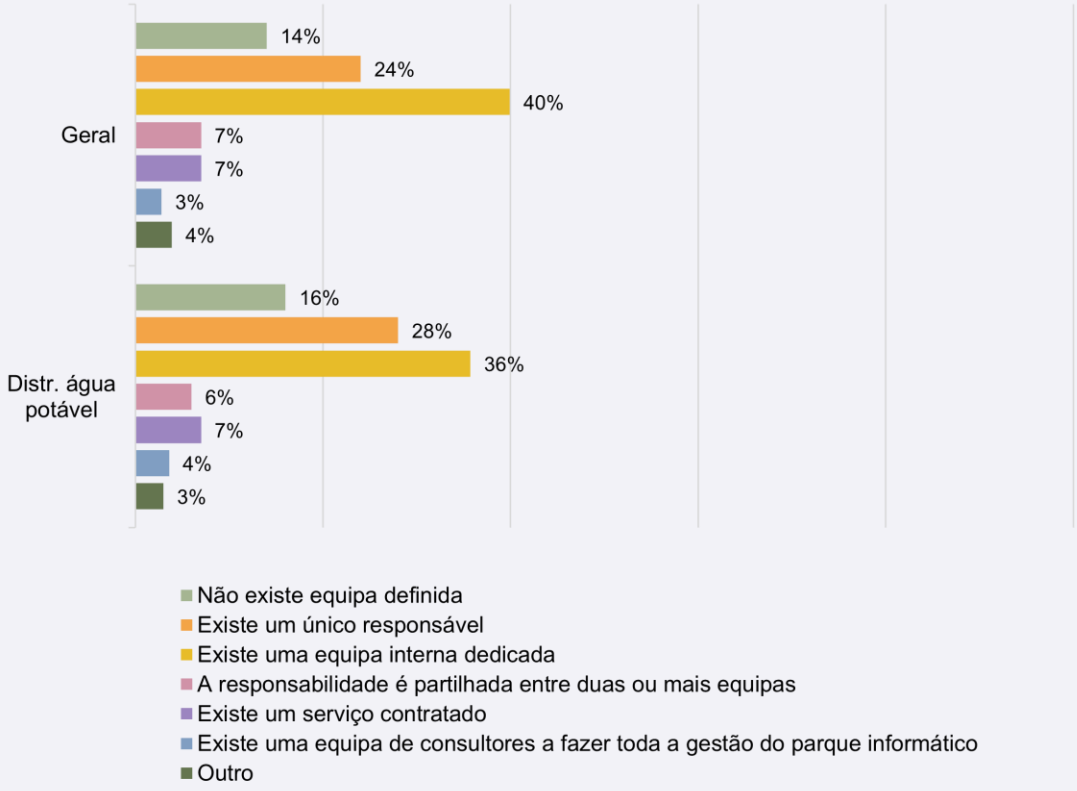


A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. Contudo, há que destacar o setor da saúde, onde 3% dos operadores indicaram haver 25%-50% de colaboradores com certificações em cibersegurança. Novamente, o resultado geral é um resultado expectável,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

De acordo com os dados disponíveis no relatório *NIS Investments* 2021, da ENISA, apenas 7,5% dos OSE na UE indicavam ter uma preocupação em certificar os colaboradores da própria organização. A nível setorial, no mesmo relatório, em nenhum dos setores se superava os 11% de OSE a certificar os seus próprios colaboradores[12].

[12] 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

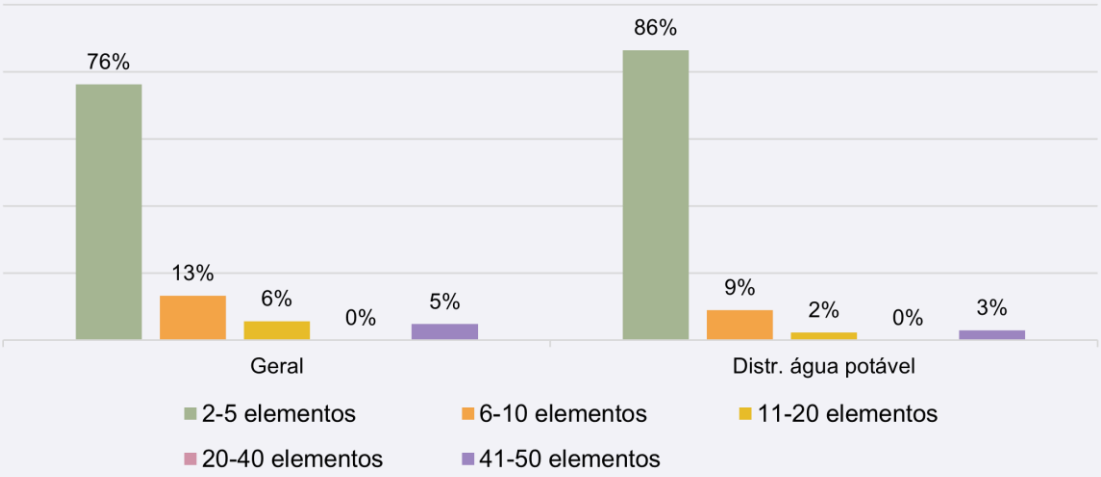


De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (25% dos casos).

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.

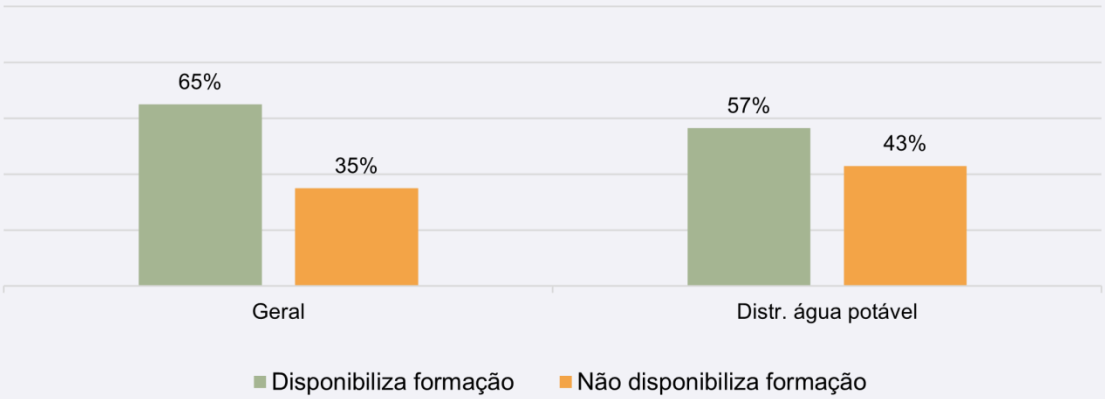
Os operadores do setor do fornecimento e distribuição de água potável contam, maioritariamente, com uma equipa dedicada (36%) ou com um único responsável (33%), e até sem qualquer responsável (16%), verificando-se também o recurso à contratação externa do serviço de *helpdesk* em 7% dos casos. Existe ainda uma equipa de consultores a fazer toda a gestão do parque informático (4%) e a partilha de responsabilidades entre duas ou mais equipas (6%). São ainda mencionados outros motivos (6%).

Gráfico 37 - Composição das equipas de *helpdesk*



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

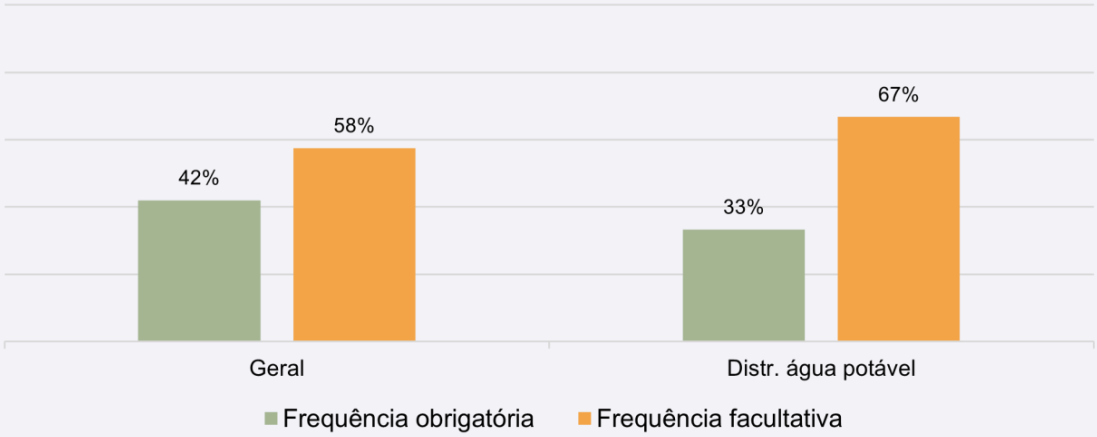
Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. As exceções a esta realidade verificam-se no setor do fornecimento de água potável, no qual 57% dos OSE indicam disponibilizar formação aos colaboradores, ficando assim 8 p.p. abaixo da percentagem geral.

Comparando com dados do Inquérito à Utilização das TIC nas Empresas (IUTICE) de 2022, realizado pelo Instituto Nacional de Estatística (INE), 63,3% das empresas em Portugal procuraram consciencializar os seus colaboradores sobre cibersegurança durante o ano de 2021[13]. Já um outro estudo, realizado pela Microsoft Portugal em setembro de 2023, intitulado "Estado da Cibersegurança em Portugal", indica que 84% das empresas portuguesas ministram formação de sensibilização para a cibersegurança. A discrepância nestes resultados poder-se-á dever à composição das amostras de cada estudo. Embora seja expectável que cada vez mais empresas disponibilizem formação em cibersegurança aos seus colaboradores, um crescimento de 20% em dois anos das entidades que disponibilizam formação em cibersegurança aos seus colaboradores é improvável.

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



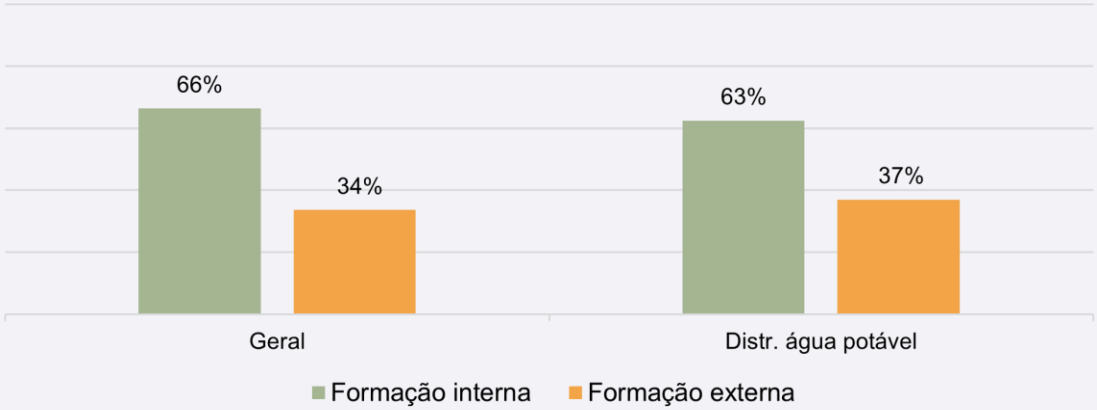
De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais esta tendência não se verifica. No setor da distribuição de água potável, apenas um terço dos inquiridos (33%) indicou que a formação em cibersegurança era de frequência obrigatória.

Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre OSE e demais empresas em Portugal. Enquanto em 42% dos OSE que disponibilizam formação, esta é de caráter obrigatório, apenas em 19,2% das empresas portuguesas há formações obrigatórias. Já ao nível das de caráter facultativo (ou voluntário, nos termos do IUTICE), os resultados são mais similares aos do questionário realizado pelo CNCS, uma vez que estas se verificam em 58% dos OSE que disponibilizam formação e em 56,2% das empresas participantes no inquérito[14].

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

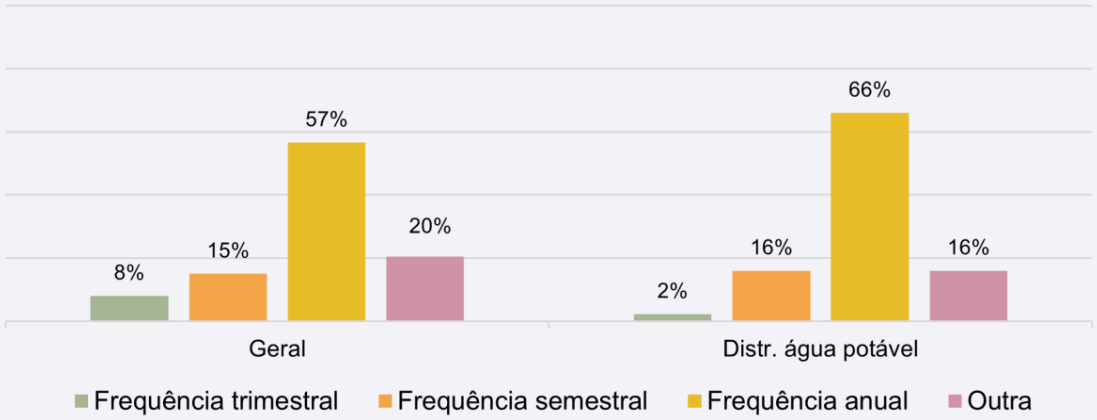
[14] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19.

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



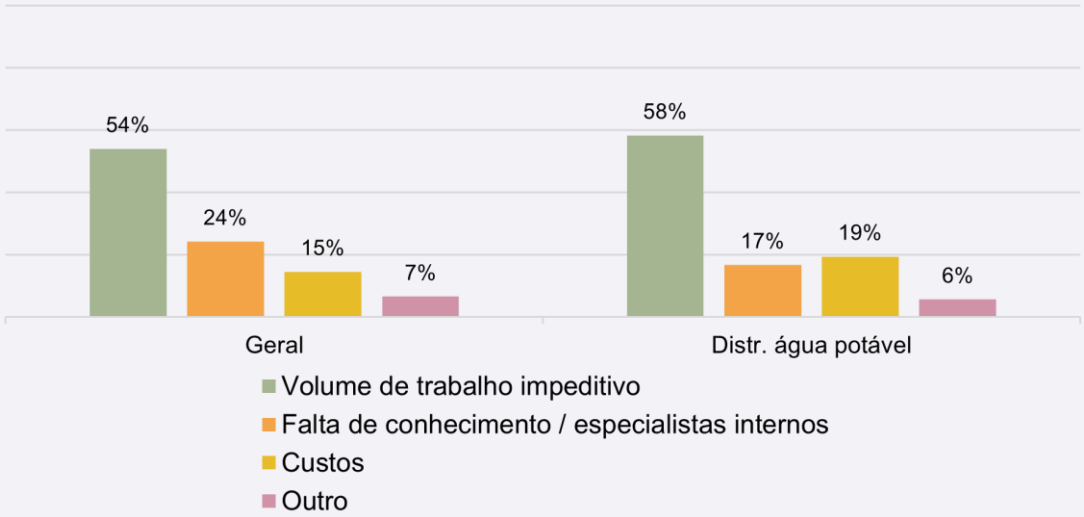
Neste gráfico, fica evidenciado o maior recurso à formação interna do que externa entre os OSE. A maioria dos inquiridos (66%) recorre aos meios internos para fins de formação aos colaboradores. Surgem em destaque os setores bancário e das infraestruturas do mercado financeiro, com as maiores percentagens de OSE a darem formação interna (88% e 100%, respetivamente). Contudo, cerca de um terço dos OSE (34%) recorre a entidades externas para formar os seus colaboradores.

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*. Por exemplo, tanto no setor da saúde como no das infraestruturas digitais, que são os que apresentam percentagens mais elevadas na opção "Outra", tanto se registaram respostas indicando momentos de formação semanais ou mesmo diários, como respostas que indicavam que não se realizaram momentos de formação em cibersegurança em mais de um ano.

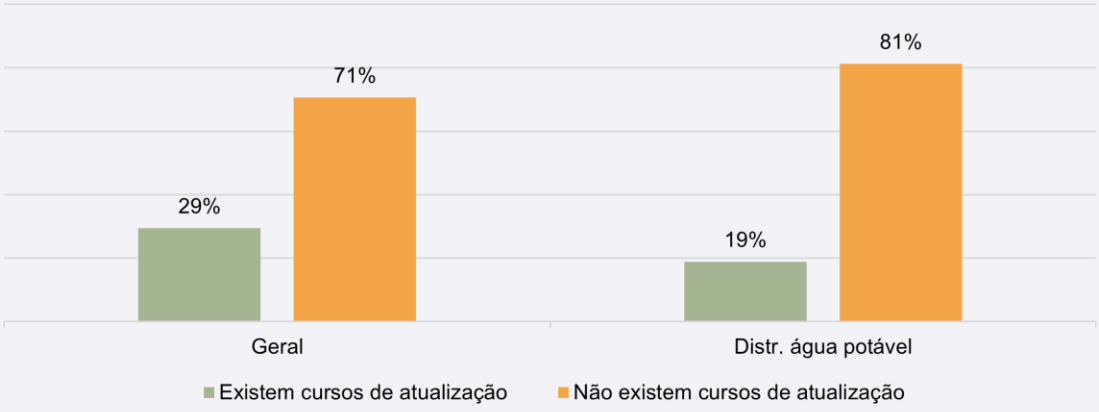
Gráfico 42 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam



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

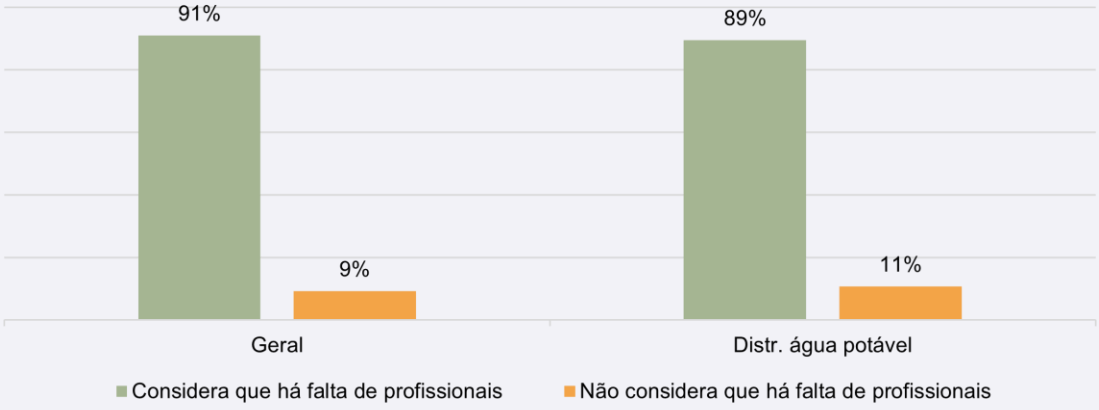
No setor da distribuição de água potável, o principal motivo indicado continua a ser o volume de trabalho impeditivo, indicado por 58% dos OSE que não disponibilizam formação. É também dos únicos a indicar "Outros" motivos para a falta de formação. Esses outros motivos passam, segundo os OSE, pela falta de planos de formação dentro das organizações e pela alocação de recursos financeiros a formação noutras áreas que não a cibersegurança.

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



A oferta de cursos ou formações de atualização em cibersegurança para os colaboradores é escassa na generalidade, com apenas 29% dos OSE inquiridos a indicarem a existência destes cursos.
O setor da distribuição de água potável supera a percentagem geral, com mais de 80% dos OSE a não disponibilizarem este tipo de cursos ou formações.

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



A vasta maioria dos OSE inquiridos (91%) considera haver um cenário de escassez de profissionais de cibersegurança e áreas relacionadas no mercado de trabalho. Especificamente, nos setores da banca e das infraestruturas do mercado financeiro, todos os OSE inquiridos consideram que há falta de profissionais na área.

A escassez de profissionais em cibersegurança é um problema que persiste há largos anos, devido à discrepância entre a velocidade a que a tecnologia evolui e o tempo que leva a formar os profissionais. Segundo o Fórum Económico Mundial, a atual escassez global de profissionais em cibersegurança é de cerca de 4 milhões de profissionais[15] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[16]. Esta falta de profissionais coloca aos empregadores na área desafios como conseguir pessoal qualificado, conseguir desenvolver equipas que possuam as capacidades técnicas desejadas e conseguir manter os bons profissionais encontrados[17]. De modo a combater esta escassez, organizações como o Fórum Económico Mundial e a ENISA têm feito diversas recomendações, que passam pela contratação de profissionais vindos de outras áreas de formação que não apenas as das TIC, engenharia e matemática, pela admissão de colaboradores menos experientes, ou mesmo sem experiência (sendo esta adquirida ao longo do desempenho das funções pretendidas), a admissão de colaboradores em trabalho totalmente remoto, e pela valorização dos profissionais, não só a nível salarial, mas também a nível das perspetivas de progressão de carreira e até mesmo do respeito pelos profissionais no local de trabalho[18] [19].

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

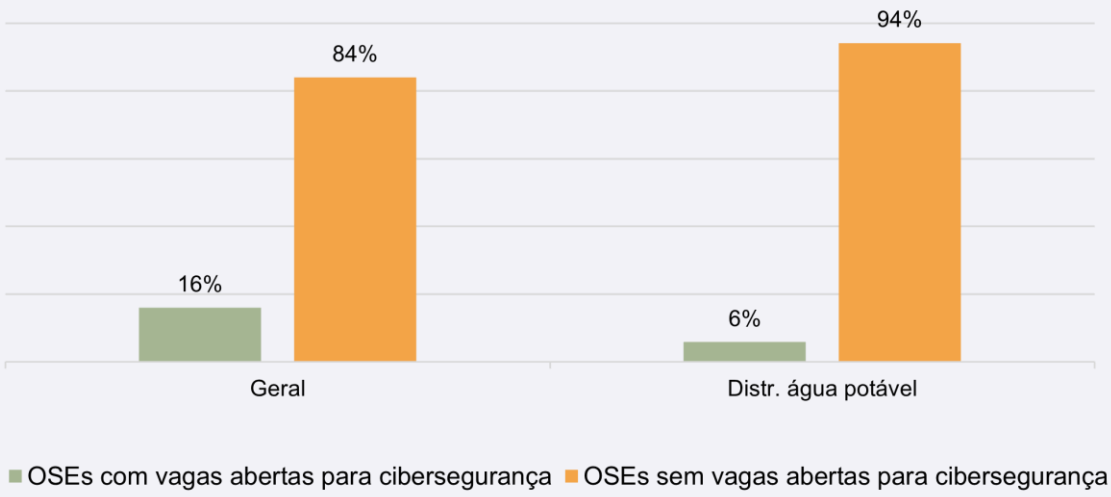
[16] ENISA, “Cybersecurity Skills Conference: Strengthening human capital in the EU”, https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.

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

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

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

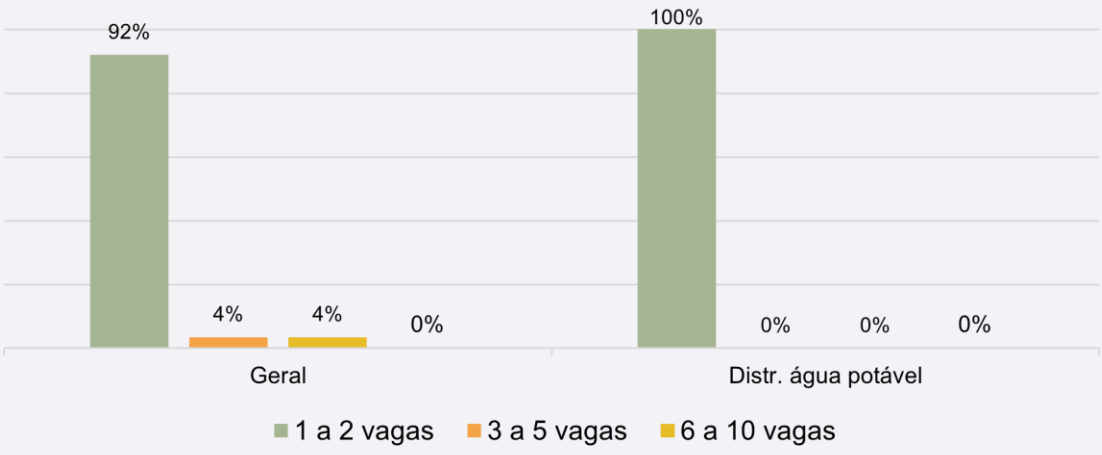
Gráfico 45 - Vagas abertas para a área de cibersegurança



À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. Sectorialmente, registaram-se duas exceções com mais de 50% a terem vagas em aberto. Contrastando, o setor da distribuição de água potável foi o que registou a percentagem mais baixa de OSE com vagas abertas para cibersegurança, atingindo apenas os 6%.

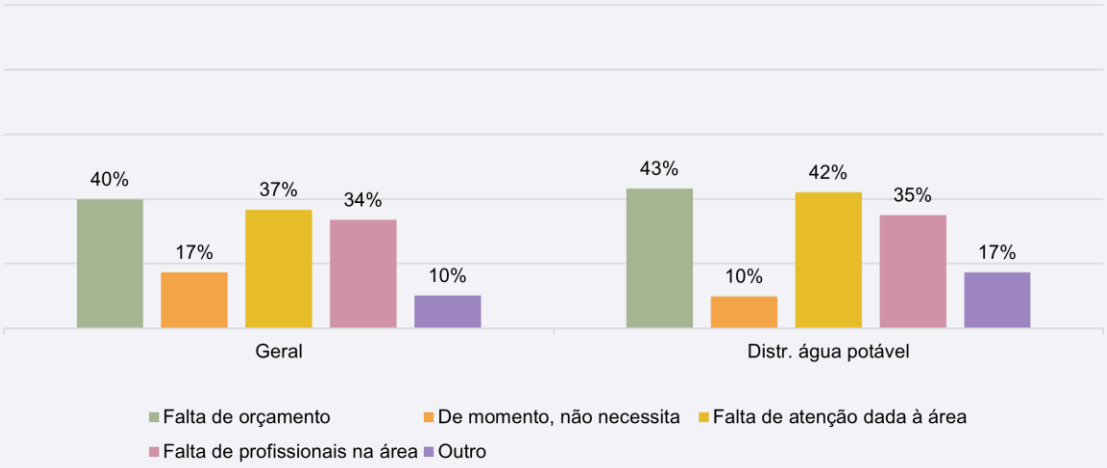
Embora não se possa fazer uma associação direta entre vagas para cibersegurança e para pessoal especialista em TIC, os dados do IUTICE de 2022 mostram que, nesse ano, apenas 6,2% das empresas portuguesas tentaram recrutar pessoal especialista em TIC.

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. Apenas no setor da saúde se registaram OSE com 3 a 5 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.

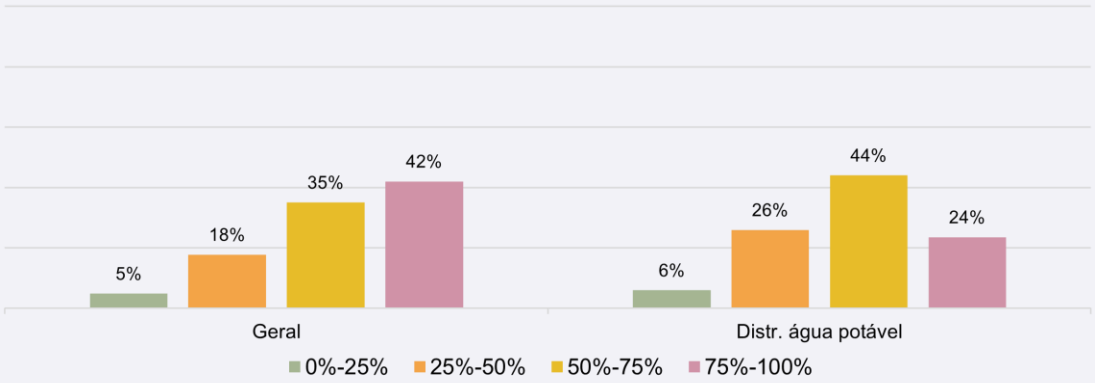
De acordo com os dados do IUTICE de 2022, 61,4% das empresas portuguesas sentiram dificuldades no recrutamento. Entre estas, 82,1% apontaram a falta de candidaturas como um problema, cerca de 57% mencionaram a falta de qualificações ou de experiência relevante dos candidatos como outra dificuldade e 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"[20], objetivo esse que não pode ser cumprido quando há falta de atenção dada à área. Tratando-se de Operadores de Serviços Essenciais, esta lacuna torna-se ainda mais grave. Recorda-se, também, que é uma boa prática constante de normativos internacionais, como a ISO/IEC 27001, que a direção/administração das organizações demonstre o seu compromisso para com segurança da informação e que esta assegure a alocação dos recursos necessários para cumprir esse desígnio[21].

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

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

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

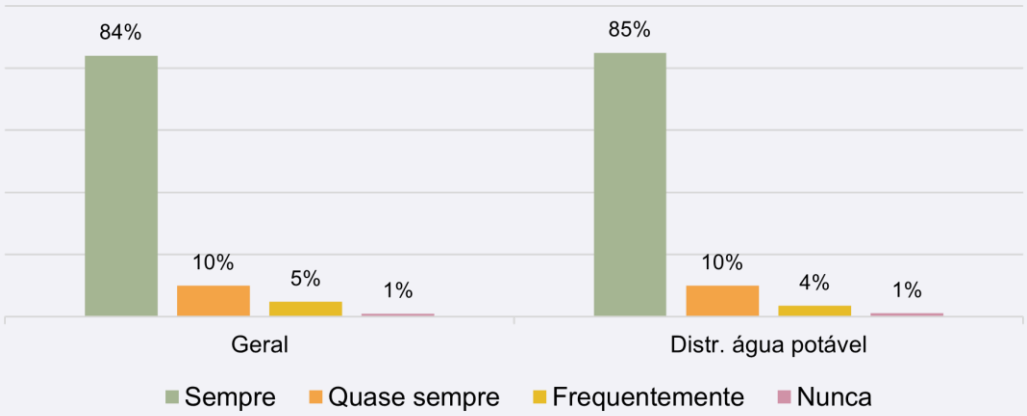


Apesar de predominar entre os OSE o intervalo 75%-100% de colaboradores com acesso a equipamentos digitais (indicado por 42% dos OSE), é visível que, com exceção de dois setores, há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos.
No setor do fornecimento e distribuição de água potável se verifica que o intervalo mais recorrente é o intervalo 50%-75% de colaboradores com acessos a esses equipamentos.

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

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

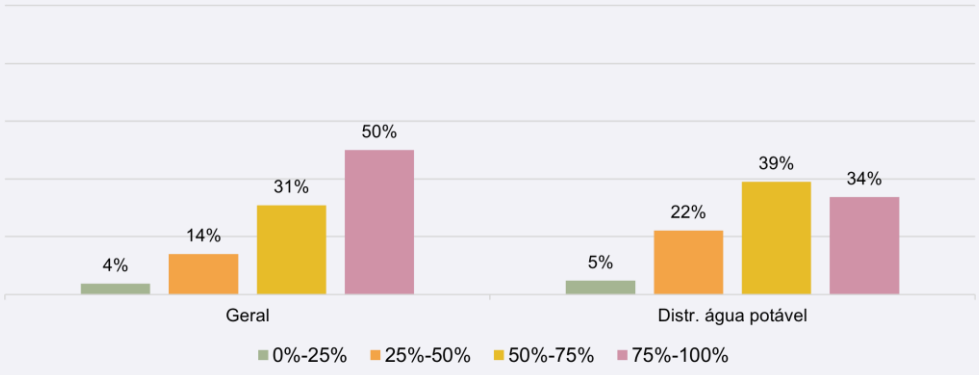
Gráfico 49 - Os OSE são responsáveis pelo funcionamento dos equipamentos necessários às funções dos colaboradores



Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. No setor do fornecimento e distribuição de água potável, registam-se alguns OSE onde nem sempre o fornecimento dos equipamentos necessários é feito pelo OSE em questão, havendo 80% de OSE a indicar que eram sempre responsáveis pelo fornecimento dos equipamentos. Ressalva-se ainda que não se registaram situações em que os operadores nunca fornecem os equipamentos, impondo esse encargo aos colaboradores.

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

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



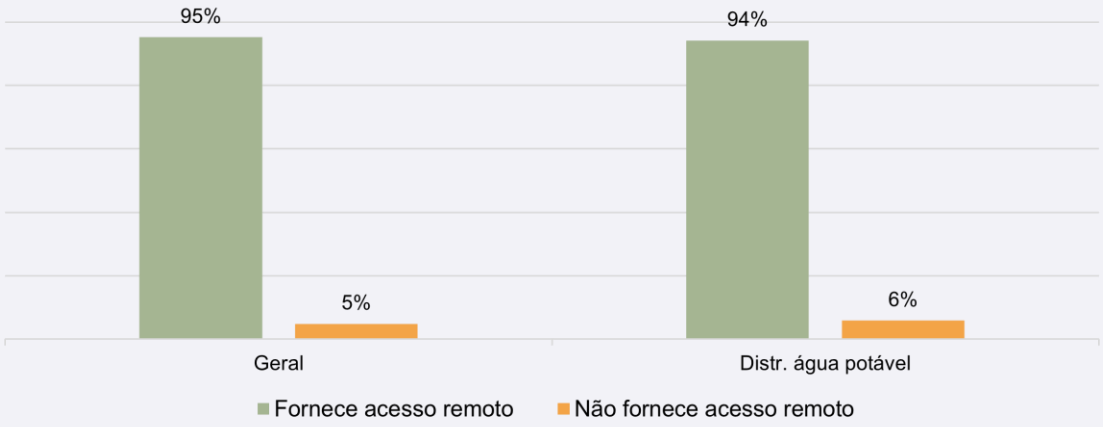
A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.

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

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

Voltando a comparar com dados do IUTICE, mas agora com o de 2023, verifica-se que há mais colaboradores com acesso à Internet no contexto específico dos OSE do que das várias empresas portuguesas. Juntando os dois intervalos onde mais de 50% dos colaboradores têm acesso à Internet, obtém-se 81% de OSE onde 50% dos colaboradores acedem à Internet no desempenho das suas funções. No contexto empresarial português, apenas 48,9% dos colaboradores têm acesso à Internet para fins de trabalho. Mesmo comparando sectorialmente onde possível, como nos setores da energia e dos transportes, os OSE continuam a apresentar mais colaboradores com acesso à Internet: segundo o IUTICE, no setor da energia, há 39,8% de colaboradores com acesso à Internet, enquanto o questionário realizado demonstra que em 89% dos OSE desse setor, 50% dos colaboradores ou mais têm acesso à Internet; e no setor dos transportes, 56,6% dos colaboradores têm acesso à Internet no contexto empresarial português, enquanto no contexto dos OSE 88% indicam haver 50% ou mais colaboradores com acesso à Internet para fins de trabalho[24].

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

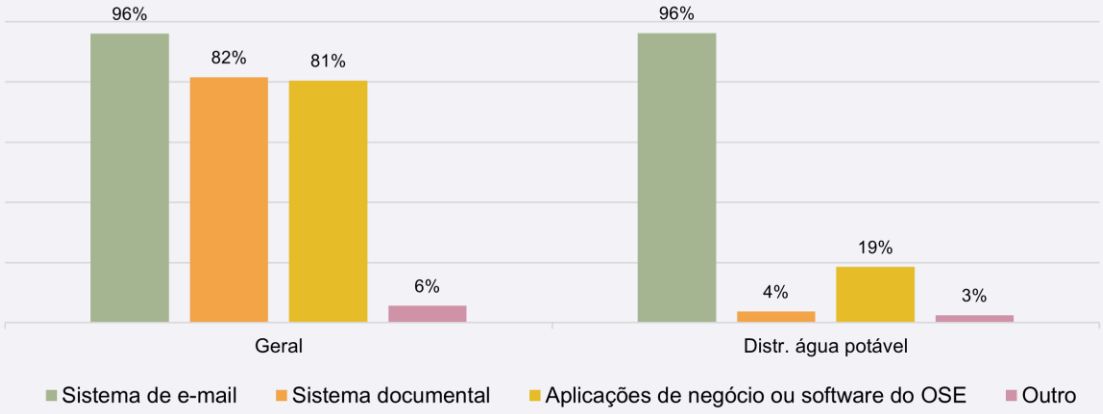


O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSE aos colaboradores é uma realidade em praticamente todos os OSE inquiridos (95%). Apenas em 2 setores, pertencendo a estes o setor da distribuição de água potável, registaram-se exceções. Ainda assim, pelo menos 94% dos operadores neste setor fornecem acesso remoto a esses sistemas aos seus colaboradores.

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

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

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



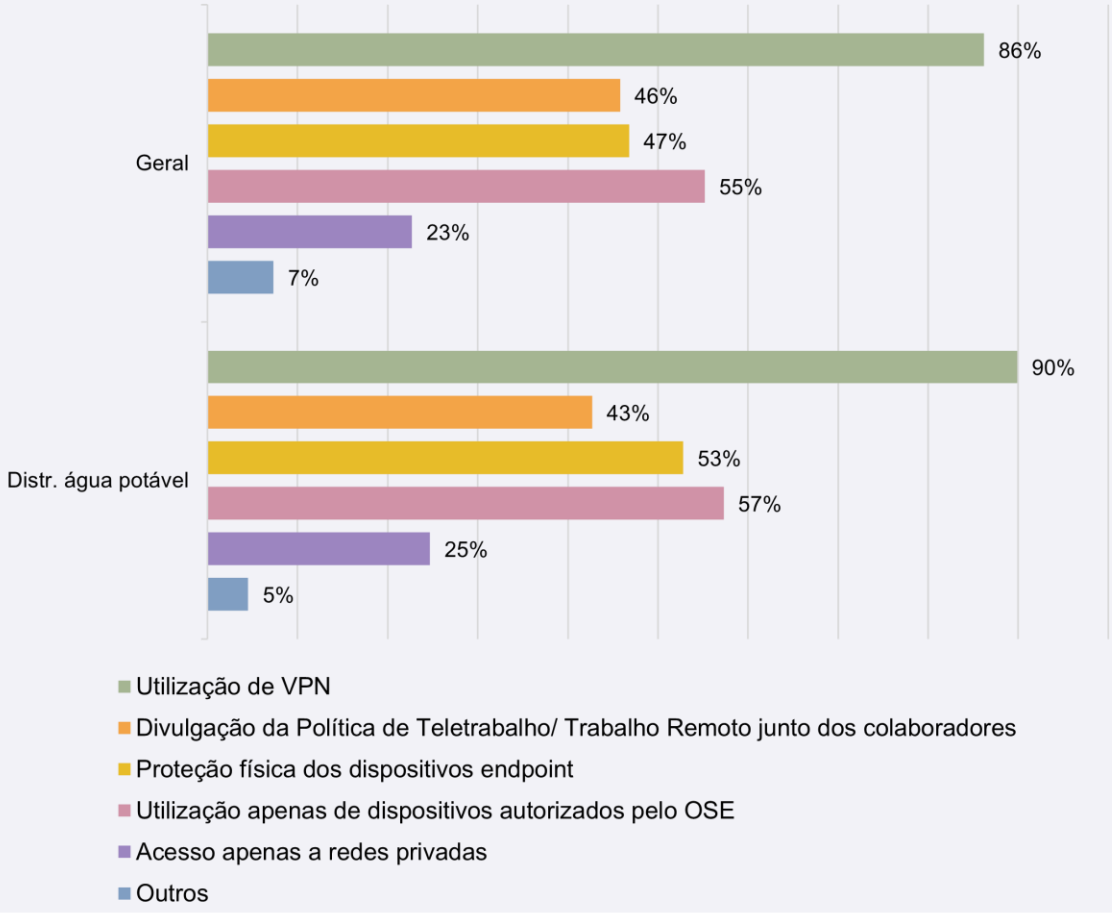
Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no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

No setor do fornecimento e distribuição de água potável, é notório que o principal sistema ao qual é dado acesso remoto é somente o de *e-mail* (96%), havendo muito menos OSE nesse setor nos quais é dado acesso remoto ao sistema documental (4%) ou a aplicações de negócio ou a *software* do OSE (19%).

Comparando novamente com dados do IUTICE de 2022, os OSE continuam a fornecer mais acesso remoto a diferentes sistemas do que a generalidade das empresas portuguesas. Tinha já sido vista a diferença na disponibilização geral de acesso remoto por parte dos colaboradores a sistemas entre OSE (95% a disponibilizar) e empresas (74,7% a disponibilizar). Revisitando essa comparação entre cada sistema, é visível que há mais OSE a dar acesso remoto aos documentos da organização do que empresas em geral (82% de OSE contra 65% de empresas) e também mais OSE a dar acesso remoto a aplicações ou *software* de negócio (81%) do que empresas (63,9%)[26].

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

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

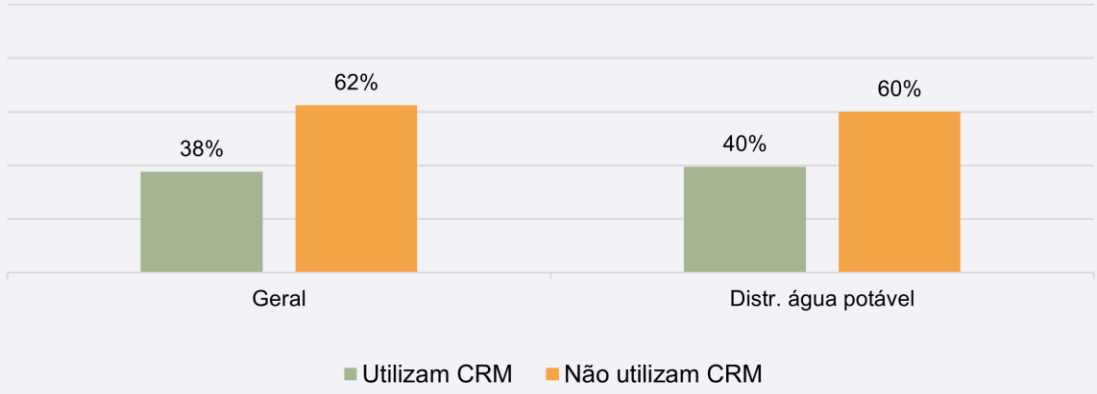


No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança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

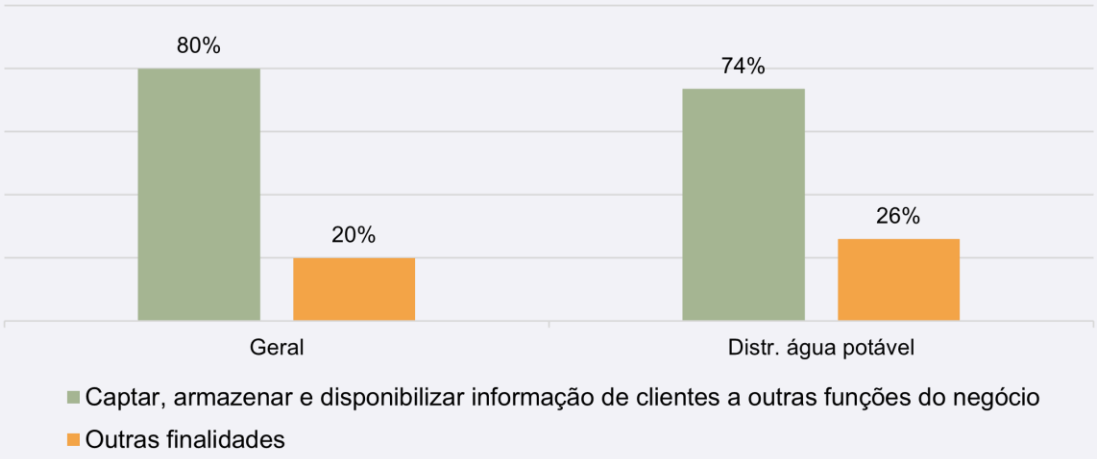
O IUTICE questiona também quais as medidas de segurança aplicadas pelas empresas, embora não enquadre a questão no caso específico do acesso remoto. Apesar de se verificar uma elevada percentagem de empresas a utilizar medidas como palavras-passe seguras (84%) e backups em local distinto (73,7%), apenas 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)[27] - 62% - do que aqueles que utilizam - 38%. Curiosamente, nos dois setores da área financeira (bancário e IMF) observa-se um grande contraste já que de todos os OSE do setor bancário utilizarem CRM e nenhum dos OSE das IMF utilizar este tipo de *software*. Quanto ao setor do fornecimento e distribuição de água potável, predominam os operadores que não utilizam CRM.

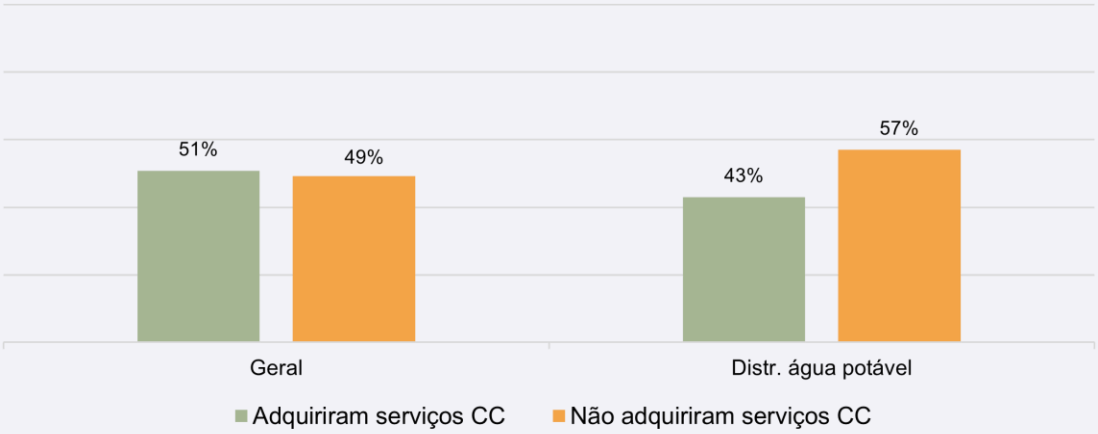
Gráfico 55 - OSE que utilizam CRM para captar, armazenar e disponibilizar informação de clientes a outras funções do negócio



Entre os operadores que utilizam CRM, a maioria utiliza-o para captar, armazenar e disponibilizar informações de clientes a outras funções do negócio (80%). Os restantes 20% utilizam CRM para outros fins não especificados. O setor onde menos OSE indicam utilizar CRM para as funções descritas é o do fornecimento e distribuição de água potável (74%).

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

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

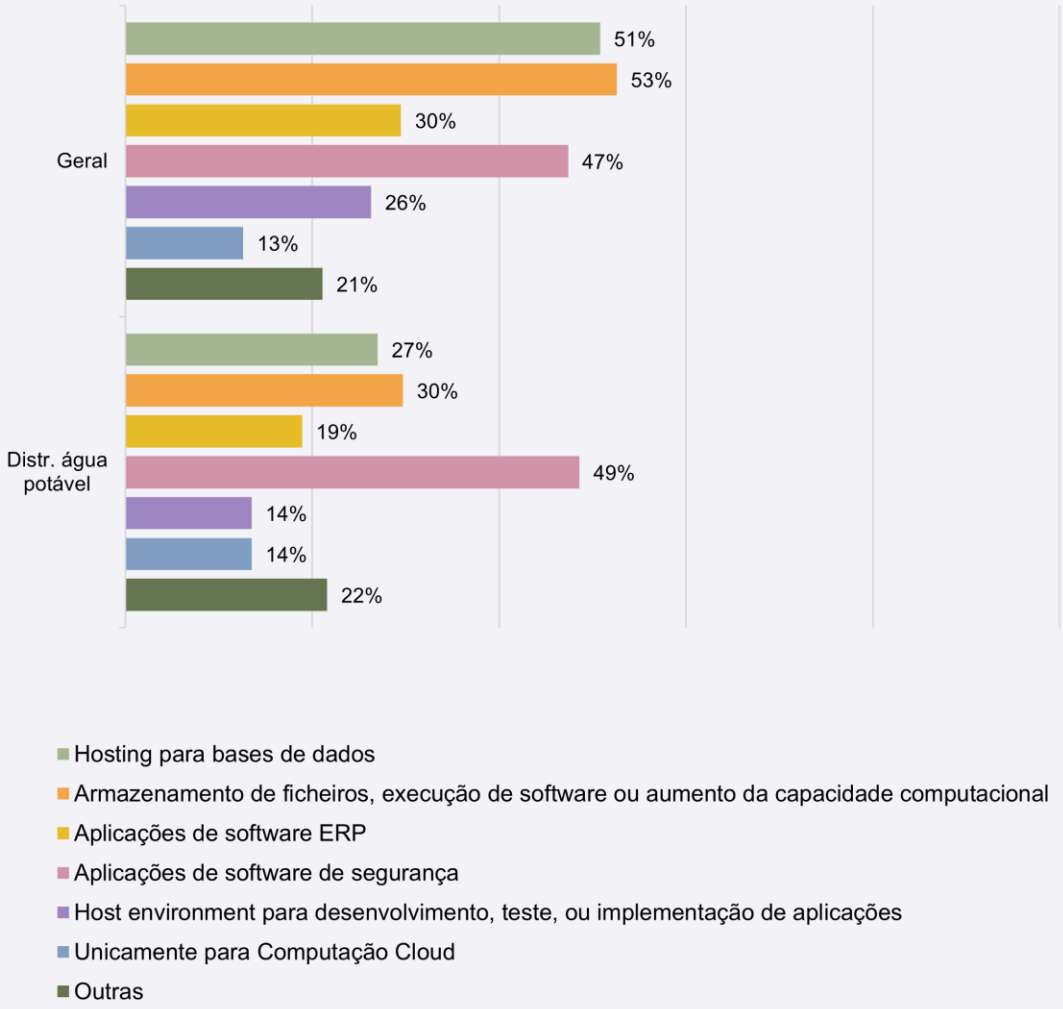


À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização.
Um dos setores onde menos de 50% dos OSE inquiridos adquiriram serviços *cloud* foi o do fornecimento e distribuição de água potável.

O relatório *NIS Investments* de 2022 demonstra que a procura por serviços *cloud* aumentou grandemente devido aos efeitos da pandemia, tendo sido uma prioridade de investimento nesse ano - cerca de 45% dos OSE colocaram o investimento em serviços *cloud* como um dos principais objetivos de 2021[28]. 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*)[29]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[30].

[28] ENISA, "NIS Investments", 2022, 11.
[29] ENISA, "NIS Investments", 2023,10.
[30] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 57 - Finalidades dos serviços de Computação *Cloud* adquiridos



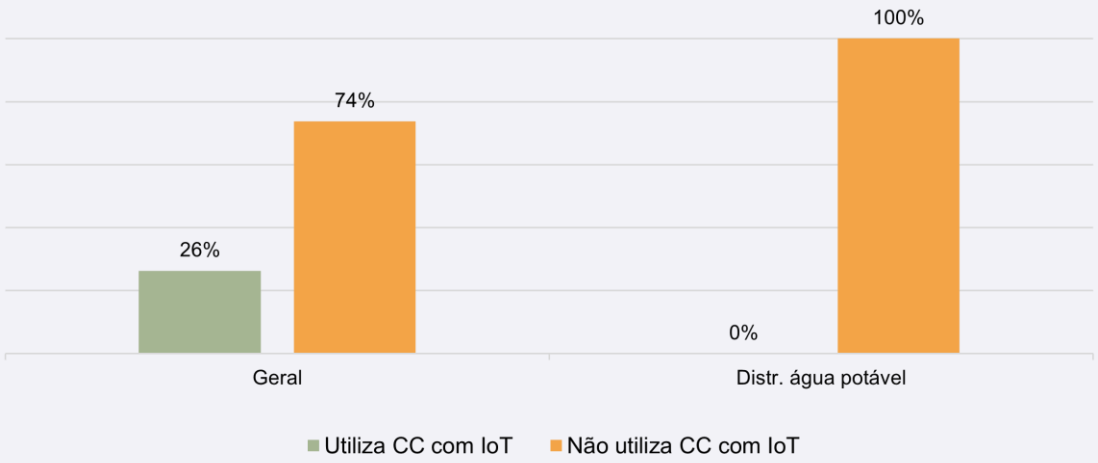
As finalidades dos serviços de Computação Cloud são múltiplas, variando entre *hosting* para bases de dados; armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional; aplicações de *software* ERP[31] aplicações de *software* de segurança; *host environment* para desenvolvimento, 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.

Na distribuição de água potável, menos finalidades foram indicadas por uma maioria significativa dos OSE. Nesse setor, apenas as aplicações de segurança rondam os 50%. As restantes finalidades foram indicadas neste setor por cerca de 30% ou menos dos OSE inquiridos.

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

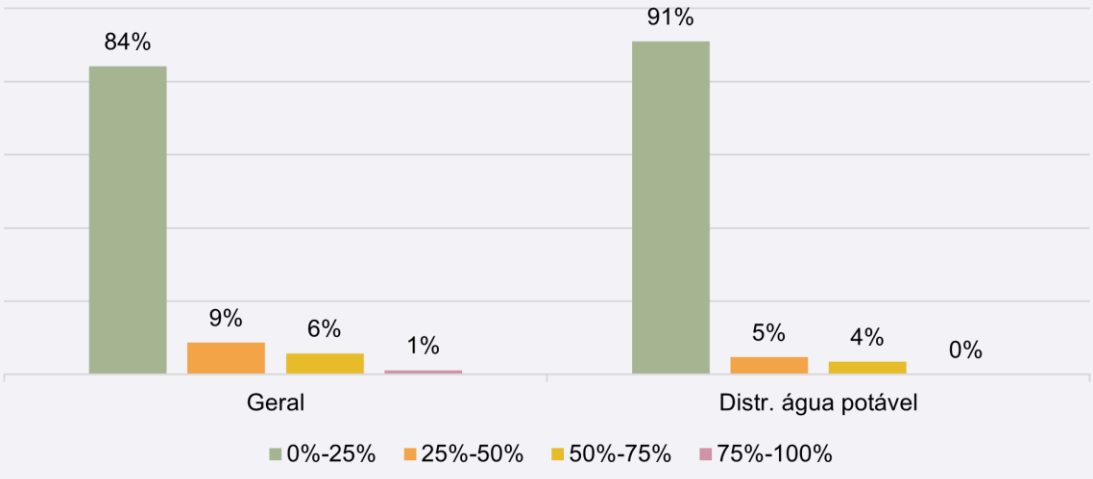
Comparando com dados do IUTICE de 2023, os serviços de *cloud computing* foram adquiridos pelas empresas em Portugal tendo em vista o funcionamento do serviço de correio eletrónico (91,1%), o armazenamento de ficheiros (73,7%), o funcionamento de *software* de aplicações de segurança (67,2%) e *software*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

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



De modo geral, não é frequente, entre os OSE, a utilização de serviços de Computação *Cloud* (CC) em conjunto com a *Internet of Things* (IoT), embora alguns operadores o façam (26%). No setor do fornecimento e distribuição de água potável, nenhum operador utiliza CC com IoT.

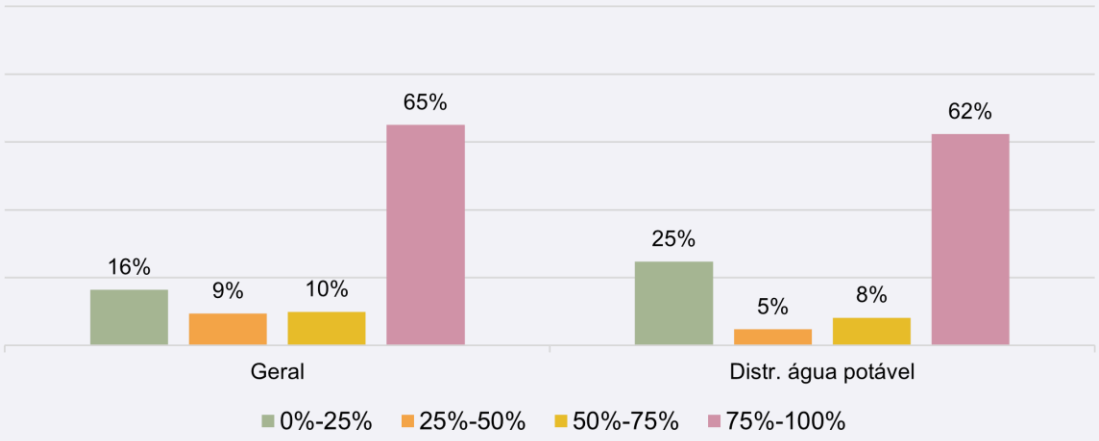
Gráfico 59 - Percentagem de sistemas core em *cloud*



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.

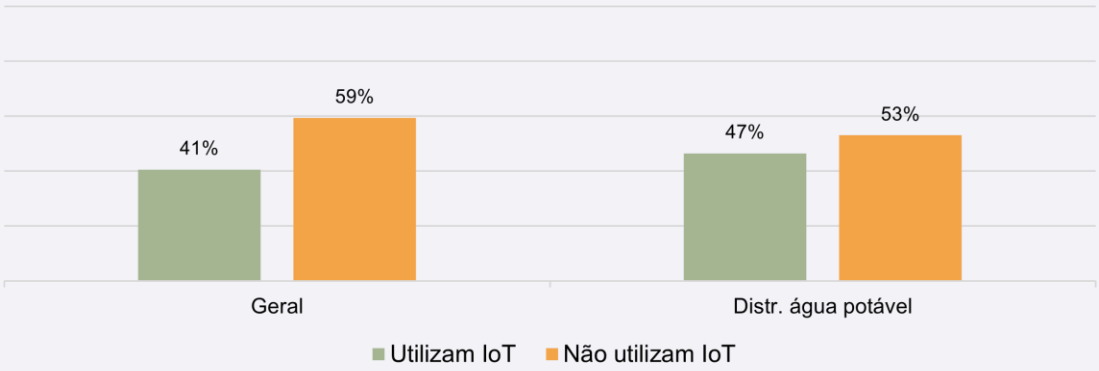
[32] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

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.

Gráfico 61 - Utilização de IoT pelos OSE

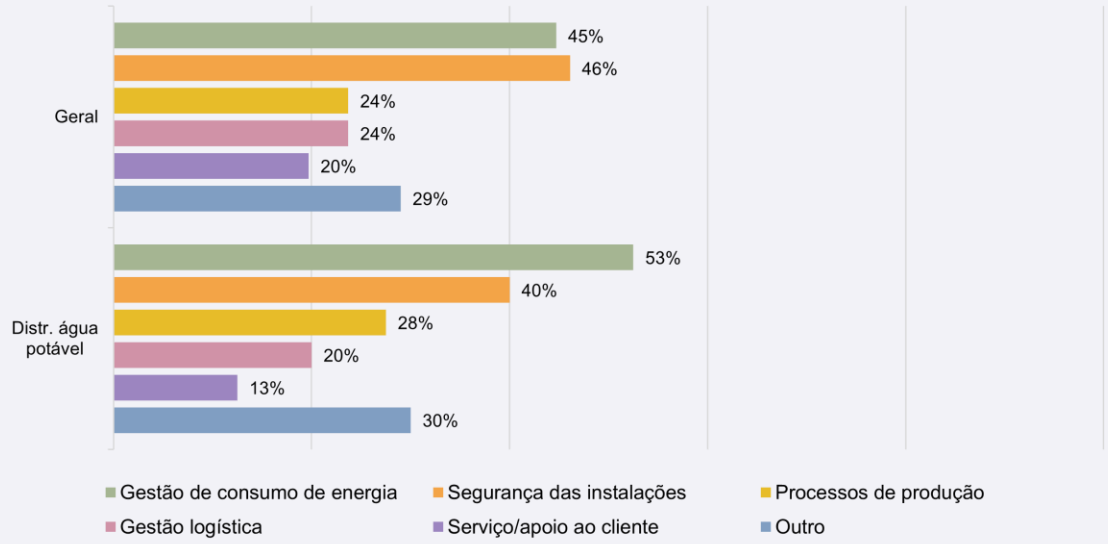


A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT.
No caso do fornecimento e distribuição de água potável, as diferenças percentuais são ténues, mas são mais os operadores que não utilizam IoT.

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%.[33]

Gráfico 62 - Contextos de utilização de IoT

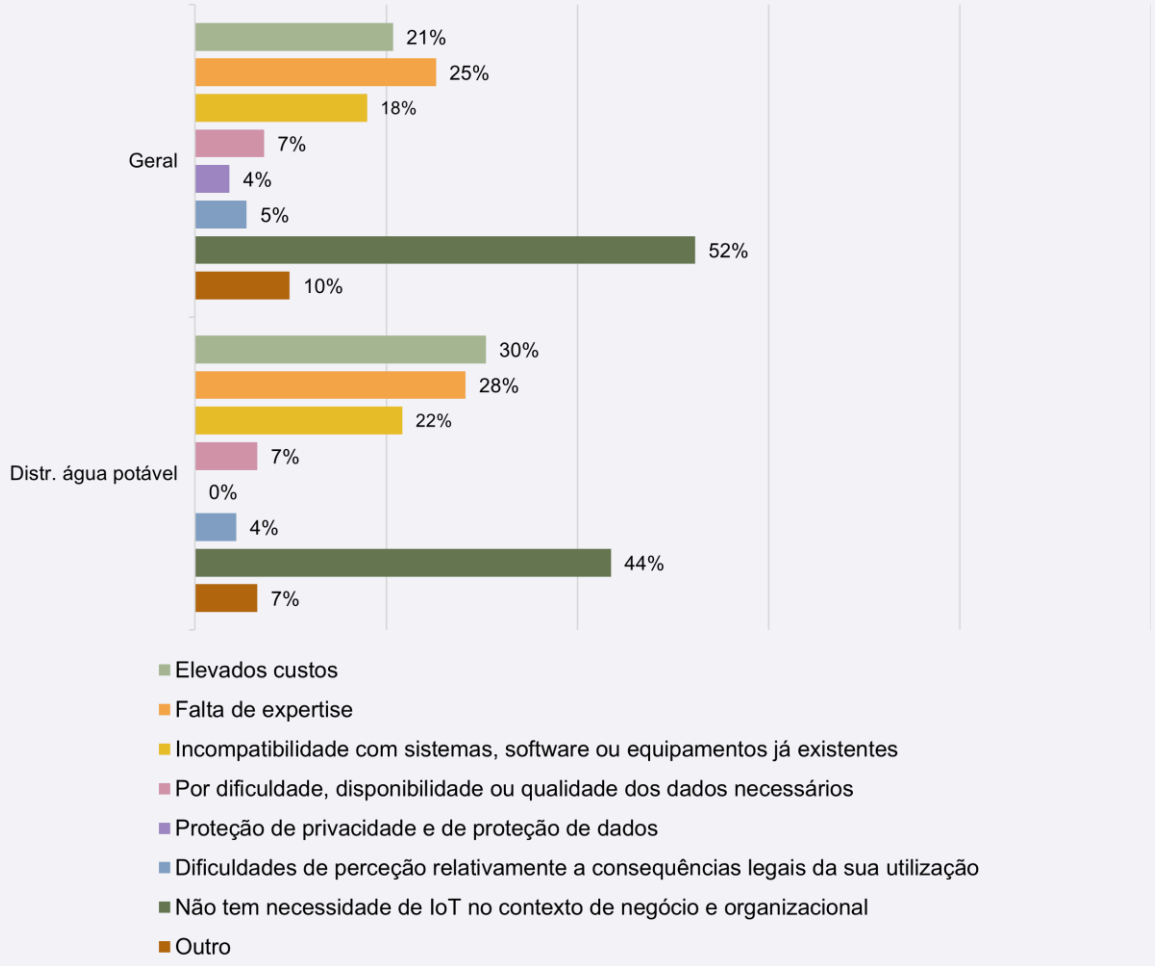


Dado que os setores bancário e infraestruturas do mercado financeiro não possuem operadores que utilizem IoT, não há dados relativos aos contextos da sua utilização nestes setores. De maneira geral, a utilização de IoT é mais comum nos contextos de gestão do consumo de energia e de segurança das instalações, respondido por cerca de 45% dos inquiridos, ao contrário da utilização de IoT para serviço/apoio ao cliente, que tem menos expressividade, cerca de 20%. No fornecimento e distribuição de água potável, destaca-se a gestão de consumo de energia.

O mesmo estudo da ANACOM mencionado no gráfico anterior indica que "os equipamentos IoT foram sobretudo utilizados para segurança das instalações (86%), gestão do consumo de energia (32%), gestão logística (21%), processos de produção (19%), monitorização das necessidades de manutenção (18%) e serviço ao cliente (13%)"[34].

[33] ANACOM, "Utilização da Internet das Coisas (IoT - *Internet of Things*)", 2022, pp. 5 e 16-20, https://www.anacom.pt/streaming/relatorioInternet_dasCoisas_IoT2022.pdf?contentId=1737940&field=ATTACHED_FILE.
[34] ANACOM, "Utilização da Internet das Coisas (IoT - *Internet of Things*)", 2022, 17.

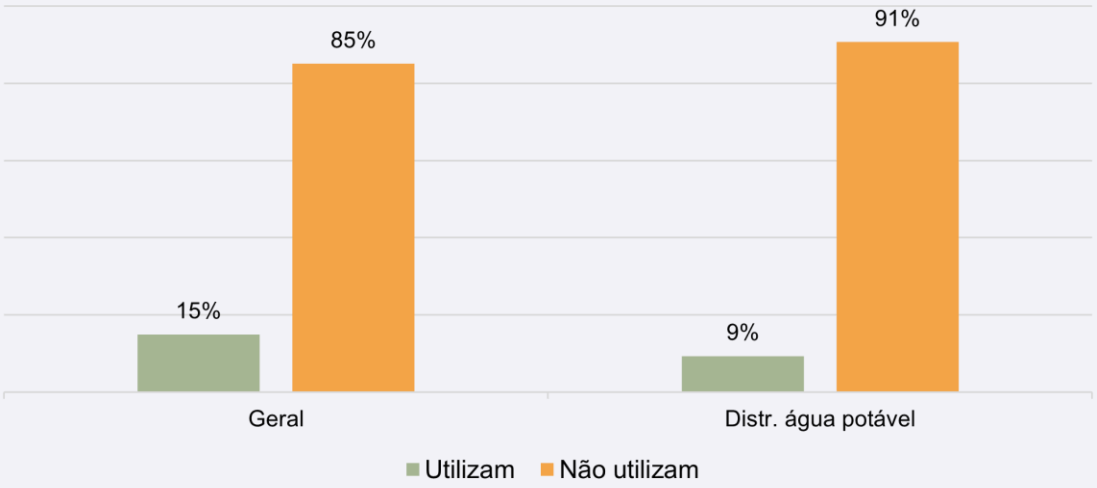
Gráfico 63 - Motivos pelos quais não utilizam IoT



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

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

Gráfico 64 - OSE que utilizam processos que recorrem a IA



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

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%)[35], 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%[36].

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

Gráfico 65 - Funções para as quais utilizam IA

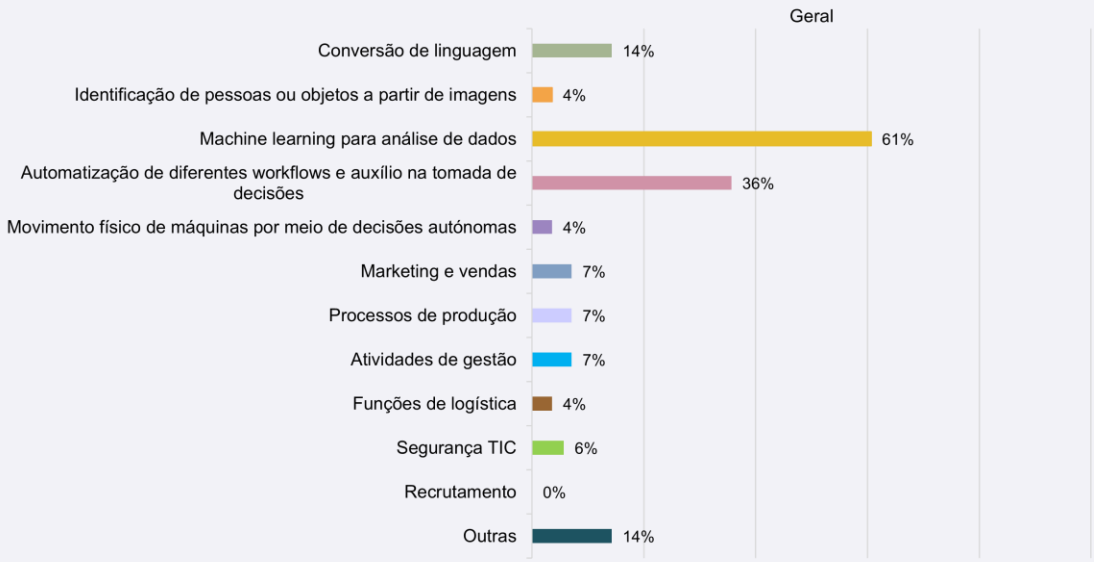
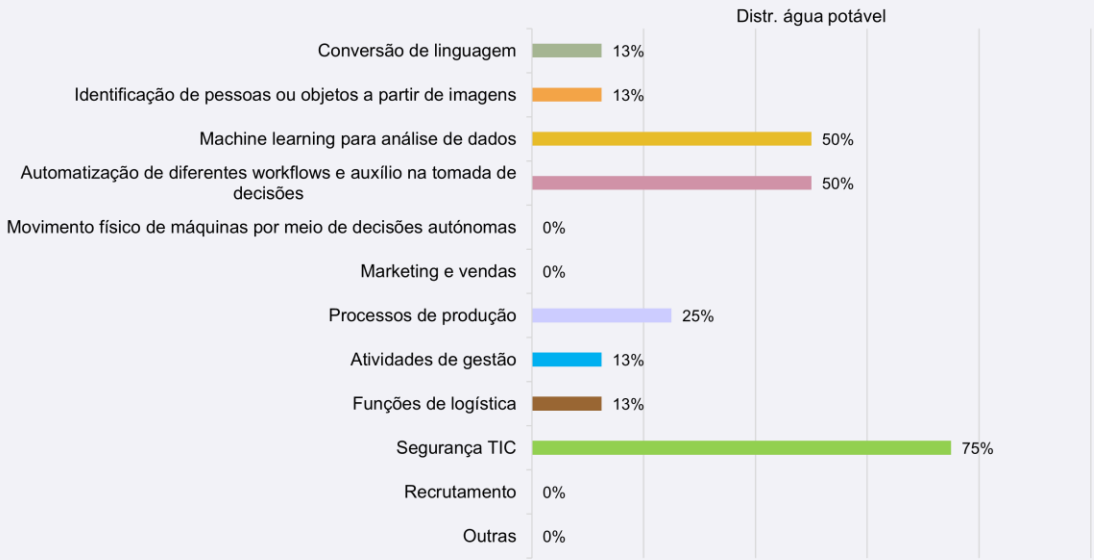


Gráfico 65.1 - Funções para as quais utilizam IA



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.

De acordo com os dados do IUTICE de 2023, entre as empresas que utilizam tecnologia de IA, 44,7% delas utilizam-na para identificar objetos ou pessoas através de imagens. Em seguida, 40,8% das empresas utilizam tecnologias que automatizam fluxos de trabalho ou auxiliam na tomada de decisão. Tecnologias para análise de linguagem escrita são utilizadas por 35% das empresas, apresentando um ligeiro. Já as tecnologias de aprendizagem automática para análise de dados, incluindo *deep learning*, são adotadas por 26,2% das empresas. A tecnologia de IA menos utilizada pelas empresas é a que permite a movimentação física de máquinas através de decisões autónomas baseadas na observação do meio ambiente, com apenas 8,3% de adoção. No entanto, no setor da Indústria e Energia, essa tecnologia é mais prevalente, sendo utilizada por 15,3% das empresas que empregam IA[37].

Segundo o estudo já referido da Microsoft sobre o estado da cibersegurança em Portugal, "embora a IA possa desempenhar um papel absolutamente estratégico na evolução da cibersegurança, a sua integração nos processos de segurança é ainda uma realidade longínqua para a maioria das organizações"[38]. Nesse estudo, 54% dos inquiridos auscultados afirmam não utilizar soluções de segurança com recurso a IA. As organizações que já o fazem – 21% – recorrem a competências de reporte de incidentes de segurança 66%, *cyber intelligence* e a exposição a ameaças 61%, sistemas preditivos de ataque 49% e resposta a incidentes 46%[39].

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

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

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

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança

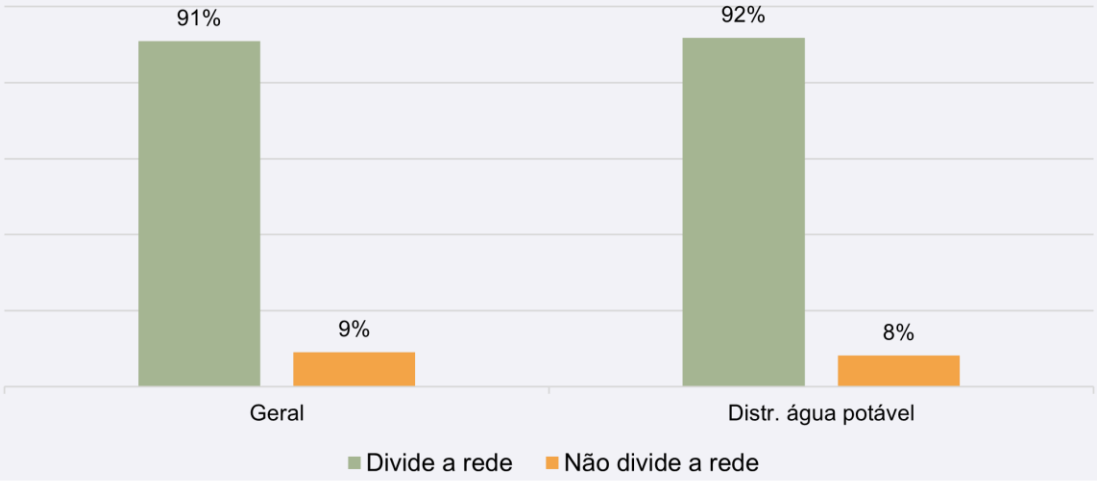
Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança

Na análise geral das medidas de segurança utilizadas pelos operadores, é possível verificar que medidas técnicas como a utilização de Firewall/WAF/Webfilter, utilização de VPN, palavras-passe de autenticação forte, aplicação de *patches* de segurança, a atualização dos softwares e backups de dados em diferentes localizações são das mais utilizadas pelos OSE dos vários setores. Verifica-se, também, que a aplicação de medidas como autenticação multifator, criptografia, ou de manutenção de *logs* para análise pós-incidente é feita por menos de 50% dos operadores inquiridos. Por outro lado, medidas como a realização de sessões de sensibilização para a cibersegurança junto dos colaboradores ou de análises de risco periódicas são também pouco utilizadas, estando aplicadas por menos de 40% e por menos de 30% dos OSE inquiridos, respetivamente. Há que destacar, no entanto, a vasta utilização das medidas de segurança mencionadas no setor bancário, com quase 90% dos operadores a fazer uso da maioria das medidas indicadas. As medidas de proteção segurança de rede em *cloud*, ter uma equipa de especialistas em cibersegurança e controlos biométricos para identificação e autenticação de utilizadores são medidas menos utilizadas pelos operadores, com menos de 25% destes a implementá-las.

Segundo o IUTICE de 2022, no que respeita às principais medidas de segurança das TIC utilizadas em 2021, 84,0% das empresas procedem à autenticação através de uma palavra-passe segura, 73,7% utiliza o *backup* de informação em local distinto (incluindo *backup* para a *cloud*), 62,5% efetua o controlo de acesso à rede (gestão dos direitos dos utilizadores na rede da empresa) e 53,8% conserva ficheiros de registo (histórico) que permitem a análise após incidentes de segurança das TIC. As restantes medidas de segurança utilizadas registam percentagens inferiores a 50%, sendo a autenticação através de métodos biométricos para aceder aos sistemas TIC da empresa a medida menos utilizada, com 12,3%[40].

Consta do estudo da Microsoft sobre o estado da cibersegurança em Portugal, que há um esforço já concretizado pelas organizações a nível nacional que importa destacar: 50% investiu mais em cibersegurança nos últimos anos, nomeadamente com a implementação de: antivírus e *malware* (81%), medidas de autenticação fortes para o acesso a sistemas críticos (71%), *firewalls* (61%), autenticação multifator (37%) e criptografia de dados, para proteger os ativos da empresa (36%)[41].

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

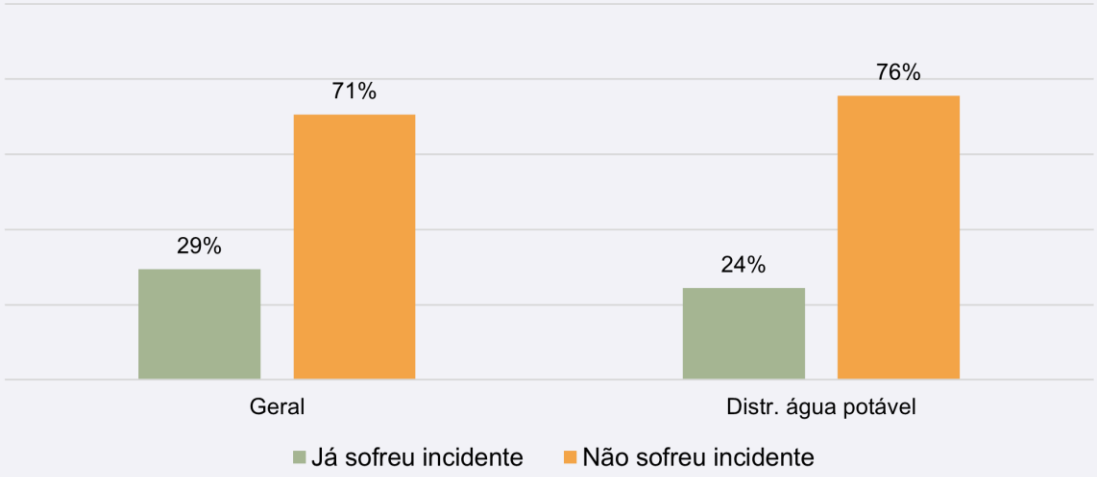


Cerca de 90% dos operadores inquiridos indicaram que distinguem a rede dos colaboradores da rede para estranhos ao serviço (rede *guest*). A quantidade de operadores que não faz essa separação não chega, em qualquer um dos setores, a atingir os 20%.

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

[41] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 7.

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



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

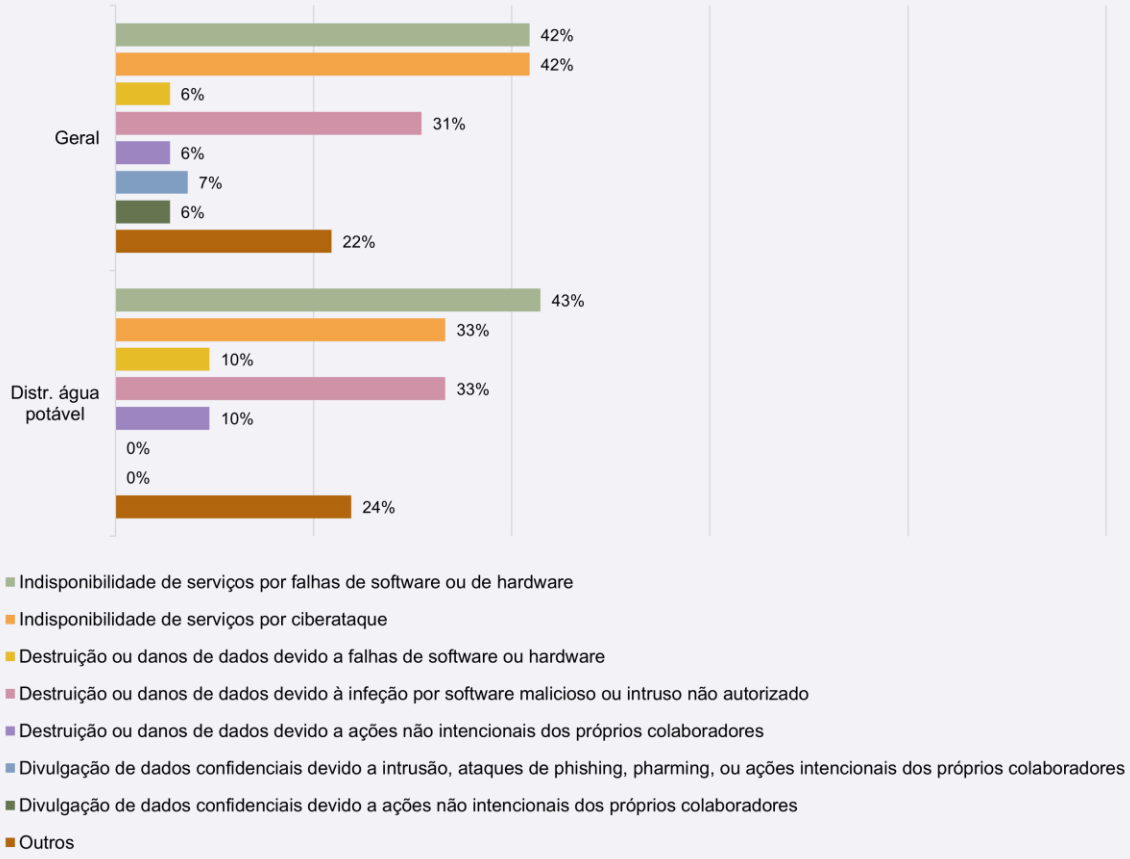
Sendo o IUTICE de 2022, Portugal registou a segunda menor proporção de empresas com incidentes de segurança das TIC na União Europeia (UE). Em 2021, 89,7% das empresas em Portugal, e 91,8% no total da UE, utilizaram pelo menos uma medida para garantir a integridade, a disponibilidade e a confidencialidade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

O Fórum Económico Mundial (FEM) publicou um inquérito em janeiro de 2024, no qual contou com 199 empresas de 49 países. Neste inquérito, cerca de 29% das organizações reportaram que foram afetadas materialmente por um incidente de cibersegurança nos últimos 12 meses. Destas empresas, cerca de 41% afirmaram que o incidente ou incidentes foram causados por terceiros[43].

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

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

Gráfico 69 - Tipos de incidentes ocorridos



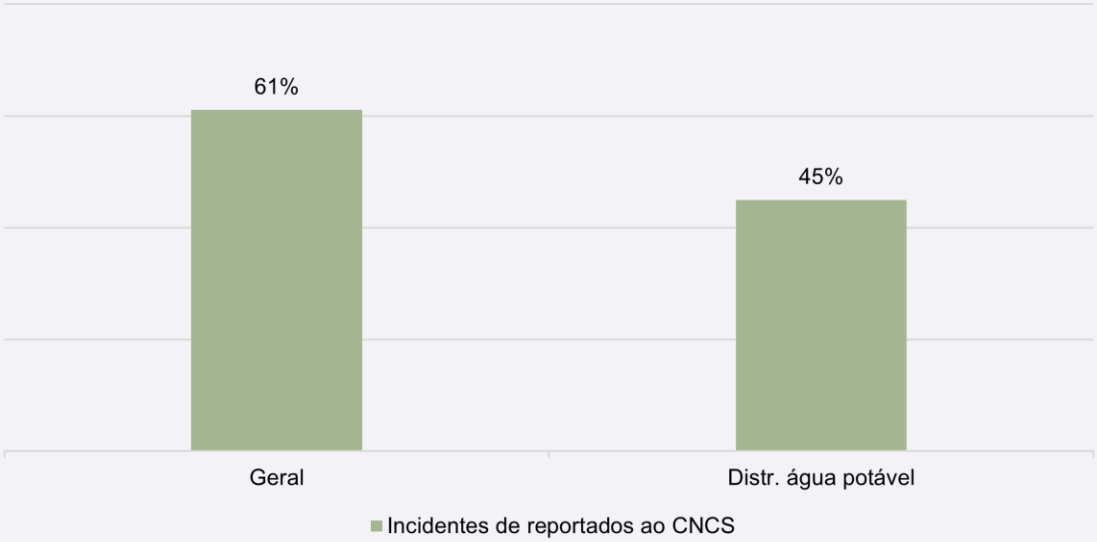
A grande maioria dos incidentes ocorridos afetou a disponibilidade dos serviços, quer por falha de *software* ou de *hardware*, quer por ciberataque. Depois destes, seguem-se os incidentes que resultaram na destruição de dados devido à infeção por *malware* ou devido a intrusão. Os operadores que referiram ter sofrido outros tipos de incidentes indicaram o comprometimento das contas de e-mail, a indisponibilidade de serviços por ataque a terceiros/prestadores de serviços e ainda tentativas de extorsão através de engenharia social.

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

Segundo dados do IUTICE de 2022, em 2021, 11,5% das empresas experienciaram pelo menos um problema, seja de indisponibilidade de serviços TIC, de destruição ou corrupção de dados, ou de divulgação de dados confidenciais, devido a um incidente de segurança relacionado com as TIC. As consequências mais referidas destes incidentes foram a indisponibilidade de serviços TIC devido a falhas de *hardware* ou *software* e a ataques do exterior (8,3% e 2,5%, respetivamente), seguindo-se a destruição ou corrupção de dados devido a infeção de *software* malicioso ou intrusão não autorizada e devido a falhas de *hardware* ou *software* (2,1% e 1,8%, respetivamente)[44].

Segundo o estudo da Microsoft sobre o estado da cibersegurança em Portugal publicado em 2023, 70% dos inquiridos destaca o *phishing*, 63% dos inquiridos destaca os *softwares* maliciosos com cifragem de dados e pedido de resgate, 29% dos inquiridos destaca os ataques de negação de serviço DDoS pela sua capacidade de explorar vulnerabilidades nas redes e dispositivos programáveis da organização e, desta forma, perturbar os serviços e recursos das aplicações[45].

Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS



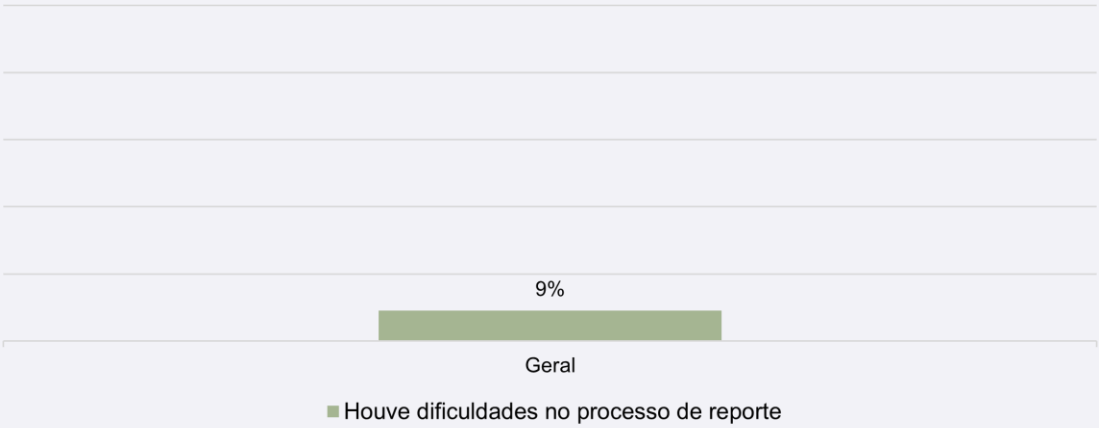
De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n. º1 do artigo 16.º da lei n. º46/2018, de 13 de agosto, os OSE estão apenas obrigados 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 71**.

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

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

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

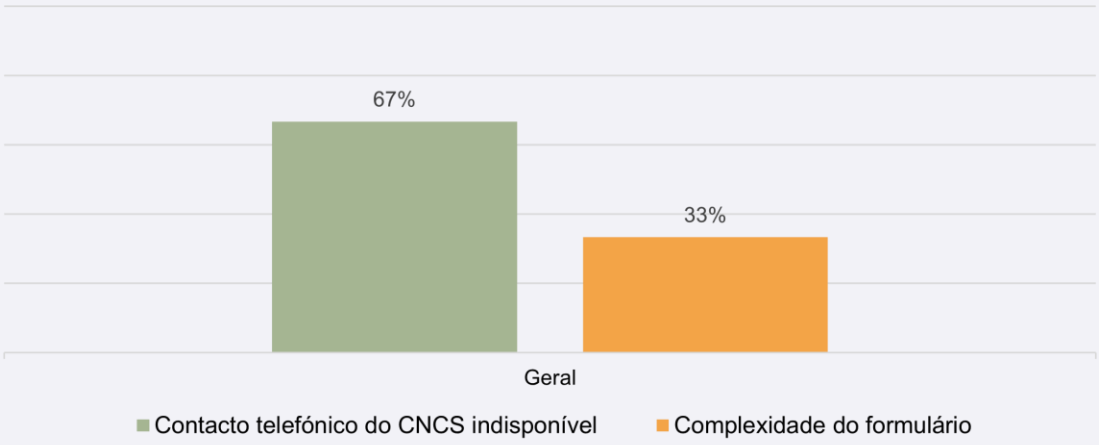
Gráfico 71 - Dificuldades no processo de notificação ao CNCS



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

No setor do fornecimento e distribuição de água potável, não existiram dificuldades no processo de notificação ao CNCS.

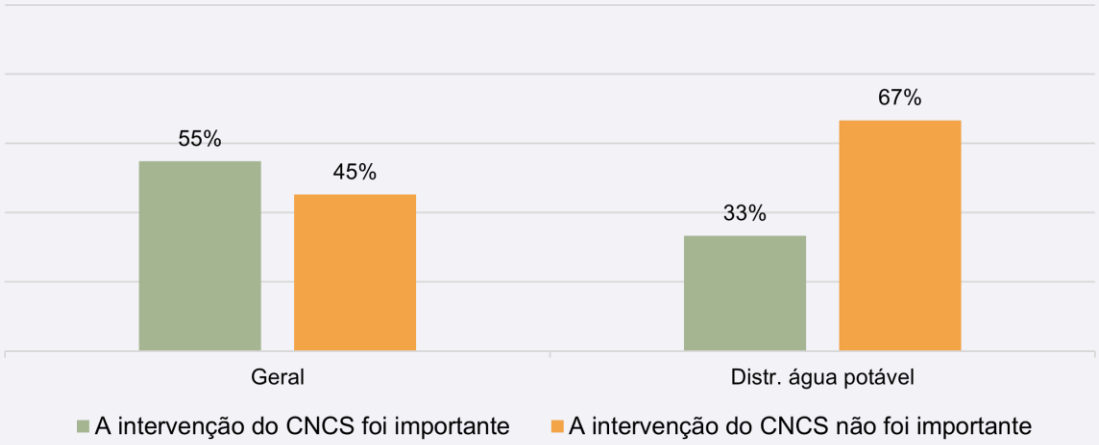
Gráfico 72 - Dificuldades encontradas pelos OSE durante a notificação de incidentes ao CNCS



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

O setor do fornecimento e distribuição de água potável não identificou dificuldades na notificação de incidentes ao CNCS.

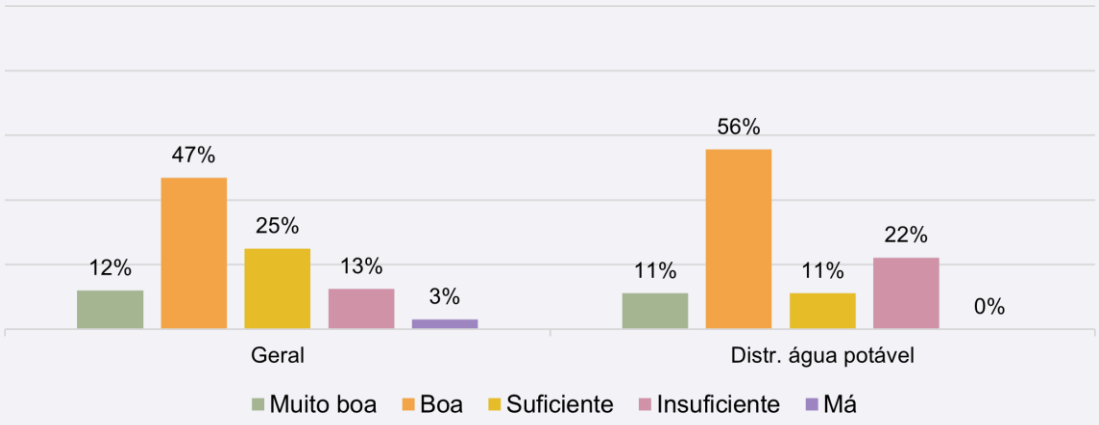
Gráfico 73 - Importância da intervenção do CNCS na resolução do incidente



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

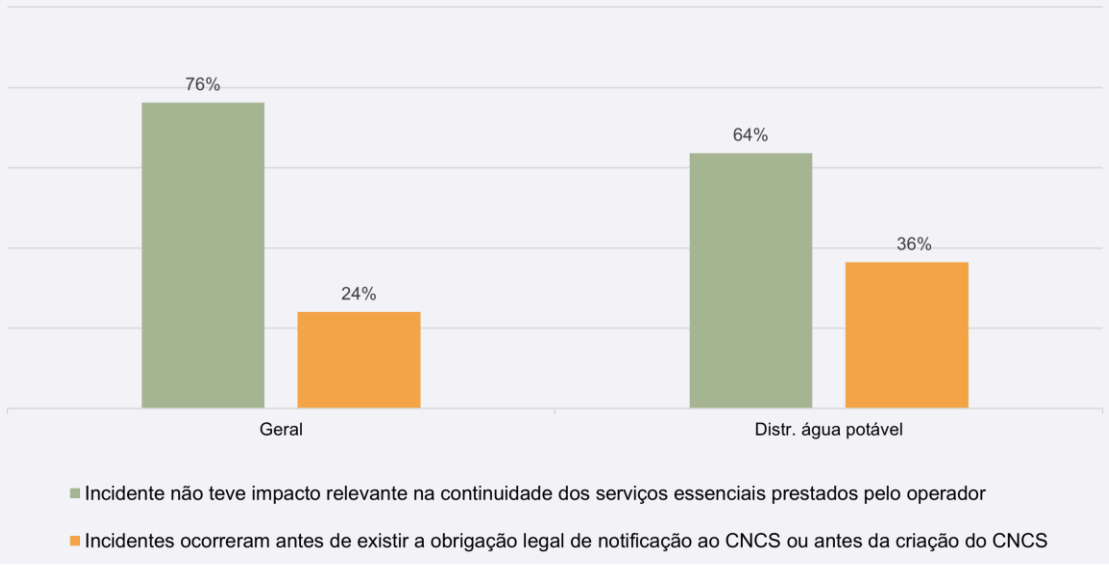
No setor do fornecimento e distribuição de água potável, predomina a opinião de que a intervenção do CNCS não foi relevante para a resolução do incidente notificado.

Gráfico 74 - Avaliação da resposta dada pelo CNCS



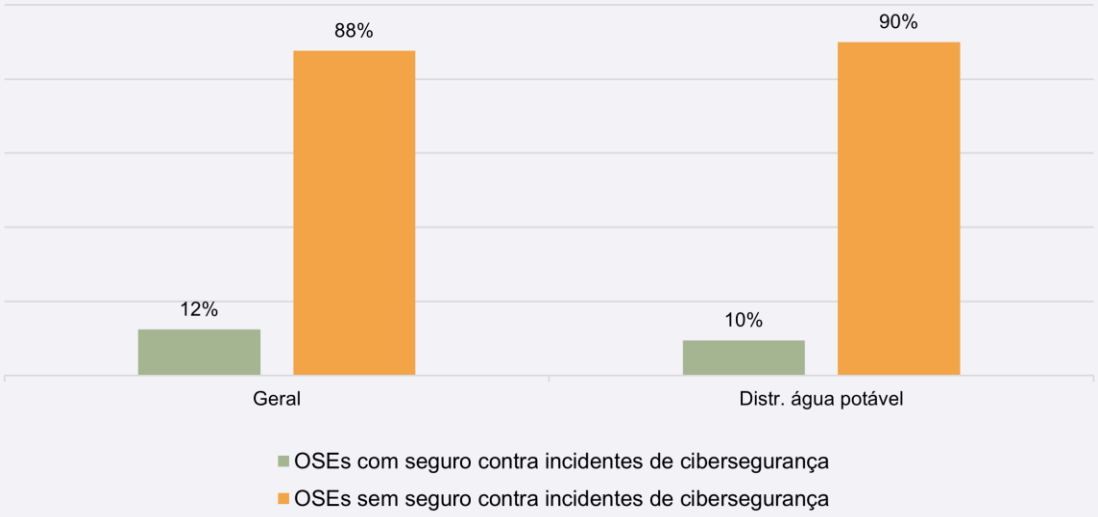
Relativamente à qualidade da resposta dada pelo CNCS ao incidente, existe alguma discrepância nas perspetivas dos diferentes operadores. Mais da metade dos operadores inquiridos (59%) considera que a resposta dada foi boa (47%) ou muito boa (12%). Um quarto dos inquiridos avaliou ainda a resposta dada como suficiente e 16% avaliaram a resposta como insuficiente (13%) ou má (3%).
No setor do fornecimento e distribuição de água potável, a perspetiva geral é novamente positiva, no entanto quase um quarto dos inquiridos classificaram a resposta do CNCS como insuficiente.

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



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

Gráfico 76 - Seguro contra incidentes de cibersegurança

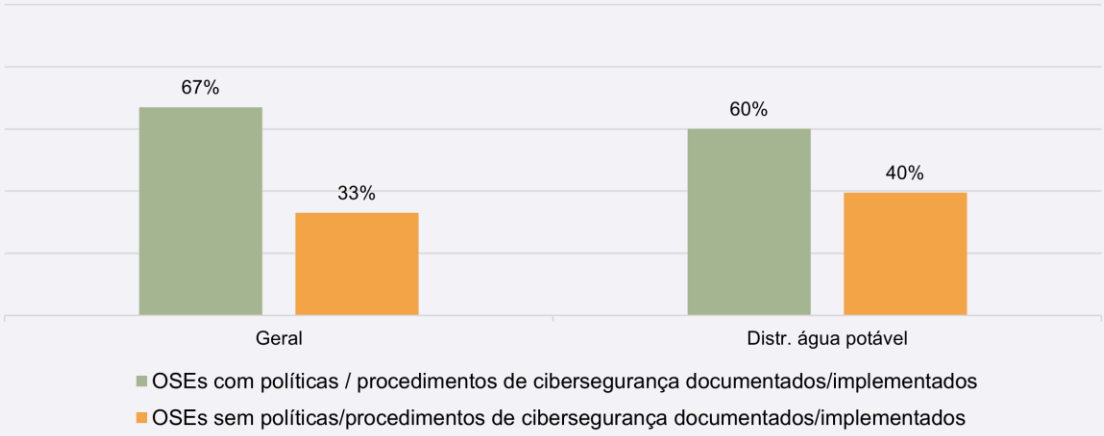


Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. A lógica geral mantém-se no setor da distribuição de água potável, com a maior parte dos inquiridos a não possuírem este tipo de seguro.

Segundo dados da ENISA (Relatório *NIS Investments* de 2023), cerca de 58% dos inquiridos não tinham qualquer seguro relacionado com cibersegurança. A discrepância entre os valores da ENISA e os obtidos pelo questionário realizado poderá dever-se à composição da amostra, uma vez que a do estudo da ENISA inclui operadores de serviços essenciais e prestadores de serviços digitais. Já o questionário realizado pelo CNCS contemplou apenas operadores de serviços essenciais[46].

No inquérito elaborado pelo Fórum Económico Mundial, as empresas foram divididas em dois tipos: empresas com receita elevada e empresas com receita baixa, o que permite observar que as empresas do primeiro tipo tendem a adquirir seguros de cibersegurança - 75% das empresas com receita elevada fizeram-no. Já entre as empresas com receitas mais baixas, apenas cerca 25% destas adquiriram seguros de cibersegurança[47].

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

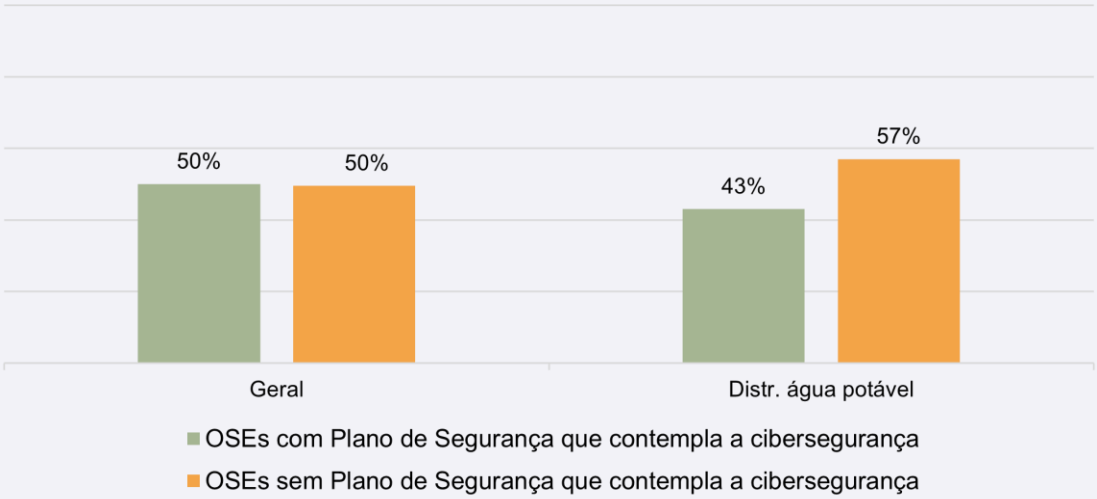


Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados.
No setor da distribuição de água potável, esta proporção é menor que a geral, mesmo assim, a maioria dos operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados.

Segundo dados do IUTICE, em 2022, cerca de 54.4% do total de empresas tinha documentos sobre medidas, práticas ou procedimentos em matéria de segurança[48].

[46] ENISA, “NIS Investments”, 2023, 16 e 24.
[47] Fórum Económico Mundial, “Global Cybersecurity Outlook 2024”, 9.
[48] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2022, 19-20.

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

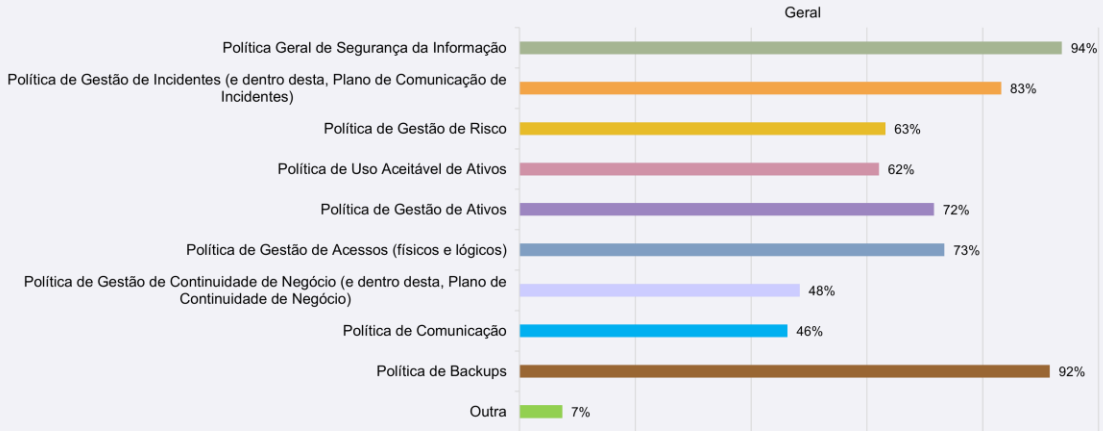


O plano de segurança é obrigatório ao abrigo do decreto-lei n.º 65/2021, de 30 de julho. No entanto, metade dos operadores inquiridos, 50%, ainda não tem um plano de segurança que contemple a área da cibersegurança.

No setor do fornecimento e distribuição de água potável, a percentagem de operadores com plano de segurança fica acima dos 40%, mas aquém dos 50%.

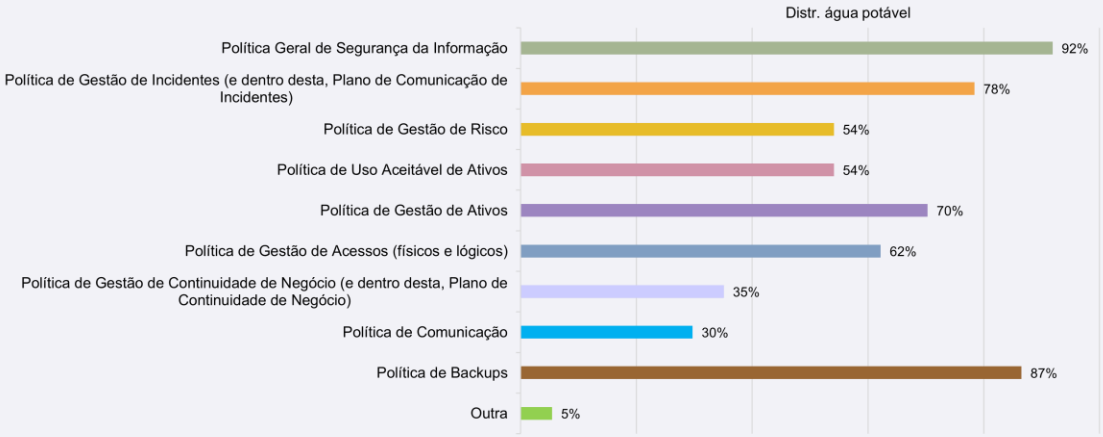
Segundo um estudo realizado pela Microsoft, mais de 40% das empresas inquiridas têm projetado um investimento em cibersegurança. Destas empresas, cerca de 69% irá investir em avaliações regulares de risco de cibersegurança e 66% em auditorias de segurança e monitorização de ameaças em tempo real[49].

Gráfico 79 - Políticas incluídas no Plano de Segurança



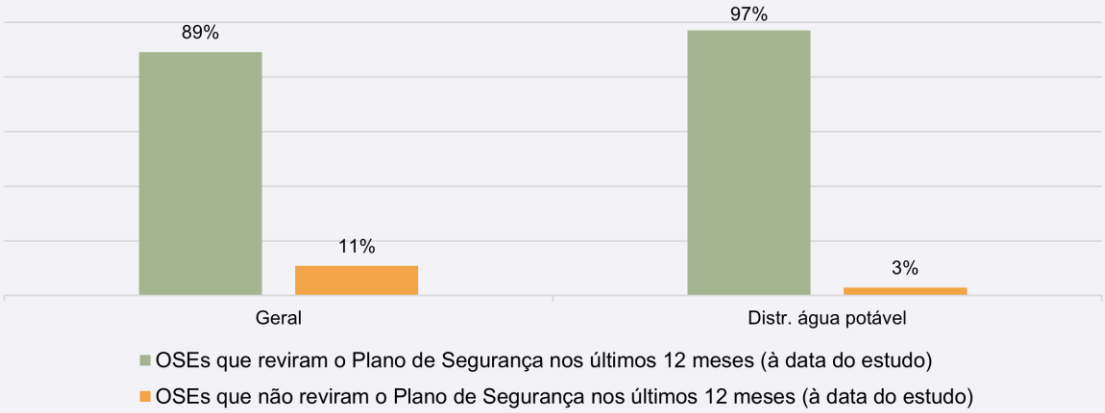
[49] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 5.

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.

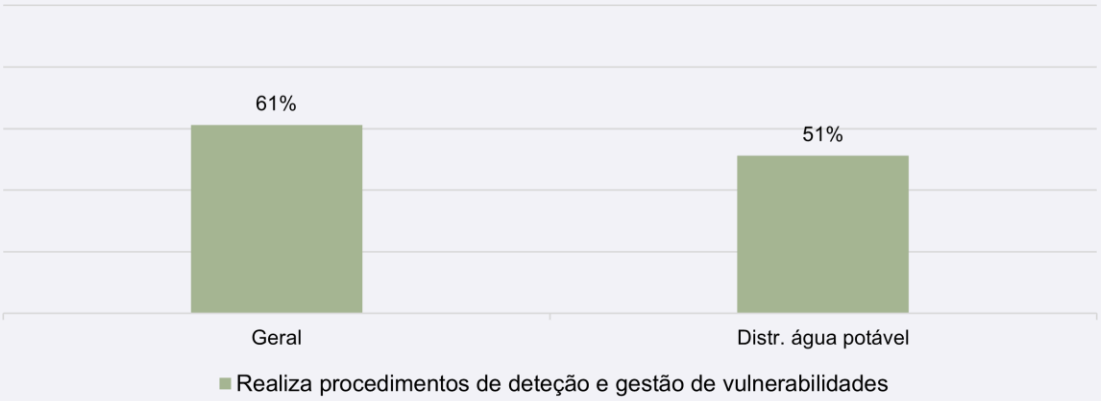
Gráfico 80 - Revisão do Plano de Segurança



Cerca de 89% dos operadores com plano de segurança fizeram a revisão anual do mesmo nos últimos 12 meses, à data do estudo, seguindo as exigências do artigo 7º do decreto-lei nº 65/2021. No setor do fornecimento e distribuição de água potável, apenas uma minoria dos operadores refere não realizar o plano de segurança nos últimos 12 meses (à data do estudo).

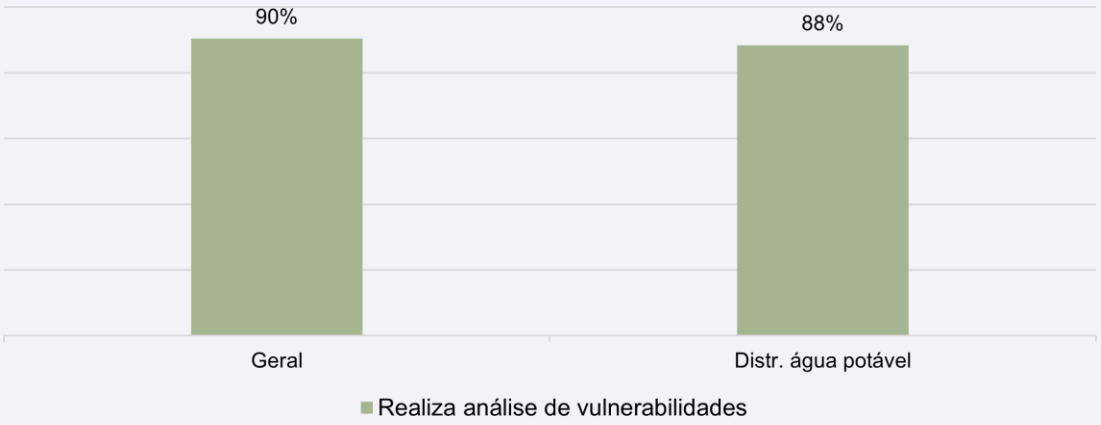
Segundo dados do IUTICE 2022, a maioria (61,7%) das empresas definiu ou fez uma revisão aos documentos sobre medidas, práticas ou procedimentos de segurança nos últimos 12 meses[50].

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

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

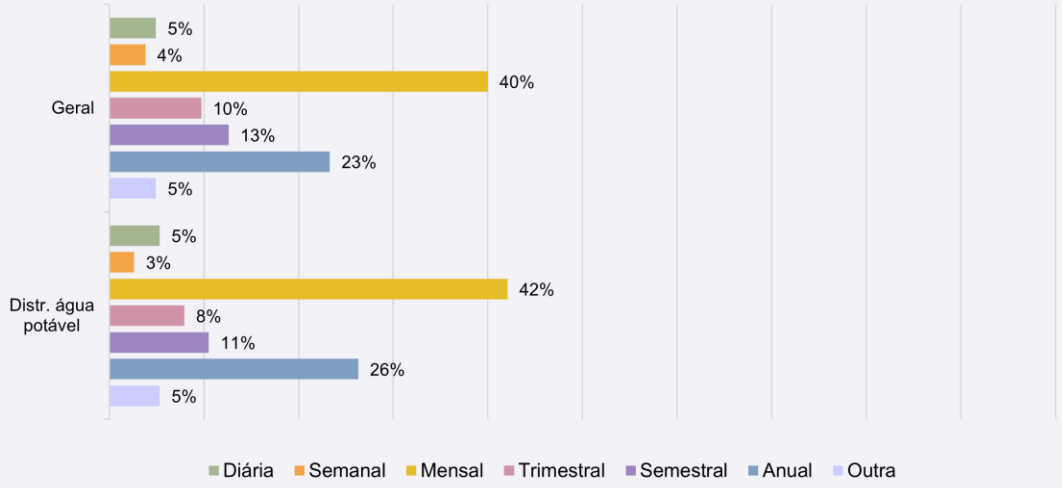


Entre os operadores que realizam procedimentos de deteção e gestão de vulnerabilidades, a vasta maioria (90%) faz também a análise das mesmas.

No setor do fornecimento e distribuição de água potável, embora a análise de vulnerabilidades não seja realizada por todos os operadores de cada setor, esta é realizada por pelo menos 88% dos operadores inquiridos.

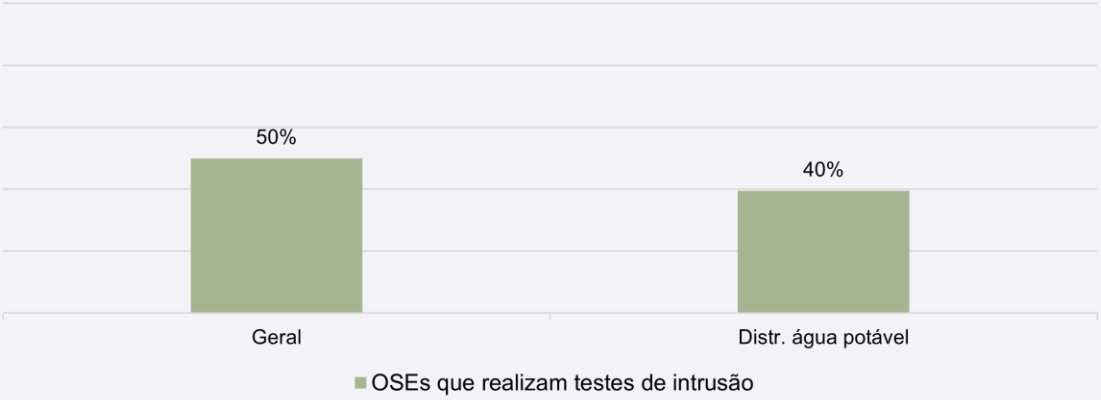
[50] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

Gráfico 83 - Frequência da análise de vulnerabilidades



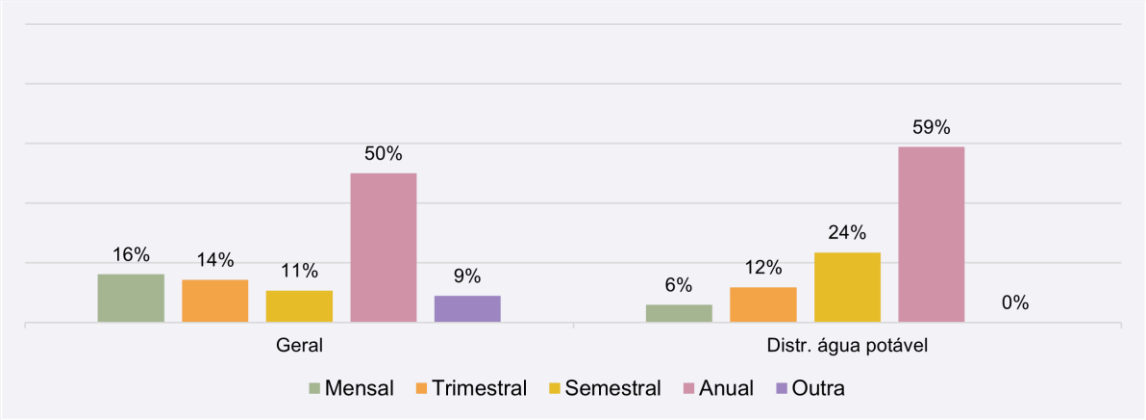
A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.
Há ainda operadores, embora poucos, que realizam análise de vulnerabilidades diariamente, sendo o setor do fornecimento e distribuição de água potável um deles.

Gráfico 84 - Realização de testes de intrusão



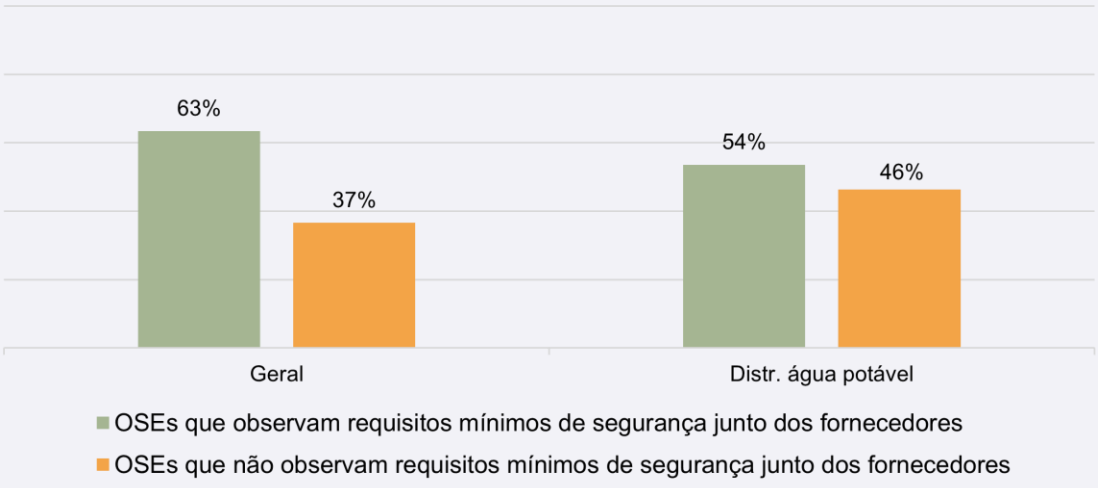
Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).
Contrastando, surgem o setor do fornecimento e distribuição de água potável, a percentagem de operadores que realiza testes de intrusão é inferior a 40%.

Gráfico 85 - Frequência de testes de intrusão



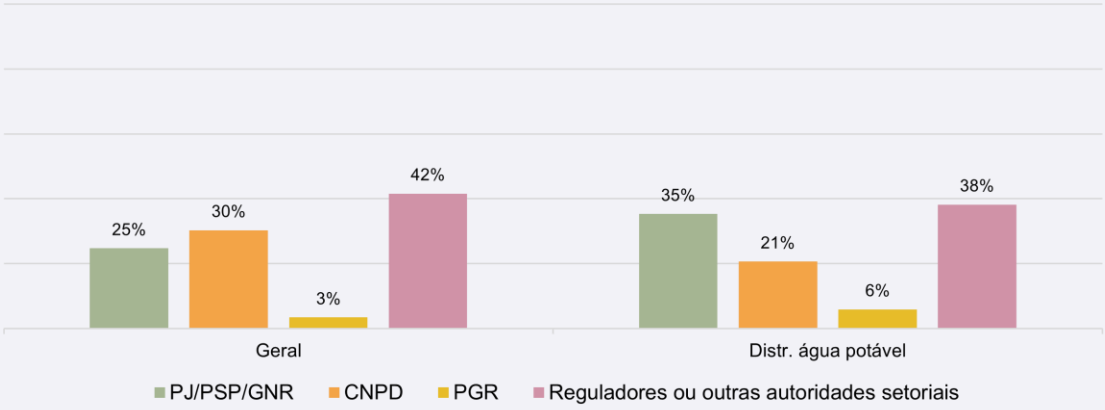
Com exceção dos operadores de serviços essenciais do setor da energia e do setor bancário, os operadores dos setores tendem a realizar testes de intrusão anualmente.
Nos restantes setores, embora prevaleça a periodicidade anual para estes testes, é possível verificar operadores a optar por períodos mais 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.

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.

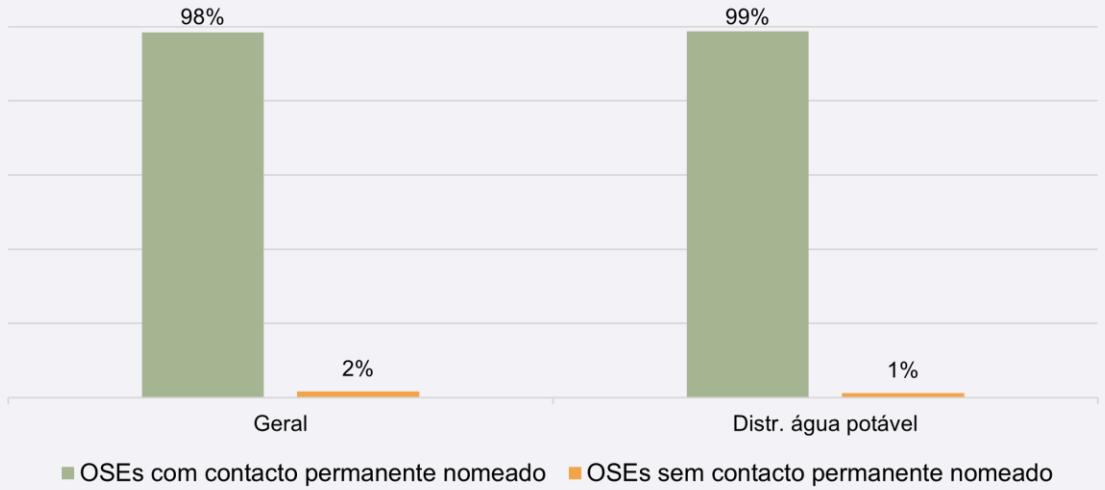
Apenas uma quantidade muito reduzida dos operadores tem previsto fazer qualquer tipo de notificação à Procuradoria-Geral da República (PGR).

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 o setor do fornecimento e distribuição de água potável onde uma minoria dos inquiridos refere optar por contactar a PGR.

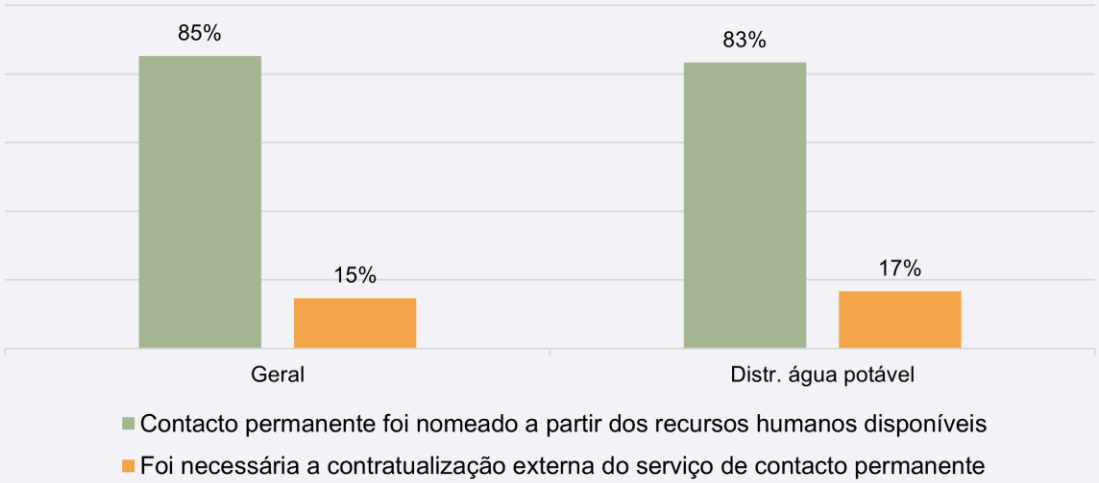
Gráfico 88 - Nomeação do contacto permanente que assegura os fluxos de informação de nível operacional e técnico com o CNCS



98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado.

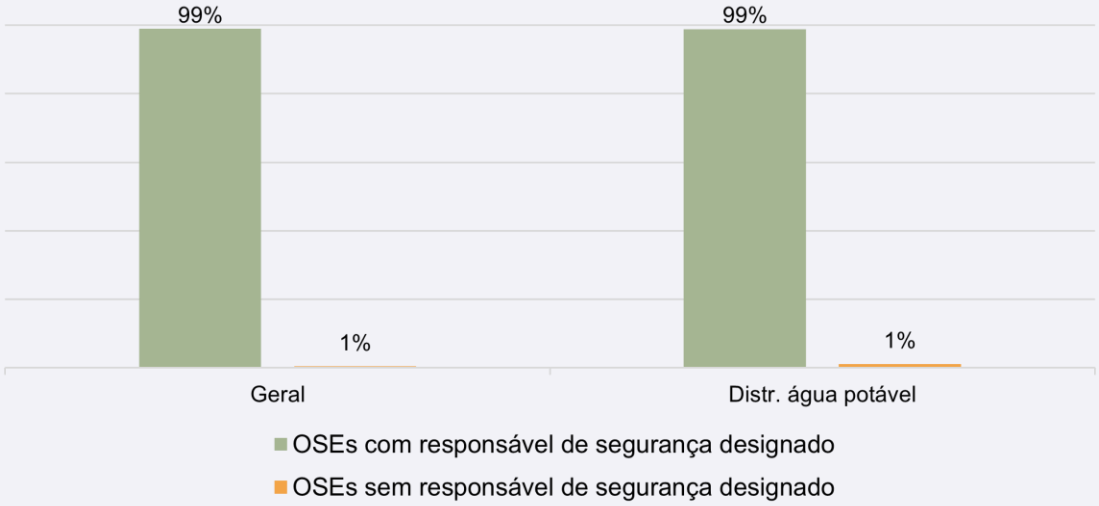
Verificam-se exceções no setor do fornecimento e distribuição de água potável, onde, houve uma entidade inquirida que ainda não tinha nomeado o contacto permanente.

Gráfico 89 - Designação do contacto permanente



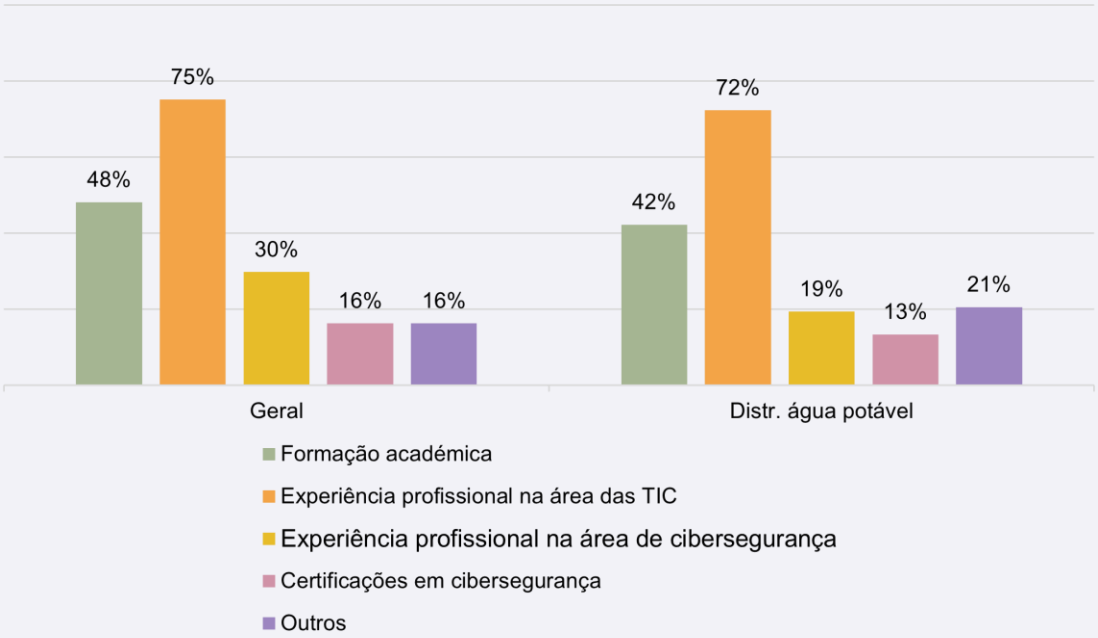
A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No entanto, houve ainda alguns operadores que tiveram de recorrer à contratualização externa do serviço de contacto permanente, com particular destaque para o setor da distribuição e fornecimento de água potável, no qual a percentagem de operadores que necessitou de contratualizar o serviço foi acima de 17%.

Gráfico 90 - Designação do responsável de segurança



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

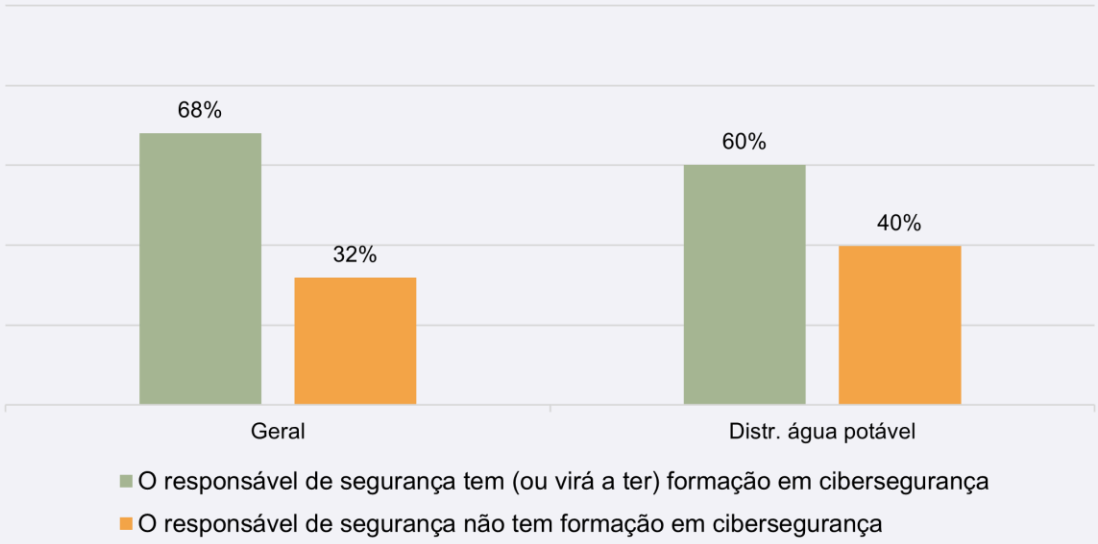
Gráfico 91 - Critérios utilizados para a designação do responsável de segurança



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

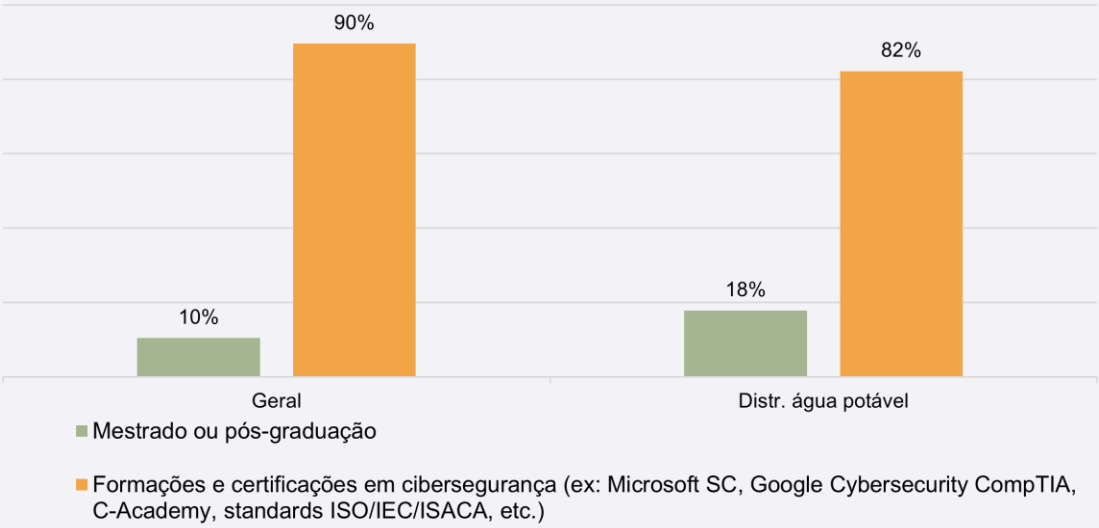
É também importante referir que se verificaram casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de câmara, 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.
Um dos setores onde mais se verificam operadores cujo responsável de segurança não tem formação em cibersegurança é o setor do fornecimento e distribuição de água potável, no qual cerca de 40% dos responsáveis de segurança não têm formação em cibersegurança, nem está planeado que venham a ter proximamente.

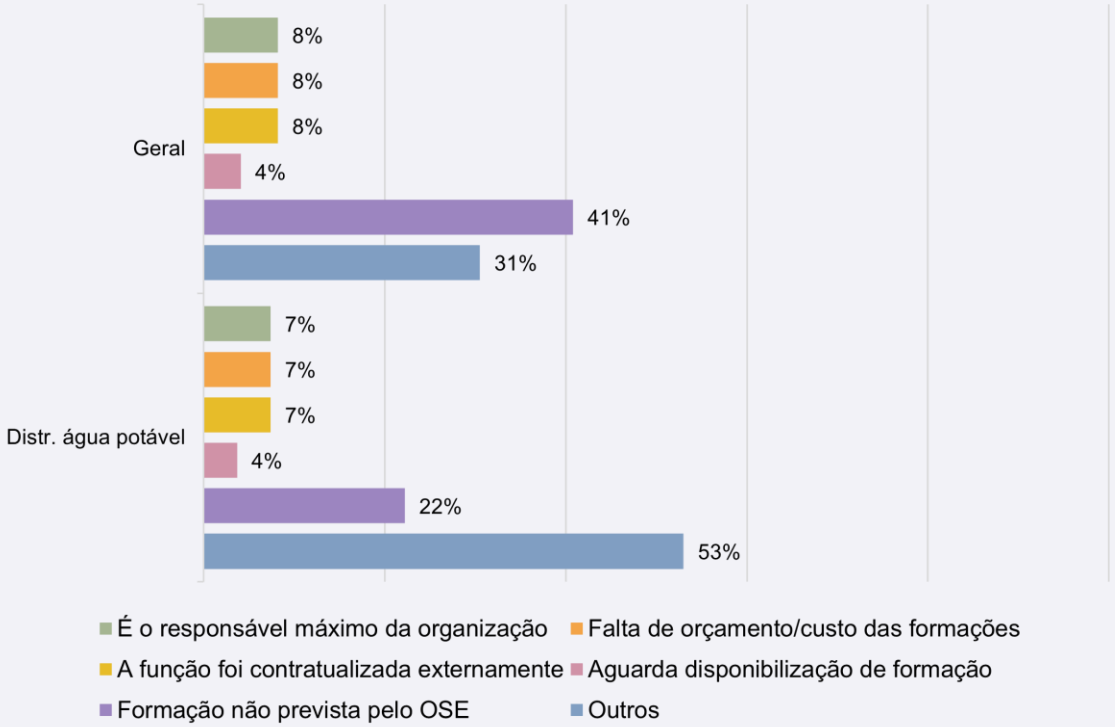
Gráfico 93 - Tipo de formação específica em cibersegurança



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

cibersegurança. Cerca de 90% dos responsáveis de segurança tem uma mais das formações do primeiro tipo.

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



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

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

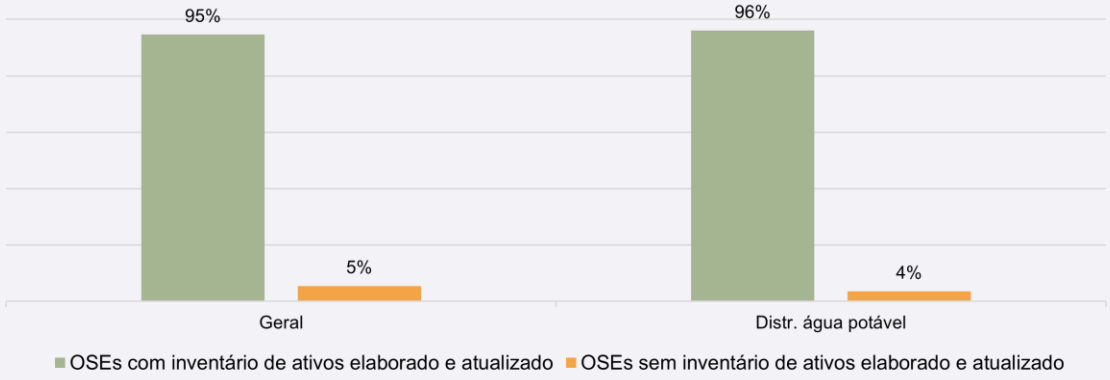
Tal como já referido, houve também situações em que a nomeação do responsável de segurança pouco teve que ver com a formação ou conhecimento em cibersegurança da pessoa nomeada, tendo em cerca de 10% dos casos sido nomeado o responsável máximo da organização. A falta de orçamento foi indicada também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

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

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

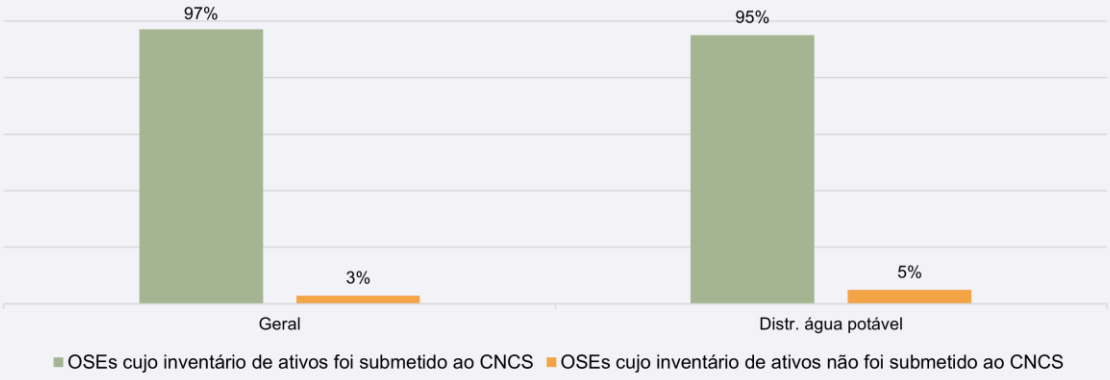
Tal como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado "Compromisso C-Academy" que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança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

Gráfico 95 - Inventário de ativos essenciais elaborado e atualizado



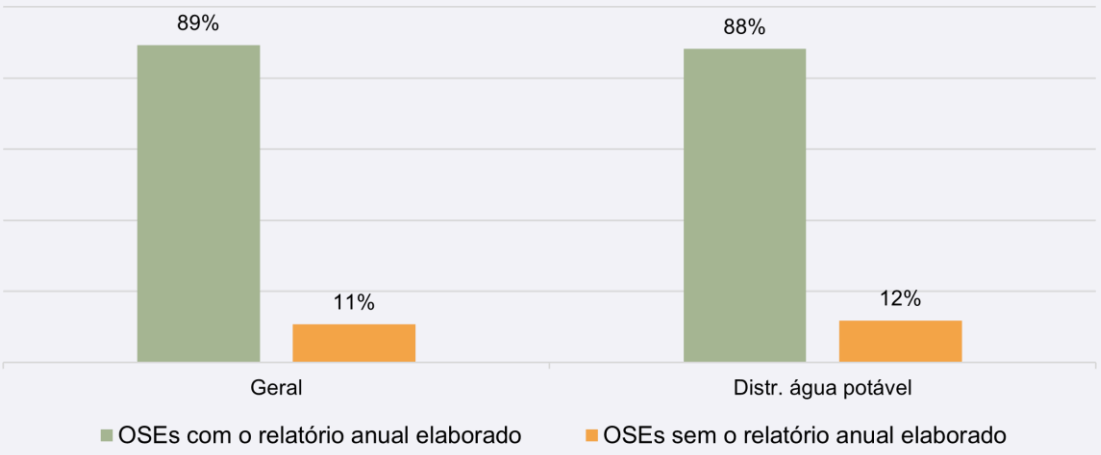
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais.

Gráfico 96 - Submissão do inventário de ativos ao CNCS



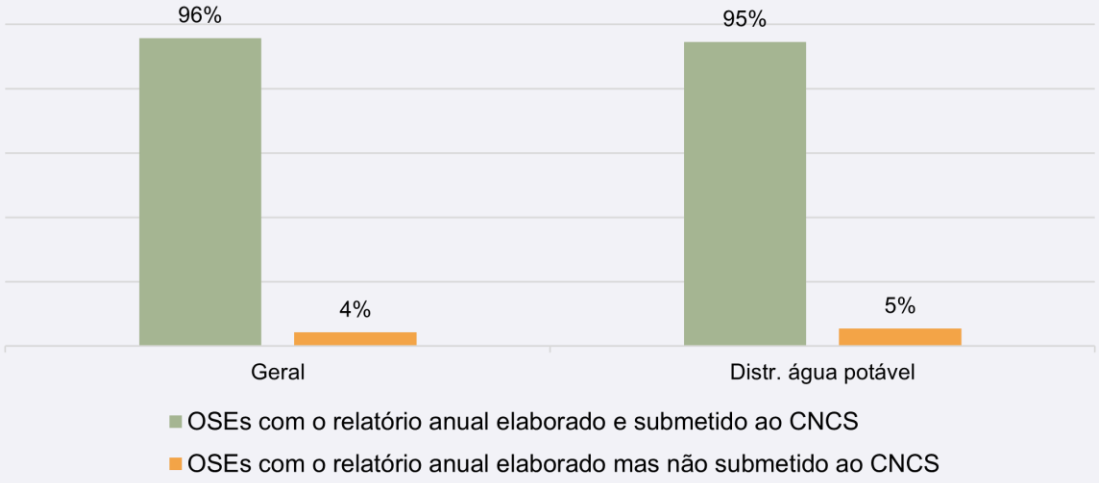
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. As exceções são observadas no setor do fornecimento e distribuição de água potável (aproximadamente 5% dos operadores não submeteram o inventário).

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



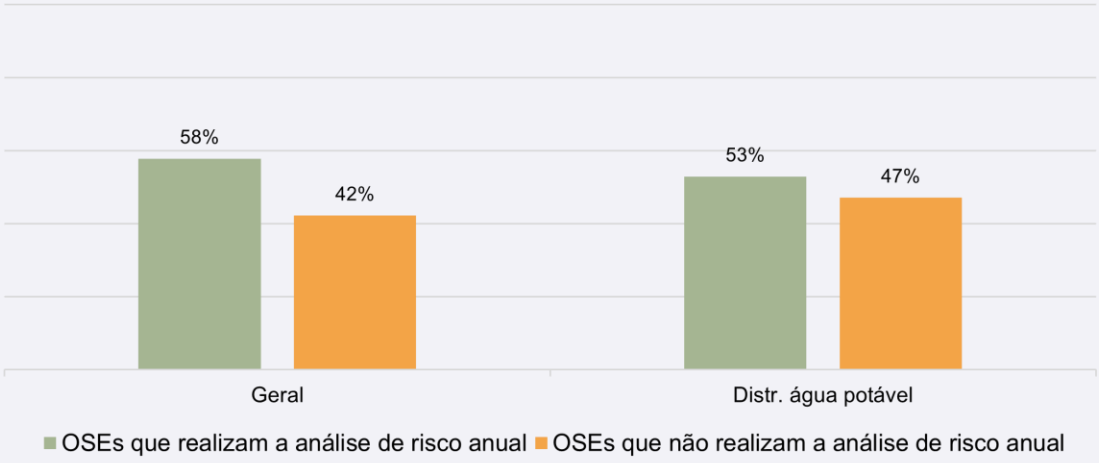
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. Há apenas dois setores onde a totalidade dos operadores refere ter elaborado o relatório anual. Nos restantes setores, a percentagem de operadores que não elaborou o relatório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

Gráfico 98 - Submissão do relatório anual ao CNCS



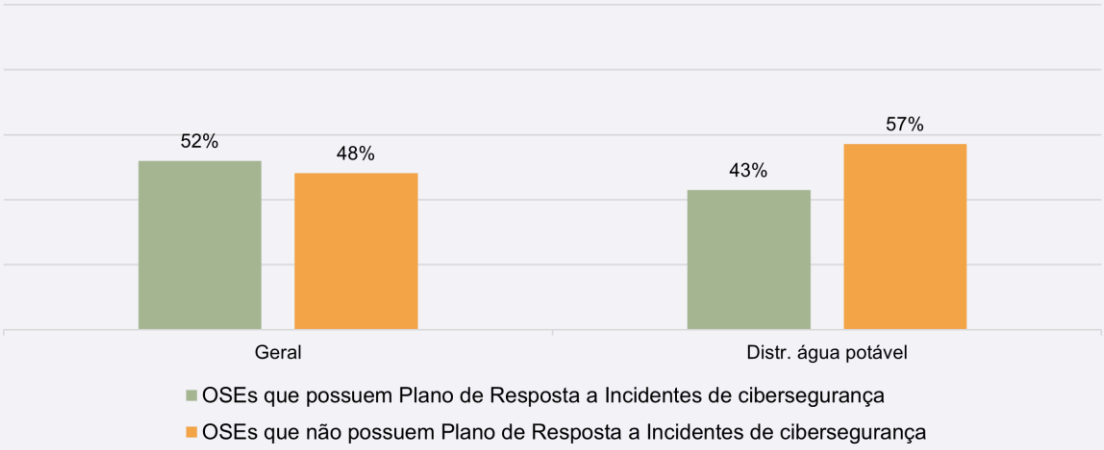
Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 97% submeteram-no ao CNCS. Os casos em que tal não se verificou, ou seja, em que o relatório foi elaborado, mas não submetido, ocorreram em operadores do setor do fornecimento e distribuição de água potável (5%).

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



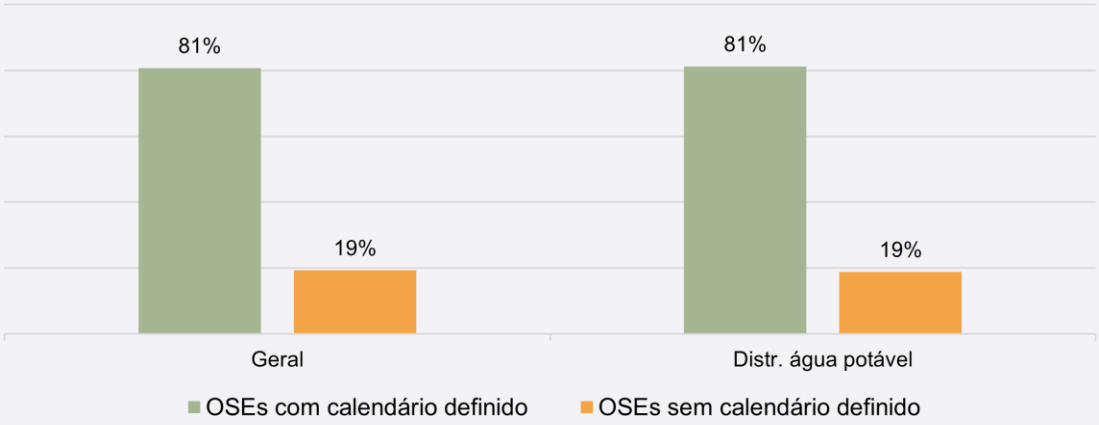
A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. No setor do fornecimento e distribuição de água potável, a percentagem de operadores que efetua a análise de risco fica aquém dos 60%, fixando-se nos 53%.

Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança



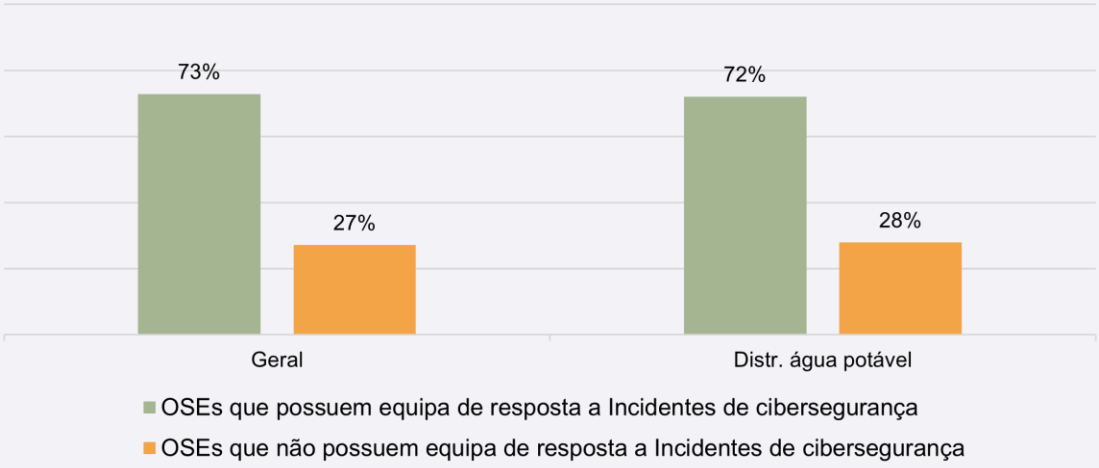
Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. No setor do fornecimento e distribuição de água potável, os operadores sem plano de resposta a incidentes superam os operadores com plano, havendo apenas 43% de operadores com plano.

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



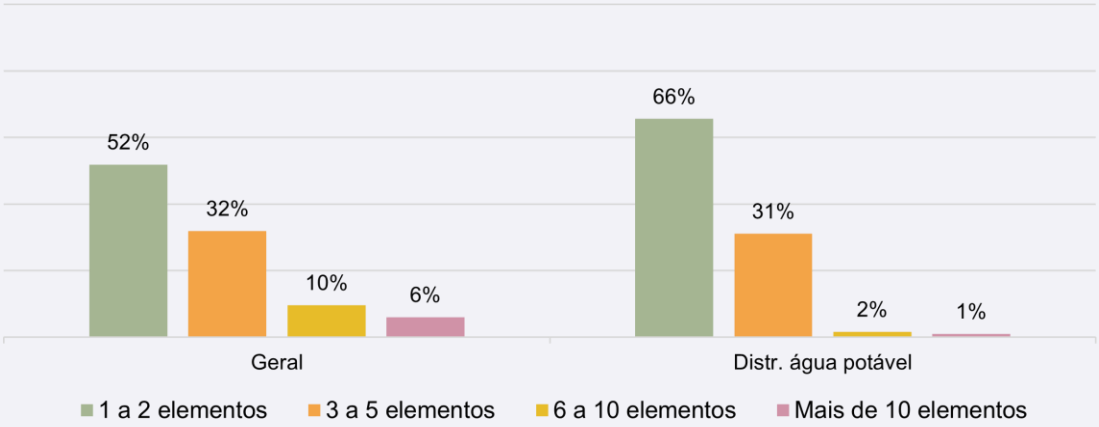
A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. O setor do fornecimento e distribuição de água potável espelha a generalidade. Há que salientar ainda que, tal como revelam os gráficos anteriores, mesmo com calendário definido, existem situações em que os operadores não elaboraram ou submeteram o seu inventário de ativos essenciais ou o seu relatório anual, como, por exemplo, no setor da energia.

Gráfico 102 - Equipa de resposta a incidentes de cibersegurança



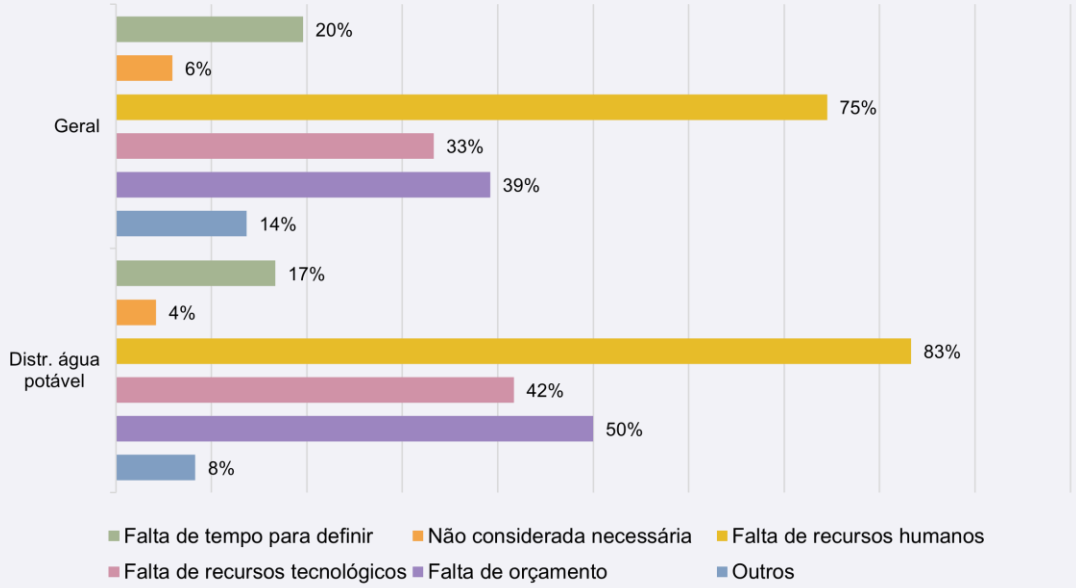
A nível geral, 73% dos operadores possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de operadores que possui tal equipa é sempre superior a 60%. Os operadores do setor do fornecimento e distribuição de água potável ficam um pouco aquém desse limiar dos 80%, mas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

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



Na visão geral, 55% dos operadores com equipa de resposta a incidentes de cibersegurança conta com equipas compostas por 1 a 2 elementos. A nível setorial, a prevalência de equipas de resposta a incidentes com 1 a 2 elementos repete-se em diversos setores sendo um deles o setor do fornecimento e distribuição de água potável (65%). 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, especialmente nos setores de Distribuição de Água Potável, com uma proporção maior de equipas muito pequenas.

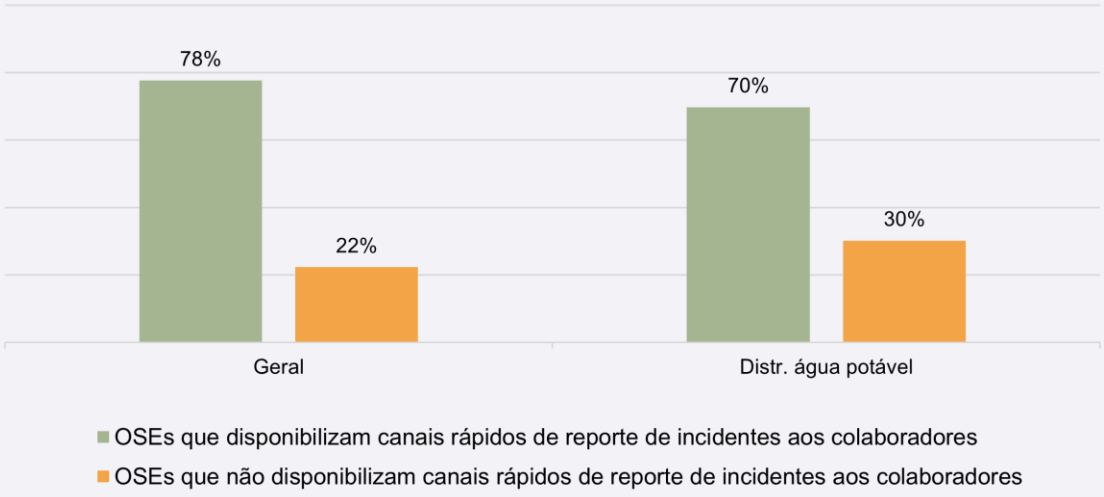
Gráfico 104 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança



O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa.

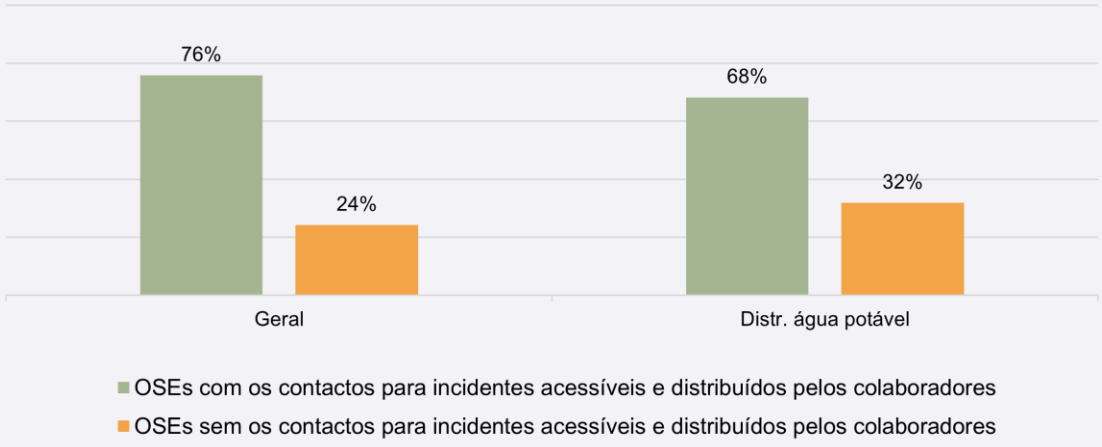
O setor que mais indica a falta de orçamento como um impedimento para que se possua equipa de resposta a incidentes é o setor do fornecimento e distribuição de água potável, onde este motivo é indicado por 50% dos operadores sem equipa, embora este motivo continue a figurar atrás da falta de recursos humanos. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores sem equipa de resposta a incidentes. Novamente, é no setor do fornecimento e distribuição de água potável que há uma maior percentagem de operadores a indicar este motivo, ultrapassando os 40%. A falta de tempo para definir a equipa surge com menos expressividade, sendo indicada por 20% dos operadores sem equipa. Os operadores que não consideram necessária uma equipa de resposta a incidentes necessária são, no cômputo geral, menos de 10%. Os operadores que selecionaram a opção “outros” (14%) indicaram motivos tais como estar a ser planeada a criação da equipa, a equipa estar a receber formação, ou mesmo o descuido para com a área de cibersegurança.

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



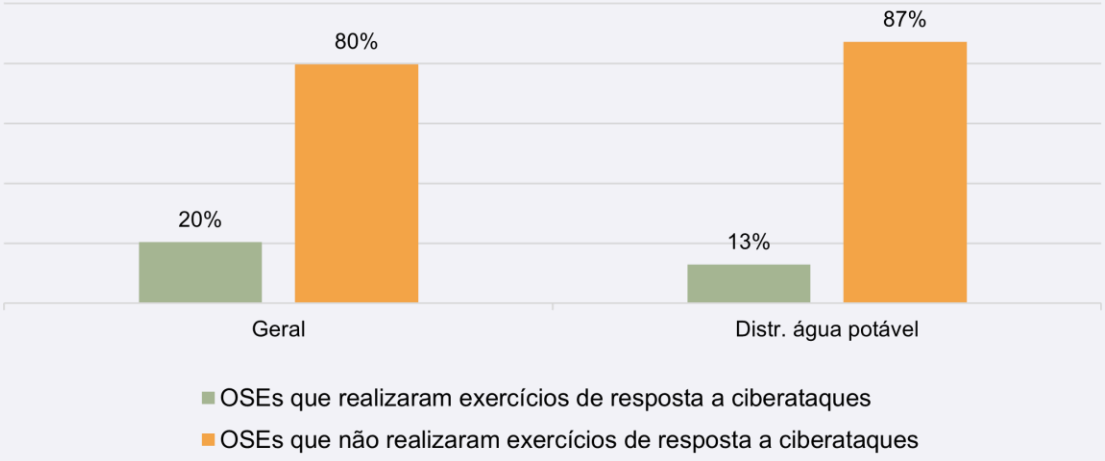
No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. O setor onde menores percentagens de operadores disponibilizam estes canais é o do fornecimento e distribuição de água potável, mas onde, ainda assim, 70% das entidades disponibilizam canais rápidos aos colaboradores.

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



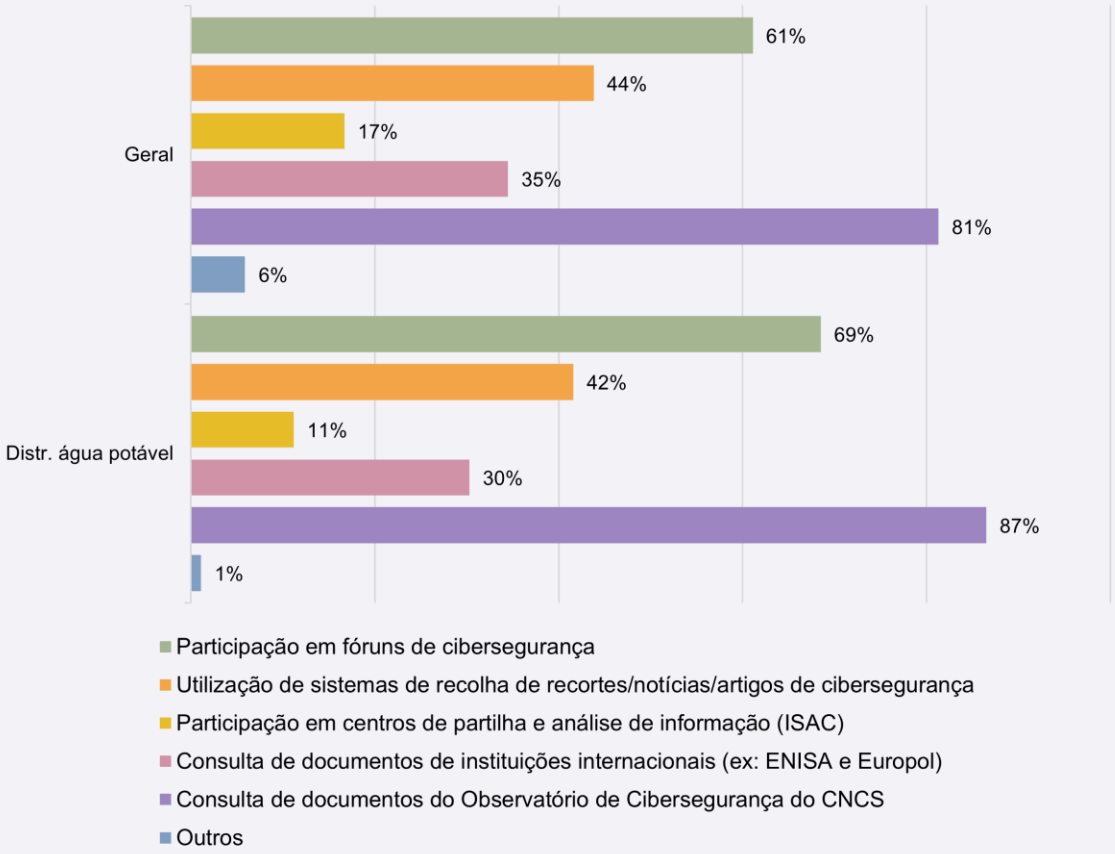
Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. No setor do fornecimento e distribuição de água potável, 68% dos operadores têm estes contactos distribuídos e acessíveis por todos os colaboradores.

Gráfico 107 - Realização de exercícios de resposta a ciberataques



De acordo com as respostas obtidas, apenas 20% dos operadores inquiridos realizam exercícios de resposta a ciberataques. No entanto, há ainda três setores que se destacam por a maioria dos operadores realizar estes exercícios. No setor do fornecimento e distribuição de água potável, a percentagem de operadores que realizam estes exercícios é de 13%.

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[51].

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.

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

A baixa participação registada nos ISACs merece alguma reflexão. Estes centros de análise e partilha de informação "consistem em parcerias para troca de informação e experiência, assentes no pressuposto de que a partilha consistente de informação e análise de incidentes, ameaças, tendências e boas práticas favorece a resiliência digital individual e coletiva"[52]. O próprio CNCS dinamiza seis ISACs, nomeadamente nos seguintes setores: energia, águas, portos marítimos; *media*; retalho e distribuição; e saúde. O CNCS dinamiza também um ISAC regional na Região Autónoma dos Açores. Há ainda um outro ISAC do setor financeiro, do qual o CNCS é membro, mas não promotor[53].

Existem também diversos ISACs de nível europeu - no setor da energia, no setor dos transportes, havendo ISACs específicos para os subsetores do transporte aéreo, ferroviário e marítimo, no setor financeiro, no setor da saúde, no setor do fornecimento e distribuição de água potável, e no setor das infraestruturas digitais[54]. A par destes, existem ainda outros ISACs europeus que não são específicos dos setores em análise, mas que se dedicam à recolha e análise de informações no âmbito dos sistemas de controlo industrial (ICS) e dos sistemas de supervisão e aquisição de dados (SCADA), e até mesmo no âmbito das cidades e órgãos de administração pública nelas presentes. Estes ISACs realizam um extenso trabalho de recolha e análise de informação no domínio da cibersegurança, reunindo os contributos de diversas entidades, produzindo, entre vários documentos, guias úteis a diversos níveis, como o da gestão do risco, do tratamento e resposta a incidentes, da gestão de informações sobre ameaças (*threat intelligence management*)[55]. Estes ISACs acabam também por fazer uma importante articulação entre os vários elementos dos diversos setores e a Comissão Europeia, sobretudo quando esta procura obter a análise e os contributos daqueles a quem nova legislação europeia será aplicável[56].

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

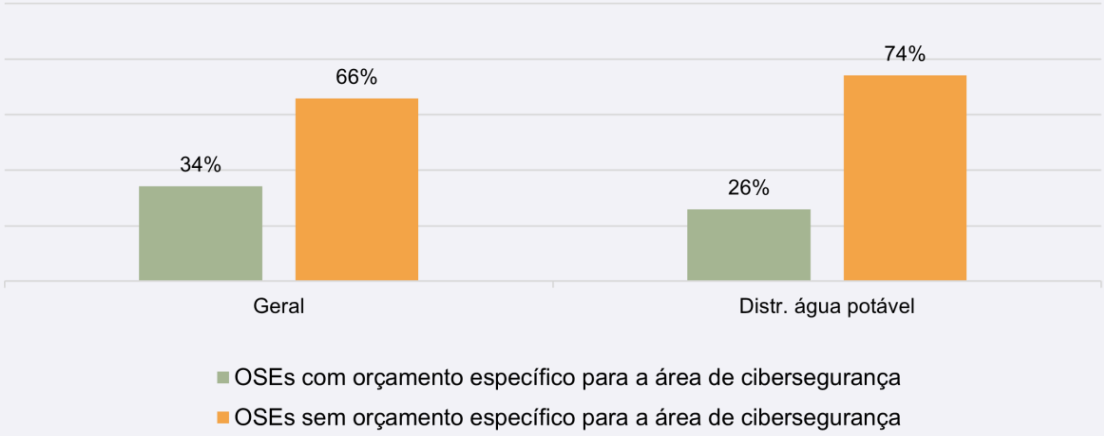
[53] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.

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

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

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

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. No setor do fornecimento e distribuição de água potável, a percentagem de OSE com orçamento fixa-se nos 26%.

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]. Este orçamento surgiu apenas em 2023, no âmbito do Programa Europa Digital, com um orçamento global de 1,3 mil milhões de euros, dos quais 375 milhões são dedicados à cibersegurança no biénio 2023-2024[59]. No âmbito da investigação e inovação, surge também o programa Horizonte Europa, com um orçamento global de 95,5 mil milhões de euros a ser executado entre 2021 e 2027, alocando 1,9 mil milhões de euros neste período à área da cibersegurança[60].

[57] ENISA, NIS Investments, 2021, 7-8.
[58] Comissão Europeia e Banco Europeu de Investimento, "European Cybersecurity Investment Platform", 2022, 29.
[59] Comissão Europeia, "€1.3 billion from the Digital Europe Programme for Europe's digital transition and cybersecurity", https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity.
[60] Conselho Europeu, "Horizonte Europa", https://www.consilium.europa.eu/pt/policies/horizon-europe/.

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

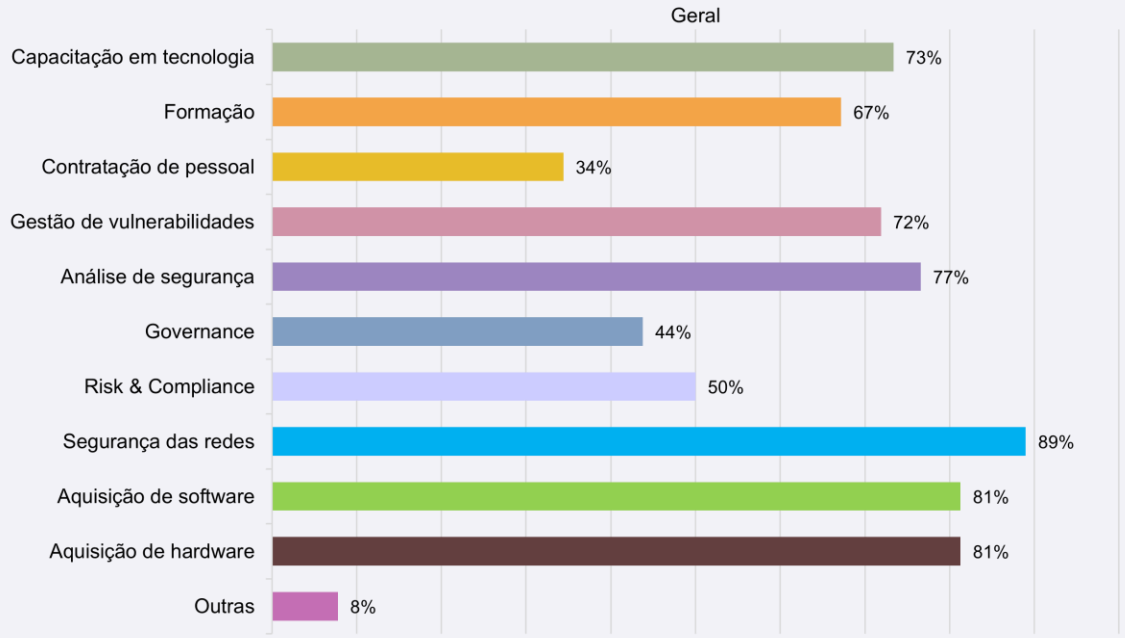
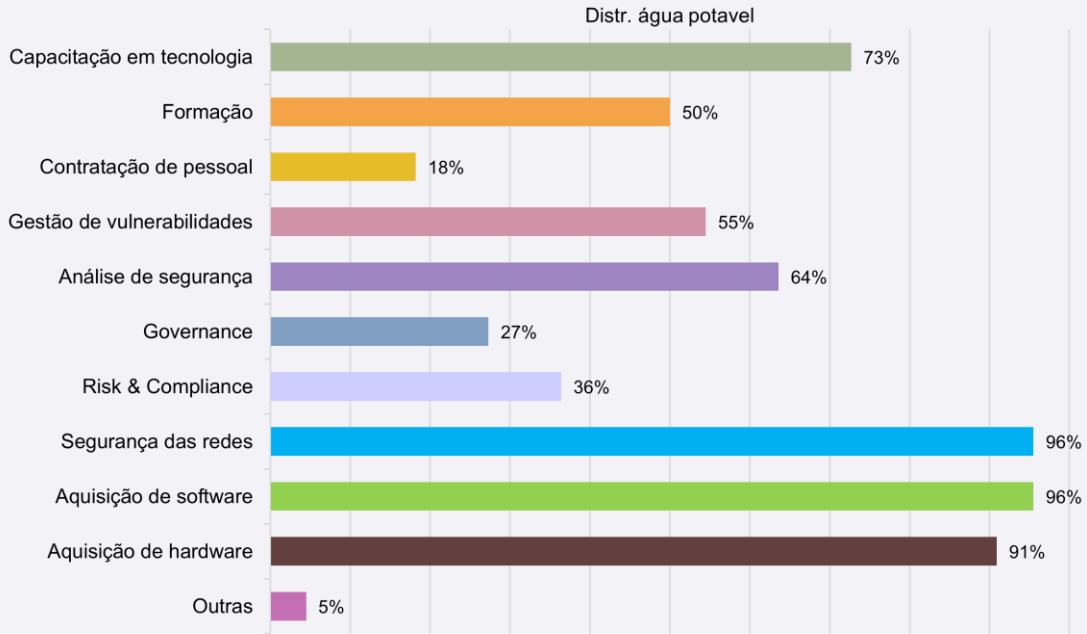


Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança

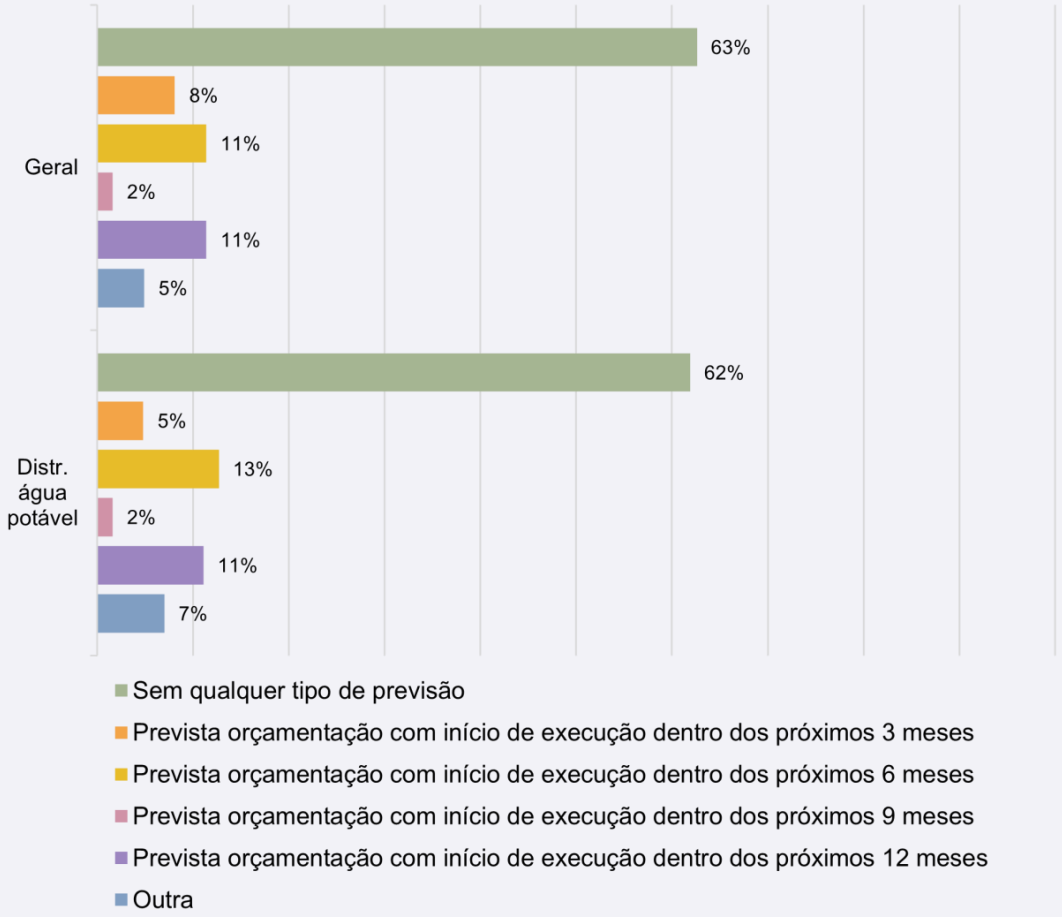


Entre os operadores que possuem orçamento específico para a cibersegurança, as áreas onde estes são mais comumente aplicados são a capacitação em tecnologia (73%), a formação dos colaboradores (67%), a gestão de vulnerabilidades (72%), análises de segurança (77%), *Risk & Compliance* (50%), segurança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

Nas “outras” áreas, surgem sobretudo a contratação de serviços externos para a área de cibersegurança, processos de implementação de normas (*standards*) como a NIST e a aquisição de serviços *cloud*.

A ENISA realizou um inquérito a 251 organizações 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

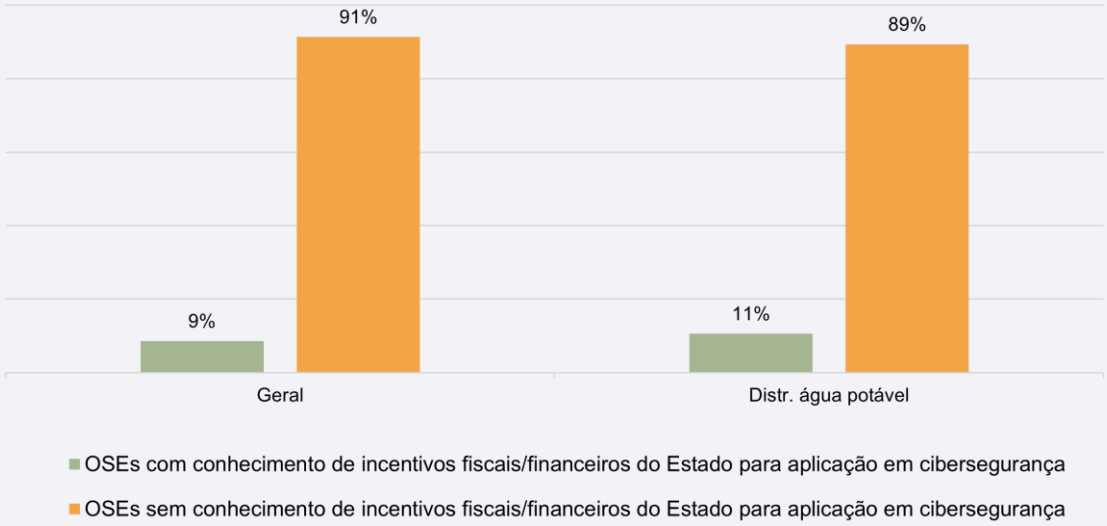


Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024. 63% destes não têm qualquer previsão de vir a ter tal orçamento. No setor do fornecimento e distribuição de água potável predomina a inexistência de qualquer previsão, correspondendo a 62% dos OSE.

[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

Quanto às "outras" respostas, estas corresponderam globalmente a situações em que os orçamentos atribuídos à cibersegurança se incluem ou decalcam dos orçamentos dedicados à área de informática.

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

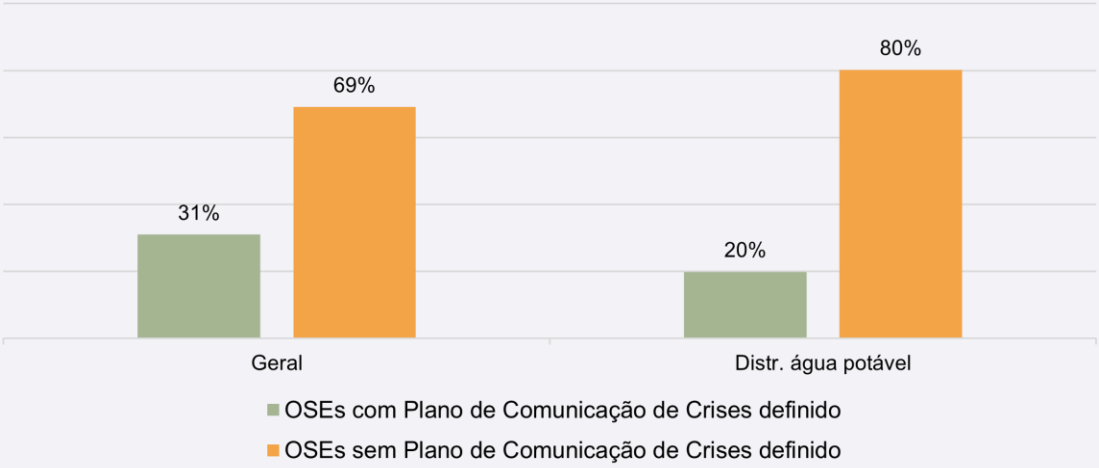


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No entanto, havia ainda alguns operadores em diversos setores, incluindo o setor do fornecimento e distribuição de água potável, com conhecimento sobre tais incentivos. As percentagens de operadores com esse conhecimento nos vários setores são, contudo, reduzidas, variando entre os 4% e os 12%.

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 do fornecimento e distribuição de água potável a percentagem de operadores com plano de comunicação de crises é de cerca de 20%.

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises

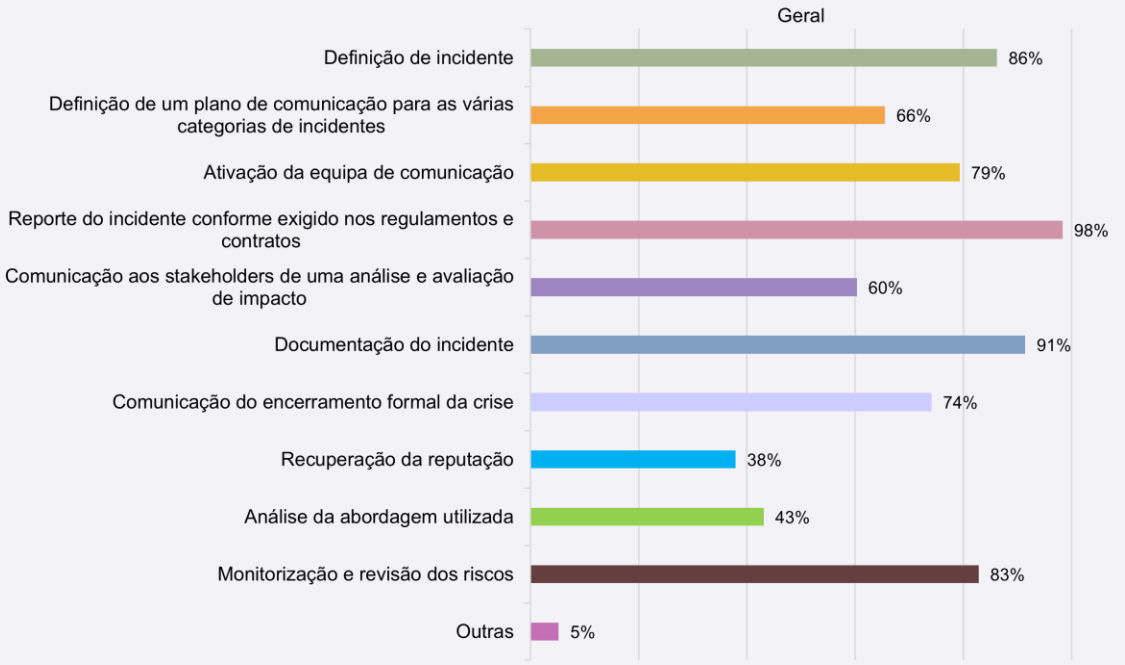
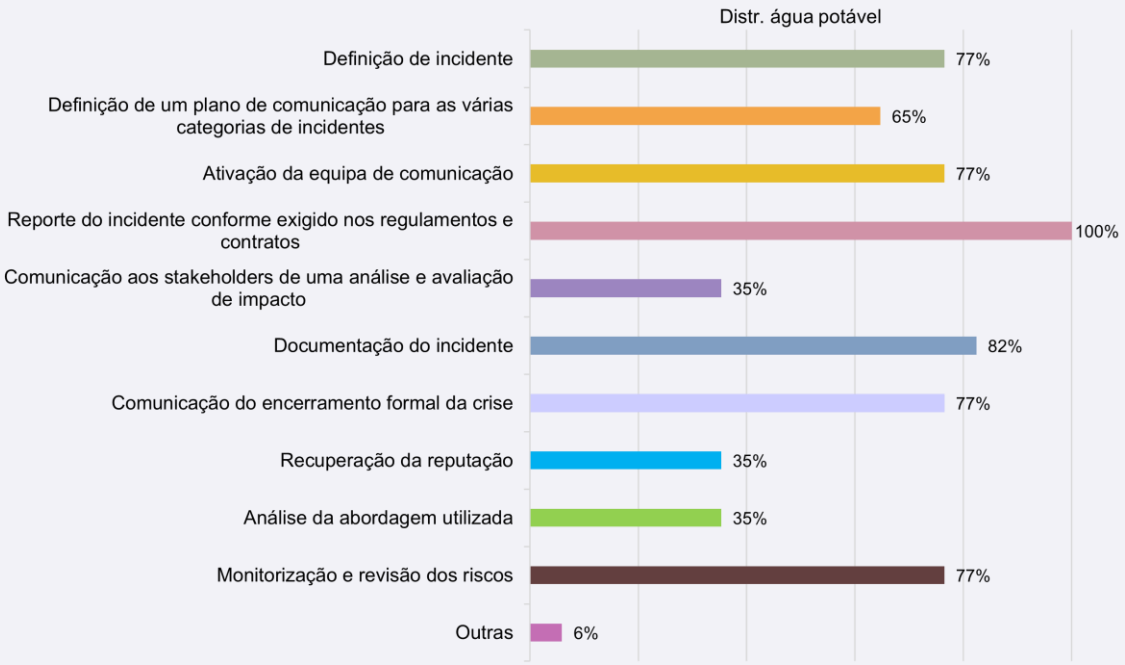


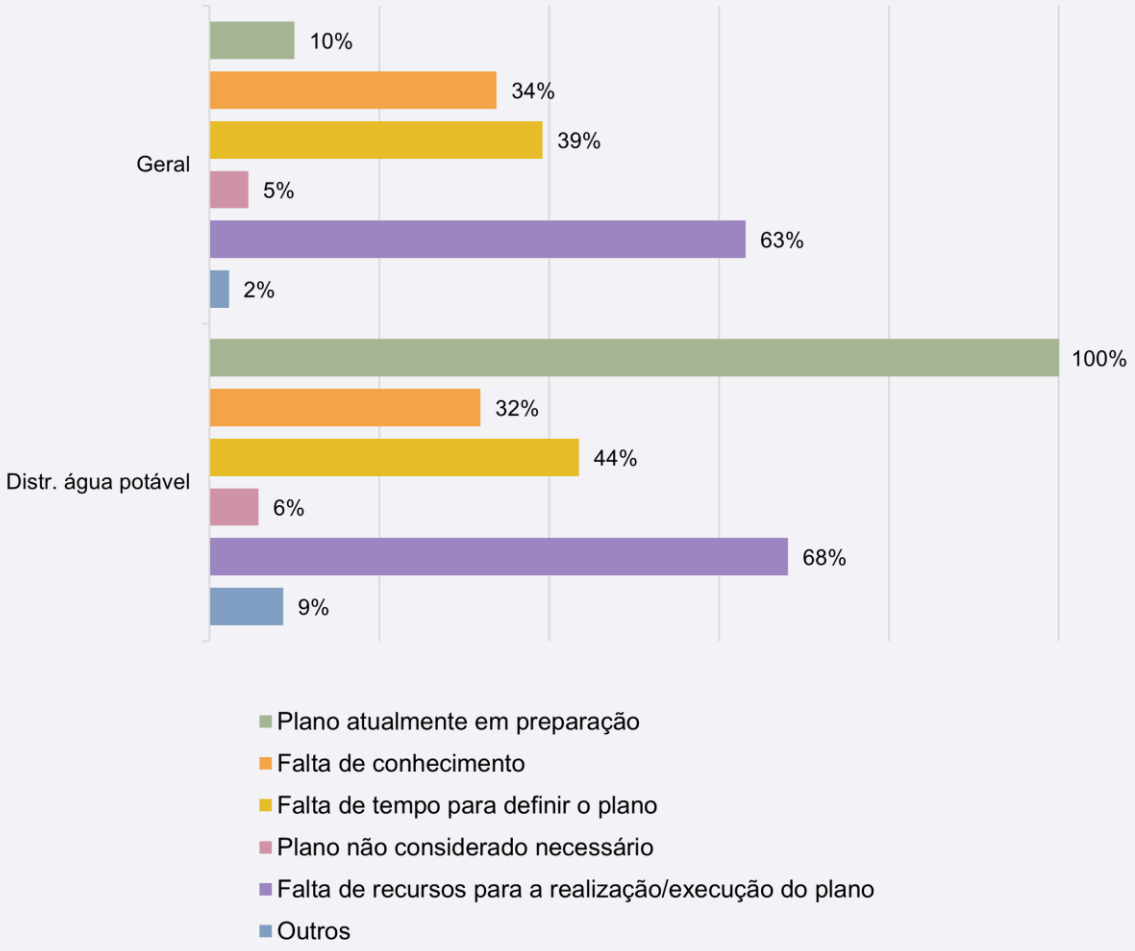
Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises



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

As sete secções mais presentes são a definição de incidente, a definição de um plano de comunicação para várias categorias de incidentes, a ativação da equipa de comunicação, a notificação do incidente conforme exigido nos regulamentos e contratos, a comunicação aos grupos de interesse de uma análise e avaliação do impacto do incidente, a documentação do incidente e a análise da abordagem utilizada.
Por sua vez, as três secções que menos vezes estão incluídas nos planos de comunicação são as relacionadas com a comunicação do encerramento formal da crise, com a recuperação da reputação, e com a monitorização e revisão dos riscos.

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



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

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

Análise Setorial

1. Fornecimento e distribuição de água potável

1.1. Contextualização setorial

O setor de águas e resíduos contribui significativamente para o desenvolvimento económico e social do país, tanto pela capacidade de gerar atividade económica e de criar emprego e riqueza, como pela crescente melhoria que tem conferido às condições de vida da população, gerando externalidades económicas positivas noutros setores. Os serviços deste setor são reconhecidos como serviços públicos essenciais pela legislação nacional, designadamente pela Lei dos Serviços Públicos Essenciais (Lei n.º 23/96, de 26 de julho, na redação atual)[64].

O acesso à água potável e ao saneamento básico foi, aliás, declarado um direito humano essencial pela Assembleia Geral da ONU em 2010. Tal significa que todos devem ter acesso adequado e seguro à água potável e ao saneamento, o que pode ser feito através de sistemas públicos tradicionais (redes de abastecimento ou de saneamento), sistemas públicos simplificados (por exemplo, fossas séticas coletivas) ou instalações individuais (por exemplo, fossas séticas individuais). Os serviços e as instalações devem estar fisicamente acessíveis, ter uma capacidade adequada e qualidade aceitável. É necessário que o acesso seja disponibilizado a todos de igual forma, colocar os cidadãos no processo de decisão e ocorrer uma monitorização e suporte. Devido ao elevado número de entidades com papel de gerir, a aplicação de um modelo único torna-se muito difícil. Nestes serviços existem monopólios naturais, pois, devido a razões tecnológicas, apenas uma entidade fornece os serviços em cada área geográfica[65].

A modernização deste setor foi, no entanto, tardia. Há cerca de 30 anos, em plena década de 1990, apenas 50% da água para consumo humano era controlada e de boa qualidade e apenas 30% da população portuguesa era servida com sistemas de tratamento de águas residuais. Também a deposição dos resíduos era feita, em larga medida, de forma não adequada, em lixeiras não controladas[66].

---

[64] ERSAR, "Relatório Anual dos Serviços de Águas e Resíduos em Portugal: Volume 1 – Caracterização do setor de águas e resíduos", 2022, 51, https://www.ersar.pt/_layouts/mpp/file-download.aspx?fileId=2169122.

[65] ERSAR, "Relatório Anual - Volume 1" (2022), 51.

[66] Águas de Portugal, "Águas de Portugal - Duas décadas que perspetivam o futuro", publicado a 6 de outubro de 2016, vídeo, Youtube, https://www.youtube.com/watch?v=2IPH9iW5wDg.

Em 1991, imperava no Grande Porto (e noutros pontos do país) uma situação de interrupção frequente e até mesmo de rutura do abastecimento de água às populações, já classificada de "pré-calamidade pública". Na origem desta, estava uma insuficiente capacidade de captação e produção de água para responder às necessidades da população e das atividades produtivas. Também no Algarve havia dificuldades semelhantes, sendo cada vez mais difícil satisfazer as necessidades de água da população residente e dos turistas, em particular durante a época balnear.

Para responder a estes e a outros problemas existentes no fornecimento e distribuição de água, o Estado iniciou, antes da reforma legislativa de 1993 que passou a permitir entrada de capitais privados neste setor, um conjunto de experiências piloto através de protocolos estabelecidos entre a Empresa Portuguesa das Águas Livres (EPAL) e grupos de municípios, tendo identificado como prioritária a intervenção nos municípios mais densamente povoados, localizados na faixa litoral, em especial o Algarve e o Grande Porto.

O racional por trás destas experiências assentava na adoção de soluções integradas, supramunicipais, que tivessem em conta a realidade física das bacias hidrográficas e que promovessem economias de escala substanciais e a fiabilidade dos serviços.

As parcerias então encetadas viriam a ser, em 1993, em boa parte convertidas nos primeiros sistemas multimunicipais de captação, tratamento e abastecimento de água para consumo dos municípios[67].

Encontrada uma parte da solução dos problemas do abastecimento de água em Portugal, veio a constituição da Águas de Portugal, nesse mesmo ano, dar resposta à inexistência de soluções empresariais, para além do caso da EPAL, que assegurassem a conciliação da realização dos avultados investimentos necessários com a boa utilização dos subsídios disponíveis nos fundos comunitários.

As primeiras empresas concessionárias dos sistemas multimunicipais de captação, tratamento e abastecimento de água foram criadas em 1995, tendo como acionistas a Águas de Portugal, com 51% do capital social, e os municípios servidos pelo respetivo sistema, com 49%.

Deu-se então início a um plano de infraestruturação sem precedentes no setor, complementado com a incorporação de infraestruturas municipais existentes, algumas das quais sofrendo obras de remodelação ou reconversão para dar respostas aos requisitos dos novos sistemas integrados.

Os investimentos realizados até 1999 (primeiro período de aplicação do Fundo de Coesão) ascenderam, na vertente do abastecimento de água, a 383 milhões de euros, dos quais 325 milhões de cofinanciamento, beneficiando cerca de 64 municípios e abrangendo cerca de 6,4 milhões de habitantes.

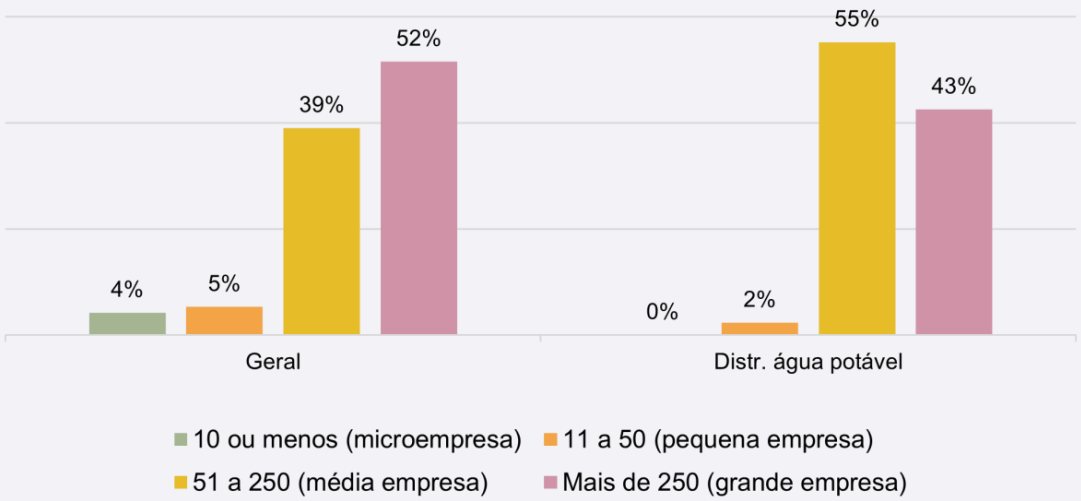
Estas soluções geraram economias de escala e permitiram uma utilização mais eficiente dos recursos, permitindo prosseguir os objetivos de melhorar a qualidade da água e os níveis de atendimento das populações, colocando Portugal entre os melhores desempenhos ambientais da Europa comunitária.

Desde então, o panorama nacional mudou. Atualmente, segundo dados de 2022, o setor abastece de água 9,8 milhões de habitantes e abrange 97% dos alojamentos do país. Por sua vez, o saneamento serve 8,7 milhões de habitantes, chegando a 86% dos alojamentos em Portugal. A qualidade da água fornecida melhorou também, com avaliações de qualidade na ordem dos 99,7%, a par dos Estados-membros da UE que obtinham melhores resultados nessas avaliações.

[67] Águas de Portugal, *Livro Águas de Portugal* (Lisboa: By the Book, 2016), 32, https://www.adp.pt/pt/media/publicacoes/downloads/pub_pdf17_pt.pdf.

De acordo com o questionário realizado, o tecido empresarial dos operadores de serviços essenciais (OSE) do setor da distribuição de água potável é sobretudo composto por médias empresas (55%), com entre 50 a 250 colaboradores, seguido por médias empresas (43%) e a restante minoria (2%) são pequenas empresas (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



O regulador do setor considera que a maturidade deste em cibersegurança é muito baixa (**Gráfico 9**), uma perceção que pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (cerca de 57% disponibiliza formação) (**Gráfico 38**) e pela falta de medidas cibersegurança adotadas.

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

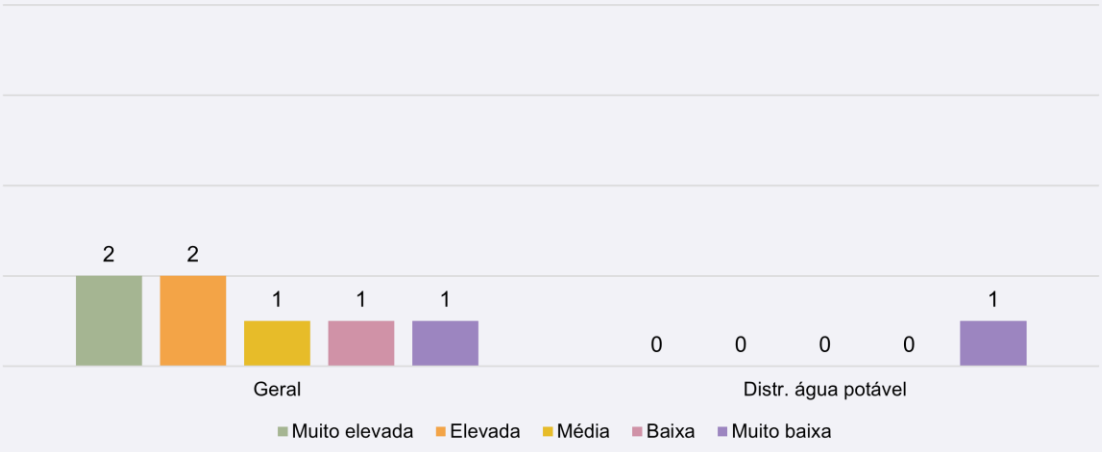
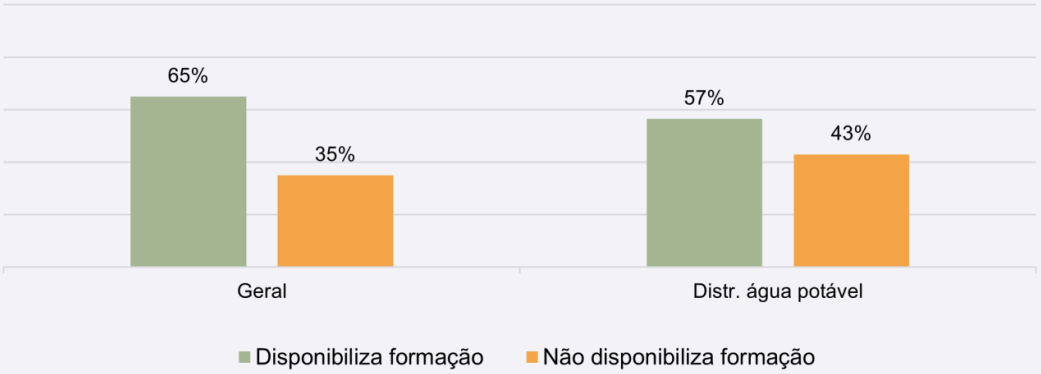


Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



As medidas menos adotadas foram: Segurança de rede em *cloud* com 12%, Equipa especialista em cibersegurança com 14%, a implementação de controlos biométricos para identificação e autenticação com 15%, Análise de risco periódicas com 25% e Sistemas de Prevenção e Deteção de Intrusão (IPDS) com 27% (**Gráfico 66.6**). A ressalvar também as políticas de cibersegurança e relacionadas implementadas, onde tanto a política de comunicação como a de continuidade de negócio estão abaixo dos 40% e pelo facto que apenas 25% dos operadores dedicarem orçamentos específicos à área de cibersegurança. É também um setor que tem, por enquanto, beneficiado de uma baixa incidência de ciberataques, onde 76% dos inquiridos nunca sofreu um incidente.

Gráfico 66.6 - Medidas de proteção contra ameaças de cibersegurança

1.1.1. Impacto socioeconómico

Tal como já foi referido, o setor do fornecimento e distribuição de água potável contribui significativamente para o desenvolvimento económico e social do país, gerando atividade económica, emprego e riqueza, bem como externalidades económicas positivas noutros setores de atividade.

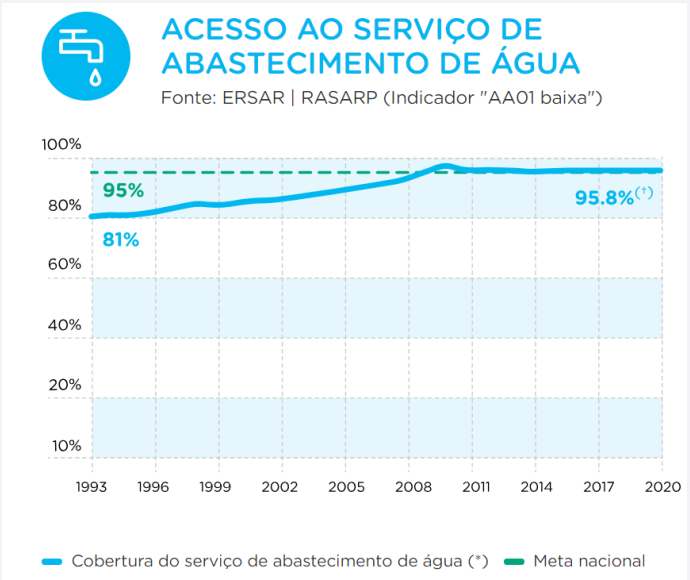
De acordo com os dados mais recentes disponíveis (respeitantes a 2021) o volume de negócios anual do setor é superior a 2,5 mil milhões de euros, com um nível de rendimentos e ganhos totais reportado de 2,99 mil milhões de euros e com resultados líquidos agregados na ordem dos 106,7 milhões de euros[68].

Ao nível do emprego, o setor empregava, no final de 2021, 9,8 mil trabalhadores (mais 1,2% do que em 2020), registando-se alguma estabilidade ao longo dos anos no número total de empregos. Ressalva-se, no entanto, que o número de trabalhadores em *outsourcing* tem vindo a aumentar na última década[69].

Já no que diz respeito ao investimento realizado no setor, este foi, em 2021, na ordem dos 16,5 mil milhões de euros[70].

O acesso à água potável foi sempre uma questão da maior importância. Indispensável à sobrevivência humana, tornou-se também indispensável a diversas atividades do quotidiano humano. As reformas iniciadas em 1993 para resolver os problemas de acesso à água potável que até então subsistiam no país são prova disso, uma vez que trouxeram significativas melhorias à vida da população portuguesa. Os gráficos seguintes traçam essa evolução e melhoria:

Figura 1 - Acesso ao Serviço de Abastecimento de Água

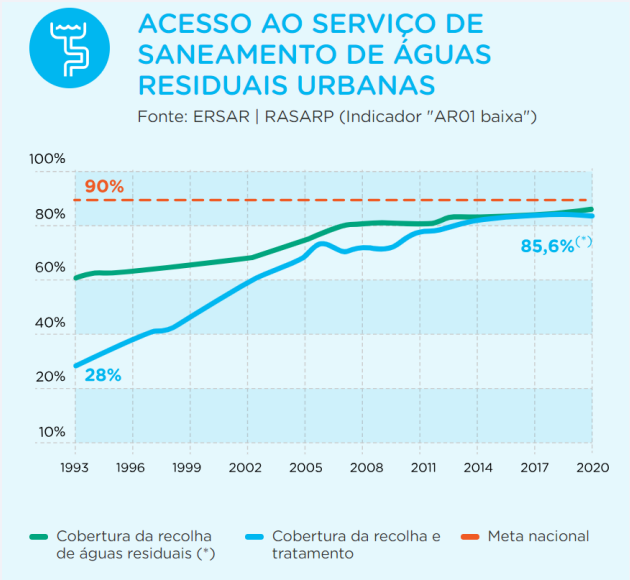


(Fonte: Waterhub - Plataforma Portuguesa da Água, "Evolução dos Serviços de Água em Portugal (1993-2017)", https://waterhub.pt/pt/portugal)

[68] ERSAR, "Relatório Anual - Volume 1" (2022), Volume 1, 380-386.
[69] ERSAR, "Relatório Anual - Volume 1" (2022), 370.
[70] ERSAR, "Relatório Anual - Volume 1" (2022), 434.

Como se demonstra pela figura acima, as reformas iniciadas em 1993 permitiram aumentar a percentagem de população com acesso ao serviço de abastecimento de água de 81% em 1993 até à meta nacional de 95% em 2010, tendo esta percentagem estabilizado desde então, fixando-se em 95,8% em 2017.

Figura 2 - Acesso ao Serviço de Saneamento de Águas Residuais Urbanas

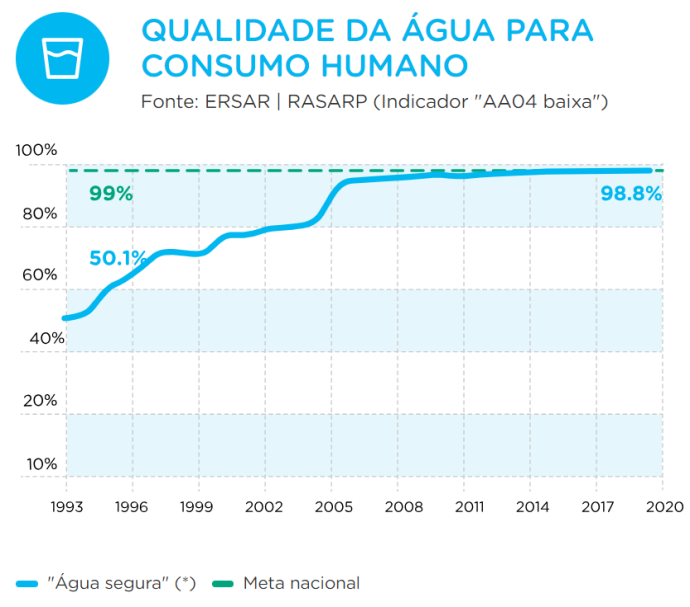


(Fonte: Waterhub - Plataforma Portuguesa da Água, "Evolução dos Serviços de Água em Portugal (1993-2017)", https://waterhub.pt/pt/portugal)

Outra grande melhoria registada com as reformas iniciadas na década de 90 foi o aumento do acesso aos serviços de saneamento de águas residuais urbanas. Como se verifica pela Figura 12, em 1993 apenas 28% da população tinha acesso a estes serviços. Essa percentagem foi aumentando de ano para ano a bom ritmo, abrandando depois a partir de 2006, mas mantendo o crescimento. Em 2017, já 85,6% da população tinha acesso a estes serviços, mas ainda se estava aquém da meta de 90%. No entanto, dados mais recentes, como os do Relatório Anual dos Serviços de Água e Resíduos em Portugal (2022, Volume 1), revelam que a cobertura de recolha e tratamento se estende, pelo menos desde 2021, a 94% da população[71], superando a meta estabelecida.

[71] ERSAR, "Relatório Anual - Volume 1" (2022), 244.

Figura 3 - Qualidade da Água para Consumo Humano



(Fonte: Waterhub - Plataforma Portuguesa da Água, “Evolução dos Serviços de Água em Portugal (1993-2017)”, https://waterhub.pt/pt/portugal)

Finalmente, a qualidade da água para consumo humano melhorou também drasticamente a partir de 1993. Ao passo que na década de 90 apenas 50,1% da água fornecida era considerada segura, em 2017 este valor atingia já os 98,8%. Dados mais recentes (2022) indicam que 99,59% da água fornecida é segura e de qualidade[72].

[72] ERSAR, “Relatório Anual - Volume 1” (2022), 199.

1.1.2. Especificidades tecnológicas

As principais especificidades tecnológicas do abastecimento e fornecimento de água potável prendem-se com as tecnologias utilizadas na captação, tratamento e distribuição de água, bem como tecnologias de monitorização da qualidade, de medição de caudal e até mesmo dispositivos de deteção de fugas desta. Estas tecnologias inserem-se no campo da tecnologia operacional (TO).

De acordo com o National Institute of Standards and Technology dos EUA (NIST), "a tecnologia operacional compreende um vasto conjunto de sistemas e dispositivos programáveis que interagem com o ambiente físico (ou gerem dispositivos que interagem com o ambiente físico). Estes sistemas e dispositivos detetam ou causam mudanças diretas através da monitorização e/ou controlo de dispositivos, processos e eventos. Exemplos [de tecnologia operacional] incluem sistemas de controlo industrial [*Industrial Control Systems* - ICS], sistemas de automação predial [*Building Automation Systems* - BAS][73], sistemas de controlo de acesso físico, sistemas de monitorização do ambiente físico e sistemas de medição do ambiente físico"[74]. A estes, acrescem ainda os sistemas de supervisão e aquisição de dados (*Supervisory Control and Data Acquisition* - SCADA), que são utilizados para recolher dados e controlar dispositivos dispersos, cuja centralização de dados é essencial para ter informação adequada sobre as operações realizadas. Estes sistemas são desenhados para recolher informação "no terreno", transferindo-a para um centro de controlo, mostrando depois a informação de forma gráfica ou textual ao operador, permitindo a monitorização e o controlo centralizados em tempo real[75].

Estes sistemas de TO estiveram, durante largos anos, separados dos sistemas de TI (Tecnologia da Informação), conferindo aos sistemas TO a segurança de não poderem ser acedidos ou atacados remotamente. No entanto, a evolução tecnológica dos últimos 20 anos tem conduzido à convergência dos dois tipos de sistemas, com a tecnologia operacional e a tecnologia da informação a estarem cada vez mais integradas uma com a outra[76]. Um exemplo disso é o *software* NAVIA, utilizado por alguns OSE no setor do fornecimento e distribuição de água potável.

De acordo com os próprios fornecedores do *software*, o NAVIA é um *software* que permite a gestão integral da infraestrutura de abastecimento de água e de recolha de águas residuais, de processos e de territórios, sendo "um agregador de dados e de conhecimento, que se integra com sistemas de telegestão (SCADA), de Laboratório (LIMS - Laboratory Information Management System), geográficos e de cadastros (SIG), financeiros (ERP) e comerciais (CRM)"[77]. A partir do mesmo, é ainda possível monitorizar, avaliar e corrigir operações através deste sistema, consoante o nível de integração deste *software* com outros sistemas[78].

[73] Sistemas de automação predial ou *Building Automation Systems* (BAS) são sistemas que controlam os três principais sistemas de um edifício: eletricidade, climatização (aquecimento e ar condicionado), e água e tratamento de resíduos.

[74] Keith Stouffer et al., "NIST Special Publication NIST SP 800-82r3: Guide to Operational Technology (OT) Security", *National Institute of Standards and Technology*, setembro de 2023, 8, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf.

[75] Keith Stouffer et al., "NIST SP 800-82r3: Guide to Operational Technology (OT) Security", 12.

[76] Keith Stouffer et al., "NIST SP 800-82r3: Guide to Operational Technology (OT) Security", 8.

[77] "Questões frequentes", FAQs, NAVIA, https://www.naviasolutions.com/faqs/.

[78] "Business & Operations Intelligence", Porquê o NAVIA, NAVIA, https://www.naviasolutions.com/porque-o-navia/.

As Águas de Portugal desenvolveram também, internamente, uma ferramenta denominada Aquamod/Modelo Técnico. Esta ferramenta possibilita às entidades participadas e à própria administração central armazenar, analisar e calcular informação recolhida de todas as entidades para as atividades de abastecimento e de saneamento. Mais concretamente, o Aquamod é uma ferramenta de gestão que, através da recolha de dados, permite realizar análises preditivas da evolução dos caudais para longos períodos, cruza-os com outros dados relativos à região, tais como população residente e flutuante, cobertura, adesão, perdas, afluências indevidas e capitações, de modo a "estabelecer cenários de viabilidade técnico-financeira das operações e (...) definir projeções tarifárias capazes de, simultaneamente, garantir a progressiva recuperação de custos, necessária à sustentabilidade do sistema, e o ajustamento social dos preços"[79]. Adicionalmente, o facto de este sistema recolher dados de mais de 220 municípios, ou seja, cerca de 82% dos municípios portugueses, acaba por criar uma base de informação que oferece um quadro da realidade nacional e regional do país, cuja utilidade não se esgota nas operações das empresas do grupo Águas de Portugal, mas que constitui também um importante contributo para a definição de indicadores de base para políticas públicas nacionais e para análises comparativas com outros países[80].

Outro sistema utilizado pelas entidades participadas do grupo Águas de Portugal é o AQUASAFE. Este sistema tem uma vocação mais operacional do que os dois sistemas já referidos, e foi desenvolvido, como o nome indica, com o objetivo de manter a água "segura". Objetivamente, o AQUASAFE recolhe e integra "informação de monitorização (...) em tempo real (sensores, telegestão, telemetria, etc.) com ferramentas de previsão e diagnóstico (modelos de previsão meteorológica, modelos técnicos dos sistemas, etc.), tornando possível antecipar problemas ou planear operações de forma mais eficiente". O AQUASAFE permite assim manter a qualidade/salubridade da água, evitar problemas decorrentes de cheias, de excesso de fluxo para as estações de tratamento, e até mesmo planear intervenções de manutenção dos sistemas de abastecimento e tratamento de resíduos[81].

A par destes, surge também o sistema WONE (*Water Optimization for Network Efficiency*), utilizado pela EPAL. Este é também um sistema de cariz mais operacional, destinado sobretudo à monitorização dos caudais e pressão e à deteção de fugas de água. Através de diversos elementos, tais como "o controlo de pressão e caudal, sistema de telemetria passivo, alarmes de pressão ativos, registos de 15 em 15 minutos e comunicações diárias", o WONE vai realizando a devida monitorização desses parâmetros, servindo-se dos dados recolhidos para detetar as referidas fugas de água. Tal como o AQUASAFE, este sistema permite também planear intervenções no terreno, bem como quantificar os volumes de água a recuperar. A utilização deste sistema permitiu, entre 2005 e 2015, reduzir, na rede de distribuição de Lisboa, o nível de água não faturada de 23% para 8%[82].

[79] Águas de Portugal, *Livro Águas de Portugal*, 55-56.

[80] Águas de Portugal, *Livro Águas de Portugal*, 56.

[81] Águas de Portugal, *Livro Águas de Portugal*, 105.

[82] "WONE: Water Optimization Network Efficiency: A Global Solution to a Global Water Challenge", WONE®, EPAL, https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/wone.

Existe ainda o Aquamatrix, o *software* de gestão comercial criado e utilizado pela EPAL. Este sistema é também comercializado para outras entidades fora do grupo Águas de Portugal há mais de uma década, em Portugal e Moçambique, e oferece diversas funcionalidades. Este *software* permite fazer a gestão da atividade e do desempenho através de indicadores variados, integrar interfaces como os de ERP, Sistemas de Informação Geográfica (GIS), os que apresentam as informações de telemetria, e outros, fazer o arquivo eletrónico de documentos, gerir processos relativos a projetos de redes prediais e urbanizações, fazer a gestão do ciclo de vida do parque de contadores e ainda realizar funções relacionadas com a leitura, faturação e cobrança dos serviços de fornecimento de água prestados. Segundo a EPAL, este *software* está atualmente presente em aproximadamente 30% do território, abrangendo cerca de 1,6 milhões de consumidores[83].

Todos estes sistemas, para além de contribuírem para a segurança da água fornecida e para a boa gestão das empresas distribuidoras, são agentes de convergência entre os sistemas de TI e os sistemas de TO. Esta integração acarreta, no entanto, alguns riscos. Como se disse no início deste subcapítulo, os ambientes TI e os ambientes TO estiveram, durante muitos anos, separados, e têm vindo a convergir entre si ao longo dos últimos cerca de 20 anos. Essa convergência e integração entre os dois ambientes oferecem aos agentes de ameaça uma nova superfície de ataque, possibilitando o acesso ao ambiente TO depois de uma intrusão bem-sucedida no ambiente TI. Esta lógica de ataque poderá parecer estranha, uma vez que a tecnologia operacional, ou os equipamentos e dispositivos que a compõem, têm normalmente longos ciclos de vida, em muitos casos ultrapassando os 20 anos de longevidade, conduzindo à existência de sistemas *legacy*, ou seja, *hardware* ou *software* que já não recebe atualizações ou *patches* de segurança dos seus fabricantes, deixando estes sistemas desprotegidos contra novas vulnerabilidades[84]. No entanto, a maioria dos ataques concretizados nos ambientes TO começaram com acessos ganhos através do ambiente TI[85], em casos onde os dois já estão integrados e interligados. Assim, a convergência entre os ambientes TI e os ambientes TO (por norma, menos seguros devido à falta de atualizações de segurança ou de capacidades de cifragem), acaba por se traduzir, na maioria dos casos, numa maior superfície de ataque para os agentes de ameaça, superfície essa onde os agentes de ameaça poderão interferir com a qualidade da água e respetivas redes de distribuição. Explorar-se-ão estas questões em maior detalhe no subcapítulo seguinte (

[83] "Boosting business inovation", Aquamatrix, EPAL, https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/aquamatrix.

[84] Keith Stouffer et al., "NIST SP 800-82r3: Guide to Operational Technology (OT) Security", 37.

[85] Amin Hassanzadeh et al., "A Review of Cybersecurity Incidents in the Water Sector", *Journal of Environmental Engineering 146* (25 de julho de 2020): 3, https://arxiv.org/pdf/2001.11144 .

1.2. Ameaças).

1.2. Ameaças

Tal como indicado no subcapítulo anterior, um ciberataque à infraestrutura de um fornecedor de água potável pode traduzir-se em manipulações mal-intencionadas na qualidade da água ou no próprio fornecimento da mesma, o que pode ter diversos impactos negativos, diretos e indiretos. Segundo o relatório "*Cybersecurity Risk & Responsibility in the Water Sector"*, produzido pela *American Water Work Association*, em 2019, os efeitos de ciberataques nas infraestruturas de abastecimento de água potável podem resultar em contaminações, mau funcionamento operacional e comprometer serviços de emergência como bombeiros ou serviços médicos[86]. O mesmo relatório menciona, para além destes impactos, os relacionados com o acesso indevido a dados sensíveis de clientes e colaboradores detidos pelas entidades de fornecimento e distribuição de água potável, acabando por tornar este um setor atrativo para a realização de ciberataques[87].

De acordo com um infográfico elaborado em outubro de 2021 pela Cybersecurity and Infrastructure Security Agency (*CISA*), dos Estados Unidos, as organizações de fornecimento e distribuição de água potável estão sujeitas a sofrer alguns ataques/ameaças. Entre os principais ataques estão os ataques de *Ransomware* e os de acesso indevido a dados. Estes ataques estão relacionados com os sistemas de TI e, de acordo com o mesmo infográfico, estes ataques podem ser evitados/reduzidos adotando boas práticas de cibersegurança dentro das redes de TI. Nos casos em que se verifica a convergência das redes de TI com as de TO, a não segmentação de rede pode ser uma ameaça, dado que as redes de TI, mais expostas, podem servir como meio para o acesso a redes de TO que foram integradas com a rede de TI. Uma forma de mitigar o risco associado a esta integração será segmentar adequadamente os sistemas de TI e TO e garantir que nenhum sistema de TO está ligado à Internet. Por último, são indicadas como principais ameaças aos sistemas de TO a falta de manutenção dos mesmos e a complexidade das redes. As medidas indicadas pela CISA passam pela aplicação dos *patches* de segurança nos sistemas e por mapeamentos de rede adequados[88].

Entre os possíveis impactos de ataques concretizados ao setor do fornecimento e distribuição de água potável destacam-se impactos como:

- Envenenamento;
- Falsos alarmes;
- Furto de água;
- Furto de recursos;
- Impacto financeiro;
- Manipulação de controlos;
- Manipulação de dados;
- Perda de dados;
- Poluição ambiental;
- Violação de dados[89].

[86] Judith H. Germano, "Cybersecurity Risk & Responsibility in the Water Sector", *American Water Work Association*, 2019, 6, https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf.

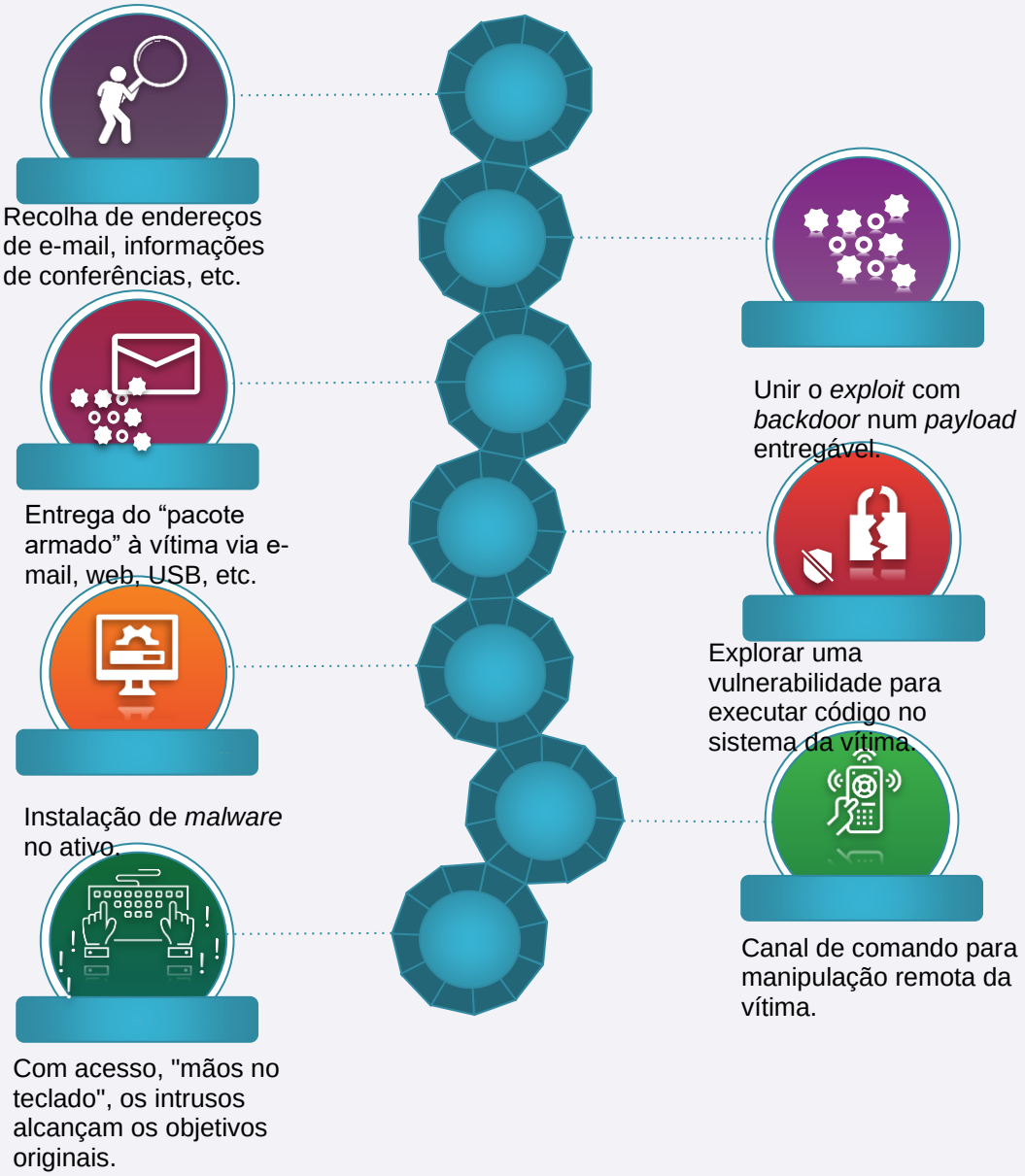
[87] Germano, "Cybersecurity Risk & Responsibility in the Water Sector", 6.

[88] "Cyber Risks and Resources for the Water and Wastewater Systems Sector", CISA, outubro de 2021, https://www.cisa.gov/sites/default/files/publications/infographic-manage-wastewater-national-critical-function-102021-508.pdf.

[89] Hassanzadeh et al., "A Review of Cybersecurity Incidents", 13.

Normalmente, um ciberataque tem um ciclo de vida que corresponde à *Cyber Kill Chain* (CKC) que inclui as etapas de Reconhecimento, Armamento (*weaponization*), entrega, exploração, instalação, comando e controlo (*C2*) e ação nos objetivos.

Figura 4 - Cyber Kill Chain (CKC)

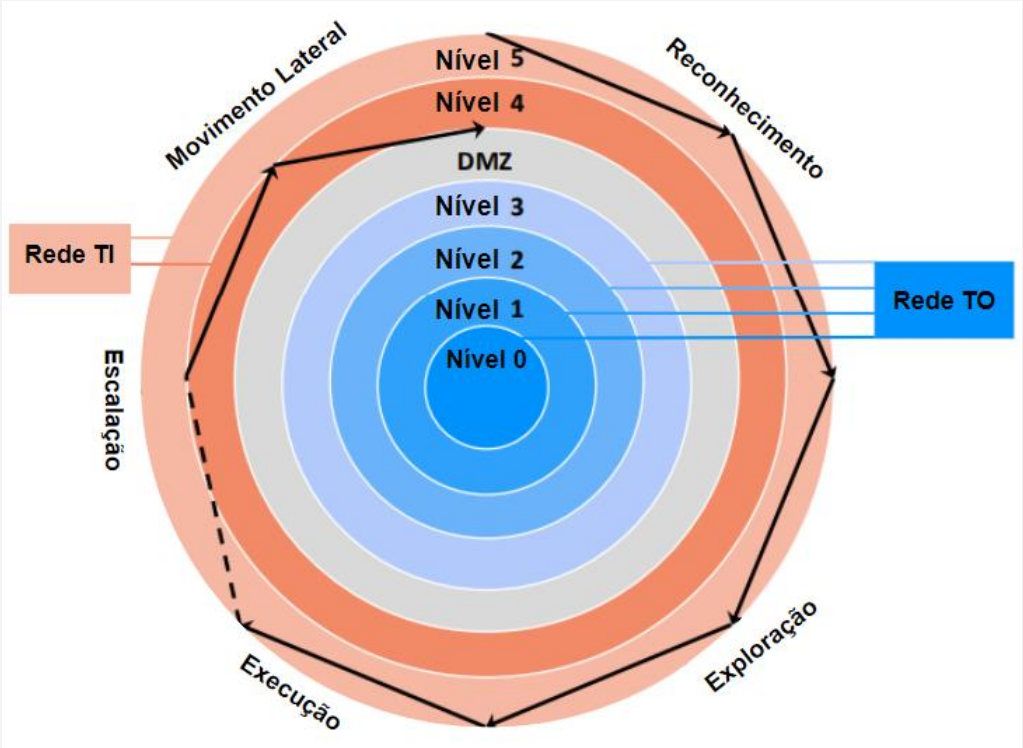


(Fonte: Cyber Kill Chain, *Lockheed Martin*, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)

Nos ambientes industriais, o caminho de ataque é ligeiramente diferente devido à arquitetura destes ambientes. O alvo é, geralmente, um ativo de TO, ao qual o agente de ameaça ganha acesso depois de ter conseguido o acesso através de um dispositivo de TI, sendo o agente de ameaça depois obrigado a mover-se lateralmente ao longo da infraestrutura, e tendo de repetir passos da CKC até chegar ao ativo de TO. Isto é, à medida que o agente de ameaça chega a novos pontos da infraestrutura, poderá ter de voltar a fazer novo reconhecimento, explorar outras vulnerabilidades, voltar a instalar *malware* e repetir a remoção de restrições e voltar a escalar privilégios para poder prosseguir dentro da rede de uma organização.

Na **Figura 5**, está representado um modelo genérico de ataque em espiral, no qual o nível 5 representa ativos mais expostos publicamente, como servidores *web* ou de *e-mail* e aos quais táticas mais comuns como o *phishing* podem dar acesso inicial. Depois de conseguir o acesso a ativos como estes, o agente de ameaça está dentro da rede da organização e é a partir daqui que se pode mover lateralmente de ativo em ativo, até chegar ao objetivo pretendido. É uma vez chegado aos ativos de TO que o agente de ameaça conseguirá manipular processos críticos na gestão da água[90]. Ressalva-se que este modelo é apenas um exemplo e que nem todos os ataques à TO partem necessariamente de ativos publicamente expostos, podendo começar de níveis inferiores, mais próximos do alvo pretendido, como nos casos em que a ameaça é interna à organização. Ver-se-ão exemplos desses na análise a alguns ataques ocorridos no setor.

Figura 5 - Modelo de ataque em espiral em redes onde convergem TI e TO



(Fonte: Amin Hassanzadeh et al, "A Review of Cybersecurity Incidents in the Water Sector", *Journal of Environmental Engineering 146* (25 July 2020), https://arxiv.org/pdf/2001.11144)

[90] Hassanzadeh et al., "A Review of Cybersecurity Incidents", 3-4.

Torna-se assim necessário analisar os ciberataques ocorridos no setor. O estudo "A Review of Cybersecurity Incidents in the Water Sector", publicado no *Journal of Environmental Engineering*, em 2020, faz uma análise de alguns dos principais ciberataques às redes de distribuição de água realizados até então, nomeadamente nos territórios da Austrália, dos Estados Unidos, do Reino Unido e da União Europeia. Os ataques em análise neste estudo são ataques que tanto visaram interferir com os ambientes TO das entidades distribuidoras de água potável, como com os seus ambientes TI. Abordam-se, de seguida, alguns dos mais relevantes, sobretudo aqueles nos quais foi possível interferir com os ambientes TO das organizações visadas, de modo a fazer-se uma ligação mais próxima com as especificidades tecnológicas deste setor.

O primeiro ataque analisado ocorreu na Austrália, no ano 2000. A entidade atacada - Maroochy Water Services -, processava cerca de 35 milhões de litros de água de esgoto, numa região com cerca de 120 mil habitantes. Entre 1997 e 2000, tinham sido instalados na entidade novos computadores, em todas as 142 estações elevatórias de águas de esgoto, que permitiam controlar remotamente e monitorizar essas estações através do sistema SCADA. No final do mês de janeiro de 2000, começaram a verificar-se falhas nesse mesmo sistema SCADA, tais como perdas de comunicação e de capacidade de controlo das estações, falsos alarmes e configurações alteradas. Estas falhas resultaram na descarga de cerca de um milhão de litros de águas residuais não tratadas no rio, nos parques e nas zonas residenciais. Em março do mesmo ano, a investigação realizada concluiu que a causa das falhas tinha sido interferência humana. Essa interferência vinha de um ex-funcionário da empresa que tinha fornecido os computadores que controlavam remotamente as estações. Esse ex-funcionário tinha-se demitido no mês anterior devido a desentendimentos dentro da sua empresa. Através de um computador do mesmo modelo daqueles que tinham sido instalados, um rádio, um computador portátil, um transformador e diversos cabos, o ex-supervisor foi capaz de causar todas as falhas referidas na tecnologia operacional da entidade visada. No final, as águas infetadas foram limpas, embora tenham sido necessários múltiplos recursos e vários dias para o fazer. O responsável acabou por ser condenado a dois anos de prisão e ao pagamento de pouco mais de 13 mil dólares à Câmara da cidade. Este caso em concreto é um bom exemplo da importância de desativar acessos imediatamente após a saída de funcionários ou colaboradores, assim como da importância de garantir uma boa gestão de ativos e a devolução dos mesmos quando se encerra uma relação laboral[91].

O segundo incidente analisado refere-se a uma intrusão numa planta de filtragem de água em Harrisburg, Pensilvânia, nos Estados Unidos, em 2006. Segundo a investigação, os agentes de ameaça terão conseguido introduzir um vírus no computador portátil de um funcionário, utilizando este como um ponto de entrada para introduzir vírus nos restantes computadores da planta. Poder-se-á dizer que, por sorte, os responsáveis pela introdução do vírus queriam apenas disseminar *e-mails* e obter dados de colaboradores, mas, caso o desejassem, poderiam ter afetado as operações da planta de filtragem, por exemplo, alterando os níveis de concentração dos desinfetantes utilizados para tratar a água. Embora não se tenha materializado, este poderia ter sido um caso em que acesso ao ambiente TO teria sido obtido através do ambiente TI. Uma vez descoberto o sucedido, os acessos remotos foram desativados e todas as palavras-passe alteradas[92].

[91] Hassanzadeh et al., "A Review of Cybersecurity Incidents", 5.

[92] Hassanzadeh et al., "A Review of Cybersecurity Incidents", 6.

Outro caso relevante foi o ocorrido com a Autoridade do Canal Tehama-Colusa em 2007 nos EUA. A Autoridade operava, nesse ano, dois canais - Canal Tehama Colusa e Canal Corning - que irrigam as plantações ao longo dos mesmos, ambos recebendo água do rio Sacramento. Neste caso, um eletricista supervisor da Autoridade acedeu ao computador utilizado para desviar água do rio para o Canal Tehama-Colusa, tendo instalado *software* não autorizado no sistema SCADA e danificado o computador em questão, crê-se, numa tentativa de afetar o fornecimento de água às referidas plantações. As suas ações não surtiram o efeito desejado, uma vez que os canais podiam continuar a ser operados manualmente, evitando estragos. Este caso exemplifica a importância de ter implementados controlos que impeçam a instalação de *software* não autorizado nos sistemas de uma organização. Este foi também o segundo caso de um ataque perpetrado por alguém da organização afetada, embora aqui se tratasse ainda de alguém em funções, e não de alguém cujo vínculo laboral tivesse acabado[93]. A este propósito, a ENISA elaborou em 2020 um relatório sobre a questão das ameaças internas às organizações. Nesse relatório, categorizam-se diferentes tipos de ameaças internas, tais como colaboradores que tratam indevidamente os dados e informações, violando as políticas de uso, colaboradores que vendem informações confidenciais para ganho próprio, colaboradores que o fazem para beneficiar entidades externas, e colaboradores amargurados que desejam apenas prejudicar as suas organizações[94]. Pode-se também ler que, em 65% dos casos, as organizações que sofrem ataques internos são fortemente impactadas a nível reputacional e financeiro e que, em média, o custo anual de um ataque interno é de 11,450 milhões de euros[95].

Outros ataques de relevo registaram-se também num passado mais próximo. Serão referidos ataques ocorridos em territórios como o de Israel e da Rússia. De seguida, descrevem-se esses ataques por ordem cronológica.

[93] Hassanzadeh et al., "A Review of Cybersecurity Incidents", 6-7.

[94] "ENISA Threat Landscape: Insider Threat", *ENISA*, abril de 2020, 2, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-insider-threat.

[95] "ENISA Threat Landscape: Insider Threat", *ENISA*, 3.

Israel sofreu um ataque em abril de 2020, mais concretamente um ataque de cloro nos abastecimentos de água do país. Este ataque teve como porta de entrada os *PLCs* (controlos lógicos programáveis) e, depois de os agentes de ameaça terem acesso aos mesmos, conseguiram tomar controlo da rede de abastecimento de água. Apesar disto, o governo israelita conseguiu evitar quaisquer consequências[96]. Em maio do mesmo ano, foi detetado outro ataque às estruturas de fornecimento de água de Israel. Este ataque foi, alegadamente, protagonizado por agentes de ameaça ligados ao governo do Irão. O ataque teve como alvo os computadores que controlam o fluxo de água e o tratamento da mesma em dois distritos rurais, sendo que as forças israelitas declararam que conseguiram detetar o ataque a tempo e, com isso, evitar quaisquer consequências danosas do mesmo[97]. O modo como o acesso aos PLCs foi obtido nunca foi oficialmente revelado, mas as hipóteses avançadas mais credíveis apontam para que o acesso inicial tenha sido obtido através de *routers* de rede móvel, comummente utilizados por fornecedores de água locais para fazer a comunicação entre sistemas ou através de ataques de *spear phishing* a prestadores terceiros com baixos níveis de segurança, mas com acesso legítimo aos sistemas dos fornecedores de água[98].

Uma empresa de gestão de águas com base em Rosvodokanal na Rússia foi atacada, alegadamente, por um grupo ucraniano. Este ciberataque ocorreu em dezembro de 2023 e teve como objetivo destruir toda a infraestrutura de TI da empresa, tendo sido apagados mais de 50 *TB* de dados como documentos de gestão internos, *backups* e as proteções de cibersegurança. Alegadamente, este ataque foi uma resposta ao ataque russo contra as telecomunicações ucranianas que também ocorreu em dezembro do mesmo ano[99].

[96] Joby Warrick e Ellen Nakashima, "Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran", *Washington Post*, 8 de maio de 2020, https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.

[97] "Attack on Israeli water utilities", *Council on Foreign Relations*, maio de 2020, https://www.cfr.org/cyber-operations/attack-israeli-water-utilities

[98] Eduard Kovacs, "Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources", *Security Week*, 30 de abril de 2020, https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources/.

[99] "Significant Cyber Incidents", Center for Strategic & International Studies, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

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[100], 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[101].
- **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[102].
- ***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[103].
- **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[104]. No caso, consideraram-se os colaboradores internos maliciosos.

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

Tabela 5 - Agentes de ameaça mais prováveis (Fornecimento e distribuição de água potável)

Tipo de ameaça	Cibercriminosos	Agentes estatais	Hacktivistas	Colaboradores internos
Ransomware	■	■	■	■
Malware	■	■	■	■
Vulnerabilidades	■	■	■	■
Phishing, Spear Phishing e *Smishing*	■	■	■	
Manipulação de Sistemas (TO)	■	■		■
Manipulação de Sistemas (TI)	■	■		■
Contaminações	■	■		

Legenda:
■ - Agente de ameaça provável

No que diz respeito a ataques ao setor em Portugal, os dados obtidos pelo CNCS, tanto através do questionário dirigido aos Operadores de Serviços Essenciais, como dos registados pelo CERT.PT, indicam uma baixa incidência. A maioria dos operadores inquiridos no setor (76%) respondeu não ter sofrido qualquer incidente em contexto de segurança TIC. O próprio CERT.PT foi, entre 2019 e 2023, notificado de um máximo de 14 incidentes em cada ano (quatro incidentes em 2019, seis incidentes em cada um dos anos entre 2020 e 2022 e 14 incidentes em 2023)[105].

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

Figura 6 - Número de incidentes no setor da Água anualmente

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

Mesmo quando sofrem ciberataques, os operadores portugueses têm sido capazes de evitar males maiores. Em Portugal, as instituições afetadas foram divididas igualmente entre públicas e privadas, com destaque para o caso da Águas do Porto, por exemplo, quando a Águas do Porto foi atacada a 30 de janeiro de 2023, o ataque não afetou a operação de serviços públicos essenciais, tendo apenas conduzido à interrupção temporária de alguns serviços de atendimento aos cidadãos[106].

[106] "Comunicado: Águas e Energia do Porto alvo de ataque informático", Águas e Energia do Porto, 8 de fevereiro de 2023, https://aguasdoporto.pt/noticias/comunicado-aedp-ataqueinformatico.

1.3. Capacitação

Embora haja ainda um longo caminho a percorrer em matéria de cibersegurança no setor, os operadores têm vindo a incluir o reforço da aposta no digital, na segurança dos sistemas de informação e na cibersegurança como prioridades estratégicas nos seus planos de atividades. Parte desse reforço passa pela formação dos colaboradores em cibersegurança. Em 2022, o Grupo Águas de Portugal deu início à concretização de um plano transversal de formação com temas basilares como ética, *corporate governance* e cibersegurança. A base para a formação em cibersegurança foi o curso "Cidadão/ã Ciberseguro", disponibilizado gratuitamente em formato *e-learning* pelo CNCS na plataforma NAU, que permitiu sensibilizar os formandos para a temática no contexto familiar, profissional e público. Em 2022, 1500 colaboradores frequentaram a formação, e estava prevista a adição de mais conteúdos à formação para o ano de 2023[107]. Mais dados relativos à formação no ano de 2023 não estavam ainda publicamente disponíveis à data da elaboração deste relatório. O Estado português tem também procurado incentivar a capacitação das várias vertentes do setor, nas quais se inclui a cibersegurança.

Foi observada uma melhoria no setor nos últimos 30 anos, existindo, ainda assim, algumas falhas que precisam de ser colmatadas, nomeadamente a gestão das águas residuais. Para responder a essas falhas, o Estado português criou o Plano Estratégico para o Abastecimento de Água e Gestão de Águas Residuais e Pluviais 2030 (PENSAARP 2030). Este Plano estabelece as diretrizes principais para o setor na próxima década e apela ao alinhamento de todos os seus atores, promovendo uma convergência de esforços e ambição. O PENSAARP 2030 é constituído por dois volumes: o Plano Estratégico, com as grandes linhas de orientação, e o Plano de Ação, com o detalhe das medidas preconizadas e respetivas métricas e incentivos[108].

O PENSAARP 2030 estabelece quatro objetivos estratégicos - o Objetivo A: Eficácia dos serviços; o Objetivo B: Eficiência dos serviços; o Objetivo C: Sustentabilidade dos serviços; Objetivo D: Valorização económica, ambiental e societal dos serviços[109]. Estes objetivos subdividem-se depois em vários outros, que são operacionalizados por diversas medidas. Para os fins deste relatório, importam sobretudo o "Objetivo A4: Segurança, resiliência e ação climática" e o "Objetivo B2: Organização, modernização e digitalização", operacionalizados pelas medidas M16 e M29, respetivamente.

[107] Águas de Portugal, "Relatório e Contas 2022", 26, https://www.adp.pt/pt/media/publicacoes/relatorios-e-contas/downloads/file597_pt.pdf .
[108] Conselho de Ministros, "PENSAARP 2030", versão de consulta pública, 1-2, https://apambiente.pt/sites/default/files/_SNIAMB_Agua/DRH/PlaneamentoOrdenamento/PlanosSetoriais/SetorUrbano/PENSAARP2030/PENSAARP_2030_Volume1.pdf.
[109] Conselho de Ministros, "PENSAARP 2030", 19.

A medida “M16 - Reforço da segurança e da resiliência dos sistemas”, associada ao Objetivo A4, assenta na promoção de “intervenções construtivas e operacionais no reforço da segurança e da resiliência dos sistemas de abastecimento de água e de águas residuais e pluviais, quer para prevenir acessos não autorizados a equipamentos, instalações, materiais, documentos e sistemas de informação e de gestão, que colocam em risco a prestação dos serviços, quer para reduzir a vulnerabilidade dos mesmos a catástrofes naturais e provocadas, como cheias, secas, incêndios nos espaços rurais, sismos e ataques cibernéticos (cibersegurança), ataques terroristas, e de preparação das respetivas respostas e recuperação, por exemplo através da interligação de sistemas de distribuição ou da otimização da gestão de albufeiras”[110]. Foram ainda identificados, como incentivos necessários para a prossecução desta medida, “a elaboração de guias técnicos sobre planos de segurança e resiliência dos sistemas, incluindo planos tipo; elaboração de cadernos de sensibilização para decisores sobre planos de segurança e resiliência; formação e capacitação em segurança e resiliência dos sistemas; ações de apoio à inovação sobre soluções tecnológicas de melhoria da segurança e resiliência dos sistemas”[111].

Por sua vez, a medida “M29 - Modernização e digitalização dos serviços”, associada ao Objetivo B2, coloca o seu foco na eficiência de processos e procedimentos, enfatizando a necessidade de agilizar procedimentos internos e de fazer uma “maior utilização de equipamento e ferramentas automáticas de recolha de dados em tempo real, processamento de informação, *big data*, reporte, gestão do risco, apoio à decisão e sistemas de alerta, numa perspetiva mais preventiva e menos reativa”, enquanto simultaneamente se prepara a integração da rede 5G, “que permitirá ao setor beneficiar de mais velocidade, maior cobertura e mais recursos, mais equipamentos ligados e menor latência destes, com menos consumo de energia”. Como incentivo necessário, identificou-se apenas a necessidade de “alteração da legislação sobre digitalização de alguns procedimentos nos serviços”[112].

Espera-se que a prossecução destes objetivos e a implementação destas medidas conduzam o setor a uma maior maturidade e resiliência em cibersegurança, capacitando o mesmo para lidar com as ciberameaças atuais e futuras.

[110] Conselho de Ministros, “PENSAARP 2030”, 37.
[111] Conselho de Ministros, “PENSAARP 2030”, 37-38.
[112] Conselho de Ministros, “PENSAARP 2030”,41.

1.4. Investimento em cibersegurança

Através da análise dos planos de atividades e orçamentos e dos relatórios de contas de diversas entidades, é possível verificar que apesar de o reforço do digital, incluindo a cibersegurança e a resiliência, fazer parte dos objetivos estratégicos a prosseguir, raros são os casos em que de facto se regista um investimento direto na área de cibersegurança.

Alguns desses raros casos são os da EPAL, da Águas e Energia do Porto, da Águas do Norte, da Águas do Algarve e da Águas do Alto Minho.

A EPAL realizou um investimento no valor de 3.249.870 euros para o desenvolvimento de ferramentas de analítica avançada de dados e diagnóstico e uma arquitetura de cibersegurança alinhada com a certificação ISO/IEC 27001, numa empreitada adjudicada à empresa Siemens[113].

A Águas e Energia do Porto definiu, para o período compreendido entre 2022 e 2024, um investimento anual de cerca de 300 mil euros, que abrange diversas soluções integradoras e de suporte aos processos, tais como telemetria, infraestrutura de redes, redundância de informação, servidores, armazenamento, CCTV e controlo de acessos (físicos e a dados) e renovação dos equipamentos usados pelos colaboradores[114].

Concomitantemente, a entidade candidatou-se também ao programa de financiamento comunitário "*Connecting Europe Facility – Telecom*", para apoio ao desenvolvimento de capacidades operacionais na área da cibersegurança e implementação da Diretiva NIS, tendo sido aprovada a atribuição de um incentivo não reembolsável de 75% das despesas elegíveis, num projeto com um custo global de 292 230 euros, executado entre agosto de 2020 e agosto de 2022, que contou com a implementação de sistemas (*software*, *hardware* e soluções de gestão de informação) com o intuito de alcançar os níveis de segurança tecnológica necessários para proteger todas as redes e infraestruturas da Águas e Energia do Porto[115].

Em 2021, a Águas do Norte foi outra candidata ao mesmo programa de financiamento que conseguiu também obter o apoio desejado ao seu plano de cibersegurança. O plano rondava também os 300 mil euros de investimento e os objetivos do mesmo passavam pela criação de um SOC com base nas plataformas SIEM (*Security Information and Event Management*) e em IA, de modo que a entidade conseguisse monitorizar todo o ecossistema, identificando e adaptando-se continuamente às ameaças de cibersegurança mais evoluídas, melhorando as suas capacidades técnicas e operacionais em matéria de cibersegurança. A Águas do Norte pretendia ainda que a solução tivesse a capacidade de fornecer informações relevantes para as partes interessadas em cibersegurança, nacionais e internacionais[116].

[113] Catarina Eusébio, Joaquim Baetas e Ana Conde, "Investimentos já em pleno desenvolvimento, com construção de infraestruturas ou contratualizados", *Águas Livres* n.º 298, maio de 2022, https://www.epal.pt/EPAL/docs/default-source/epal/newspaper-2014/2022/05-2022.pdf.

[114] Águas e Energia do Porto, "Instrumentos de Gestão Previsional 2022-2024", 60, https://aguasdoporto.pt/files/uploads/cms/adp/24/files/1647269981-EVymV2FxC3.pdf.

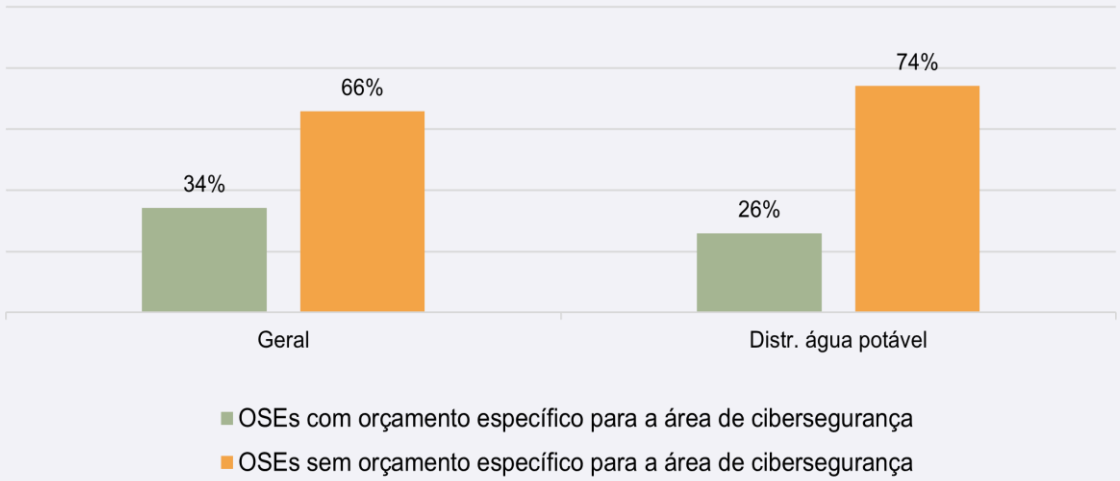
[115] Águas e Energia do Porto, "Instrumentos de Gestão Previsional 2022-2024", 60-61.

[116] "Águas do Norte inicia implementação de um Security Operations Center", *Computer World - Especial Cibersegurança*, 2021, 36.

Outras entidades, como a Águas do Algarve, não fazem menções específicas ao investimento em cibersegurança, mas indicam ter investido entre 95.000 e 98.000 euros em assessoria informática[117]. As Águas do Alto Minho, por sua vez, investiram na telegestão, tendo lançado o concurso para a contratação do *software* e *hardware* para a sala de comando de telegestão e respetiva instalação num valor aproximado de 800 mil euros. Nota-se ainda o investimento em *software* e serviços conexos para a solução de gestão documental no valor de cerca de 13 mil euros[118].

Deste setor, cerca de 26% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança

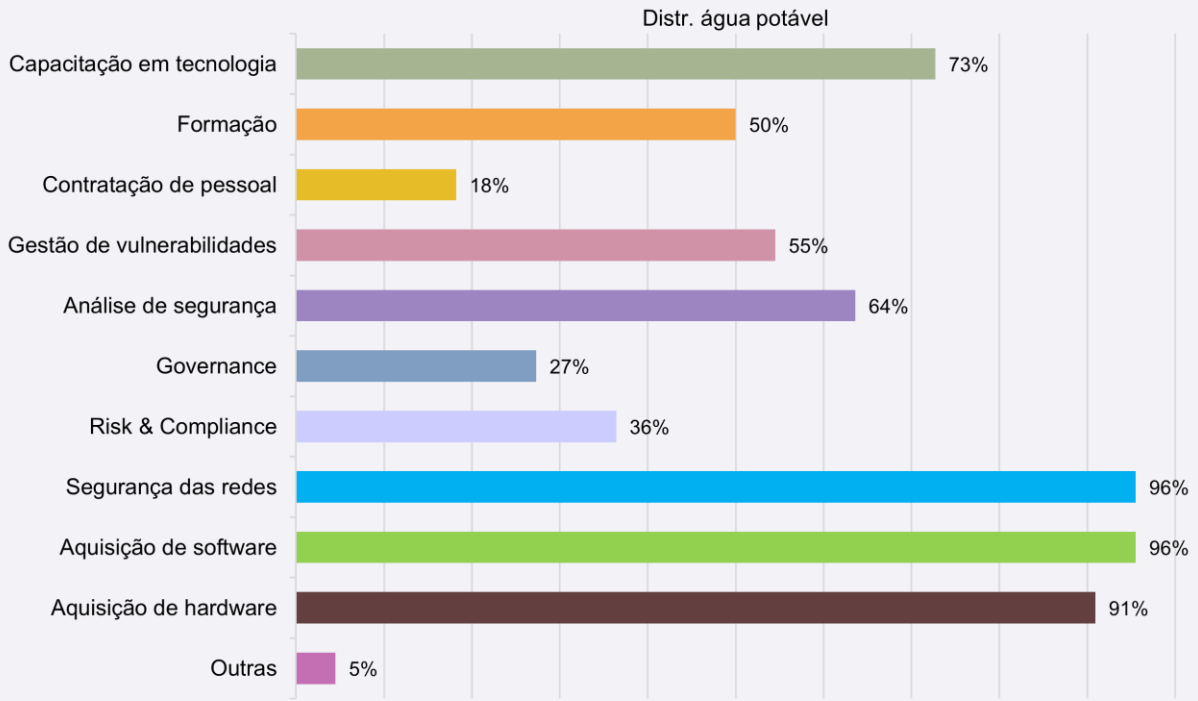


[117] Águas do Algarve, "Plano de Atividades e Orçamento para o ano de 2022 (e projeções para 2023 e 2024)", 106, https://www.aguasdoalgarve.pt/sites/aguasdoalgarve.pt/files/paginas_base/inf_financeira/pao-2022_28_10_2021_signedca_signed.pdf.

[118] Águas do Alto Minho, "Relatório & Contas 2022", 72 e 82, https://adam.pt/component/phocadownload/category/23-relatorio-e-contas?download=262:2022-relatorio-e-contas.

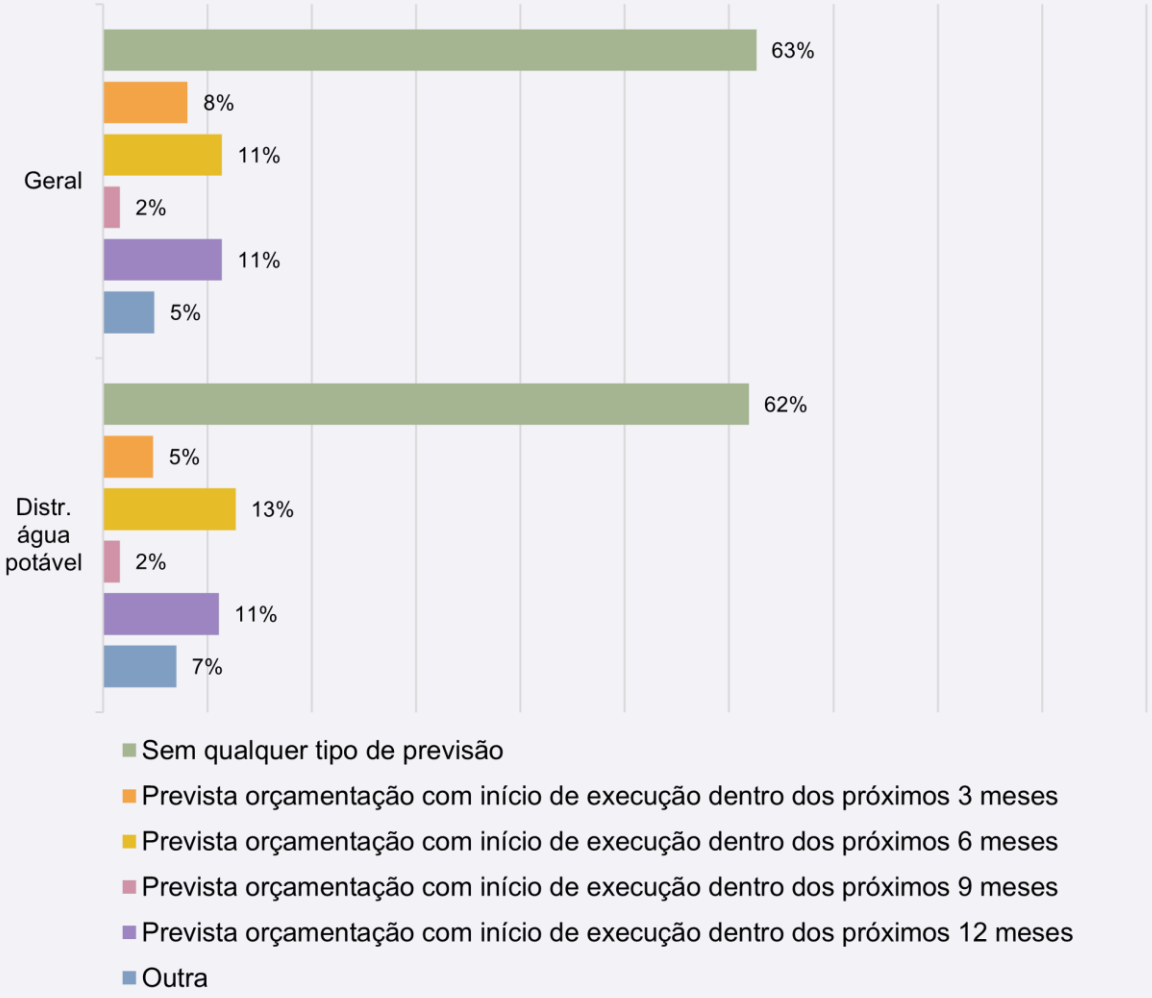
Relativamente às áreas de aplicação do orçamento de cibersegurança, 96% aplica na segurança das redes, 73% na capacitação em tecnologia e aquisição de *hardware* e 55% em gestão de vulnerabilidades, 64% em análise de segurança e cerca de 90% em aquisição de *software* e *hardware*. Em comparação com a média geral, este setor tem uma menor análise de segurança e gestão de vulnerabilidades. Por outro lado, tem está na média na capacitação em tecnologia e superior na aquisição de *software* e *hardware*. (**Gráfico 110.5**).

Gráfico 110.5 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 62% não tem qualquer previsão para a orçamentação, 5% tem previsto a orçamentação dentro dos próximos 3 meses, 13% tem previsto a orçamentação para os próximos 6 meses e 11% tem previsto a orçamentação para os próximos 12 meses. Este setor está dentro da média geral, a maior diferença, cerca de 3%, está na orçamentação com início de execução dentro dos próximos 6 meses (**Gráfico 111**).

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



Como se viu em **1.3. Capacitação**, o recurso a soluções formativas de caráter gratuito pode ser uma das causas que leva a que se verifique menos investimento expresso na área de cibersegurança.

1.5. RJSC e legislação setorial

O setor do fornecimento e distribuição de água potável não é um setor que possua uma vasta legislação setorial em matéria de cibersegurança. Alguma legislação setorial, tal como a Lei da Água (Lei n.º 58/2005), que transpõe a Diretiva n.º 2000/60/CE, do Parlamento Europeu e do Conselho, de 23 de outubro obriga os operadores deste setor a "proteger e melhorar o estado dos ecossistemas aquáticos", a "promover uma utilização sustentável de água" e a "assegurar o fornecimento em quantidade suficiente de água de origem superficial e subterrânea de boa qualidade"[119], mas não faz qualquer menção específica à cibersegurança, segurança informática ou segurança da informação. Menciona, no entanto, a "proteção e valorização dos recursos hídricos", bem como a "prevenção e a proteção contra riscos de cheias e inundações, de secas, de acidentes graves de poluição e de rotura de infraestruturas hidráulicas"[120], de onde se pode subentender a necessidade fortalecer a componente de cibersegurança por parte dos operadores.

Existe também o Decreto-Lei n.º 306/2007, de 27 de agosto, que estabelece o regime da qualidade da água destinada ao consumo humano e impõe obrigações como a da implementação de um programa de controlo de qualidade da água ou de um Plano de Segurança da Água (PSA). Um PSA é suportado pela análise de perigos e avaliação do risco efetuada sistematicamente ao longo do sistema de abastecimento de água, desde a captação de água bruta, passando pelo processo de tratamento da água, pela rede de distribuição e rede predial até à torneira dos consumidores"[121]. É uma ferramenta que auxilia a mitigação, a redução e o controlo dos riscos associados às operações necessárias para distribuir de forma ininterrupta e segura água de qualidade aos consumidores, incluindo os riscos de cibersegurança.

Conta-se, ainda, com a Diretiva (UE) 2016/1148 (Diretiva NIS)[122], publicada em 2016, e cuja transposição deu origem ao Regime Jurídico da Segurança do Ciberespaço, através da Lei n.º 46/2018, de 13 de agosto[123], e do Decreto-Lei que a regulamenta, o Decreto-Lei n.º 65/2021, de 30 de julho[124]. O RJSC acaba assim por se qualificar como o primeiro diploma legal que de facto impõe obrigações ao nível da cibersegurança de forma direta neste setor, tais como a nomeação de um contacto permanente para articulação com o CNCS, a nomeação de um responsável de segurança, a elaboração de um inventário de ativos, de um plano de segurança, de um relatório anual, de análise, gestão e tratamento do risco, e de notificação de incidentes[125]. Apesar do elevado nível de cumprimento de algumas destas obrigações, verifica-se que 47% dos OSE inquiridos ainda não realizam anualmente avaliações de risco de cibersegurança e que 57% não possuem qualquer tipo de plano de resposta a incidentes de cibersegurança, segundo os dados obtidos através do questionário realizado.

---

[119] Lei n.º 58/2005 de 29 de dezembro (Lei da Água), *Diário da República*, 1.ª série - n.º 249, 29 de dezembro de 2005. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1191&tabela=leis&ficha=1&pagina=1.

[120] Lei n.º 58/2005 de 29 de dezembro (Lei da Água).

[121] "Plano de Segurança da Água", Avaliação do Risco, ERSAR, https://www.ersar.pt/pt/o-que-fazemos/controlo-da-qualidade-da-agua/avaliacao-do-risco.

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

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

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

[125] Decreto-Lei n.º 65/2021, artigos 4.º a 15.º.

O setor está ainda obrigado ao cumprimento da Diretiva (UE) 2022/2555[126], ou Diretiva NIS 2, que veio atualizar a Diretiva anterior, passados seis anos sobre a sua publicação. A Diretiva NIS 2 classifica dois tipos de setores: "setores de importância crítica"[127] e "outros setores críticos"[128]. Os setores já visados pela Diretiva anterior inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

O setor do fornecimento e distribuição de água potável é um dos setores que recebe algumas modificações. Passa a ser denominado como setor da "água potável" passa-se também a incluir o setor das "águas residuais", que não era considerado pela primeira Diretiva[129].

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[130]. 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[131].

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como "ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques"[132].

Com a publicação de nova legislação, como a NIS 2, e com novas ações governativas, tal como o PENSAARP 2030, espera-se que a perceção da importância da cibersegurança seja melhorada, e que processos ainda em falta, como o da análise de risco anual, sejam implementados.

[126] 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

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

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

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

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

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

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

1.6. Standards e boas práticas aplicáveis

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

Tabela 6 - Standards e Boas Práticas (Água)

Standards	Boas práticas
• ISO 27001 Information technology - Security techniques - Information security management systems - Requirements • IEC 62443-2-1 • ISO 24512:2024 Activities relating to drinking water and wastewater services - Guidelines for the management of drinking water utilities and for the assessment of drinking water services	• ANSI/AWWA G430-09: Security Practices for Operations and Management • NIST Cybersecurity Framework (CSF) • NIST SP 800-82r3 • EN 15975-2

- **ISO 27001 Information technology - Security techniques - Information security management systems - Requirements**: Estabelece um quadro de políticas e processos para gerir a segurança da informação de forma sistemática, garantindo assim a confidencialidade, integridade e disponibilidade das informações[133];
- **IEC 62443-2-1**: É um conjunto de normas internacionais focadas na segurança de sistemas de controlos e automação industrial. Fornece diretrizes para estabelecer e operar um programa de segurança para sistemas de controlo e automação industrial (IACS), ajuda a mitigar riscos específicos nos sistemas industriais e aborda todo o ciclo de vida de segurança dos mesmos[134];
- **ISO 24512:2024 Activities relating to drinking water and wastewater services - Guidelines for the management of drinking water utilities and for the assessment of drinking water services**: *Standard* para a gestão de serviços de abastecimento de água potável para as populações e meio ambiente. Inclui métodos para avaliar a qualidade e eficiência dos serviços de água potável e promove práticas de gestão, a nível ambiental e de saúde pública[135];
- **ANSI/AWWA G430-09: Security Practices for Operations and Management**: Define práticas recomendadas para garantir a segurança física e operacional das instalações e operações de abastecimento de água. Inclui métodos para identificar e mitigar riscos de segurança das operações de água[136];

[133] ISO, "ISO/IEC 27001:2022", https://www.iso.org/standard/27001

[134] International Electrotechnical Commission, "Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners", 2024, https://webstore.iec.ch/en/publication/62883.

[135] ISO, "Activities relating to drinking water and wastewater services — Guidelines for the management of drinking water utilities and for the assessment of drinking water services", 2024, https://www.iso.org/standard/82490.html.

[136] American Water Works Association, "Security Practices For Operation And Management", https://webstore.ansi.org/standards/awwa/awwag43009?srsltid=AfmBOopxVXFQqfg7_VmKEeA34CyCkDf-czdhzHBps1dxXD8WktOp58Lc.

- **NIST Cybersecurity Framework (CSF)**: Utilizado para ajudar as organizações a entender e gerir os riscos de cibersegurança. Está organizado em cinco funções principais: Identificar, Proteger, Detetar, Responder e Recuperar[137];
- **NIST SP 800-82r3**: Guia para a segurança de tecnologia operacional. Fornece orientações detalhadas sobre como proteger sistemas de controlo industrial (ICS) contra ameaças de cibersegurança[138];
- **EN 15975-2**: Guia para a segurança do abastecimento de água potável, gestão de riscos e crises. Inclui orientações para desenvolver e implementar planos de gestão de crises relacionadas ao abastecimento de água[139].

[137] NIST, "NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral", fevereiro de 2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf.

[138] NIST, "Guide to Operational Technology (OT) Security", 26 de abril de 2022, https://csrc.nist.gov/pubs/sp/800/82/r3/ipd.

[139] European Standards, "General Information", 14 de agosto de 2023, https://standards.iteh.ai/catalog/standards/cen/39c119d3-607d-4a49-9ab7-74f51574ab42/en-15975-2-2013?srsltid=AfmBOoqHieQKOaJjD8Wnu57c-zFcHTCY1zv392baYX23wWb5a98ws5er.

1.7. Desafios

Analisando o relatório "*Cybersecurity Risk and Responsibility in the Water sector",* da *American Water Work Association*, de 2019, é possível verificar que os principais desafios do setor estão relacionados com as infraestruturas que o compõem. Como se viu em 6.1.3. Especificidades tecnológicas, a TO, que muitas vezes inclui sistemas *legacy* que não podem ser integrados com tecnologias mais avançadas e mais seguras, constituem uma fragilidade no setor[140].

Além disso, a gestão das infraestruturas de abastecimento de água é muitas vezes partilhada com entidades municipais que, em Portugal, têm sido alvos preferenciais para a realização de ciberataques[141].

Acresce ainda que embora se verifique, nos últimos 30 anos, uma elevada evolução dos serviços do setor da água (abastecimento de água e gestão de águas residuais), os desafios que este setor encara baseiam-se na dificuldade que entidades maiores e menores têm em evoluir ao mesmo ritmo, provocando um acentuado desequilíbrio entre entidades mais modernizadas e entidades mais tradicionais.

Tratando-se de um setor que depende diretamente das condições climáticas, todos os impactos, positivos e negativos, que estão associados aos respetivos fenómenos (escassez hídrica, degradação das massas de água, risco de ocorrência de inundações, necessidade de controlo de poluentes emergentes, entre outros) constituem desafios acrescidos à atividade do setor. Além dos desafios ambientais, acrescentam-se a este contexto desafios económicos (oportunidades a explorar e a necessidade de maior circularidade e valorização ambiental e territorial dos serviços) e desafios societais (adaptabilidade do mercado de trabalho).

Para responder a estes desafios os Estados Unidos da América, por parte do NCCoE (*National Cybersecurity Center of Excellence*, pertencente ao NIST), lançaram um projeto, em junho de 2023, com o objetivo de melhorar a cibersegurança nos sistemas de água e de esgoto. Esta iniciativa concentra-se, em grande parte, em melhorar as soluções práticas utilizando as tecnologias disponíveis. Tais soluções para mitigar riscos de cibersegurança nos sistemas de água e esgoto vão resultar num guia de práticas de cibersegurança da *NIST* que irá ser disponibilizado de forma gratuita a todas as organizações do setor[142].

---

[140] Germano, "Cybersecurity Risk & Responsibility in the Water Sector", 14.

[141] Lusa, "Ciberataques a autarquias aumentam com a transição digital", *SIC Notícias*, 18 de outubro de 2023, https://sicnoticias.pt/pais/2023-10-18-Ciberataques-a-autarquias-aumentam-com-a-transicao-digital-e984cece.

[142] "Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems", National Cybersecurity Center of Excellence (NCCoE), junho de 2023, 4, https://www.nccoe.nist.gov/sites/default/files/2023-06/securing-water-and-wastewater-utilities-project-description-final.pdf.

Neste projeto, os principais desafios de cibersegurança no setor da água e dos esgotos dos Estados Unidos da América foram:

- **Gestão de ativos**: Identificar e categorizar todos os dispositivos na rede de forma a ser possível detetar potenciais riscos de equipamentos vulneráveis;
- **Integridade dos dados**: Proteger a integridade dos dados tanto em trânsito como em repouso. É esperado a criação de métodos para manter essa integridade e, também, fornecer soluções para testes;
- **Acesso remoto**: Detetar possíveis falhas na rede analisando o comportamento da mesma, implementar o controlo e autenticação de acessos externos à rede e garantir a segurança de todos os dispositivos e sistemas;
- **Segmentação da rede**: Isolar a rede para garantir uma maior segurança utilizando produtos com código aberto. Serão também incluídos controlos de segurança na segmentação da rede[143].

As normas e orientações mais relevantes utilizadas neste projeto foram:

- ***NIST Cybersecurity Framework* (*CSF*)**: Utilizado para ajudar as organizações a entender e gerir os riscos de cibersegurança;
- ***NIST SP 800-82r3***: Guia para a segurança de tecnologia operacional;
- ***NIST SP 800-53r5***: Catálogo de controlos de segurança e privacidade para sistemas de informação[144].

[143] "Cybersecurity for the Water and Wastewater Sector", *National Cybersecurity Center of Excellence (NCCoE)*, 6-8.

[144] "Cybersecurity for the Water and Wastewater Sector", *National Cybersecurity Center of Excellence (NCCoE)*, 11.

1.8. Recomendações

A reconhecida importância do setor do fornecimento e distribuição de água potável, bem como os potenciais efeitos de ciberataques no mesmo, levaram a que a Comissão Europeia elaborasse, em 2022, um plano de segurança da água, cujo principal objetivo é sensibilizar e garantir, junto das autoridades locais, dos proprietários e dos operadores dos sistemas de água, que a sua principal prioridade deve ser o fornecimento ininterrupto de água com qualidade para o consumo humano. Nesse sentido, estes deverão também ter preparado um plano para qualquer tipo de emergência (desastres naturais, ciberataques, pandemias, entre outros) e os planos deverão ter uma série de instruções a indicar como proceder e como é que a emergência em questão pode afetar os sistemas de água[145].

Este plano recomenda a utilização de uma ferramenta para a identificação de possíveis cenários de risco e criar sugestões de forma a reduzir esse mesmo risco. Essa ferramenta denominada *RIDB* (*Risk Identification Database*) ajuda a identificar o tipo de ameaças, a origem dos riscos, a descrição dos eventos e o tipo de consequências que estes podem produzir. O propósito desta ferramenta não é substituir a identificação de riscos por parte das aplicações, mas sim funcionar de forma complementar às mesmas[146].

Relativamente a sistemas de monitorização de incidentes de cibersegurança, o plano indica algumas soluções tais como:

- Sensores de tráfego de rede e sistemas de análise que utilizam algoritmos não supervisionados que, com isto, conseguem criar um modelo de comportamento normal do sistema de água. Caso ocorra uma variação, este sistema consegue detetar um comportamento anómalo e lançar um alerta;
- Um sistema de deteção de dados em tempo real que pode ser usado para garantir a integridade dos dados gerados;
- Implementar um SIEM (*Security Information and Event Management*) que seja capaz de lançar alertas de uma perspetiva de negócio levando em conta todos os eventos gerados[147].

[145] Rui Teixeira et al., "JRC Technical Report: Water Security Plan Implementation Manual for Drinking Water Systems", Comissão Europeia, 3, https://ec.europa.eu/newsroom/cipr/items/738662/en.

[146] Teixeira et al., "Water Security Plan Implementation Manual", Comissão Europeia, 11.

[147] Teixeira et al., "Water Security Plan Implementation Manual", Comissão Europeia, 21.

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

Tabela 7 - Cenários de risco

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (*SQL Injection* ou *Cross-site Scripting*).
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
Um agente de ameaças consegue o acesso às INSTALAÇÕES FÍSICAS da entidade, acedendo indevidamente a dispositivos, furtando material informático e modificando dados sensíveis armazenados.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade,** sendo pedido um resgate em bitcoins, sob a ameaça da sua destruição ou exposição ao público.
Desenvolvimento de ações de CIBERESPIONAGEM, através de *malware* ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

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

Com base nos resultados obtidos no questionário dirigido aos Operadores de Serviços Essenciais, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor da distribuição de água potável, surgem diversas recomendações que se consideram pertinentes para as entidades do setor, que se apresentam de seguida.

Formação

Os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor disponibilizarem formação em cibersegurança aos seus colaboradores (**Gráfico 38**), as formações são, na maioria dos OSE inquiridos (cerca de 65%) são de caráter facultativo, e não obrigatório (**Gráfico 39**).

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

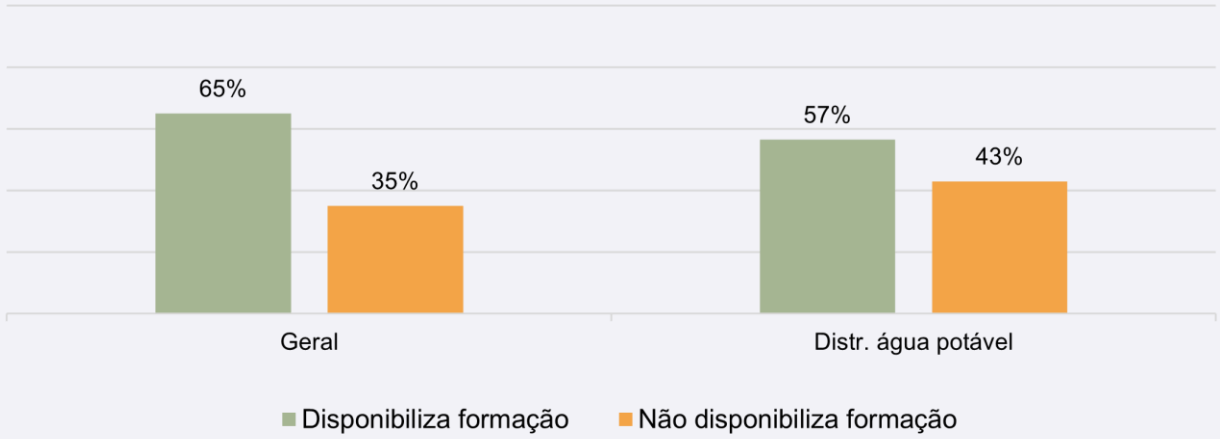
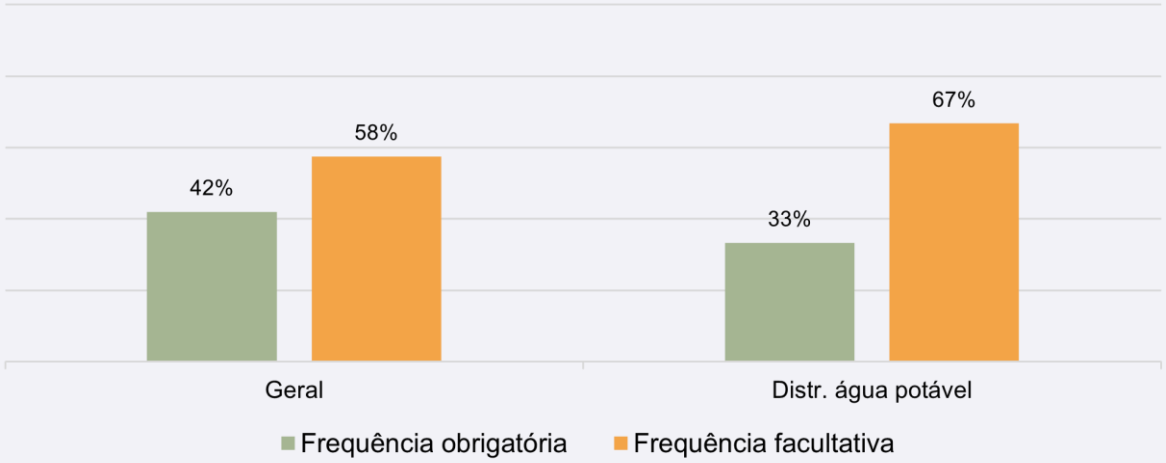
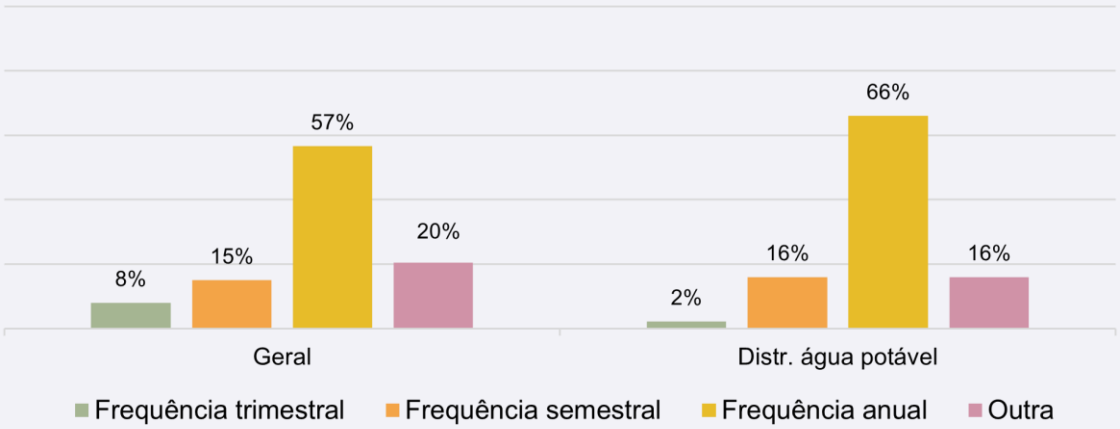


Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



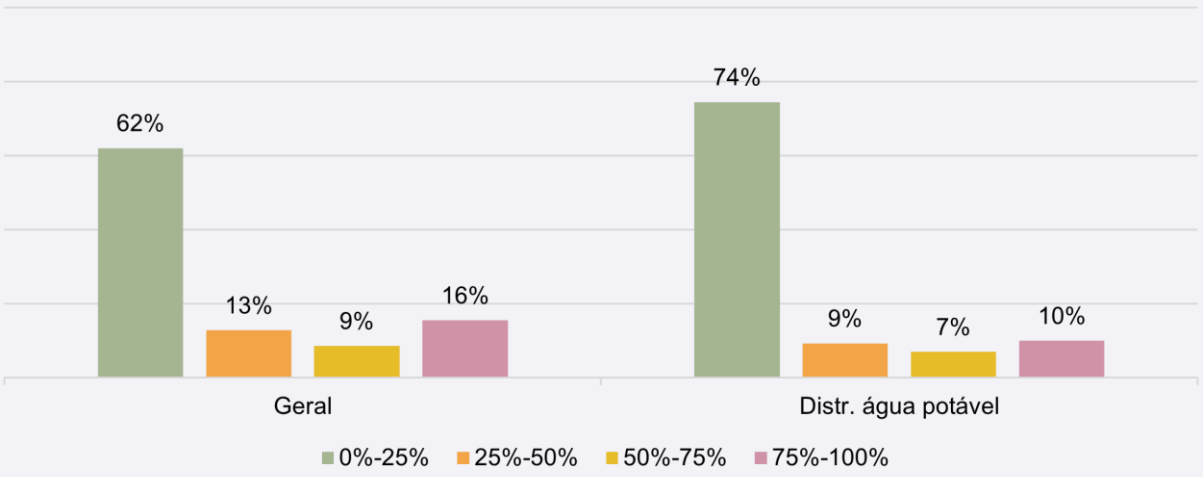
O facto de os momentos de formação serem, na sua maioria, anuais (**Gráfico 41**), sem obrigatoriedade de participação poderá conduzir a que passe demasiado tempo sem que os colaboradores tomem conhecimento sobre boas práticas ou riscos de cibersegurança.

Gráfico 41 - Frequência média dos momentos de formação



O facto de cerca de três quartos dos OSE indicarem que apenas entre 0%-25% dos colaboradores têm formação básica em cibersegurança (**Gráfico 33**) poderá corroborar esta hipótese. Concomitantemente, a maturidade do setor nesta área é considerada, pelo regulador, muito baixa. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória. É importante referir que a existência de cursos de atualização no setor é muito baixa (verifica-se em apenas cerca de um quarto dos inquiridos), sendo que estes tipos de cursos são importantes para manter os colaboradores atualizados para novas ameaças.

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



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor da distribuição de água potável, comparativamente com os restantes, é um dos setores onde menos se observa a autenticação multifator, a existência de sensibilização sobre segurança, a utilização de sistemas de gestão de palavras-passe, a existência de controlos biométricos para a identificação e autenticação de utilizadores, a implementação de um *SIEM* e a manutenção de *logs* para futura análise após incidentes de cibersegurança.

Nesse sentido, recomenda-se aos OSE do setor da distribuição de água potável que:

- Implementem, onde possível, métodos de autenticação multifator;
- Desenvolvam programas de sensibilização sobre segurança e disponibilizam aos seus colaboradores;
- Utilizem sistemas de gestão de palavras-passe, de modo a viabilizar a utilização de diversas palavras-passe complexas e seguras para cada sistema;
- Implementem, onde possível, controlos biométricos para a identificação e autenticação de utilizadores;
- Mantenham os *logs* durante um período mínimo de 90 dias para ser possível a análise dos mesmos caso ocorra um incidente de cibersegurança.

Políticas, procedimentos e planos de cibersegurança

Com base nos dados reunidos no questionário, apenas 60% dos OSE do setor possuíam políticas e procedimentos de cibersegurança documentados e implementados. Além disso, apenas 43% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

Diante desta situação, recomenda-se aos OSE do setor que ainda não o tenham feito que elaborem e implementem uma política de cibersegurança que verse sobre:

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

Considerando a baixa percentagem de OSE do setor que indicaram possuir uma política de continuidade de negócio (35%), recomenda-se também a elaboração de uma política de continuidade de negócios alinhada com a política de cibersegurança.

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

Apenas cerca de metade (51%) dos OSE do setor da distribuição de água potável realizam procedimentos de deteção e gestão de vulnerabilidades, sendo importante implementar estes procedimentos tendo em vista a diminuição e antecipação de possíveis ataques. A deteção e análise, e correção de vulnerabilidades é uma prática importante para a proteção proativa e preventiva dos sistemas e aplicações em utilização em qualquer setor de atividade.

Quanto à realização de testes de intrusão, embora não exista uma obrigação legal no setor da distribuição de água potável de os realizar, o setor do fornecimento e distribuição de água potável surge como o segundo que menos realiza estes testes (40% dos OSE), somente atrás do setor da saúde. Apesar da baixa incidência de ataques registada, a realização de testes de intrusão é mais uma maneira de identificar vulnerabilidades, corrigi-las e tornar os OSE mais resilientes em matéria de cibersegurança.

Reforço da segurança da Tecnologia Operacional (TO)

Sendo o setor de fornecimento e distribuição de água potável um setor essencial, a segurança da TO é crucial, isto porque envolve sistemas críticos que controlam a distribuição e o tratamento da água para consumo. De forma a reforçar a segurança da Tecnologia Operacional podem ser seguidas algumas recomendações, tais como:

- **Controlar acessos**: Implementar controlos rigorosos de acesso físico aos locais onde se encontram os sistemas de TO, tais como centrais de controlo e instalações de tratamento de água;
- **Monitorizar**: Instalar câmaras de vigilância e sensores de movimento de forma a detetar atividades suspeitas;
- **Segmentação da rede**: Separar as redes de TO das redes de TI de forma a minimizar o risco de algum possível ataque se propagar da rede de TI para a rede de TO;
- ***VLANs***: Utilizar *VLANs* na segmentação do tráfego da rede dentro da infraestrutura TO para isolar as diferentes partes do sistema e assim conter possíveis invasões;
- ***IDS/IPS***: Implementar sistemas de detecção e prevenção específicos para TO, de forma a supervisionar e bloquear possível tráfego malicioso;
- **Normas**: Assegurar a conformidade com as normas e regulamentações relevantes, como a ISO/IEC 62443 para a segurança de sistemas de controlo industrial e a ISO/IEC 27001 que fornece diretrizes para implementar melhores práticas na gestão e redução de riscos de cibersegurança.

Implementar, pelo menos, algumas destas recomendações pode ajudar a proteger melhor todas as infraestruturas críticas de TO do setor de fornecimento e distribuição de água potável contra possíveis ameaças de cibersegurança.

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

- **Controlos básicos**: controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais**: controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais**: controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*[148].

No setor da distribuição de água potável, os controlos fundacionais, relacionados com segurança de rede, desempenham um papel especialmente crítico. Infraestruturas essenciais, como estações de tratamento de água, sistemas de monitorização e controlo de distribuição, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, a disponibilidade e a continuidade dos serviços de abastecimento. Falhas ou configurações inadequadas nesses sistemas podem ser exploradas para interromper o fornecimento de água, adulterar os processos de tratamento, ou comprometer a segurança e a qualidade da água distribuída, colocando em risco a saúde pública e o bem-estar das comunidades.

148 "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[149]:

Tabela 8 - Controlos de Segurança da CIS

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)

149 "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

- Águas de Portugal. “Águas de Portugal - Duas décadas que perspetivam o futuro”, vídeo publicado a 6 de outubro de 2016, Youtube. https://www.youtube.com/watch?v=2IPH9iW5wDg.
- Águas de Portugal. “Relatório e Contas 2022”. https://www.adp.pt/pt/media/publicacoes/relatorios-e-contas/downloads/file597_pt.pdf .
- Águas de Portugal. *Livro Águas de Portugal.* Lisboa: By the Book, 2016. https://www.adp.pt/pt/media/publicacoes/downloads/pub_pdf17_pt.pdf.
- Águas do Algarve. “Plano de Atividades e Orçamento para o ano de 2022 (e projeções para 2023 e 2024)”. https://www.aguasdoalgarve.pt/sites/aguasdoalgarve.pt/files/paginas_base/inf_financeira/pao-2022_28_10_2021_signedca_signed.pdf.
- Águas do Alto Minho. “Relatório & Contas 2022”. https://adam.pt/component/phocadownload/category/23-relatorio-e-contas?download=262:2022-relatorio-e-contas.
- Águas e Energia do Porto. “Comunicado: Águas e Energia do Porto alvo de ataque informático”, 8 de fevereiro de 2023. https://aguasdoporto.pt/noticias/comunicado-aedp-ataqueinformatico.
- Águas e Energia do Porto. “Instrumentos de Gestão Previsional 2022-2024”. https://aguasdoporto.pt/files/uploads/cms/adp/24/files/1647269981-EVymV2FxC3.pdf.
- American Water Works Association, “Security Practices For Operation And Management”, https://webstore.ansi.org/standards/awwa/awwag43009?srsltid=AfmBOopxVXFQqfg7_VmKEeA34CyCkDf-czdhzHBps1dxXD8WktOp58Lc.
- 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.
- Center for Internet Security. “The 18 CIS Critical Security Controls”, CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list.
- Center for Strategic & International Studies. “Significant Cyber Incidents”. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
- CISA. “Cyber Risks and Resources for the Water and Wastewater Systems Sector”, outubro de 2021. https://www.cisa.gov/sites/default/files/publications/infographic-manage-wastewater-national-critical-function-102021-508.pdf.
- CNCS, “Compromisso C-Academy”. https://www.cncs.gov.pt/pt/c-academy-compromisso/.
- CNCS, “Estratégia Nacional de Segurança do Ciberespaço 2019-2023”. https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf.
- CNCS, “Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança”, dezembro de 2022. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.
- CNCS, ISAC. https://www.cncs.gov.pt/pt/isac/.

- CNCS. “Incidentes e Setores: 2019-2023”. Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024. https://www.cncs.gov.pt/pt/estatistica/.
- CNCS. “Incidentes e Setores”. Conhecimento Situacional: Estatísticas. https://www.cncs.gov.pt/pt/estatistica/#cert.pt.
- CNCS. “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancacncs.pdf.
- CNCS. “Relatórios”, Conhecimento Situacional: Observatório de Cibersegurança. https://www.cncs.gov.pt/pt/observatorio/#relatorios.
- 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 de Ministros. “PENSAARP 2030”, versão de consulta pública. https://apambiente.pt/sites/default/files/_SNIAMB_Agua/DRH/PlaneamentoOrdenamento/PlanosSetoriais/SetorUrbano/PENSAARP2030/PENSAARP_2030_Volume1.pdf.
- Conselho Europeu, “Horizonte Europa”. https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Council on Foreign Relations. “Attack on Israeli water utilities”, maio de 2020. https://www.cfr.org/cyber-operations/attack-israeli-water-utilities
- 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
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. *Jornal Oficial da União Europeia*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.
- Diretiva (UE) 2016/1148 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
- 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. “ENISA Threat Landscape: Insider Threat”, abril de 2020. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-insider-threat.

- ENISA. “NIS Investments”, 2021. https://www.enisa.europa.eu/publications/nis-investments-2021.
- EPAL, “WONE: Water Optimization Network Efficiency: A Global Solution to a Global Water Challenge”. https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/wone.
- EPAL. “Aquamatrix: EPAL, Boosting business inovation”. https://www.epal.pt/EPAL/menu/produtos-e-servi%C3%A7os/aquamatrix.
- ERSAR. “Plano de Segurança da Água”. Avaliação do Risco. https://www.ersar.pt/pt/o-que-fazemos/controlo-da-qualidade-da-agua/avaliacao-do-risco.
- ERSAR. “Relatório Anual dos Serviços de Águas e Resíduos em Portugal: Volume 1 – Caracterização do setor de águas e resíduos”, 2022. https://www.ersar.pt/_layouts/mpp/file-download.aspx?fileId=2169122.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), “Impact”. https://www.ee-isac.eu/impact/#.
- European Standards. “General Information”, 14 de agosto de 2023. https://standards.iteh.ai/catalog/standards/cen/39c119d3-607d-4a49-9ab7-74f51574ab42/en-15975-2-2013?srsltid=AfmBOoqHieQKOaJjD8Wnu57c-zFcHTCY1zv392baYX23wWb5a98ws5er.
- Eusébio, Catarina, Joaquim Baetas e Ana Conde, “Investimentos já em pleno desenvolvimento, com construção de infraestruturas ou contratualizados”, *Águas Livres* n.º 298, maio de 2022. https://www.epal.pt/EPAL/docs/default-source/epal/newspaper-2014/2022/05-2022.pdf.
- 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.
- Germano, Judith. “Cybersecurity Risk & Responsibility in the Water Sector”. *American Water Work Association*, 2019. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf.
- Hassanzadeh, Amin, Amin Rasekhb, Stefano Galellic, Mohsen Aghashahid, Riccardo Taorminae, Avi Ostfeldf e Katherine Banksg. “A Review of Cybersecurity Incidents in the Water Sector”. *Journal of Environmental Engineering 146*: 25 de julho de 2020. https://arxiv.org/pdf/2001.11144.
- 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.
- International Electrotechnical Commission. “Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners”, 2024. https://webstore.iec.ch/en/publication/62883.
- ISO, “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- ISO. “Activities relating to drinking water and wastewater services — Guidelines for the management of drinking water utilities and for the assessment of drinking water services”, 2024. https://www.iso.org/standard/82490.html.
- ISO. “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- Kovacs, Eduard. “Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources”. *Security Week*, 30 de abril de 2020. https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources/.
- Lei n.º 46/2018, de 13 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- Lei n.º 46/2018, de 13 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.

- Lei n.º 58/2005 de 29 de dezembro (Lei da Água), *Diário da República*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1191&tabela=leis&ficha=1&pagina=1.
- Lusa. "Ciberataques a autarquias aumentam com a transição digital". *SIC Notícias*, 18 de outubro de 2023. https://sicnoticias.pt/pais/2023-10-18-Ciberataques-a-autarquias-aumentam-com-a-transicao-digital-e984cece.
- Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- National Cybersecurity Center of Excellence (NCCoE). "Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems", junho de 2023. https://www.nccoe.nist.gov/sites/default/files/2023-06/securing-water-and-wastewater-utilities-project-description-final.pdf.
- NIST. "Guide to Operational Technology (OT) Security", 26 de abril de 2022. https://csrc.nist.gov/pubs/sp/800/82/r3/ipd.
- NIST. "NIST Cybersecurity Framework 2.0: Guia de Recursos e Visão Geral", fevereiro de 2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.por.pdf.
- PORDATA, "Empresas: total e por dimensão", dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman. "NIST Special Publication NIST SP 800-82r3: Guide to Operational Technology (OT) Security". *National Institute of Standards and Technology*, setembro de 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf.
- Sulaiman Asif, "Cyber Threat Analysis: Types, Benefits, Tools, Approaches", *Knowledge Hut*, September 5, 2023. https://www.knowledgehut.com/blog/security/threat-analysis.
- Teixeira, Rui, Ofer Carmi, Peter Gattinesi e Philipp Hohenblum. "JRC Technical Report: Water Security Plan Implementation Manual for Drinking Water Systems", Comissão Europeia. https://ec.europa.eu/newsroom/cipr/items/738662/en.
- Warrick, Joby e Ellen Nakashima. "Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran". *Washington Post*, 8 de maio de 2020. https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.
- World Bank. "Strategic Cybersecurity Talent Framework - White Paper", abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.

www.cncs.gov.pt/

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Observatório
de **Cibersegurança**

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU